شبکه

صفر تا صد

فهرست مطالب:

مقدمه مولف ۷

بخش اول؛ سازمانها، پروتکل‌ها و اصطلاحات .....

فصل اول؛ سازمان های توسعه دهنده شبکه و اینترنت ۲۳

مبحث اول؛ سازمان های بین المللی ۲۵

سازمان بین المللی استانداردسازی(ISO) ۲۵

کمیسیون بین المللی برق و الکترونیک(IEC) ۲۶

اتحادیه بین المللی مخابرات (ITU) ۲۷

موسسه مهندسان برق و الکترونیک (IEEE) ۲۸

نیروی ویژه مهندسی اینترنت (IETF) ۲۹

نهاد تخصیص آدرس های اینترنت (IANA) ۳۱

شرکت اینترنتی برای نام ها و شماره های واگذار شده (ICANN) ۳۲

کنسرسیوم وب جهان گستر (W3C) ۳۳

جامعه اینترنت (ISOC) ۳۴

مبحث دوم؛ موسسات و شرکت های پیشرو تکنولوژی ۳۵

موسسه ملی استاندارد امریکا (ANSI) ۳۵

اتحادیه صنایع مخابرات (TIA) ۳۶

اتحادیه تولید کنندگان کامپیوتر اروپا (ECMA) ۳۷

شرکت IBM ۳۸

شرکت Apple ۳۹

شرکت Xerox ۴۱

شرکت تجهیزات دیجیتال (DEC) ۴۲

شرکت Novell ۴۲

شرکت سیسکو (Cisco) ۴۴

شرکت مایکروسافت (Microsoft) ۴۵

شرکت Intel ۴۶

دره سیلیکون ۴۷

فصل دوم؛ مدل و پروتکل شبکه ۴۹

مبحث اول؛ مدل مرجع شبکه ۵۱

مدل OSI ۵۱

ساختار مدل OSI ۵۱

مبحث دوم؛ پروتکل TCP/IP ۵۴
TCP/IP ۵۴
ساختار مدلTCP/IP ۵۵
پروتکل IPv4 ..... ۵۷
انواع آدرس دهی در شبکه‌هایIP ۵۸
کلاس های IPv4 ..... ۵۹
نکات مهم کلاس بندی آدرس هایIP ۶۰
آشنایی با Network Mask ۶۰
انواع حالت نمایش Net Mask ۶۱
زیر شبکه سازی (Subnetting) ۶۲
نحوه محاسبه Subnetting ۶۲
Wildcard Mask ۶۳
آدرس‌های عمومی و خصوصی ۶۴
دروازه (Gateway) ۶۵
پروتکل کنترل انتقال (TCP) ۶۵
پروتکل UDP ۶۵
پورت (Port) ۶۶
شماره پروتکل (Protocol Number) ۶۷
مبحث سوم؛ پروتکل IPv6 ..... ۶۸
پروتکل IPv6 ..... ۶۸
ویژگی هایIPv6 ..... ۶۹
تبدیل آدرس دودویی به آدرس شانزده شانزدهی ۷۱
ساختارIPv6 ..... ۷۱
نحوه نمایش Prefix در IPv6 ..... ۷۳
مکانیزم EUI-64 ..... ۷۳
انواع آدرس دهی درIPv6 ..... ۷۵
انواع آدرس Unicast ۷۵
آدرس های خاص IPv6 ..... ۷۹

فصل سوم؛ استانداردها، پروتکل ها و اصطلاحات ۸۱
مبحث اول؛ استانداردها و پروتکل ها ۸۳
ایترنت(Ethernet) ۸۳
آدرس MAC ۸۴
پروتکل تحلیل آدرس (ARP) ۸۵
پروتکل DHCP ۸۶
سامانه نام دامنه (DNS) ۸۶

پروتکل انتقال فایل(FTP) ۸۷
پروتکل انتقال ساده فایل (TFTP) ۸۹
پروتکل زمان شبکه (NTP) ۸۹
پروتکل ICMP ۸۹
پروتکل IGMP ۹۲
Telnet ۹۲
Rlogin ۹۳
حداکثر واحد انتقال (MTU) ۹۳
مبحث دوم؛ اصطلاحات و نرم افزارها..... ۹۴
رابط خط فرمان(CLI) ۹۴
TCPdump ۹۴
مدارهای مجتمع با کاربرد خاص(ASIC) ۹۵
Wireshark ۹۵
بهترین شیوه(Best Practice) ۹۵
کتابخانه زیرساخت فناوری اطلاعات(ITIL) ۹۶

بخش دوم؛ سخت افزار شبکه .....
فصل چهارم؛ شبکه های محلی ۱۰۱
مبحث اول؛ شبکه محلی ۱۰۳
هاب(Hub) ۱۰۳
پل (Bridge) ۱۰۴
سوئیچ (Switch) ۱۰۵
روش های سوئیچینگ ۱۰۷
انواع پورت سوئیچ ۱۰۹
انواع استاندارد Ethernet ۱۱۰
≺≺≺ سناریو(۱)؛ یک شبکه محلی کوچک ۱۱۲
≺≺≺ سناریو(۲)؛ گسترش شبکه محلی ۱۱۵
مبحث دوم؛ شبکه محلی مجازی (VLAN) ۱۱۹
روش های عضوپذیری VLAN ۱۲۱
VLAN Database ۱۲۱
انواع VALN ۱۲۲
اتصال Trunk ۱۲۲
انواع پروتکل Trunk ۱۲۳
پروتکل DTP ۱۲۴
Native VLAN ۱۲۴

نکات تخصیص شماره به VLANها ۱۲۴
انواع وضعیت پورت سوئیچ ۱۲۵
پیکربندی اولیه تجهیزات سیسکو..... ۱۲۶
≺≺≺ سناریو(۳)؛ ایجادVALN ۱۲۹
پروتکل VTP ۱۳۷
نسخه‌های VTP ۱۳۷
انواع وضعیت VTP ۱۳۸
انواع پیام VTP ۱۳۹
حوزه VTP ۱۳۹
VTP Password ۱۴۰
شماره اصلاح پیکربندی ۱۴۰
VTP Pruning ۱۴۰
≺≺≺ سناریو(۴)؛ راه اندازیVTP ۱۴۲
مبحث سوم؛ پروتکل درخت پوشا (STP)..... ۱۴۶
سوئیچ ریشه (Root Switch) ۱۴۷
نحوه انتخاب سوئیچ ریشه ۱۴۷
پیام BPDU ۱۴۹
پیام TCN ۱۴۹
انواع پورت درSTP ۱۴۹
فرآیند تعیین نقش پورت‌ها ۱۵۱
نسخه‌هایSTP ۱۵۲
ویژگی Portfast ۱۵۳
≺≺≺ سناریو(۵)؛ راه اندازیSTP ۱۵۴
مبحث چهارم؛ Inter-VLAN Routing ۱۶۵
توپولوژی پایه Inter-VLAN Routing ۱۶۵
Inter-VLAN Routing بر روی یک اتصالTrunk ۱۶۶
Inter-VLAN Routing توسط سوئیچ Multilayer ۱۶۷
انواع پورت لایه ۳ در سوئیچ Multilayer ۱۶۷
سوئیچینگ لایه۳ ..... ۱۶۹
تکنولوژیCEF ۱۶۹
اجزایCEF ۱۷۰
حالت‌های عملکردCEF ۱۷۰
پشتیبانی رسانه‌ها درCEF ۱۷۲
LoadBalancing در CEF ۱۷۲
مرجع دستورCEF ۱۷۳
≺≺≺ سناریو(۶)؛ راه اندازیInter-VLAN Routing توسط روتر ۱۷۴

⮜⮜⮜ سناریو(۷)؛ Inter-VLAN Routing توسط روتر و اتصال Trunk ۱۸۲
⮜⮜⮜ سناریو(۸)؛ Inter-VLAN Routing توسط سوئیچ Multilayer ۱۸۸

فصل پنجم؛ شبکه‌های گسترده؛ مسیریابی ۱۹۳

مبحث اول؛ مبانی مسیریابی ۱۹۵

تفاوت مفهوم Routed Protocol با Routing Protocol ۱۹۵
آدرس‌دهی Classful ۱۹۶
آدرس‌دهی Classless ۱۹۶
روش CIDR ۱۹۷
ماسک زیرشبکه با طول متغیر (VLSM) ۱۹۷
ویژگی Subnet-Zero ۱۹۸
جدول مسیریابی ۱۹۹
انواع مسیریابی ۱۹۹
انواع مسیر Static ۲۰۰
فرآیند انتخاب مسیر توسط روتر ۲۰۲
الگوریتم‌های مسیریابی پویا ۲۰۳
جدول مقایسه الگوریتم‌های مسیریابی ۲۰۴
همگرایی (Convergence) ۲۰۵
سیستم خودمختار (AS) ۲۰۵
Load Balancing ۲۰۶
ویژگی Passive Interface ۲۰۷
اینترفیس Loopback ۲۰۷
اینترفیس Null ۲۰۷
ویژگی Auto-Summary ۲۰۸
ترجمه آدرس شبکه (NAT) ۲۰۹
انواع NAT ۲۰۹
⮜⮜⮜ سناریو(۹)؛ Static Route ۲۱۲
⮜⮜⮜ سناریو(۱۰)؛ ترجمه آدرس شبکه ۲۲۵

مبحث دوم؛ پروتکل RIP ۲۳۳

نسخه اول RIP ۲۳۳
نسخه دوم RIP ۲۳۴
طریقه عملکرد RIP ۲۳۴
زمان سنج‌های RIP ۲۳۵
تعامل بین RIP v1 و RIP v2 ..... ۲۳۶
ویژگی Authentication ۲۳۷
⮜⮜⮜ سناریو(۱۱)؛ راه اندازی RIP ۲۳۹

مبحث سوم؛ پروتکلEIGRP ۲۴۸
پروتکلIGRP ۲۴۸
پروتکلEIGRP ۲۴۹
پروتکلRTP ۲۵۰
الگوریتمDUAL ۲۵۰
جداول پروتکلEIGRP ۲۵۱
مراحل انتخاب مسیر ۲۵۲
محاسبهMetric ۲۵۳
انواع پیام‌ها در EIGRP ۲۵۵
زمان سنج‌های پروتکلEIGRP ۲۵۶
Load Balancing در EIGRP ۲۵۶
≺≺≺ سناریو(۱۲)؛ راه اندازی EIGRP ۲۵۷
مبحث چهارم؛ پروتکلOSPF ۲۷۰
انواع پیام‌های OSPF ۲۷۱
انواع پیام‌های LSA ۲۷۲
جداول پروتکل OSPF ۲۷۴
ناحیه (Area) ۲۷۴
انواع Area ۲۷۵
قوانین استفاده از Area ۲۷۷
ویژگی Virtual Link ۲۷۸
طبقه بندی روترها ۲۷۸
طریقه محاسبهMetric ۲۸۰
نحوه انتخاب روتر DR و BDR ۲۸۳
انواع شبکه در OSPF ۲۸۴
≺≺≺ سناریو(۱۳)؛ راه اندازی OSPF ۲۸۶
مبحث پنجم؛ پروتکلBGP ۲۹۶
نحوه تخصیص شمارهAS ۲۹۷
انواع عملکرد پروتکلBGP ۲۹۸
انواع پیام‌های BGP ۲۹۹
اصطلاحات روترها درBGP ۳۰۰
انواع وضعیت روتر در BGP ۳۰۱
پایگاه اطلاعات مسیریابی(RIB) ۳۰۲
Path Attributes ۳۰۲
پارامتر Weight ۳۰۷
الگوریتم انتخاب بهترین مسیر در BGP ۳۰۷

انواع توپولوژی دسترسی به اینترنت ۳۰۹
انواع ارسال Update ۳۱۳
BGP Filtering ۳۱۴
سناریو(۱۴)؛ راه‌اندازی BGP ۳۲۰

فصل ششم؛ شبکه های گسترده؛ مسیریابی با IPv6 ۳۳۷

مبحث اول؛مفاهیم مسیریابی درIPv6 ۳۳۹
نحوه تخصیص آدرسGlobal ۳۳۹
مهاجرت و همزیستی IPv4 با IPv6 ۳۴۰
پروتکلNDP ۳۴۲
تشخیص آدرس تکراری(DAD) ۳۴۳
روش‌های تخصیص آدرس در IPv6 ۳۴۳
Static Route ۳۴۵
Static Default Route ۳۴۵
استاندارد NPTv6 ۳۴۶
سناریو(۱۵)؛ ipV6 Static Route ۳۴۷
سناریو(۱۶)؛ ipV6 Static Default Route ۳۵۵

مبحث دوم؛ پروتکلRIPng ۳۶۱
زمان سنج‌ها ۳۶۲
نحوه پیکربندی RIPng ۳۶۲
جدول دیتابیس RIPng ۳۶۳
سناریو(۱۷)؛ راه اندازی RIPng ۳۶۴

مبحث سوم؛ پروتکلEIGRP for IPv6 ۳۷۲
نحوه پیکربندی EIGRP for IPv6 ۳۷۳
فرآیند محاسبه Router ID ۳۷۴
سناریو(۱۸)؛ راه اندازی EIGRP for IPv6 ۳۷۵

مبحث چهارم؛ پروتکل OSPFv3 ۳۸۴
نکات مربوط به OSPFv3 ۳۸۵
نحوه پیکربندی OSPFv3 ۳۸۶
سناریو(۱۹)؛ راه اندازی OSPFv3 ۳۸۷

فصل هفتم؛ مباحث ویژه ۳۹۷

مبحث اول؛ مدل سلسله مراتبی سیسکو ۳۹۹
تعریف Campus ۴۰۰
طراحی سلسله مراتبی شبکه ۴۰۰

لایه هسته(Core Layer) ۴۰۱
لایه توزیع (Distribution Layer) ۴۰۱
لایه دسترسی (Access Layer) ۴۰۳
مزایای استفاده از مدل سلسله مراتبی ۴۰۴
مبحث دوم؛ High Availability ۴۰۶
پروتکلHSRP ۴۰۸
نحوه انتخاب روتر در HSRP ۴۰۹
زمان سنج‌های HSRP ۴۱۰
نحوه آدرس‌دهی Gateway در HSRP ۴۱۱
Load Balancing با HSRP ۴۱۳
پروتکل VRRP ۴۱۴
پروتکل GLBP ۴۱۵
روتر Active Virtual Gateway ۴۱۵
روتر Active Virtual Forwarder ۴۱۶
GLBP Load Balancing ۴۱۷
فعال سازی GLBP ۴۱۸
جدول مقایسه پروتکل‌های HA ۴۲۰
مبحث سوم؛ Redistribution ۴۲۱
دلایل استفاده از Redistribution ۴۲۲
مفاهیم Redistribution و فرآیندها ۴۲۲
Redistribution در EIGRP ۴۲۴
Redistribution در OSPF ۴۲۵
Redistribution در RIP ۴۲۶
Redistribution در BGP ۴۲۶
مبحث چهارم؛ سایر پروتکل‌ها ۴۲۷
پروتکلCDP ۴۲۷
استانداردPoE ۴۲۹
تکنولوژی EtherChannel ۴۳۱
ویژگیIP Helper ۴۳۵

بخش سوم؛ امنیت شبکه
فصل هشتم؛ امنیت، مفاهیم کلی ۴۳۹
مبحث اول؛ استاندارد سیستم مدیریت امنیت اطلاعات (ISMS) ۴۴۱
استانداردهای خانواده ISMS ۴۴۲

مروری بر استانداردهای خانوادهISMS ۴۴۳
اصطلاحات و تعاریف ۴۴۶
مروری بر ISMS ۴۴۹
اصولPDCA ۴۵۱
برقراری، نظارت، نگهداری و بهبود عملکرد ISMS ۴۵۱
مبحث دوم؛ مدل امنیتی سیسکو ۴۵۳
اصطلاحات و تعاریف ۴۵۴
چارچوب کنترل امنیتی سیسکو (Cisco Security Control Framework) ۴۵۶
اجزایSCF ۴۵۷
مدلSCF سیسکو ۴۵۸
اهداف امنیتی ۴۵۹
اقدامات امنیتی ۴۶۱
سازماندهی کنترل‌ها با SCF سیسکو ۴۶۳
مبحث سوم؛ تجهیزات و نرم افزارهای امنیتی ۴۶۵
فایروال (Firewall) ۴۶۵
انواع فایروال ۴۶۷
سیستم تشخیص نفوذ(IDS) ۴۶۹
اجزایIDS ۴۶۹
تکنولوژی‌های مورد استفاده در IDS ۴۷۰
اصطلاحات IDS ۴۷۱
سیستم پیشگیری از نفوذ(IPS) ۴۷۲
سرویس پروکسی (Proxy) ۴۷۲
فیلترینگ محتوا (Content Filtering) ۴۷۳
آنتی ویروس(Anti-Virus) ۴۷۳
روش‌های شناسایی کدهای مخرب ۴۷۴
مدیریت یکپارچه تهدیدات (UTM) ۴۷۵

فصل نهم؛ امنیت شبکه ۴۷۷

مبحث اول؛ Hardening تجهیزات شبکه ۴۷۹
Management Plane ۴۷۹
مقاوم سازی عمومی Management Plane ۴۷۹
کنترل خطوط tty و vty ۴۸۰
مدیریت Password ۴۸۰
بهبود امنیت کلمه عبور ۴۸۳
قفل کلمه عبور در صورت تکرار اشتباه ۴۸۴
سرویس عدم بازیابی کلمه عبور ۴۸۴

غیرفعال کردن سرویس‌های بلااستفاده ۴۸۵
دستور EXEC Timeout ۴۸۸
دستور Keepalive برای نشست TCP ۴۸۸
استفاده از اینترفیس مدیریت ۴۸۸
هشدار آستانه حافظه ۴۸۹
هشدار آستانه CPU ۴۸۹
رزرو حافظه جهت دسترسی کنسول ۴۹۱
آشکارساز نشت حافظه ۴۹۲
تمهیدات پروتکل NTP ۴۹۲
محدود کردن دسترسی‌ها ۴۹۴
فیلتر بسته‌های ICMP ۴۹۴
ویژگی Management Plane Protection ۴۹۵
رمزگذاری نشست‌های مدیریتی ۴۹۶
پورت‌های کنسول و AUX ۴۹۷
اعلامیه هشدار ۴۹۸
مقاوم سازی پروتکل SNMP ۴۹۹
بهترین شیوه‌های رویداد نگاری ۵۰۲
مدیریت پیکربندی ۵۰۴
سرویس AAA ۵۰۷
مبحث دوم؛ امنیت سوئیچینگ ۵۱۱
محدود کردن حوزه پخش همگانی ۵۱۱
امنیت پروتکل STP ۵۱۲
بهترین شیوه‌های امنیتی VLAN ۵۱۶
ویژگی Port Security ۵۱۷
کنترل طوفان ترافیک ۵۲۲
ویژگی DHCP Snooping ۵۲۵
IP Source Guard ۵۲۷
ویژگی DAI ۵۲۸
شبکه شخصی مجازی (PVLAN) ۵۲۹
پورت حفاظت شده ۵۳۰
استاندارد IEEE 802.1x ۵۳۱
مبحث سوم؛ امنیت مسیریابی ۵۳۵
Access Control List ۵۳۵
انواع ACL ۵۳۵
قوانین و نکات ACL ۵۳۶
نحوه ایجاد و اعمال ACL ۵۳۷

Route-Maps ۵۳۹
شباهت ACL با Route-Map ۵۳۹
تفاوت ACL با Route-Map ۵۴۰
دستورات Route-Map ۵۴۱
ویژگی Passive Interface ۵۴۲
ترجمه آدرس شبکه ۵۴۲
استاندارد RFC 2827 ..... ۵۴۳

منابع ۵۴۵

بخش اول

سازمانها، پروتکل ها و اصطلاحات

فصل اول

سازمانهای توسعه دهنده شبکه و اینترنت

- ☑ مبحث اول: سازمانهای بین المللی
- ☑ مبحث دوم: شرکت های پیشرو تکنولوژی شبکه

دنیای شبکه و کامپیوتر با سرعتی برق آسا در حال پیشرفت و نوآوری است. از طرفی نیازهای جدید انسان و از طرف دیگر رقابت بین شرکت ها برای تولید محصولات جدید با خصوصیاتی متفاوت در جهت جلب مشتری، باعث بوجود آمدن ایده ها، تکنولوژی ها، ابتکارات و اختراعات در زمینه شبکه و دیگر محصولات مرتبط با کامپیوتر گردیده است. برخی از نوآوریهای تکنولوژی می توانند بدون استاندارد شدن و حتی بصورت انحصاری تولید شده و مورد اقبال عمومی نیز قرار بگیرند. اما نوآوری هایی که برای استفاده و توسعه، نیاز به همکاری شرکت ها و کارشناسان دارند، باید به صورت استاندارد درآمده و یک سازمان متولی امور مربوط به آن پروتکل یا تکنولوژی گردد. همچنین شرکت ها برای تولید بعضی از محصولات خود باید به اسناد همین موسسات درباره پروتکل های مرتبط رجوع کرده و محصولات خود را بر اساس استانداردها تولید نمایند.

شبکه و محصولات مبتنی بر آن، یکی از مهمترین موضوعاتی می باشد که بدون پروتکل های استاندارد قابلیت کار و توسعه را ندارند.

ما در این بخش به معرفی دو گروه موسسات و شرکت های مرتبط با شبکه می پردازیم. اول گروه سازمانهای بین المللی متولی استانداردها و دوم شرکت های خصوصی پیشرو در صنعت شبکه و کامپیوتر که در اکثر مواقع طراح اولیه پروتکل های استاندارد نیز هستند.

☑ مبحث اول

سازمانهای بین المللی

سازمان بین المللی استاندارد سازی (ISO)

سازمان‌بین‌المللی استاندارد سازی (International Organization for Standardization) که بطور خلاصه آنرا ایزو می نامند، یک موسسه بین المللی متشکل از نمایندگان موسسات ملی استاندارد است که در سال 1947 در ژنو سوئیس آغاز به کار نموده و اکنون حدود ۱۶۰ کشور جهان، از جمله ایران عضو این سازمان می‌باشند.

سازمانISO بطور گسترده به وضع استانداردهای جزئی و کلی تجاری و صنعتی جهان مشغول می باشد. ایزو در زمینه IT نیز دارای استانداردهایی می‌باشد که مهمترین آن، استاندارد مدل مرجع شبکه OSI[1] می‌باشد.

از جمله استانداردهای ایزو در زمینه سیستم های کامپیوتری می توان به موارد زیر اشاره نمود:

- ایزو ۷۹۴۲ مربوط به هسته‌های کارتهای گرافیکی کامپیوتر
- ایزو ۸۶۵۲ مربوط به فنآوری اطلاعات – زبان‌های برنامه نویسی
- ایزو ۱۰۰۱۷ مربوط به تجزیه و تحلیل داده‌ها و اطلاعات
- ایزو ۱۱۵۷۸:۱۹۹۵۶ مربوط به فنآوری اطلاعات – تبادل اطلاعات و سازگاری بین سیستم‌های متفاوت با استانداردهای متفاوت OSI
- ایزو ۱۳۲۳۹ مربوط به کنترل سطح بالای پیوندهای داده‌ای HDLC
- ایزو ۱۴۴۹۶ مربوط به فرمت فایل‌های تصویری MPEG-4
- ایزو ۱۷۷۹۹ رمزهای تمرینی برای مدیریت امنیت اطلاعات
- ایزو ۲۰۰۰۰:۲۰۰۵ مربوط به مدیریت آی.تی
- ایزو ۲۷۰۰۱ مربوط به سیستم مدیریت امنیت اطلاعات (ISMS)

---

[1] Open System Interconnection

آرم (Logo) و آدرس اینترنتی سازمان بین المللی استاندارد سازی، بصورت زیر می باشد:

http://www.iso.org

کمیسیون بین المللی برق و الکترونیک (IEC)

کمیسیون بین المللی برق و الکترونیک (International Electrotechnical Commission)، یکی از سه سازمان خواهر جهانی (ISO,IEC,ITU) می باشد که وظیفه توسعه استانداردهای بین المللی را بر عهده دارند.

این سه خواهر برای تصویب استانداردها، دارای کمیته های مشترکی هستند تا از تناسب، یکپارچگی و مکمل هم بودن استانداردهای بین المللی با یکدیگر اطمینان حاصل نمایند.

IEC در سال1906 در شهر ژنو کشور سوئیس بنا نهاده شد. IEC سازمانی پیشرو جهت آماده سازی و انتشار استانداردهای بین المللی در تمامی زمینه های برق، الکترونیک و فناوریهای مرتبط (که در مجموع "الکتروتکنولوژی" نامیده می شود) می باشد.

تمام استانداردهای بین المللیIEC، به طور کامل مبتنی بر اجماع و نشان دهنده نیازهای ذی نفعان کلیدی عضو می باشد. هر کشور عضو، فارغ از وسعت و جمعیت، دارای یک رای در راستای ایجاد استاندارد می باشد. از جمله مهمترین استانداردهای IEC در زمینه شبکه، میتوان به استاندارد امنیت شبکه (ISO/IEC 27001)، که بطور مشترک با ISO ارائه گردید، اشاره نمود.

برای مشاهده لیست استانداردهای IEC می توانید به سایت اینترنتی این کمیسیون به آدرس http://www.iec.ch، مراجعه نمایید.

اتحادیه بین المللی مخابرات (ITU)

اتحادیه بین المللی مخابرات (International Telecommunication Union)، یکی از آژانس های تخصصی سازمان ملل متحد بوده که در زمینه فناوری اطلاعات و ارتباطات فعالیت می نماید. تشکیلات این اتحادیه بر اساس مشارکت بخش دولتی (کشورهای عضو) و بخش خصوصی (دانشگاه ها و همکاران) شکل گرفته است. اعضای ITU شامل ۱۹۳ کشور عضو و بیش از ۷۰۰ بخش خصوصی متشکل از اشخاص و یا موسسات آموزشی، می باشند.

تخصیص طیف فرکانس رادیویی و مدارهای ماهواره ای، توسعه استانداردهای فنی برای اطمینان از اتصال یکپارچه شبکه ها و فناوری ها و همچنین تلاش در جهت بهبود دسترسی به فناوری اطلاعات و ارتباطات به جوامع محروم در سرتاسر جهان، از جمله وظایف ITU می باشد.

اتحادیه ITU به سه بخش تقسیم بندی می گردد:

۱- بخش مخابرات رادیویی ITU Radio communication (ITU-R)

۲- بخش استاندارد سازی مخابرات Telecommunication Standardization (ITU-T)

۳- بخش توسعه مخابرات ITU Telecommunication Development (ITU-D)

از جمله استانداردهای ITU، می توان به سری استانداردهای تکنولوژی xDSL اشاره نمود:

- ITU G.992.1 مربوط به ADSL
- ITU G.992.3 مربوط به ADSL2
- ITU G.991.2 مربوط به SHDSL
- ITU G.993.2 مربوط به VDSL2

دفتر مرکزی ITU در ژنو سوئیس می باشد. این اتحادیه دارای ۱۲ منطقه و همچنین دفاتری در سرتاسر جهان می باشد. برای بازدید از سایت و آشنایی بیشتر با استانداردهای ITU، می توانید از آدرس http://www.itu.int، استفاده نمایید.

موسسه مهندسان برق و الکترونیک (IEEE) [۱]

مؤسسه مهندسان برق و الکترونیک(The Institute of Electrical and Electronics Engineers) در سال 1963 از پیوستن دو انجمن مهندسی برق و مهندسی رادیو در کشور ایالات متحده امریکا تشکیل گردید. اساسنامه IEEE، سازمان را بدین صورت تعریف کرده است: "سازمانی علمی و آموزشی، به سوی تعالی در ابعاد تئوری و عملی در زمینه‌های برق، الکترونیک، مخابرات و مهندسی کامپیوتر و نیز علوم کامپیوتر و شاخه‌های وابسته مهندسی، علمی و هنری."

IEEE یک سازمان بین المللی حرفه ای بوده که تخصصا در زمینه مهندسی برق و کامپیوتر فعالیت می کند. مهمترین استانداردها در زمینه تجهیزات الکترونیکی شبکه، توسط این سازمان ارائه می گردد.

از جمله استانداردهای IEEE در زمینه ارتباطات می توان به موارد زیر اشاره نمود:

- IEEE 802.1 تعریف پل[۲] در لایه ۲ شبکه
- IEEE 802.3 پروتکل ایترنت[۳]
- IEEE 802.3af پروتکل انتقال برق بر روی ایترنت (POE) [۴]
- IEEE 802.11 پروتکل شبکه های بی سیم محلی (WiFi) [۵]
- IEEE 802.15.1 پروتکل شبکه های بی سیم شخصی که با نام Bluetooth شهرت داشته و موارد کاربرد زیادی در وسایل جانبی دارد.
- IEEE 802.16 پروتکل دسترسی بی سیم پهن باند(WiMAX). [۶]

سایت IEEE از طریق آدرس http://www.ieee.org، بر روی اینترنت قابل دسترس است.

---

[۱] بصورت: آی-تریپِل-ئی/ai tripl i:/ تلفظ می گردد.

[2] Bridge

[3] Ethernet

[4] Power Over Ethernet

[۵] علامت تجاری مورد استفاده برای شبکه های بی سیم محلی

[6] Worldwide Interoperability for Microwave Access

نیروی ویژه مهندسی اینترنت (IETF)

نیروی ویژه مهندسی اینترنت (The Internet Engineering Task Force)، یک انجمن بزرگ بین المللی استاندارد باز است که عملکرد آن بر مبنای کار گروهی می باشد. گروه های کاری بر اساس بخشهایی نظیر مسیریابی، حمل و نقل و امنیت شبکه ایجاد گردیده است. با توجه به اینکه نحوه ارتباط این گروه ها بر اساس لیست های پستی[1] است، پس بنابراین نیاز زیادی به جلسات حضوری نداشته و تنها سه بار در سال تشکیل جلسه می دهند.

نحوه ورود به این انجمن، عضویت در یکی از کار گروه های مورد نظر بوده که برای هر فرد علاقه مند میسر می باشد.

هر گروه کاری به یک ناحیه تقسیم شده و هر ناحیه توسط مدیر ناحیه اداره می گردد. مدیران ناحیه، عضو گروهی به نام راهبری مهندسی اینترنت IESG[2] می باشند. گروه IESG تحت نظارت گروه هیئت مدیره معماری اینترنتIAB[3] می باشد. صدور امتیاز برای گروه های IESG و IAB توسط جامعه اینترنت ISOC[4] انجام می گیرد.

انجمن IETF شامل ۸ ناحیه به شرح زیر می باشد:

۱- ناحیه کاربردی (Application Area)
۲- ناحیه عمومی (General Area)
۳- ناحیه اینترنت (Internet Area)
۴- ناحیه عملیات و مدیریت (Operation and Management Area)
۵- ناحیه زیرساخت و برنامه های بلادرنگ (Real-time Application and Infrastructure Area)
۶- ناحیه مسیر یابی (Routing Area)
۷- ناحیه امنیتی (Security Area)
۸- ناحیه حمل و نقل (Transport Area)

انجمن IETF بطور تخصصی بر روی مجموعه پروتکل اینترنت متمرکز بوده و استانداردهای مربوطه را ایجاد کرده یا بهبود می‌بخشد و در نهایت آنها را در قالب مستندات RFC منتشر می‌نماید. RFC سر نام عبارت Request For Comment و به معنی درخواست برای توضیح

---

[1] Mailing List
[2] Internet Engineering Steering Group
[3] Internet Architecture Board
[4] Internet Society

است. RFC ها مراجعی به صورت فایلهای متنی هستند که برای تشریح مجموعه پروتکل‌های اینترنت منتشر می‌شوند.

از جمله اسناد RFC میتوان به موارد زیر اشاره نمود:

- RFC 768 پروتکل UDP
- RFC 791 پروتکل اینترنت (IP)
- RFC 792 پروتکل پیامهای کنترلی اینترنت (ICMP)
- RFC 793 پروتکل کنترل انتقال (TCP)
- RFC 1058 پروتکل اطلاعات مسیریابی (RIP v1)
- RFC 1157 پروتکل مدیریت ساده شبکه (SNMP)
- RFC 2131 پروتکل کنترل آدرس دهی پویا (DHCP)
- RFC 2460 پروتکل اینترنت نسخه ۶ (IPv6)
- RFC 4787 پروتکل ترجمه آدرس شبکه (NAT)

IETF®

تشریح ماموریت IETF در RFC 3935 آمده است. برای دسترسی به سایت IETF و مشاهده لیست کامل RFC ها می توانید از آدرس http://www.ietf.org استفاده نمایید.

نکته:

مدیونید اگر از دیدن نام پروتکل‌هایی که در لیست‌های فوق آمده و احتمالا با آنها آشنایی ندارید، ترس به خود راه دهید! لیست‌های آورده شده در این بخش صرفا برای آشنایی شما با نحوه کار سازمان‌ها می‌باشد. توضیحات پروتکل های مورد نیاز، در بخش های مربوطه بطور مبسوط آورده خواهد شد.

نهاد تخصیص آدرس‌های اینترنت (IANA)

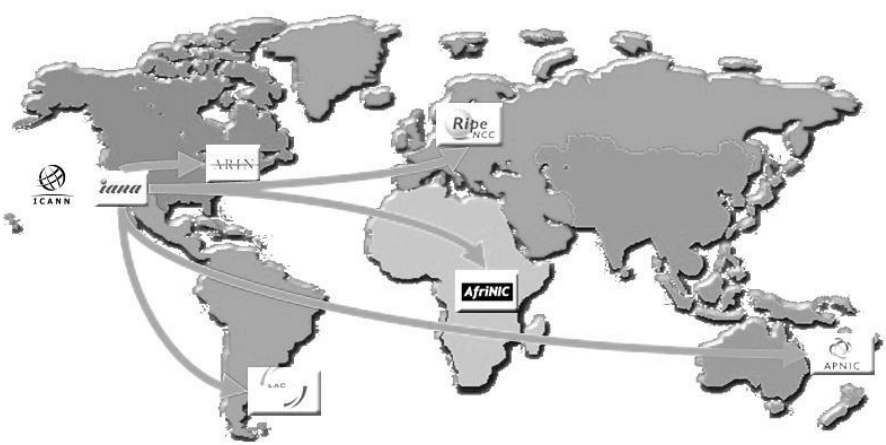
نهاد تخصیص آدرس های اینترنت (Internet Assigned Numbers Authority)، یکی از قدیمی ترین نهادهای اینترنت است که قدمت آن به دهه 1970 میلادی بر می گردد.

گسترش روز افزون اینترنت در سرتاسر دنیا و احساس نیاز به یک سازمان هماهنگ کننده مرکزی باعث تشکیل نهاد تخصیص آدرس های اینترنت گردید. نهاد IANA، یک سازمان غیرانتفاعی بین المللی سازمان یافته توسط جامعه اینترنت است که مسئولیت خدمت رسانی به مناطق مختصات خود در جهان را بر عهده دارد.

Internet Assigned Numbers Authority

نهاد IANA، جهت تخصیص منابع پروتکل اینترنت و حفظ کد منحصر بفرد آدرسها، جهان را به پنج گروه زیر تقسیم بندی نموده است:

۱- آفریقا
۲- آسیا و اقیانوسیه
۳- آمریکای شمالی
۴- آمریکای لاتین و برخی از جزایر کارائیب
۵- اروپا، خاور میانه و آسیای مرکزی



تیم IANA مسئول اجرای جنبه های عملیاتی هماهنگ کننده شناسه های منحصر بفرد اینترنت و حفظ اعتماد جامعه به ارائه این خدمات در شیوه ای بی طرفانه، مسئولانه و موثر می باشد.

این نهاد که مسئولیت سرپرستی تخصیص آدرس های پروتکل اینترنت را بر عهده دارد، فعالیت های خود را به سه گروه زیر تقسیم بندی می نماید:

۱- نام دامنه[1]

۲- منابع شماره تخصیص یافته به هر منطقه[2]

۳- تکالیف پروتکل های مربوط به اینترنت[3]

نهاد IANA ابتدا توسط موسسه علوم اطلاعات دانشگاه کالیفرنیای جنوبی مدیریت می گردید، اما در حال حاضر این نهاد به صورت عضوی از سازمان ICANN در آمده است.

برای بازدید از وب سایت IANA و آشنایی با وضعیت آدرس دهی به مناطق مختلف جهان، می‌توانید به آدرس http://www.iana.org، مراجعه نمایید.

شرکت اینترنتی برای نام ها و شماره های واگذار شده (ICANN)[4]

شرکت اینترنتی برای نام ها و شماره های واگذار شده (Internet Corporation for Assigned Names and Numbers)، یک سازمان بین المللی غیرانتفاعی می باشد که در سال 1998 طی تفاهم نامه ای با وزارت بازرگانی ایالات متحده، در شهر لس آنجلس ایالت کالیفرنیا تاسیس گردید. اکثر خدمات محول شده به این شرکت، قبلا توسط نهاد تخصیص آدرس های اینترنت (IANA) انجام می‌گرفت.

[1] Domain Name
[2] Number Resource
[3] Protocol Assignment
[4] آیکان /ˈaɪkæn/

سازمان ICANN مسئول پروتکل اینترنت، نام دامنه، تخصیص فضا، تعیین پروتکل، مدیریت سیستم دامنه‌های کشوری (ccTLD)[1]، مدیریت سیستم دامنه های عمومی (gTLD)[2] و مدیریت سیستم سرور ریشه[3] است.

لازم به ذکر است ICANN همچنان تخصیص آدرس IP را به IANA ارجاع می دهد. به عبارتی دیگر در حال حاضر IANA، به همان وظایف قبلی خود تحت نظر ICANN ادامه می دهد.

جهت بازدید از وب سایت ICANN، می توانید به آدرس http://www.icann.org، مراجعه نمایید.

کنسرسیوم وب جهان گستر (W3C)

کنسرسیوم وب جهان گستر (World Wide Web Consortium)، در سال 1994 برای توسعه استانداردهای وب تشکیل گردید. رهبری این کنسرسیوم بر عهده مخترع وب، تیم برنزلی[4] و مدیر عاملی آن نیز بر عهده جفری ژافه[5] می باشد.

ماموریت W3C، راهبری عمومی وب جهان گستر(WWW)، بوسیله توسعه پروتکل‌ها و دستورالعمل ها و اطمینان در مورد سازگاری سیستم ها می باشد.

در طراحی استاندارد وب دو اصل مهم مورد توجه این کنسرسیوم می باشد:

۱- **وب برای همه (Web for all)**

یکی از اهداف اصلی W3C، قرار دادن مزایای وب در دسترس همه مردم جهان با هر نوع فرهنگ، زبان مادری، توانایی جسمی، موقعیت جغرافیایی و داشتن هرگونه سخت افزار، نرم افزار و زیرساخت شبکه می باشد.

---

[1] Country Code
[2] General Code
[3] Root Server System
[4] Tim Berners-Lee
[5] Jeffrey Jaffe

۲- **وب بر روی همه چیز (Web on everything)**

یکی دیگر از اهداف در قسمت طراحی W3C، امکان استفاده از وب بر روی تمام تجهیزاتی است که ممکن است یک شخص از آنها استفاده کند. امروزه بجز کامپیوترها، تجهیزاتی مثل گوشی تلفن همراه، کنسول بازی، تلویزیون، PDA، تبلت ها و حتی برخی لوازم خانگی نیز می توانند به وب دسترسی داشته باشند.

از جمله استانداردهای منتشر شده توسط W3C می توان به موارد زیر اشاره نمود:

- HTTP؛ پروتکل ارتباط بین سرویس گیرنده و سرویس دهنده
- HTML؛ استاندارد ساختار اسناد متنی در وب
- XML؛ زبان نوشتاری قابل گسترش
- CSS؛ زبان توصیف نحوه ارائه صفحات وب. مثل رنگ، طرح و فونت
- AJAX؛ نحوه ایجاد صفحات وب پویا بدون نیاز به بارگذاری مجدد صفحه

برای بازدید از وب سایتW3C، می توانید از آدرس http://www.w3c.org استفاده نمایید.

جامعه اینترنت (ISOC)

جامعه اینترنت (Internet Society)، یک سازمان غیرانتفاعی بین المللی است که در سال 1992 برای راهبری استانداردها، آموزش و سیاست های مرتبط با اینترنت تاسیس گردید.

ISOC ماموریت خود را چنین بیان می کند: "ترویج توسعه باز استانداردها، تکامل استانداردها و استفاده از اینترنت به نفع تمام مردم در سرتاسر جهان."

جامعه اینترنت (ISOC)، مستقیما در بوجود آوردن و منتشر کردن استانداردها نقشی ندارد؛ اما به عنوان سازمان متولی اینترنت، مسئولیت صدور امتیاز برای گروه هایIESG وIAB که ناظر استانداردهای ایجاد شده توسط IETF می باشند، را بر عهده دارد.

ISCO با همکاری انجمن مهندسی اینترنت، مجله ای به نام IETF منتشر می نماید. این مجله، با هدف فراهم کردن امکان مرور راحت و قابل فهم از آنچه که درباره استانداردهای اینترنت رخ می‌دهد، ایجاد شده است. تمرکز اصلی این مجله بر روی فعالیت کار گروه های IETF و موضوعات داغی که در جلسات و لیست های پستی (Mailing List) مورد بحث است، می باشد.

برای دانلود مجلات منتشر شده می توانید از آدرس اینترنتی زیر استفاده نمائید:

http://www.isoc.org/publications/ietf-journal

☑ مبحث دوم

موسسات و شرکت‌های پیشرو تکنولوژی

در این مبحث به معرفی موسسات و شرکتهای غیر بین المللی که بصورت خصوصی و یا در سطح ملی بنا نهاده شده اند ولی پیشرو در زمینه ایجاد تکنولوژیهای جدید ICT بوده و حتی خاستگاه اولیه برخی استانداردها می باشند، می پردازیم.

موسسه ملی استاندارد امریکا (ANSI)

موسسه ملی استاندارد امریکا(American National Standards Institute)، در سال1918 از ادغام پنج انجمن مهندسی و سه آژانس دولتی به ساختار اولیه خود رسید. پس از چند تغییر در ساختار و نام، نهایتا در سال 1969 به عنوان موسسه ملی استاندارد امریکا، جهت نظارت بر روند ایجاد استانداردها در تمامی زمینه ها در ایالات متحده، شناخته شد.

ANSI

American National Standards Institute

ANSI بطور مستقیم در ایجاد استانداردها نقشی ندارد، اما تعیین اعتبار موسسات استاندارد سازی در امریکا و روند توسعه استانداردها را بر عهده دارد. اتحادیه صنایع مخابرات (TIA) که یکی از موسسات استاندارد سازی در امریکا می باشد و نقش مهمی نیز در ارائه استانداردهای شبکه دارد، تحت نظر ANSI بوده و توسط همین موسسه اعتبار سنجی می گردد.

این موسسه مسئول انطباق استانداردهای امریکا با استانداردهای جهانی، جهت امکان استفاده از آنها در سراسر جهان، نیز می باشد. موسسه ANSI در تلاش است تا استانداردهای آمریکا را در جامعه جهانی مورد پذیرش قرار دهد و در صورت نیاز استانداردهای بین‌المللی را که مورد نیاز است در آمریکا به کار برد. لذا برای حصول اطمینان از تطبیق استانداردهای این اتحادیه با

استانداردهای بین المللی مربوطه، اتحادیه ANSI، عضویت در سه سازمان خواهر جهانی (ISO,IEC,ITU) را بصورت فعال دنبال می نماید.

جهت دسترسی به وب سایت ANSI، می توانید از آدرس http://www.ansi.org، استفاده نمایید.

اتحادیه صنایع مخابرات (TIA)

اتحادیه صنایع مخابرات (Telecommunication Industry Association)، در سال 1988 از ادغام اتحادیه عرضه کنندگان مخابرات ایالات متحده(USTSA)[1]، گروه فناوری اطلاعات و اتحادیه صنایع الکترونیک(EIA) [2]، بنا نهاده شد.

این اتحادیه که مورد تایید موسسه ملی استاندارد امریکا (ANSI) قرار گرفته بود، در پاییز سال 2000 با اتحادیه مخابرات چند رسانه ای (MIMTA)[3] ، نیز ادغام گردید.

اتحادیهTIA به عنوان یک اتحادیه پیشرو، آخرین فناوریهای اطلاعات و ارتباطات (ICT)، را در رابطه با توسعه استانداردها، شناخت فرصت های جدید تجاری، ابتکار در رویه ها و امکان تعامل شرکت ها و موسسات فعال در این حوزه را در سطح جهان فراهم می نماید.

اکثر استانداردهای شناخته شده و مورد استفاده توسط TIA در زمینه های مرتبط با قسمت غیر فعال شبکه[4]، مثل کابل مسی، کابل فیبر نوری و کانکتورها می باشد.

علیرغم اینکه TIA یک موسسه بین المللی نمی باشد ولی دارای بخش توسعه استانداردهای مختص به خود بوده که غالبا با همکاری موسسه ملی استاندارد امریکا در غالب استانداردی از ANSI یا TIA و یا هر دو، ارائه می شود.

به دلیل اینکه کمپانی های بزرگ تولید کننده و صاحب تکنولوژی صنعت ICT، غالبا در ایالات متحده قرار دارند، لذا مجبور به رعایت استانداردهای ملی ایجاد شده توسط ANSI و موسسات

---

[1] United States Telecommunications Suppliers Association
[2] Electronic Industries Alliance
[3] MultiMedia Telecommunications Association
[4] Passive

ذیربط امریکا هستند. این امر باعث گردیده استانداردهای ارائه شده توسط این اتحادیه، شبیه به استانداردهای بین المللی توسط جامعه ICT مورد پذیرش و استفاده قرار بگیرد.

استانداردهای TIA مبنای بسیاری از استانداردهای بین المللی مربوطه می باشند. پس از آنکه ANSI استانداردهای TIA را به سازمان های بین المللی ارائه می کند، در اغلب موارد استانداردها تایید شده و توسط ISO/IEC به صورت جهانی معرفی و منتشر می شوند.

از جمله استانداردهای معرفی شده توسط TIA می توان به موارد زیر اشاره نمود:

- ANSI/TIA 942؛ استاندارد زیرساخت مخابراتی مراکز داده[1]
- ANSI/TIA/EIA 568؛ استاندارد کابل کشی ساخت یافته
- ANSI/TIA 4966؛ استاندارد زیرساخت مخابراتی ساختمان ها و فضاهای آموزشی
- ANSI/TIA 862؛ استاندارد کابل کشی برای نقاط دسترسی بی سیم
- ANSI/TIA 1005؛ استاندارد زیر ساخت مخابراتی ساختمان های صنعتی
- TIA 604؛ استاندارد کانکتورهای فیبر نوری

برای بازدید از سایت TIA، و بررسی بیشتر استانداردها می توانید از آدرس اینترنتی زیر استفاده نمایید: http://www.tiaonline.org

اتحادیه تولید کنندگان کامپیوتر اروپا (ECMA)

اتحادیه تولید کنندگان کامپیوتر اروپا (European Computer Manufacturers Association) ، یک اتحادیه صنعتی می باشد که در سال 1961 در ژنو سوئیس تاسیس گردید.

استاندارد سازی فناوری اطلاعات و ارتباطات (ICT) و لوازم الکترونیک، از وظایف اتحادیه ECMA می باشد. همچنین استاندارد سازی زبان های برنامه نویسی را می توان از بارزترین فعالیت های این اتحادیه ذکر نمود.

هر چند استانداردهای این اتحادیه برای قاره اروپا بوده و امکان استفاده مستقیم در سطح بین المللی را ندارد، اما غالبا استانداردهای ECMA به عنوان پایه و مبنای استانداردهای مرتبط منتشر شده توسط ISO و IEC مورد استفاده قرار می گیرد.

[1] Data Center

در جدول زیر چند مثال از استانداردهای EMCA که توسط ISO و IEC بصورت بین المللی منتشر شده، آمده است:

ECMA Standard	Standard's description	ISO/IEC Standard
ECMA-108	Measurement of High-Frequency Noise emitted by Information Technology and Telecommunications Equipment, 5th edition (December 2010)	ISO 9295
ECMA-142	Private Integrated Services Network (PISN) - Circuit Mode 64kbit/s Bearer Services - Service Description, Functional Capabilities and Information Flows (BCSD), 3rd edition (December 2001)	ISO/IEC 11574
ECMA-321	Streaming Lossless Data Compression Algorithm - (SLDC) (June 2001)	ISO/IEC 22091
ECMA-355	Corporate Telecommunication Networks - Tunnelling of QSIG over SIP, 3rd edition (June 2008)	ISO/IEC 22535
ECMA-357	ECMAScript for XML (E4X) Specification, 2nd edition (December 2005)	ISO/IEC 22537

از جمله استانداردهای ECMA می توان به موارد زیر اشاره نمود:

- ECMA-376؛ استاندارد فایلهای XML
- ECMA-334؛ زبان برنامه نویسی C#
- ECMA-400؛ کنترل و نظارت مراکز داده هوشمند
- ECMA-74؛ اندازه گیری نویز ایجاد شده توسط تجهیزات ICT
- ECMA-395؛ قابلیت بازنویسی روی دیسک نوری CD/RW

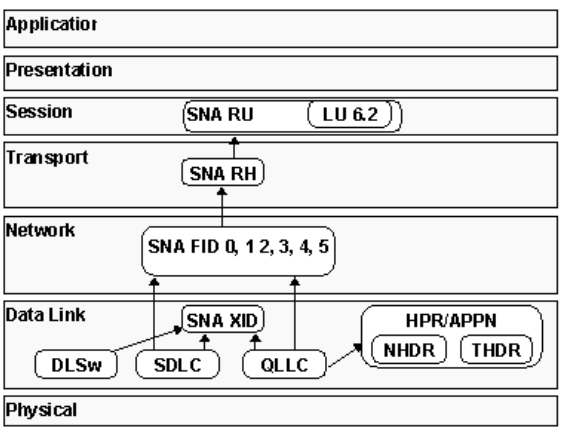
جهت بازدید از سایت اتحادیه ECMA و ملاحظه لیست استانداردها می‌توانید از آدرس http://www.ecma-international.org استفاده نمایید.

شرکت IBM

شرکت آی بی ام (International Business Machines Corporation)، یک شرکت امریکایی چند ملیتی می‌باشد که در سال 1911 با ادغام چند شرکت با یکدیگر، تشکیل گردید.

هر چند که IBM تولید کننده طیف وسیعی از سخت افزارها و نرم افزارها می‌باشد، اما شهرت زیاد آن به دلیل تولید کامپیوترهای بزرگ (Mainframe) می‌باشد.

همچنین IBM توانست با ارائه معماری سیستم های شبکه(SNA)[1]، که اولین مدل لایه‌ای شبکه بود، نام خود را به عنوان عضو پیشتاز تکنولوژی شبکه نیز ثبت نماید. در حال حاضر IBM یکی از تولید کنندگان سیستم عامل شبکه نیز محسوب می گردد.



نمایش معماری SNA بر اساس لایه بندی مدل OSI

برای بازدید از وب سایت شرکت IBM می توانید از آدرس http://www.ibm.com، استفاده نمایید.

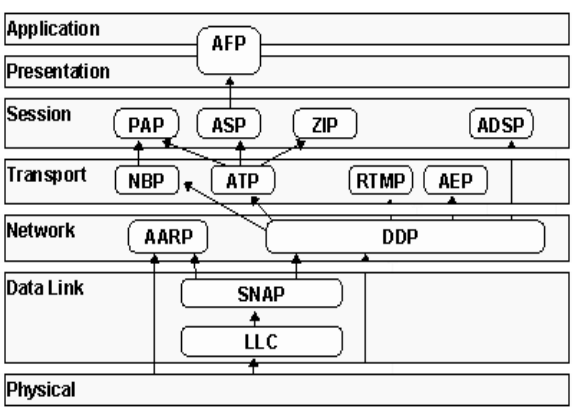
شرکت Apple

شرکت اپل(Apple)، یک شرکت چند ملیتی امریکایی است که در سال 1976 توسط استیو جابز، استیو وزنیاک و رونالد وین در دره سیلیکون تاسیس گردید.

[1] Systems Network Architecture

شرکت اپل همواره در حال ارائه طرح های جدید و خاص در زمینه تجهیزات کامپیوتری بوده و توانسته جایگاه خوبی را در جهان برای خود بدست آورد؛ تا جایی که در سال 2012 به عنوان "برترین و گرانترین برند جهان"، دست یافت.

هر چند شهرت اپل بیشتر بر اساس طراحی های خاص و نوآوری در محصولاتش می باشد، اما این شرکت توانست با معرفی مجموعه پروتکل AppleTalk، نام خود را به عنوان پیشتازان تکنولوژی شبکه نیز ثبت نماید.



نمایش مجموعه پروتکلAppleTalk بر اساس لایه بندی مدل OSI

مجموعه پروتکل AppleTalk شامل مجموعه ای از پروتکل ها برای ایجاد شبکه است. این پروتکل ها ابتدا مخصوص تجهیزات اپل بودند، ولی اپل توانست با انتشار نسخه سازگار با کامپیوترهای IBM، شهرت و عمومیت بیشتری به مدل شبکه خود ببخشد.

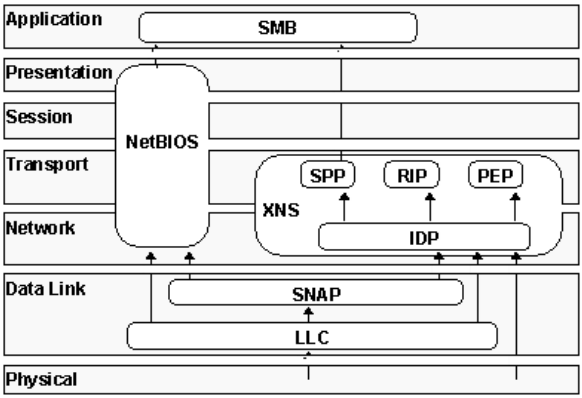
جهت دسترسی به وب سایت اپل می توانید از طریق آدرس http://www.apple.com ، اقدام نمایید.

شرکت Xerox[1]

شرکت زیراکس (Xerox)، یک شرکت امریکایی چند ملیتی است که در سال 1906 تاسیس گردید. تولید طیف وسیعی از پرینترهای رنگی و سیاه سفید، سیستم های چند منظوره، دستگاه چاپ عکس، تجهیزات چاپ دیجیتال و غیره، از فعالیت های این شرکت می باشد.

در زمینه تکنولوژی شبکه نیز، معماری XNS (Xerox Network System Architecture)، توسط شرکت زیراکس ایجاد و معرفی گردید. همچنین از فعالیت های مهم زیراکس می توان به ایجاد پروتکل Ethernet نیز اشاره نمود. پس از ایجاد Ethernet، زیراکس با همکاری شرکت های Intel و DEC، توانست این پروتکل را گسترش دهد. در نهایت پروتکل Ethernet، توسط سازمان IEEE در قالب استاندارد سری 802 توسعه یافت و در حال حاضر اصلی ترین پروتکل مورد استفاده در لایه اول مدل TCP/IP، در شبکه های محلی می باشد.

لازم به ذکر است که گروه ایجاد کننده Ethernet، پس از چندی از زیراکس جدا شده و در قالب شرکت 3COM به فعالیت تخصصی خود در زمینه شبکه ادامه دادند. در نهایت 3COM نیز در سال 2010 توسط شرکت hp خریداری و در این شرکت ادغام گردید.



نمایش معماریXNS بر اساس لایه بندی مدل OSI

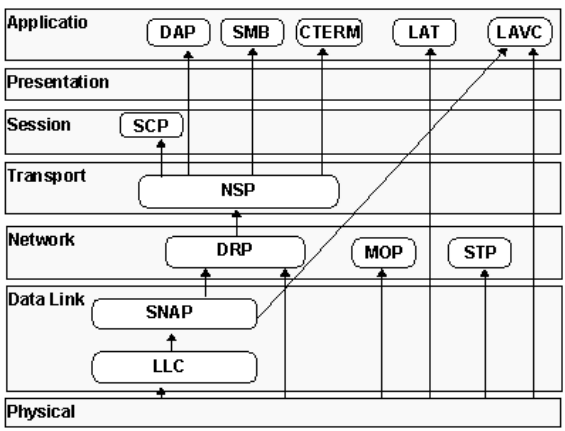
برای آشنایی با محصولات متنوع زیراکس می توانید از آدرس http://www.xerox.com ، استفاده نمایید.

[1] زیراکس /ˈziərɒks/

شرکت تجهیزات دیجیتال (DEC)

شرکت تجهیزات دیجیتال (Digital Equipment Corporation)، یک شرکت امریکایی بود که در سال 1957 تاسیس گردید. این شرکت در زمان خود به عنوان شرکتی موفق در صنعت کامپیوتر شناخته می شد.

شرکت DEC از پیشتازان ایجاد پروتکل های شبکه نیز بود. این شرکت مجموعه پروتکل DECnet را برای ایجاد شبکه های کامپیوتری معرفی نمود. شرکت DEC همچنین در توسعه پروتکل محبوب Ethernet نیز نقش مهمی ایفا نمود.



نمایش مجموعه پروتکلDECnet بر اساس لایه بندی مدل OSI

شرکت DEC در سال 1998 توسط شرکت Compaq خریداری شد. هر چند که خود شرکت Compaq هم چند سال بعد و در سال 2002 توسط شرکت hp خریداری گردید. با این تفاسیر، در نهایت دو گروه از سه گروه ایجاد کننده پروتکل مشهورEthernet در شرکت hp ادغام شدند.

شرکت Novell

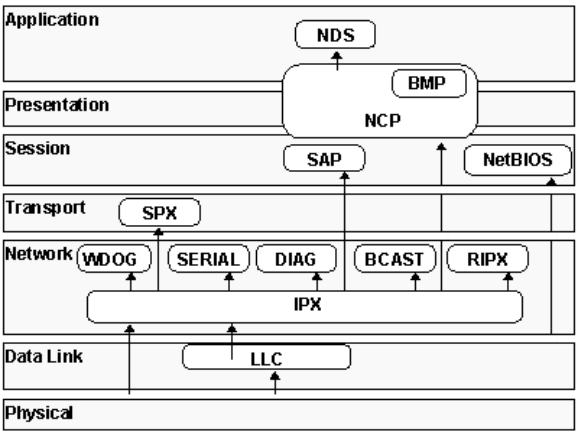
شرکت ناول (Novell)، یک شرکت چند ملیتی تولید کننده نرم افزارهای کامپیوتری می باشد که در سال 1979 در شهر پروو[1] ایالت یوتا[2] و در غرب امریکا تاسیس گردید.

Novell®

[1] Provo
[2] Utah

شهرت اصلی ناول به دلیل ارائه سیستم عامل شبکه Novell Netware می باشد. این سیستم عامل که زودتر از سیستم عامل شبکه شرکت مایکروسافت عرضه گشت، در زمان خود به عنوان قدرتمندترین سیستم عامل شبکه شناخته می شد.

شرکت ناول برای ورود به دنیای شبکه اقدام به معرفی مجموعه پروتکل Novell نمود. این مجموعه پروتکل، در طراحی و پیاده سازی، تا حد بسیار زیادی تحت تاثیر معماری XNS شرکت زیراکس قرار داشت. این مجموعه پروتکل که شامل IPX[1] یکی از مشهورترین پروتکل های لایه ۳ شبکه نیز می باشد، مورد پشتیبانی گسترده سیستم عامل کامپیوتر های دسکتاپ از جمله داس، ویندوز، مکینتاش و یونیکس قرار گرفت.



نمایش مجموعه پروتکل Novell بر اساس لایه بندی مدل OSI

در حال حاضر شرکت ناول در زمینه تولید سیستم عامل شبکه، فعالیت خود را بر روی توسعه Linux Suse متمرکز نموده است.

سایت Novel از طریق آدرس http://www.novell.com ، در دسترس می باشد.

نکته:

پس از ارائه مدل مرجع OSI و پروتکل TCP/IP، مدلهای فوق یا منسوخ شده و یا در موارد و محصولات خاص استفاده می شوند، لذا ذکر آنها صرفا جهت آشنایی شما با فعالیت پیشتازان عرصه شبکه می باشد. تشریح مدل OSI و پروتکل TCP/IP، که دارای استاندارد بین المللی نیز می باشند، در فصل دوم همین بخش آمده است.

[1] Internet Protocol Exchange

شرکت سیسکو (Cisco)

شرکت سیسکو سیستمز (Cisco Systems)، در سال 1984 توسط لن بزاک و سندی لرنر، زوج دانش آموخته علوم کامپیوتر دانشگاه استانفورد، در دره سیلیکون کالیفرنیا تاسیس گردید.

سیسکو از اصلی ترین بنیان گذاران مسیریابی در شبکه بوده و همچنان نیز برترین تولید کننده تجهیزات مسیر یابی در جهان به شمار می آید. همچنین سیسکو توانست با خرید شرکت های دیگر، حضور خود را در زمینه هایی مثل سوئیچینگ، شبکه های بی سیم و امنیت نیز پر رنگ نماید. از همین رو می توان یکی از دلایل پیشرفت همه جانبه سیسکو را خرید تعداد زیادی شرکت های کوچک و بزرگ موفق در تولید محصولات مرتبط با شبکه و ادغام آنها در شرکت سیسکو دانست.

اگر چه عرضه اصلی تولیدات سیسکو به بازار، به صورت سخت افزاری می باشد، ولی در عین حال سیسکو تولید کننده نرم افزارهایی برای مدیریت و نظارت شبکه، مدیریت مرکزی تلفن های تحت شبکه و مدیریت کنترل دسترسی به منابع شبکه نیز می باشد. لازم به ذکر است که سیسکو در روند همکاری خود با شرکت های مجازی سازی مثل VMware، اقدام به عرضه سوئیچ های نرم افزاری برای کار در محیط های مجازی نیز نموده است.

سیسکو در کنار پروتکل های مختص به خود، بنای اولیه پروتکل های استانداردی در رابطه با مسیریابی، افزونگی[1]، سوئیچینگ و تلفن تحت شبکه[2] را نیز گذاشته است.

از پروتکل های مخصوص سیسکو می توان به VTP[3]، CDP[4]، GLBP[5]، HSRP[6]، CEF[7] و IGRP[8] اشاره نمود.

---

[1] Redundancy
[2] IP telephony
[3] VLAN Trunking Protocol
[4] Cisco Discovery Protocol
[5] Gateway Load Balancing Protocol
[6] Hot Standby Router Protocol
[7] Cisco Express Forwarding
[8] Interior Gateway Routing Protocol

همچنین از استانداردهای منتشر شده توسط سازمان‌های بین المللی که بر مبنای پروتکل‌های سیسکو می باشند، می توان از پروتکل هایی مثلTACACS[1]، EtherChannel، VRRP[2]، MSTP[3] و MPLS[4] نام برد.

سیسکو دارای بخش آموزشی، انتشارات و ارائه مدارک تخصصی نیز می باشد. به دلیل گستردگی و فراگیر بودن استفاده از محصولات سیسکو، مدارک این شرکت در زمینه شبکه از اعتبار قابل ملاحظه ای در سطح جهان برخوردار است.

برای بازدید از وب سایت شرکت سیسکو می توانید از آدرس http://www.cisco.com ، استفاده نمایید.

نکته: با توجه به اینکه محصولات سیسکو رایج ترین تجهیزات شبکه ای مورد استفاده در ایران است، آموزش این کتاب در زمینه سخت افزار شبکه، بر اساس تجهیزات سیسکو خواهد بود.

شرکت مایکروسافت (Microsoft)

مایکروسافت (Microsoft)، یک شرکت چند ملیتی تولید نرم افزارهای کامپیوتری می باشد که در سال 1975 توسط بیل گیتس و پل آلن در ایالات متحده تاسیس گردید.

شرکت مایکروسافت را می توان بزرگترین شرکت نرم افزاری دنیا دانست. هر چند فعالیت اصلی این شرکت در زمینه طراحی، توسعه و تولید انواع نرم افزارهای کامپیوتری می باشد، اما شهرت مایکروسافت به دلیل سیستم عامل ویندوز و نرم افزار نشر رومیزی Office می باشد.

شرکت مایکروسافت با ارائه سیستم عامل تحت شبکه ویندوز، وارد عرصه شبکه نیز گردید و با امکاناتی که روزبه روز به نسخه‌های سیستم عامل و نرم افزارهای مربوطه‌اش اضافه می‌نمود، توانست محبوبیت خود را افزایش داده و سهم قابل توجه‌ای از بازار را در اختیار خود قرار دهد.

---

[1] Terminal Access Control Access Control System
[2] Virtual Router Redundancy Protocol
[3] Multiple Spanning Tree Protocol
[4] Multi-Protocol Label Switching

این سیستم عامل به قدری در بین کاربران گسترش پیدا کرده که به سختی می توان برنامه ای را پیدا کرد که نسخه تحت ویندوز آن ارائه نشده باشد.

سیستم عامل تحت شبکه، سیستم عامل کامپیوتر های شخصی، سیستم عامل تلفن همراه، نرم افزار نشر رومیزی، نرم افزارهای های برنامه نویسی، نرم افزارهای امنیتی، آنتی ویروس، دیتابیس و نرم افزارهای پست الکترونیک از جمله تولیدات نرم افزاری مایکروسافت می باشد.

جالب آنکه، این شرکت به تولید نرم افزار بسنده نکرده و سخت افزارهایی از قبیل کنسول بازی و تجهیزات جانبی کامپیوتر نیز به بازار ارائه نموده است.

مایکروسافت دارای بخش انتشارات، آموزش و مدارک تخصصی نیز می باشد. مدارک این شرکت جهت معرفی متخصصین شبکه های مبتنی بر سیستم عامل ویندوز بوده و دارای اعتبار جهانی می باشد.

شرکت مایکروسافت در زمینه سیستم عامل شبکه دارای پروتکل‌های مخصوص به خود می‌باشد. همچنین در روند ایجاد برخی استانداردها نیز دارای نقش اساسی بوده است.

برای دسترسی به وب سایت شرکت مایکروسافت به آدرس http://www.microsoft.com مراجعه نمایید.

شرکت Intel

اینتل (Intel)، یک شرکت چند ملیتی امریکایی است که در سال 1968 توسط رابرت نویس و گوردن مور در دره سیلیکون ایالت کالیفرنیا تاسیس گردید.

اینتل که در حال حاضر قدرتمندترین تولید کننده پردازنده های کامپیوتری می باشد، فعالیت خود را با تولید نیمه رسانه ها که بنیان اصلی قطعات الکترونیک است آغاز کرد. همچنین بسیاری از تکنولوژی های جدید و نوآوری ها در زمینه پردازنده ها و مدارات مجتمع(IC) توسط همین شرکت ایجاد می گردد. اینتل در زمینه شبکه نیز همکاری بسیار نزدیکی با دیگر برندها برای به وجود آوردن پروتکل های استاندارد و فراگیر داشته است. از جمله می توان به همکاری اینتل با زیراکس و DEC برای توسعه Ethernet اشاره نمود.

جهت بازدید از وب سایت اینتل، می توانید به آدرسhttp://www.intel.com، مراجعه نمایید.

دره سیلیکون (Silicon Valley)

دره سیلیکون (Silicon Valley) نام رایج ولی غیر رسمی منطقه ای خوش آب و هوا در حدود ۷۰ کیلومتری جنوب شرقی شهر سانفرانسیسکو واقع در ایالت کالیفرنیا در کشور امریکا می باشد. این دره از لحاظ کشاورزی منطقه ای غنی بوده به حدی که تا اواخر جنگ جهانی دوم باعث رونق صنایع غذایی در منطقه گردیده بود.

اما از آنجا که این دره در نزدیکی دانشگاه استانفورد قرار داشت، سرنوشت این دره دگرگون گردید. دانش آموختگان دانشگاه استانفورد با ایجاد شرکت هایی در زمینه الکترونیک و کامپیوتر باعث ایجاد یک منطقه صنعتی در این دره گردیدند. نام سیلیکون اولین بار در سال 1971 توسط یک روزنامه نگار به دلیل تعدد شرکت های تولید کننده قطعات الکترونیکی که سیلیکون ماده اصلی تشکیل دهنده آنهاست، بر این دره گذارده شد.

شرکت hp اولین شرکتی بود که در سال 1937 کار خود را در گاراژی واقع در دره سیلیکون آغاز کرد. اما در حال حاضر دره سیلیکون در بر گیرنده بزرگترین و پرآوازه ترین شرکت های تولید کننده صنایع الکترونیک و کامپیوتر می باشد. به نوعی می توان گفت امروزه مبدا ایجاد بسیاری از تکنولوژی ها و نوآوری ها در جهان، دره سیلیکون می باشد.

از جمله شرکت های مهم واقع در دره سیلیکون می توان از Cisco، hp، Intel، Apple، ASUS، Adobe، AMD و Yahoo نام برد. جالب آنکه اکثر شرکت های بزرگ کامپیوتری دیگر که دفتر مرکزی آنها در شهر یا حتی کشور دیگری قرار دارد، برای عقب نماندن از کورس تکنولوژی، حداقل دارای دفتر نمایندگی در دره سیلیکون می‌باشند.

فصل دوم

مدل و پروتکل شبکه

- ☑ مبحث اول: مدل مرجع شبکه
- ☑ مبحث دوم: پروتکل TCP/IP
- ☑ مبحث سوم: پروتکل IPv6

☑ مبحث اول

مدل مرجع شبکه

مدل OSI[1] (Open Systems Interconnection)

در سال1984 سازمانISO جهت ایجاد مدلی استاندارد برای پروتکل های شبکه کامپیوتری، اقدام به معرفی مدل OSI نمود. این مدل که به عنوان مدل مرجع برای عملیات ارتباطات شبکه ای مورد استفاده قرار می گیرد از هفت لایه برای تشریح فرآیندهای مربوط به ارتباطات استفاده می‌کند.

شکستن وظایف شبکه به قسمت های کوچکتر که در اینجا "لایه" نامیده می شوند، باعث می شود مجموعه ای از پروتکلهای پیچیده به قسمت های کوچک تقسیم شده تا بحث در مورد مفاهیم، نحوه اجرا و پیاده سازی و مهمتر از همه اشکال زدایی را آسانتر نماید. همچنین این نوع تقسیم بندی باعث می شود که هر کارشناس و یا شرکت سازنده بتواند تمرکز خود را روی لایه مورد نظر گذاشته و محصول مربوطه را بصورت مستقل پیاده سازی نماید و پیاده سازی لایه های دیگر را بر عهده سایر متخصصین و شرکت ها گذارد.

ساختار مدل OSI

تشریح کامل مدل OSI می تواند وقت گیر و حوصله سربر باشد ولی با توجه به مرجع بودن این مدل، به قدر نیازمان در این کتاب، به توضیح مختصری از لایه ها بسنده می کنیم.

- **لایه اول: لایه فیزیکی**

  لایه فیزیکی مربوط به اتصالات شبکه است که در مورد خصوصیات رسانه انتقال بحث می کند. این لایه وظیفه انتقال بیت‌ها از طریق کانال های مخابراتی را بر عهده دارد. مسائل طراحی در این لایه عمدتاً از نوع فیزیکی، جریان الکتریکی، تایمینگ، مدولاسیون و رسانه فیزیکی انتقال است. واحد داده در این لایه "Bit" می باشد.

---

[1] بعضی از علمای اهل فن آنرا " اُزی" و برخی دیگر " اُ اِس آی " تلفظ می کنند.

- **لایه دوم: لایه پیوند داده**

این لایه نحوه تحویل داده از طریق یک لینک، توسط پروتکلهای وابسته به نوع رسانه را مشخص می کند. فریم بندی داده‌ها، رفع خطاهای فیزیکی، هماهنگی سرعت بین گیرنده و فرستنده از وظایف این لایه است. واحد داده در این لایه "Frame" است.

- **لایه سوم: لایه شبکه**

از وظایف این لایه میتوان به کنترل عملکرد زیر شبکه، مسیر یابی، آدرس دهی منطقی و تحویل پکت ها از یک نقطه انتهایی به نقطه انتهایی دیگر[1] اشاره نمود. این لایه یکی از مهمترین و پر کابردترین لایه ها در مباحث مربوط به شبکه بوده که برای قورت دادن شبکه جزء لاینفک لقمه بزرگ شما می باشد. واحد داده در این لایه "Packet" می باشد.

- **لایه چهارم: لایه انتقال**

این لایه مسئول پشتیبانی کنترل جریان داده ها، بمنظور تقسیم بلوک های بزرگ داده به قسمت های کوچکتر در سمت ارسال کننده و یکپارچه کردن اطلاعات دریافتی مربوط به هر برنامه در سمت گیرنده و همچنین بررسی خطا و جبران آن می باشد.

واحد داده در این لایه "Segment" می باشد.

- **لایه پنجم: لایه جلسه**

جلسه به مکالمات شکل گرفته بین دو سیستم انتهایی گفته می شود؛ که این لایه وظیفه برقراری، مدیریت و خاتمه آنرا بر عهده دارد. با نظارت این لایه بر جلسات، می توان ابتدا از جابجایی کامل مکالمات هر دو طرف اطمینان حاصل کرد و سپس داده را به لایه نمایش ارائه داد.

واحد داده در لایه پنجم "Data" می باشد.

- **لایه ششم: لایه نمایش**

این لایه وظیفه مدیریت ساختار پیام‌ها را برای انتقال از لایه کاربرد به لایه های پایین تر برعهده دارد؛ و همچنین مدیریت ساختار دیتا از لایه های پایین تر به لایه کاربرد.

واحد داده در لایه ششم "Data" می باشد.

- **لایه هفتم: لایه کاربرد**

برنامه‌های کاربردی نظیر مرورگرهای اینترنتی، برنامه‌های مدیریت ایمیل، انتقال فایلها در این لایه قرار می‌گیرند و به صورت کلی واسط بین کاربر و دنیای شبکه می‌باشد.

واحد داده در لایه هفتم نیز "Data" می باشد.

---

[1] End-to-End

در جدول زیر برخی از پروتکل های مورد استفاده در لایه های مختلف OSI نام برده شده است.

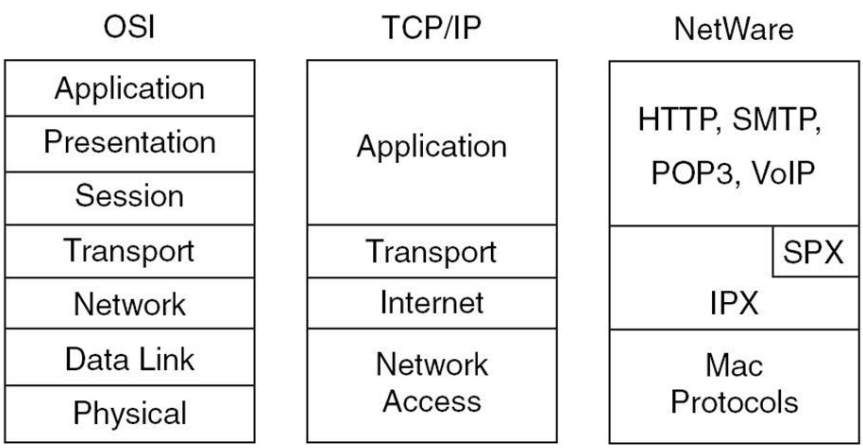
OSI model
7. Application layer
NNTP / SIP /SSI / DNS / FTP / Gopher / HTTP / NFS / NTP / SMPP / SMTP / SNMP / Telnet / DHCP / (more)
6. Presentation layer
MIME / XDR / ASCII / PICT / GIF / JPEG / MIDI / MPEG
5. Session layer
Named pipe / NetBIOS / SAP / PPTP / RTP / SOCKS / SPDY / TLS/SSL
4. Transport layer
TCP / UDP / SCTP / DCCP / SPX
3. Network layer
IP (IPv4 & IPv6) / ARP / ICMP / IPsec / IGMP / IPX / AppleTalk
2. Data link layer
ATM / SDLC / HDLC / CSLIP / SLIP / GFP / PLIP / IEEE 802.2 / LLC / L2TP / IEEE 802.3 / Frame Relay / ITU-T G.hn DLL / PPP / X.25
1. Physical layer
EIA/TIA-232 / EIA/TIA-449 / ITU-T V-Series / I.430 / I.431 / PDH / SONET / SDH / DSL / IEEE 802.3 / IEEE 802.11 / IEEE 802.15 / IEEE 802.16 / IEEE 1394 / USB / Bluetooth / RS-232 / RS-449

☑ مبحث دوم

پروتکل TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol):

شرکت های مختلفی همچون Novell، IBM، DEC و ARPA[1] پروتکل هایی را برای ارتباطات شبکه ای معرفی نموده و تجهیزات و نرم افزارهایی را بر پایه این پروتکلها به بازار عرضه نمودند. به دلیل استاندارد نبودن هیچ یک از این پروتکلها، تجهیزات ساخته شده شرکتهای مختلف با یکدیگر سازگاری[2] نداشتند و همین امر موجب می شد که حتی پس از راه اندازی یک شبکه بر اساس یک برند خاص، در زمان توسعه شبکه، تعویض قطعات و یا بروز رسانی تجهیزات، شما همچنان با محدودیت روبرو باشید. این محدودیت بیش از همه وقتی کارشناسان را آزرده خاطر می کرد که نیاز به کاری مثل اشتراک گذاری فایل بین دو سیستم با دو برند متفاوت را داشتند.



هر چند که بعضی از شرکتها مثل Novell وIBM سعی کردند با ارائه مدلهای جدیدتر شبکه بین بعضی از سیستم های مختلف اشتراکاتی را بوجود آورند، اما مشکلات بسیار زیاد نبود یک

---

[1] ARPA موسسه تحقیقاتی وابسته به وزارت دفاع ایالات متحده می باشد.

[2] Compatibility

پروتکل استاندارد، بالاخره باعث شد بین علمای اهل فن تجمیع نظر بوجود آمده و بر سر یک پروتکل به توافق برسند. آن پروتکل چیزی نبود جز پروتکل محبوب و جامع TCP/IP که پیش از این توسط موسسه تحقیقاتی ARPA به نام مدلDOD[1] معرفی و شبکه ARPAnet نیز بر اساس آن شکل گرفته بود.

ساختار مدل TCP/IP

مدلTCP/IP شامل مجموعه ای از پروتکل های تعریف شده توسط نیروی ویژه مهندسی اینترنت می باشد که در قالب استاندارد RFC 1180 منتشر شده است. این پروتکل ها می توانند باعث برقراری ارتباط بین کامپیوترها (فارغ از برند آنها) در شبکه گردند.

در بعضی از منابع شبکه مدل TCP/IP را در پنج لایه تعریف می کنند؛ اما مدلDOD که TCP/IP بر پایه آن شکل گرفته، هفت لایه مدلOSI را در چهار لایه خلاصه و تعریف می نماید که در ادامه هر لایه به اختصار توضیح داده می شود.

- **لایه اول: لایه واسط شبکه**

این لایه دربرگیرنده وظایف لایه اول و دوم مدل OSI است و دارای تعریفی مشابه این دو لایه نیز می باشد. این لایه وظیفه انتقال داده در بستر فیزیکی شبکه را بر عهده دارد. از جمله تعریف نوع سوکت، نحوه کابل بندی، سطوح ولتاژ و کانکتورها جهت ارتباطات فیزیکی شبکه توسط این لایه تعریف می شوند.

- **لایه دوم: لایه اینترنت**

لایه اینترنت متناظر لایه سوم مدل OSI است. پروتکل اینترنت (IP) که جهت آدرس دهی منابع شبکه استفاده می شود، در این لایه تعریف گشته است. در همین مبحث به توضیحات بیشتری در مورد IP خواهیم پرداخت.

- **لایه سوم: لایه انتقال**

لایه فوق متناظر لایه چهارم مدل OSI است و عهده دار همان مسئولیت پشتیبانی کنترل جریان داده ها، بررسی خطا و جبران آن می باشد.

- **لایه چهارم: لایه کاربرد**

این لایه تلفیق لایه های پنجم، ششم و هفتم مدلOSI می باشد. تمامی برنامه ها و ابزارهای کاربردی در این لایه تعریف می شوند.

---

[1] Department of Defense (DOD) Model

در جدول زیر برخی از پروتکل های مورد استفاده در هر لایه نشان داده شده است.

TCP/IP model
4. Application layer
BGP / DHCP / DNS / FTP / GTP / HTTP / IMAP / IRC / LDAP / MGCP / NNTP / NTP / POP / RIP / RPC / RTP / RTSP / SDP / SIP / SMTP / SNMP / SOAP / SSH / Telnet / TLS/SSL / XMPP
3. Transport layer
TCP / UDP / DCCP / SCTP / RSVP / ECN
2. Internet (Network) layer
IP (**IPv4**, IPv6) / ICMP / ICMPv6 / IGMP / IPsec
1. Network Access layer
ARP / InARP / NDP / OSPF / Tunnels (L2TP) / PPP / ISDN / FDDI

نکته: پروتکل TCP/IP دارای گستردگی مفاهیم و پروتکلهای گوناگونی می باشد که برای شرح آن کتابهایی مختص به این موضوع نگاشته شده و مقالات فراوانی نیز منتشر گشته است. در صورت نیاز میتوانید به آن منابع رجوع کنید!

یکی از مهمترین این لایه ها برای کارشناسان شبکه، لایه سوم مدل OSI یا لایه دوم مدل TCP/IP است. در این کتاب از این پس، این لایه را لایه شبکه نامیده و به دلیل قرار گرفتن آن در مرتبه سوم مدل OSI، تجهیزاتی که در این لایه کار می کنند را تجهیزات لایه سه می نامیم.

مهم ترین پروتکل استانداردی که در لایه شبکه کار می کند و شبکه اینترنت بر اساس آن شکل گرفته، پروتکل اینترنت یا همان IP (Internet Protocol) می باشد. اولین نسخه عملیاتی این پروتکل، IPv4 بود که در سال های اخیر به دلیل زیاد شدن کاربران اینترنت و نیاز به تعداد بیشتری آدرس IP، کارشناسان را مجبور به بروز رسانی این پروتکل نمود که نتیجه این بروز رسانی معرفی IPv6 شد. البته در حال حاضر IPv6 بصورت عمومی و اجباری در جهان استفاده نمی گردد و همچنان IPv4 در دنیا و بالاخص در ایران مورد استفاده قرار می گیرد.

پروتکل IPv4

اگر شما بخواهید از تهران با یکی از دوستان خود در یک کشور خارجی صحبت کنید، گوشی تلفن خود را برداشته و تلفن دوست عزیزتان را شماره گیری می کنید. مثلا اگر دوست شما در سفارت جمهوری اسلامی ایران در کشور فرانسه و شهر پاریس کار می کند شما باید شماره ای شبیه ۰۰۳۳-۱-۴۰۶۹۷۹۰۰ را داشته باشید. یک سوال! مخابرات چطور متوجه می شود این شماره ای که شما گرفتید را باید به چه کسی و در کجای دنیا متصل کند؟ حتما مخابرات مراحل زیر را انجام می دهد:

۱- مخابرات با توجه به شماره گیری دو صفر ابتدای شماره متوجه می شود که این یک تلفن خارج از شبکه محلی است.

۲- شماره ۰۰۳۳ طبق قراردادی بین المللی متعلق به کشور دوست و برادر! فرانسه است. پس مخابرات درخواست شما را به شرکت مخابرات فرانسه تحویل میدهد.

۳- بچه های شرکت مخابرات فرانسه با توجه به قسمت دوم شماره، یعنی عدد ۱ ، متوجه می شوند که شماره مربوط به شهر پاریس است، پس درخواست شما را برای همکاران پایتخت نشین خود ارسال می کنند.

۴- حالا بچه های شرکت مخابرات پاریس متوجه می شوند که شماره ۴۰۶۹۷۹۰۰ متعلق به سفارت جمهوری اسلامی ایران است و درخواست مکالمه شما را با سفارت برقرار می کنند. در نهایت شما می توانید یک مکالمه خصوصی دو طرفه با دوستتان داشته باشید.

پس ما برای مکالمه تلفنی نیاز به یک شماره تلفن منحصر بفرد که در آن کشور، شهر، محله و شخص مورد نظر مشخص شده باشد، داریم.

کامپیوترها و دیگر تجهیزات شبکه هم برای تعامل با یکدیگر نیاز به یک آدرس منحصر بفرد در سراسر شبکه خواهند داشت. این آدرس دهی بر اساس پروتکل اینترنت انجام می شود و به آن آدرس آی پی می گویند. همانند شماره تلفن که مشخص کننده کشور و شهر است، آدرس های IP نیز از دو قسمت تشکیل شده تا بتوانند شبکه و میزبان مورد نظر را آدرس دهی نمایند.

پروتکل IPv4 که در RFC 791 تعریف گشته است، یک آدرس ۳۲ بیتی بر مبنای دودویی (باینری)[1] می باشد که به فرم ده دهی (دسیمال)[2] و بصورت چهار Octet که با نقطه از هم جدا گردیده، نمایش داده می شود. هر Octet شامل یک عدد دسیمال متغیر از 0 تا 255 می باشد که نشان دهنده یک بایت (۸ بیت) آدرس بر مبنای دودویی می باشد.

[1] Binary
[2] Decimal

به دلیل اینکه کامپیوتر فقط صفر و یک را می شناسد، مبنای آدرس دهی به صورت دودویی می باشد. اما از آنجا که برای کارشناسان شبکه و کاربران استفاده از آدرس های باینری سخت و مشکل زا است، فرم نمایش آدرس IP بر مبنای ده دهی انجام می پذیرد.

نمونه یک آدرس IP بر مبنای باینری و دسیمال:

آدرس بر مبنای دودویی : 00001010 00000001 11110001 01000011

نمایش آدرس فوق به فرم ده دهی: 10.1.241.67

البته شکر خدا با وجود ماشین حساب و به لطف برنامه های آنلاین و قابل دانلود، امروزه مشکل خاصی در تبدیل این دو فرم به یکدیگر نخواهید داشت؛ بر عکس زمان ما!

انواع آدرس دهی در شبکه‌های IP

نحوه آدرس دهی در شبکه های IP به سه حالت زیر تقسیم می شود:

۱- **آدرس دهی تک پخشی (Unicast):**

به هر رابط شبکه یک آدرس منحصر بفرد IP تخصیص داده می شود، این آدرس امکان برقراری ارتباط های یک به یک را در شبکه فراهم می نماید. در این صورت پیام فقط به آدرس مقصد مورد نظر ارسال می گردد.

۲- **آدرس دهی همگانی (Broadcast):**

آدرس دهی همگانی که به آن پخش همگانی نیز می گویند باعث می شود که یک پیام صادر شده از یک دستگاه به تمامی دستگاههای موجود در همان بخش (Segment) شبکه ارسال شود.

به عنوان مثال از پیام پخش همگانی برای ارسال درخواست هایی استفاده می شود که کلاینت اطلاعی از آدرس سرویس دهنده مورد نظر نداشته باشد. مثل درخواست دریافت آدرس IP، که کلاینت این درخواست را بصورت پخش همگانی ارسال می کند.

۳- **آدرس دهی چند پخشی (Multicast):**

در صورتی که بخواهیم پیام ها فقط بین گروه خاصی از آدرس های شبکه منتقل شود، از پیام های چند پخشی استفاده می کنیم.

از جمله کاربردهای پیام چند پخشی می توان استفاده از این نوع پیام ها را در پروتکل های مسیریابی پویا[1] و همچنین برنامه های چند رسانه ای[2] نام برد.

---

[1] Dynamic Routing Protocols

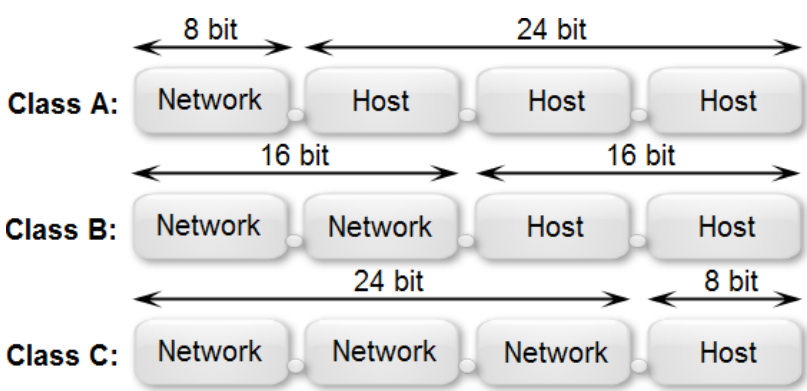
[2] Multimedia

کلاس های IPv4

همانطور که قبلا اشاره شد، آدرسIP از دو قسمت شبکه و میزبان[1] تشکیل شده است. طبق استانداردRFC 1466 تعداد شبکه و میزبان پروتکلIP در ۵ کلاس آدرس دهی تعریف شده است.

سه کلاس برای آدرس دهی در شبکه، یک کلاس برای پیام های Multicast و یک کلاس هم برای سازمان IETF در نظر گرفته شده است. فضای آدرس های اختصاص داده شده به هر کلاس در جدول زیر نمایش داده شده است:

کلاس	تعداد بیت شبکه	تعداد بیت میزبان	تعداد آدرس شبکه	تعداد آدرس میزبان	محدوده آدرسها
A	8	24	$2^7 - 2$	$2^{24} - 2$	1.0.0.0 126.0.0.0
B	16	16	$2^{14} - 2$	$2^{16} - 2$	128.1.0.0 191.254.0.0
C	24	8	$2^{21} - 2$	$2^8 - 2$	192.0.1.0 223.255.254.0
D	آدرسهای کلاسD برای اهدافMulticast رزرو گردیده است.				224.0.0.0 239.255.255.255
E	این رنج توسطIETF برای اهداف خاص رزرو گردیده است.				240.0.0.0 255.255.255.255



[1] Host

نکات مهم کلاس بندی آدرس‌های IP

- آدرس های IP شامل سه کلاس اصلی A، B و C می باشند.
- کلاسD آدرس های مورد استفاده برای پیام های Multicast می باشد.
- کلاس E توسط انجمن IETF برای پروژه های تحقیقاتی رزرو شده و در شبکه ها مورد استفاده قرار نمی گیرد.
- رنج آدرس 127.255.255.255 – 127.0.0.0 برای سیستم عامل رزرو شده است. از جمله می توان به آدرس 127.0.0.1 اشاره نمود که به عنوان آدرس Loopback یا Local host مورد استفاده قرار می گیرد. این رنج آدرس IP قابل مسیریابی در اینترنت نمی باشد.
- رنج آدرس169.254.255.255 – 169.254.0.0 توسط نهادIANA برای خصیصه ای[1] به نامAPIPA[2] رزرو گردیده تا در مواقع ضروری مورد استفاده قرار گیرد. مواقع ضروری وقتیست که هیچ کس به درخواست های سیستم جهت دریافت آدرس IP جوابی نمی دهد و کاربر هم یا بلد نیست یا نمی خواهد که آدرس را بصورت دستی به سیستم خود اختصاص دهد. این خصوصیت بصورت پیش فرض در نسخه های مختلف سیستم عامل ویندوز فعال می باشد. این رنج آدرس IP قابل مسیریابی در اینترنت نمی باشد.
- اگر تمام بیت های مشخصه میزبان دارای ارزش"1" باشند، این آدرس به عنوان آدرس Broadcast مورد استفاده قرار می گیرد.
- اگر تمام بیت های مشخصه میزبان دارای ارزش"0" باشند، این آدرس به عنوان Network ID مورد استفاده قرار می گیرد.

آشنایی با Network Mask

Network Mask یک عدد دودویی ۳۲ بیتی شبیه آدرس IP می باشد که مشخص کننده تعداد بیت های استفاده شده برای شبکه (Net ID) می باشد. این عدد۳۲ بیتی نیز همانندIP به فرم ده دهی و در چهارOctet نمایش داده می شود. توسط Net Mask می توان رنج آدرس هایIP مورد استفاده در یک شبکه را مشخص نمود. تعداد 1 در این الگو مشخص کننده تعداد شبکه و تعداد 0 مشخص کننده تعداد میزبان می باشد.

---

[1] Feature
[2] Automatic Private IP Addressing

Network Mask کلاس های استاندارد در جدول زیر نمایش داده شده است:

کلاس A		
	Binary Mode	Decimal Mode
Start	00000001 00000000 00000000 00000000	1.0.0.0
End	01111110 00000000 00000000 00000000	126.0.0.0
Subnet Mask	11111111 00000000 00000000 00000000	255.0.0.0
کلاس B		
Start	10000000 00000001 00000000 00000000	128.1.0.0
End	10111111 11111110 00000000 00000000	191.254.0.0
Subnet Mask	11111111 11111111 00000000 00000000	255.255.0.0
کلاس C		
Start	11000000 00000000 00000001 00000000	192.0.1.0
End	11011111 11111111 11111110 00000000	223.255.254.0
Subnet Mask	11111111 11111111 11111111 11111111 00000000	255.255.255.0

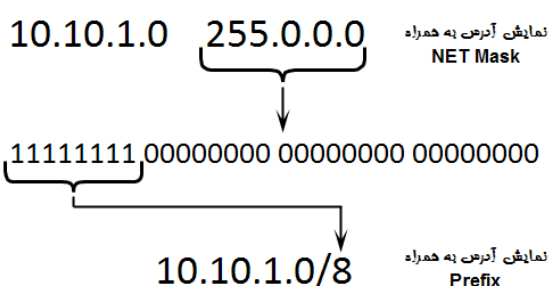
انواع حالت نمایش Net Mask

بطور معمول نمایش Net Mask در کنار IP به یکی از دو روش زیر انجام می پذیرد:

۱- در این روش Net Mask را به فرم ده دهی کنار آدرس IP مورد نظر می نویسند:

Class A: 10.10.1.0 255.0.0.0
Class B: 130.100.10.0 255.255.0.0
Class C: 192.210.1.0 255.255.255.0

۲- در روش دوم تعداد بیت های با ارزش "1" موجود در Net Mask را در کنار آدرس IP مورد نظر می نویسند. به این عدد که نشان دهنده تعداد 1 های تعلق گرفته به شبکه می باشد Prefix گفته می شود. برای مثال در کلاس A که Net Mask در حالت باینری دارای ۸ بیت اول با ارزش "1" است را به این صورت نمایش می دهند:



زیر شبکه سازی (Subnetting)

همانطور که در قسمت قبل توضیح داده شد، آدرس هایIP در سه کلاس متفاوت با طول بیت های از پیش مشخص شده جهت تعیین تعداد شبکه و تعداد میزبان تقسیم بندی شده اند. اگر شبکه ای که شما مسئول راه اندازی آن هستید دارای تعداد شبکه و میزبان نزدیک به یکی از این سه کلاس باشد، شما آدم خوش شانسی هستید و می توانید به راحتی از یک یا چند رنج آدرس از کلاس مورد نظر استفاده کنید. اما اگر تعداد شبکه و میزبان مورد نظر شما با هیچ یک از این سه کلاس همخوانی نداشت، چه کاری انجام می دهید؟

برای رفع ایراد فوق، از روشی به نام زیر شبکه سازی یا همان Subnetting استفاده می شود. در این روش شما می توانید یک رنج آدرس از هر کلاس را به تعداد شبکه و میزبان کوچکتر تقسیم کنید. در این صورت نیز همچنان قوانین کلاس A، B و C برقرار است، اما یک شبکه با کلاس های فوق به تعدادی زیر شبکه مستقل از یکدیگر تبدیل شده اند.

پس از انجام عملیات Subnetting، با نمایش Subnet Mask در کنار آدرسIP مورد نظر، می توان تعداد شبکه، تعداد میزبان، Net ID و آدرس پخش همگانی زیر شبکه مورد نظر را متوجه شده و از آن استفاده نمود.

نحوه محاسبه Subnetting

همانطور که گفته شد ما دارای سه کلاس اصلی آدرسIP هستیم، فراموش نکنید که قوانین این کلاسها همیشه پابرجا می ماند. ما در بحث Subnetting با کم کردن بیت های مربوط به میزبان و اختصاص دادن آن به بیت های شبکه، باعث بوجود آمدن زیر شبکه هایی می شویم که تعداد آنها وابسته به بیت های جا به جا شده می باشد. با این عمل تعداد میزبان های کلاس جدید نسبت به حالت کلاس استاندارد کمتر خواهد شد. یاد ضرب المثل قدیمی " از میزبان کم کن و بر شبکه افزای" افتادم!!!

به عنوان مثال، فرض بفرمایید یک رنج آدرسIP از کلاس A بصورت 20.0.0.0 255.0.0.0 به سازمان شما اختصاص داده شده است. در این صورت ما دارای یک عدد شبکه و تعداد $2^{24} - 2$ عدد میزبان هستیم. حال اگر سازمان شما دارای ۱۰ ساختمان در سراسر ایران باشد، پس قاعدتا نیاز به حداقل ۱۰ عدد زیر شبکه خواهید داشت. برای تقسیم کلاس فوق به ده زیر شبکه توسط مکانیزم Subnetting، باید تعدادی بیت از بیت های مربوط به میزبان برداشته و دو دستی تقدیم قسمت شبکه نمائیم. در مرحله اول Subnet Mask ما بر مبنای دودویی به این صورت است : 11111111 00000000 00000000 00000000

حال اگر ما ۳ بیت از میزبان کم کنیم و به شبکه بیافزاییم، می شود : $2^3 = 8$. یعنی ما می توانیم ۸ زیر شبکه داشته باشیم. با توجه به اینکه ما حداقل به ۱۰ زیر شبکه نیاز دایم پس یک بیت دیگر هم قرض می گیریم:$2^4 = 16$. خوب در این حالت تعداد زیر شبکه های بوجود آمده می تواند حداقل تعداد شبکه مورد نیاز ما را پوشش دهد. با تخصیص 4 بیت بیشتر به شبکه، Subnet Mask به صورت زیر در می آید:

11111111 11110000 00000000 00000000 = 255.240.0.0 = /12

پس از انجام مراحل فوق، یک رنج آدرسIP کلاسA خواهیم داشت که با تغییر بیت های مربوط به شبکه، آنرا به 16 زیر شبکه به صورت زیر تقسیم کرده ایم:

شبکه های مشتق شده از 255.240.0.0 20.0.0.0 یا به عبارتی 20.0.0.0/12			
20.0.0.0/12	20.1.0.0/12	20.2.0.0/12	20.3.0.0/12
20.4.0.0/12	20.5.0.0/12	20.6.0.0/12	20.7.0.0/12
20.8.0.0/12	20.9.0.0/12	20.10.0.0/12	20.11.0.0/12
20.12.0.0/12	20.13.0.0/12	20.14.0.0/12	20.15.0.0/12

با این عمل هنرمندانه ای که انجام دادیم، حالا ما از یک رنج آدرسIP، توانسته ایم $2^4 = 16$ زیر شبکه و تعداد $2^{20} - 2$ میزبان به ازای هر زیر شبکه داشته باشیم.

شاید با دیدن $2^{20} - 2$ ، این سوال برایتان پیش بیاید که دلیل -2 چیست؟ همانطور که قبلا گفتیم اولین آدرس IP به عنوان معرف شبکه (Net ID) و آخرین آدرس هر Subnet مربوط به پخش همگانی (Broadcast) همان زیر شبکه می باشد. به همین دلیل این دو آدرس قابل اختصاص به میزبان خاصی در شبکه نیستند. و اگر سوال پیش بیاید که چرا برای زیر شبکه ها از -2 استفاده نکردید، فقط اجمالا حضورتان عرض می کنم به دلیل خاصیت IP Subnet Zero؛ ولی تشریح بیشتر آن را در فصل های بعد تقدیم حضورتان می کنم.

Wildcard Mask

نوعی ماسک شبکه می باشد که در نوشتن Access Listها و بعضی از پروتکل های مسیریابی مثل OSPF به جای Subnet Mask مورد استفاده قرار می گیرد.

ماسک Wildcard کاملا بر عکس Subnet Mask می باشد. به این معنی که تمام 0 های Subnet Mask به 1 و تمام 1 ها به 0 تبدیل می شوند.

به عنوان مثال، اگرSubnet Mask شبکه ای برابر 255.255.252.0 باشد، ماسک Wildcard آن بصورت 0.0.3.255 خواهد بود.

Subnet Mask
Binary: 11111111.11111111.11111100.00000000 ==> Decimal:255.255.252.0
Wildcard Mask
Binary: 00000000.00000000.00000011.11111111 ==> Decimal:0.0.3.255

آدرس های عمومی و خصوصی

نهاد تخصیص آدرس های اینترنت(IANA)، آدرس های IP را به دو قسمت آدرس های عمومی (Public) و آدرس های خصوصی (Private) تقسیم بندی می نماید.

۱- **آدرس های عمومی:**

سازمان IANA وظیفه اختصاص آدرس های IP منحصر بفرد به تمام کاربران اینترنت را بر عهده دارد. این آدرسها که باید در سراسر جهان یکتا باشد در اختیار موسسات مجاز قرار گرفته تا آنها نیز این آدرسها را به کاربران اختصاص دهند. این آدرس ها به دلیل داشتن قابلیت مسیریابی سراسری در اینترنت قابلیت تکرار یا اختصاص به چند کاربر یا سازمان را ندارند. به دلیل اینکه میزبان های دارای آدرس های فوق برای اعضای اینترنت قابل دسترسی هستند، این آدرس ها را آدرس های عمومی یا Public می نامند.

۲- **آدرس های خصوصی:**

از آنجا که سازمان ها و یا کاربران برای دریافت IP باید متحمل پرداخت هزینه گردند و از طرف دیگر با توجه به محدودیت تعداد آدرس های IP، امکان اختصاص آدرس IP به تمام کاربران در سراسر جهان نیز مقدور نمی باشد. لذا سازمان IANA از هر کلاس A، B و C یک رنج آدرس را برای شرکت ها و شبکه های خصوصی اختصاص داده است. به دلیل اینکه این سه رنج آدرس IP قابلیت آدرس دهی و مسیریابی در اینترنت را ندارند و فقط در شبکه های خصوصی می توانند مورد استفاده قرار بگیرند، با نام آدرس های خصوصی یا Private شناخته می شوند.

در جدول زیر لیست آدرس های خصوصی نمایش داده شده است.

Class	IP / Netmask	Start / End IP Address
A	10.0.0.0 255.0.0.0	10.0.0.0 10.255.255.255
B	172.16.0.0 255.255.0.0	172.16.0.0 172.31.255.255
C	192.168.0.0 255.255.255.0	192.168.0.0 192.168.255.255

دروازه (Gateway)

یک شبکه برای ارتباط با شبکه های دیگر نیاز به یک درگاه ورودی و خروجی دارد که به آن Gateway می گویند. در واقع Gateway یک آدرسIP می باشد که بر روی یک اینترفیس به عنوان دروازه اصلی ورود و خروج به آن شبکه تنظیم گردیده است.

وظیفه Gateway در شبکه بر عهده تجهیزاتی گذارده می شود که توانایی کار در لایه سوم مدل OSI را داشته باشند.

پروتکل کنترل انتقال (TCP)

پروتکل کنترل انتقال TCP(Transmission Control Protocol)، یکی از اصلی ترین پروتکل های مجموعه TCP/IP و یکی از دو مؤلفه اصلی این مجموعه است که در نهایت باعث بوجود آمدن پروتکلTCP/IP می شود. TCP پروتکلی اتصال گرا[1] است که وظیفه اصلی آن اطمینان از صحت انتقال اطلاعات می باشد. همچنین این پروتکل، وظیفه کنترل جریان داده ها[2] و جبران خطا را نیز بر عهده دارد.

پروتکلTCP به دلیل اتصال گرا بودن دارای مکانیسم تصدیق صحت اطلاعات توسط گیرنده بوده و همواره می توان از درستی انتقال اطلاعات توسط این پروتکل اطمینان حاصل نمود. البته یکی از معایب پروتکل های اتصال گرا استفاده بیشتر پهنای باند شبکه و کند تر بودن آن نسبت به سایر پروتکلها می باشد. نکته دیگر در مورد اتصالاتTCP این است که به دلیل اتصال گرا بودن این پروتکل، امکان استفاده از آدرس های Broadcast و Multicast وجود ندارد.

این پروتکل از پیام ACK(Acknowledgment) برای تصدیق اطلاعات و از Negative acknowledgment)NACK) جهت رد صحت اطلاعات دریافتی، استفاده می نماید.

پروتکل TCP توسط استاندارد RFC 793 تعریف گردیده است.

پروتکلUDP

پروتکلUDP(User Datagram Protocol) پروتکلی غیر اتصال گرا[3] می باشد که توسط RFC 768 و در لایه انتقال تعریف گردیده است. از نظر سرعتUDP سریعتر ازTCP عمل می کند، اما دارای قابلیت تصدیق اطلاعات نمی باشد.

---

[1] Connection-Oriented
[2] Sequence Number
[3] Connection-Less

در برنامه های حساس به زمان و یا در موارد نیاز به انتقال سریع اطلاعات بدون نیاز به سطح بالایی از اطمینان، می توان از UDP استفاده نمود. همچنین UDP قابلیت کار با آدرس های پخش همگانی (Broadcast) و چند پخشی (Multicast) را نیز دارد که همین امر موجب استفاده از این پروتکل در برنامه هایی نظیر ویدئو تحت شبکه، گردیده است.

پورت (Port)

در بحث شبکه های کامپیوتری، پورت به معنای درگاه ورودی یا خروجی مورد استفاده توسط پروتکل ها و نرم افزارهای مختلف می باشد.

ممکن است بر روی شبکه شما چندین برنامه که از پروتکل TCP یا UDP استفاده می کنند، بطور همزمان اجرا شده باشند. در صورت وجود نداشتن پورت، بین برنامه ها تصادم بوجود آمده و باعث اختلال در شبکه می گردد. اما در صورت استفاده هر برنامه از یک پورت خاص، تمام برنامه ها و پروتکل ها بدون ایجاد هیچ مشکلی بر روی شبکه اجرا خواهند شد.

اهمیت مشخص نمودن شماره پورت مبدا و مقصد در پروتکل های مورد استفاده در لایه انتقال، مطابق با درجه اهمیت مشخص نمودن آدرس IP مبدا و مقصد می باشد.

پورت ها در RFC 6335 تعریف گردیده است و شامل اعداد 1 تا 65535 بوده که جهت اختصاص به پروتکل ها، به ۳ رنج زیر تقسیم می شوند:

۱- از شماره 1 تا 1023 ، برای پروتکل های استاندارد شده توسط IETF، تخصیص داده شده است.

۲- از شماره 1024 تا 49151، بنا به درخواست شرکت ها و یا اشخاص از IANA، برای پروتکل های ایجاد شده توسط آنها در نظر گرفته می شود.
البته لازم به ذکر است که این تخصیص پورت از طرف IANA، به معنای قبول پروتکل مورد نظر جهت استاندارد سازی و یا تایید آن برای استفاده کاربران نمی باشد.

۳- از شماره 49152 تا 65535، محدوده ای است که توسط IANA ثبت نمی شود و جهت استفاده های پویا و موقتی کاربران و نرم افزارها در نظر گرفته شده است.

جدول زیر شامل لیست تعدادی از پورت های اختصاص داده شده به پروتکل های مختلف می باشد:

Port	TCP	UDP	Description
20	TCP	UDP	FTP data transfer
21	TCP		FTP control (command)

Port	TCP	UDP	Description
22	TCP	UDP	Secure Shell (SSH)
23	TCP	UDP	Telnet protocol
25	TCP		Simple Mail Transfer Protocol (SMTP
80	TCP		Hypertext Transfer Protocol (HTTP)
110	TCP		Post Office Protocol v3 (POP3)
115	TCP		Simple File Transfer Protocol (SFTP)
443	TCP		HTTPS (Hypertext Transfer Protocol over SSL/TLS)
514		UDP	Syslog—used for system logging
520		UDP	Routing Information Protocol (RIP)
554	TCP	UDP	Real Time Streaming Protocol (RTSP)
990	TCP	UDP	FTPS Protocol (control): FTP over TLS/SSL
991	TCP	UDP	NAS (Netnews Administration System)
992	TCP	UDP	TELNET protocol over TLS/SSL
993	TCP		Internet Message Access Protocol over SSL (IMAPS)

شماره پروتکل (Protocol Number)

در سرآیند[1] پروتکل IPv4، فیلدی ۸ بیتی با نامProtocol وجود دارد که از آن برای شناسایی پروتکل سطح بعدی استفاده می شود. عدد مورد استفاده در این فیلد، شماره پروتکل یا Protocol Number، نامیده می شود.

عددProtocol Number توسطIANA به پروتکل ها اختصاص داده می شود و لیست آن توسط RFC 5237 منتشر می گردد. برای مثال می توان به پروتکل های زیر اشاره نمود:

- ICMP : Protocol Number 1
- IGMP : Protocol Number 2
- TCP : Protocol Number 6
- L2TP : Protocol Number 115

لازم به ذکر است بیشترین استفاده از Protocol Number، در پیکربندی تجهیزات امنیت شبکه می باشد.

[1] IP header

☑ مبحث سوم

پروتکل IPv6

پروتکلIPv6

در زمان شروع به کار IPv4، هیچ کس فکر نمی کرد که شبکه اینترنت بر اساس این پروتکل با سرعتی دور از ذهن تا به این حد گسترش پیدا کرده و روز به روز به تعداد کاربران این شبکه در سرتاسر جهان افزوده شود، تا حدی که اختصاص آدرسIP را به کاربران جدید غیر ممکن سازد. اما امروز ما به لحظه تمام شدن آدرس هایIP خیلی خیلی نزدیک شده ایم. به همین علت راهی جز کوچ اجباری از پروتکل قدیمی ولی محبوب IPv4 به یک پروتکل جدید با ظرفیت آدرس دهی بالاتر برای ما باقی نمانده است.

انجمنIETF با تجدید نظر در نسخه IPv4، نسخه جدید را با نام (Internet Protocol version 6)IPv6 همراه با قابلیت های جدید، توسط RFC 2460 تعریف و ارائه نمود.

پروتکلIPv6 امکان استفاده از آدرس128 بیتی را در اختیار ما قرار می دهد. این آدرس که بر مبنای دودویی می باشد، در قالب ۸ گروه ۱۶ بیتی جدا شده توسط کاراکتر " : " و به فرم شانزده شانزدهی[1] نمایش داده می شود. در IPv6 این گروه های ۱۶ بیتی "Hextet" نامیده می شوند. (بماند که فرآیند این نام گذاری باعث ایجاد یک پیش نویسRFC نیز گردید.[2])

نمونه ای از آدرس IPv6 در قالب دودویی و تبدیل آن به شانزده شانزدهی در ادامه آمده است. آدرس در قالب دودویی :

0010000000000001:110110001000:001000000000:001100000000:010000000000:
010100000000:0001001000110100:0101011001111000

اگر بخواهیم آدرس دودویی فوق را در قالب شانزده شانزدهی نشان دهیم، بصورت زیر خواهد بود:

2001:D88:200:300:400:500:1234:5678

---

[1] Hexadecimal

[2] http://tools.ietf.org/html/draft-denog-v6ops-addresspartnaming-04

پروتکل IPv4 تنها می تواند تعداد $2^{32} = 4,294,967,296$ عدد آدرس منحصر به فرد را به کاربران اینترنت اختصاص دهد، یعنی کمتر از هر نفر یک عدد آدرسIP (با توجه به جمعیت جهان در سال ۲۰۱۲). اما با توجه به 128 بیتی بودن IPv6، تعداد آدرس های آن می تواند $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ عدد باشد. با این حساب برای همان تعداد جمعیت[۱]، می توان به ازاء هر نفر در حدود 4.8×10^{28} عدد آدرسIP اختصاص داد. به عبارت دیگر به هر نفر از جمعیت زمین می توان بیش از تعداد کل آدرس های IPv4، آدرس IPv6 اختصاص داد. تمام شدن این تعداد آدرس تا آخر دنیا هم بعید به نظر می رسد. البته بماند که زمان تصویب IPv4 هم ۴ نفر پروفسور! مثل ما فکر می کردند که آدرس های ۳۲بیتی هم تا آخر دنیا ادامه پیدا می کنه!

ویژگیهای IPv6

پروتکلIPv6 دارای خصوصیات بارزی نسبت به نسخه قبلی خود می باشد که باعث بهبود عملکرد این پروتکل گردیده است. از مزایای این پروتکل میتوان به موارد زیر اشاره نمود:

- **فضای آدرس دهی گسترده**

با توجه به گسترش روز افزون دستگاه های با قابلیت اتصال به شبکه و افزایش جمعیت جهان و درخواست اتصال آنها به شبکه جهانی، نیاز به تعداد آدرس IP منحصر بفرد زیادی ایجاد شده است که نسخه ششم پروتکل اینترنت با آدرسی به طول ۱۲۸ بیت این نیاز را براحتی برطرف می سازد.

وجود فضای گسترده آدرس دهی در پروتکل IPv6، این پروتکل را در استفاده از ویژگی ترجمه آدرس شبکه(NAT/PAT)[۲] بی نیاز نموده است.

- **آدرس دهی اتوماتیک در IPv6**

پروتکل IPv6 دارای چند روش اختصاص آدرس بصورت پویا می باشد. این پروتکل ضمن امکان استفاده از DHCP، می تواند بدون حضور سرور DHCP و بصورت Stateless نیز آدرس دهی پویا را انجام دهد.

---

[۱] بر اساس اعلام اداره آمار امریکا، جمعیت جهان در سال ۲۰۱۲ بیش از ۷ میلیارد نفر می باشد.

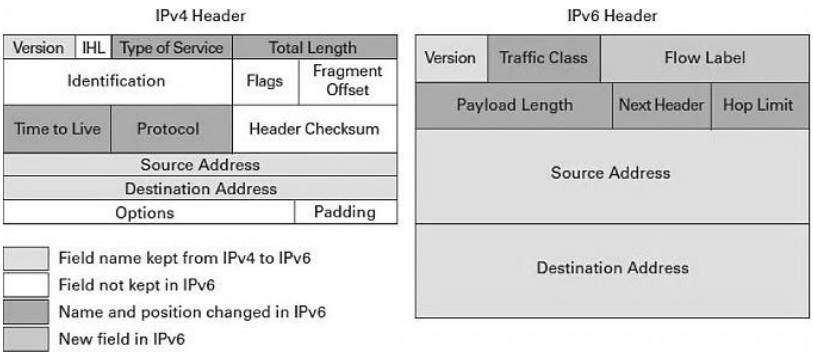
[2] Network Address Translation / Port Address Translation

- **امکان اجرای همزمان IPv4 و IPv6**

برای ایجاد امکان همکاری بین هر دو نسخه این پروتکل و اجرای آنها در کنار هم، دو روش وجود دارد. اول پیکربندی همزمان هر دو پروتکل روی هر کدام از رابط های شبکه. دوم امکان استفاده از روش IPv6 over IPv4[1]، جهت حمل اطلاعات مربوط به IPv6 بر روی بستر ایجاد شده بر اساس پروتکل IPv4.

- **Header ساده**

هر چند که طول Header پروتکل IPv6 از IPv4 طولانی تر است، اما ساده تر بودن Header پروتکلIPv6 نسبت به IPv4 باعث بهبود عملکرد این پروتکل در شبکه گردیده است.



- **امنیت**

پروتکل IPv6 به صورت توکار[2] از پروتکل امنیتیIPsec [3] پشتیبانی می کند. با توجه به اجباری بودن استفاده از IPsec در پروتکل IPv6، تمامی شبکه های مبتنی برIPv6 بصورت پیش فرض[4] از IPsec استفاده می کنند که همین امر موجب بالا رفتن امنیت ارتباطات در این نوع شبکه ها گردیده است.

- **پویایی (Mobility)**

خاصیت پویایی امکان برقراری ارتباط بی سیم افراد با شبکه را ایجاد می نماید. این خاصیت امکان جا به جایی دستگاه های بی سیم متصل به شبکه را بدون قطع ارتباط فراهم می آورد. خاصیت Mobility بصورت توکار در IPv6 تعبیه شده است.

---

[1] RFC 3056
[2] Built-in
[3] Internet Protocol Security
[4] By Default

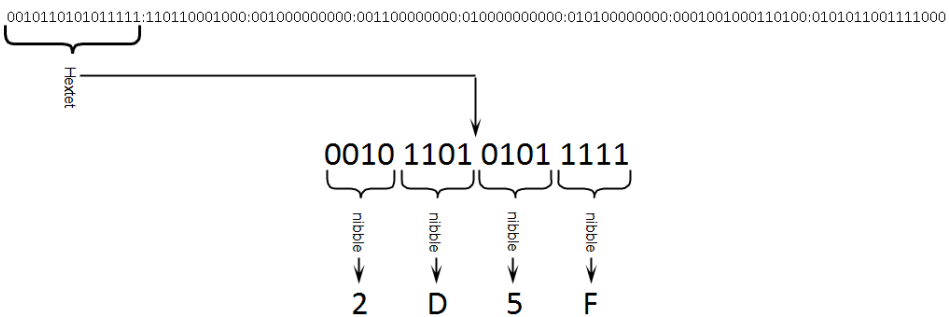
تبدیل آدرس دودویی به شانزده شانزدهی

برای تبدیل آدرس های دودویی به شانزده شانزدهی، باید هر چهار بیت Binary را توسط جدول زیر به یک عدد در مبنای شانزده شانزدهی تبدیل نمود:

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Binary	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

همانطور که ملاحظه می نمایید از عدد10 تا 15 از حروف انگلیسی برای تبدیل شانزده شانزدهی استفاده می شود.

با توجه به اینکه هر Hextet آدرسIPv6 از 16 بیت عدد دودویی تشکیل شده است، برای تبدیل آن به آدرس شانزده شانزدهی باید هر 4 بیت آدرس (که به آن nibble گفته می شود) را به یک عدد شانزده شانزدهی تبدیل نمود:



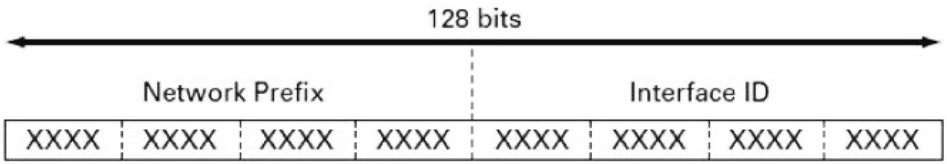
در نهایت تبدیل آدرس دودویی فوق به آدرس شانزده شانزدهی به صورت زیر خواهد بود:

2D5F:D88:200:300:400:500:1234:5678

ساختار آدرس IPv6

آدرس های IPv6 همانند آدرس های IPv4 دارای دو قسمت برای آدرس دهی شبکه و آدرس دهی میزبان می باشند.

آدرس هایIPv6 دارای 128 بیت می باشند که بصورت پیش فرض 64 بیت آن برای قسمت Network Prefix و 64 بیت آن برای قسمت Interface Local مورد استفاده قرار می گیرد.



XXXX = 0000 through FFFF

در نحوه نوشتن آدرس های IPv6 در قالب شانزده شانزدهی به نکات زیر توجه نمایید:

- می توان از نوشتن اعداد صفر ابتدای هر Hextet صرف نظر کرد.
- تمامی فیلدهای 0 متوالی را می توان بصورت" :: "نوشت.

برای مثال آدرس 090C:0000:0000:0000:0000:0000:0000:1 را می توان بصورت 90C::1 نیز نوشت.

- ویژگی فوق (استفاده از ::) فقط یک بار می تواند در یک آدرس مورد استفاده قرار گیرد. به عنوان مثال آدرس 090C:0000:0000:2001:0000:0000:0000:1 را می توان به یکی از دو صورت زیر نوشت:

90C::2001:0000:0000:0000:1
90C:0000:0000:2001::1

البته می توانید به جای نوشتن صفرهای متوالی در یک Hextet ، فقط به نوشتن یک صفر بسنده کنید:

90C::2001:0:0:0:1
90C:0:0:2001::1

- در شبکه هایی که از هر دو پروتکل IPv4 وIPv6 استفاده می شود، می توان در نوشتن آدرس های IPv6 از شبیه سازی آدرس های IPv4 بهره برد.

به دو طریق می توان آدرس های IPv4 را در آدرس های IPv6 شبیه سازی نمود:

در روش اول که IPv4-Compatible IPv6 Address نامیده می شود، ۹۶ بیت اول آدرس مقدار 0 داشته و در ۳۲ بیت آخر آن، آدرس شبیه IPv4 نمایش داده می شود. در این حالت آدرس IPv4 مورد استفاده، باید آدرس منحصر به فرد باشد.

روش دوم IPv4-Mapped IPv6 Address نام دارد. در این روش به۸۰ بیت اول مقدار 0 و ۱۶ بیت پس از آن، مقدار 1 داده می شود. ۳۲ بیت آخر نیز همانند روش قبلی وظیفه نمایش آدرس را بصورت IPv4 بر عهده دارد.

به عنوان مثال به آدرس های زیر توجه کنید:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

آدرس های فوق را در حالت فشرده می توان به صورت زیر نوشت:

::13.1.68.3
::FFFF:129.144.52.38

نحوه نمایش Prefix در IPv6

همانطور که به یاد دارید در پروتکل IPv4 برای مشخص نمودن تعداد بیت های مربوط به شبکه از Subnet Mask و Prefix استفاده می شد. اما در پروتکل IPv6 چیزی شبیه به Subnet Mask وجود نداشته و برای مشخص کردن تعداد بیت های مربوط به شبکه، تنها از Prefix استفاده می شود. نحوه نمایش Prefix در پروتکل IPv6 به صورت زیر می باشد:

IPv6-Address / Prefix-Length

عبارت Prefix-Length، یک عدد بر مبنای ده دهی است که نشان دهنده تعداد بیت های اختصاص داده شده به شبکه می باشد.

به عنوان مثال به آدرس زیر توجه نمایید:

نمایش آدرس IPv6	2001:0DB8:0:CD30:123:4567:89AB:CDEF
نمایش آدرس به همراه Prefix	2001:0DB8:0:CD30: 123:4567:89AB:CDEF /60
نمایش Subnet در IPv6	2001:0DB8:0:CD30:: /60

همانطور که در مبحث IPv4 گفتیم، پس از Subnetting آدرس ها، نمی توان از اولین و آخرین آدرس به دست آمده استفاده نمود. دلیل این اتفاق، استفاده از آدرس های مذکور به عنوان Net ID و Broadcast می باشد. اما در پروتکل IPv6 نه از Broadcast خبری است و نه نیازی به از دست دادن یک آدرس برای مشخص نمودن NET ID می باشد.

مکانیزم EUI-64

سازمان IEEE برای سهولت در آدرس دهی منحصر بفرد کلاینت ها در IPv6، اقدام به معرفی مکانیزم EUI-64(Extended Unique Identifier) نموده است.[1]

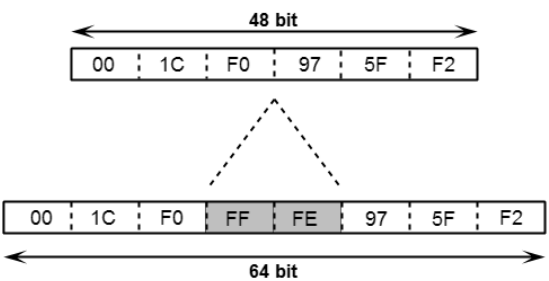
[1] http://standards.ieee.org/develop/regauth/tut/eui64.pdf

از طریق مکانیسم EUI-64، یک میزبان می تواند بدون نیاز به پیکربندی دستی و یا حضور سرورDHCP، اقدام به تخصیص مقدار به ۶۴ بیت مربوط به قسمت Interface ID خود نماید. این مقدار بر اساس آدرس MAC موجود بر روی اینترفیس مربوطه محاسبه می گردد. همچنین ۶۴ بیت مربوط به Network Prefix نیز بر اساس نوع آدرس مورد استفاده مشخص می گردد.

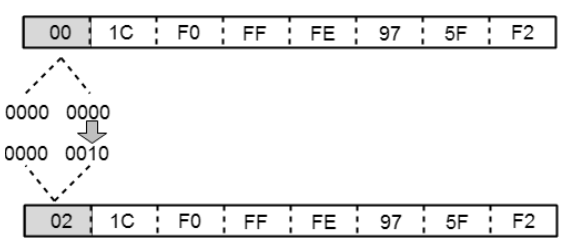
همانطور که در مبحث اول فصل سوم تشریح خواهد شد، آدرس MAC موجود بر روی واسط های شبکه بصورت منحصر بفرد به آنها تخصیص داده می شود. اما این آدرس دارای ۴۸ بیت بوده و ما برای Interface ID نیاز به ۶۴ بیت آدرس داریم. به همین دلیل بر طبق مکانیسم EUI-64 باید مقدار FF-FE را به وسط آدرس شبکه اضافه نموده تا یک آدرس ۶۴ بیتی به دست آوریم. سپس باید بیت هفتم این آدرس بررسی شود تا منحصر به فرد بودن آن احراز گردد.

ایجاد آدرس بر اساس مکانیسم EUI-64 در دو مرحله بصورت زیر انجام می پذیرد:

۱- در گام اول باید با اضافه کردن مقدار FF-FE به آدرس MAC، یک آدرس ۶۴ بیتی به وجود می آید. به عنوان مثال اگر آدرس MAC رابط شبکه ما 00-1C-F0-97-5F-F2 باشد، تبدیل آدرس به صورت زیر خواهد بود:



۲- در گام بعدی بیت هفتم آدرس بوجود آمده مورد بررسی قرار می گیرد. در صورتیکه بیت هفتم آدرس 0 باشد به 1 و اگر 1 باشد به 0 تبدیل می گردد.



پس از طی مراحل فوق در نهایت آدرس به دست آمده بر اساس مکانیسم EUI-65 بصورت زیر خواهد بود:

021C:F0FF:FE97:5FF2

انواع آدرس دهی در IPv6

طبق استاندارد RFC 4291، سازمان IETF انواع آدرس دهی پروتکل IPv6 را به سه بخش زیر تقسیم نموده است:

۱- **Unicast**

از Unicast برای آدرس دهی یک اینترفیس مشخص استفاده می شود.

بسته‌ای که مقصد آن توسط آدرس Unicast مشخص شده باشد، فقط تحویل اینترفیسی خواهد شد که دارای آدرس مورد نظر می باشد.

۲- **Anycast**

آدرس Anycast شناسه گروهی از اینترفیس ها می باشد که معمولا متعلق به Nodeهای مختلفی در شبکه می باشند.

یک بسته ارسال شده به آدرس Anycast، تنها به یکی از اینترفیس های شناخته شده توسط این آدرس تحویل داده خواهد شد و معمولا این اینترفیس نزدیکترین اینترفیس به مبدا می باشد که آدرس آن توسط Anycast مربوطه شناسایی گردیده است.

۳- **Multicast**

آدرس Multicast شناسه یک گروه از اینترفیس های مورد نظر می باشد که معمولا متعلق به Nodeهای مختلفی در شبکه می باشد.

یک بسته ارسال شده به آدرس Multicast، به تمام اینترفیس های شناسایی شده توسط این آدرس تحویل داده خواهد شد.

همانطور که در حالت های فوق مشخص است، پروتکل IPv6 بر خلاف IPv4 از آدرس‌های پخش همگانی(Broadcast) استفاده نمی نماید.

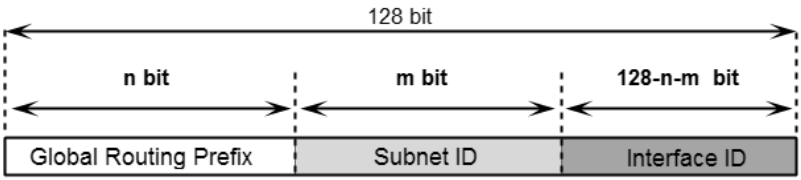
انواع آدرس Unicast

همانطور که گفتیم از آدرس های Unicast برای برقراری ارتباط یک به یک بین میزبان ها استفاده می شود. آدرس دهیUnicast در پروتکل IPv6 به سه نوع زیر تقسیم بندی می شود:

- **Global Unicast**

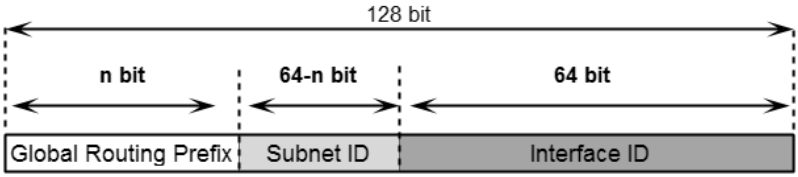
آدرس های Global Unicast شبیه آدرس های Public درIPv4 می باشند.

فرمت کلی آدرس Global Unicast بصورت زیر می باشد:



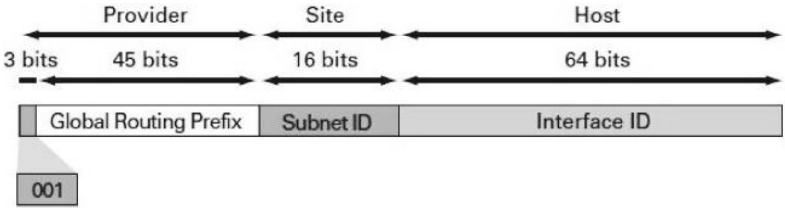
فیلد Global Routing Prefix ارزش اختصاص داده شده به یک سایت می باشد که بطور معمول ساختار سلسله مراتبی دارد. فیلدSubnet ID نیز بیانگر شناسه زیر شبکه می باشد. فیلدInterface ID هم شناسه تخصیص داده شده بهHost مورد نظر بوده که این امر می تواند به طرق مختلفی صورت پذیرد.

البته توجه به این نکته ضروریست که تمام آدرس های Unicast (بجز آدرس هایی که با 000 شروع می شوند) باید۶۴ بیت آخر را بهInterface ID اختصاص داده تا آدرس دهیHost بر اساس مکانیزم EUI-64 امکانپذیر باشد. قالب این نوع آدرس بصورت زیر خواهد بود:



در آدرس فوق نیز فیلدGlobal Routing Prefix مقدار اختصاص یافته جهت شناسایی یک سایت می باشد. برای اینکه این آدرس در سطح اینترنت منحصر به فرد باشد، سازمانIETF اقدام به اختصاص مقدار خاص به بیت های اول مربوط به Global Routing Prefix می نماید.

در حال حاضر IETF برای این نوع آدرس، مقدار سه بیت اول را بصورت ثابت 001 تعیین نموده است. با توجه به اینکه بیت چهارم می تواند 0 یا 1 باشد، Hextet اول این نوع آدرس در رنج 2000::/3 تا 3000::/3 قرار خواهد داشت.



سه بیت اول بصورت ثابت 001 می باشد که بیانگر آدرس Global Unicast است. ۴۵ بیت بعدی به عنوان شناسه سایت و ۱۶ بیت میانی نیز برای زیر شبکه سازی سایت ها مورد استفاده واقع می شوند.

به دلیل اینکه این نوع آدرس‌ها باید بصورت منحصر بفرد بر روی اینترنت قرار داشته باشند، وظیفه تخصیص آدرس های این رنج بر عهده سازمان IANA گذارده شده است. شما می‌توانید لیست آدرس‌های اختصاص داده شده را در سایت IANA مشاهده نمایید.[1]

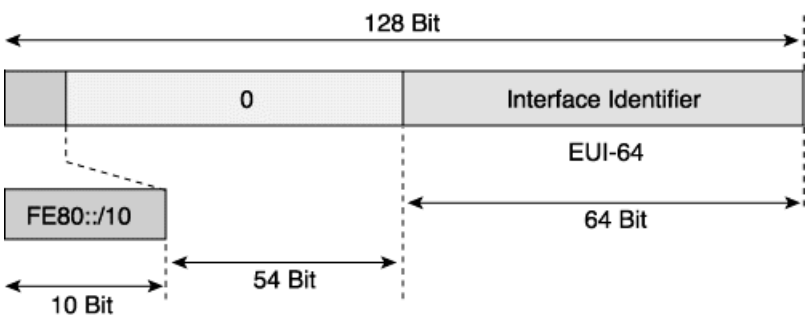
به عنوان مثال آدرس IPv6 سایت های www.ietf.org و www.iana.org بصورت زیر می باشد:

www.ietf.org ==> 2001:1890:126c::1:1e
www.iana.org ==> 2001:500:88:200::8

- **Link-Local Unicast**

آدرس Link-Local Unicast پس از فعال شدن پروتکلIPv6 بر روی یک اینترفیس، به صورت خودکار به آن اینترفیس اختصاص داده می شود. از این نوع آدرس برای عملیات های مختلف از جمله کشف همسایه(NDP)[2] و اختصاص پویای آدرسIPv6 استفاده می گردد. همچنین مواقعی که روتر در شبکه موجود نباشد این نوع آدرس دهی کاربرد دارد.

این آدرس‌ها فقط در بین گره‌های متصل به یک لینک محلی مورد استفاده قرار گرفته و هیچگاه بین زیر شبکه های مختلف مسیردهی نمی گردند.



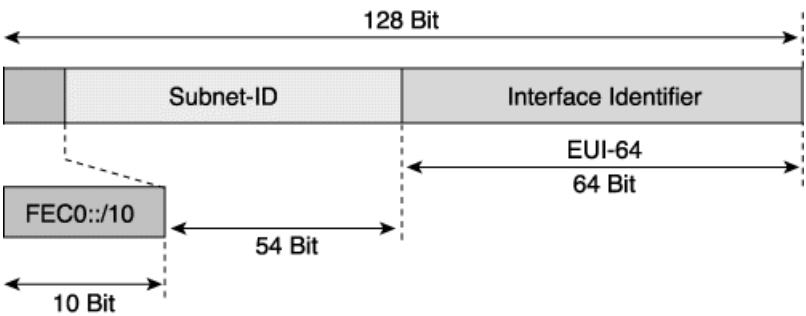
[1] http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml
[2] Network Discovery Protocol

همانطور که در تصویر ملاحظه می کنید، آدرس های Link-Local بصورت FE80::/10 می باشند. که در آن ۱۰ بیت اول بصورت1111111010 ثابت بوده و مشخص کننده رنج آدرس‌های Link-Local می باشد. همچنین به بیت ۱۱ تا ۵۴ همواره مقدار 0 اختصاص داده شده و در نهایت ۶۴ بیت آخر نیز بر اساس مکانیسم EUI-64 آدرس دهی می شوند.

- **Site-Local Unicast**

این نوع آدرس بر خلاف Link-Local به صورت خودکار تخصیص داده نمی شود و باید توسط مدیر شبکه پیکربندی گردند.

آدرس Site-Local شبیه آدرسPrivate درIPv4 می باشد. این آدرس ها می‌توانند در شبکه‌های داخلی مورد استفاده قرار گرفته و بین سایت های مختلف یک سازمان مسیردهی گردند. اما توجه داشته باشید که همچنان امکان مسیردهی این نوع آدرس در محیط اینترنت ممکن نمی باشد.



آدرس های Site-Local در رنج FEC0::/10 قرار دارند. همچنان که ملاحظه می نمایید مقدار۱۰ بیت اول این نوع آدرس بصورت ثابت1111111011 تعیین گردیده که نمایانگر آدرس Site-Local می باشد.

از ۵۴ بیت بعدی هم برای زیر شبکه سازی (Subnetting) استفاده می گردد. در این صورت امکان داشتن $2^{54} = 18,014,398,509,481,984$ عدد زیر شبکه را خواهیم داشت. همچنین در صورت دلخواه می توان اختصاص مقدار به ۶۴ بیت آخر را به مکانیزم EUI-64 سپرد. به عنوان مثال می توانید Subnetهای زیر را در اختیار داشته باشید:

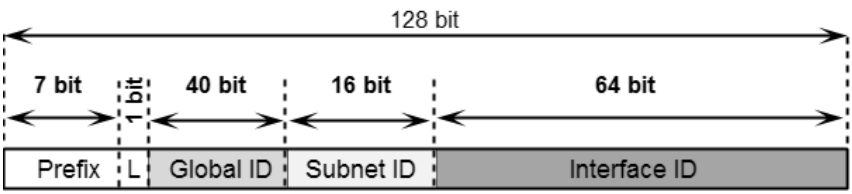
FEC0:0:0:0001::/64	FEC0:0:0:0002::/64
FEC0:0:0:0003::/64	FEC0:0:0:0004::/64
FEC0:0:0:0005::/64	FEC0:0:0:0006::/64

- **Unique-Local Unicast**

این نوع آدرس در عین حال که بصورت منحصر بفرد می باشد ولی برای استفاده در شبکه‌های محلی تعریف گردیده است. این آدرس‌ها نباید در اینترنت مسیردهی شوند ولی مسیردهی آنها بین سایتهای محدود امکان پذیر می باشد.

هر چند که این آدرس ها کاربرد داخلی دارند ولی با توجه به منحصر بفرد بودن آنها، در صورتی که به واسطه DNS و یا مسیریابی به خارج از شبکه محلی راه پیدا کنند، هیچ تداخلی با آدرس های اینترنت پیدا نخواهد نمود.

به دلیل اینکه هفت بیت اول این نوع آدرس به صورت 110 1111 مشخص گردیده، لذا رنج آدرس Unique-Local Unicast به صورت FC00::/7 نمایش داده می شود.



تعریف فیلدهای مورد استفاده در تصویر فوق بصورت زیر می باشد:

فیلد Prefix : همان FC00::/7 می باشد.

فیلد L : اگر اختصاص Prefix بصورت محلی باشد، مقدار 1 به L داده می شود. مقدار 0 نیز برای تعریف در آینده کنار گذارده شده است.

فیلد Global ID: از این ۴۰ بیت برای ایجاد یک Prefix منحصر بفرد استفاده می شود.

فیلد Subnet ID: جهت مشخص نمودن زیر شبکه می باشد.

فیلد Interface ID: مشخص کننده آدرس Interface می باشد.

آدرس‌های خاص IPv6

در جدول زیر آدرس‌های خاص مورد استفاده درIPv6 به همراه توضیح مختصری نمایش داده شده است. همچنین استاندارد مربوطه نیز برای تحقیقات بیشتر ذکر گردیده است.

Prefix	Assignment	Purpose	Routing Scope	Reference
::1/128	Loopback Address	Loopback Address	Scoped (link)	RFC 4291
::/128	Unspecified	Configuration	Not routed	RFC 4291

Prefix	Assignment	Purpose	Routing Scope	Reference
	Address			
::FFFF:0:0/96	IPv4-mapped Address	Internal Representation	Not routed	RFC 4291
0100::/64	Discard-Only Prefix	Remote triggered black hole routing	Intra AS	RFC 6666
2001:0000::/32	TEREDO	Anycast	Scoped	RFC 4380
2001:0002::/48	BMWG	Benchmarking	Not Routed	RFC 5180
2001:db8::/32	Documentation Prefix		Not routed	RFC 3849
2001:10::/28	ORCHID	Overlay	Not Routed	RFC 4843
2002::/16	6to4	Transition Tunneling	Global	RFC 3056
FC00::/7	Unique-Local	Local use	Scoped	RFC 4193
FE80::/10	Linked-Scoped Unicast	Single-link Communications	Not routed	RFC 4291
FF00::/8	Multicast	Multicast Communication	Routing scope embedded in address	RFC 4291

فصل سوم

استانداردها، پروتکل‌ها و اصطلاحات

- ☑ مبحث اول: استانداردها و پروتکل ها
- ☑ مبحث دوم: اصطلاحات و نرم افزارها

☑ مبحث اول

استانداردها و پروتکل ها

برای شروع به راه اندازی شبکه نیاز به دانستن بعضی اصطلاحات و پروتکل ها اجتناب ناپذیر است. در ادامه بعضی از این اصطلاحات و پروتکل ها که مورد نیاز است بصورت اجمالی توضیح داده می شود. لازم به ذکر است که در این فصل، پروتکل ها و اصطلاحات عمومی توضیح داده می شود و درباره پروتکل‌های تخصصی تر در بخش های مربوطه بحث خواهد شد. حضراتی که کمی حرفه ای تر هستند می توانند از خیر این بخش بگذرند!

ایترنت (Ethernet)

ایترنت فراگیرترین فناوری شبکه های محلی رایانه ای می باشد که در لایه اول مدل TCP/IP [۱] و بر اساس استاندارد IEEE 802.3 منتشر گردیده است.

استاندارد ایترنت مشخص کننده نوع سیم کشی، سوکت[۲]، سیگنالینگ و توپولوژی شبکه می‌باشد. از جمله ویژگی های ایترنت می توان به آدرس MAC و فریم بندی دیتا اشاره نمود.

سیستم های ارتباطی که بر روی ایترنت کار می کنند، جریان داده ها را به قسمت هایی به نام فریم تقسیم بندی می نمایند. هر فریم شامل آدرس مبدا، مقصد و همچنین امکان بررسی خطای روی داده می باشد، بطوریکه می تواند داده‌های آسیب دیده را شناسایی و مجددا ارسال نماید.

استاندارد ایترنت با استفاده از توپولوژی ستاره ای[۳] و سوئیچ توانست به اوج کارایی خود در شبکه برسد. توپولوژی ستاره‌ای و سوئیچ دو مؤلفه‌ای بودند که باعث از بین رفتن تصادم[۴] و امکان برقراری ارتباط دو طرفه[۵] همزمان در شبکه شده و سرعت و کارایی شبکه را به طرز چشم گیری افزایش دادند.

---

[۱] لایه اول مدل TCP/IP شامل لایه های ۱ و ۲ مدل OSI می باشد.

[2] Socket
[3] Star Topology
[4] Collision
[5] Full Duplex

استاندارد ایترنت جهت انتقال دیتا، دارای دو حالت می باشد:

- **Half Duplex**

در این حالت، امکان انتقال دیتا فقط از طریق یک طرف گفتگو امکان پذیر است. مادامی که یک دستگاه در حال دریافت دیتا می باشد، توانایی ارسال دیتا را نخواهد داشت.

- **Full Duplex**

در این حالت، امکان انتقال دو طرفه دیتا بصورت همزمان ممکن می باشد. یک دستگاه در حالیکه در حال انتقال دیتا است، می تواند عملیات دریافت دیتا را نیز انجام دهد.

امروزه تقریبا تمام تجهیزات شبکه محلی بر اساس استاندارد ایترنت تولید می شوند. ایترنت از زمان ایجاد تا کنون شامل تغییراتی در سرعت، سیگنال، نوع کابل و توپولوژی گردیده است. در نهایت ایترنت به چهار گروه Ethernet، Fast Ethernet، Gigabit Ethernet و 10Gig تقسیم بندی شده که در جدول زیر تعدادی از آنها ذکر شده است:

گروه	استاندارد	نوع کابل	پهنای باند	حداکثر طول کابل
Ethernet	10Base2	Coax	10 Mbps	185m
	10Base5	Coax	10 Mbps	500m
	10BaseT	UTP (CAT 3 or higher)	10 Mbps	100m
Fast Ethernet	100BaseTX	UTP (CAT 5 or higher)	100 Mbps	100m
	100BaseFX	Fiber Optic	100 Mbps	400m/ 2km
Gigabit Ethernet	1000BaseT	UTP (CAT 5e or higher)	1 Gbps	100m
	1000BaseSX	Fiber Optic	1 Gbps	MMF 550m
	1000BaseLX	Fiber Optic	1 Gbps	SMF 10km
	1000BaseCX	Fiber Optic	1 Gbps	100m
10Gig	10GbaseSR	Fiber Optic	10 Gbps	300m
	10GbaseLR	Fiber Optic	10 Gbps	SMF 10km

آدرس MAC [1]

هر کارت رابط شبکه موجود بر روی هر نوع سیستمی اعم از کامپیوتر، پرینت سرور، دوربین تحت شبکه، مسیریاب و هر نوع دستگاه دیگری که قابلیت اتصال به شبکه را داشته باشد؛ بصورت داخلی و توسط شرکت سازنده دارای یک آدرس منحصر به فرد ۴۸ بیتی بر مبنای

[1] Media Access Control

شانزده شانزدهی[1] می باشد که بمنظور آدرس دهی در لایه ۲ مدل OSI مورد استفاده قرار می‌گیرد. این آدرس که به آن آدرس فیزیکی یاMAC Address می گویند، توسطIANA و بر اساسRFC 5342 به شرکت های تولید کننده تجهیزات شبکه اختصاص می یابد. با توجه به منحصر بفرد بودن آدرسMAC، می توان شرکت تولید کننده تجهیزات شبکه را شناسایی نمود.

علیرغم اینکه این آدرس برای منحصر بفرد بودن باید غیر قابل تغییر باشد ولی در سیستم عامل های مختلف امکان تغییر موقتی آدرسMAC به کاربر داده می شود. البته این کار در بعضی از مواقع توسط هکرهای عزیز! نیز برای عبور از فایروال ها و دور زدن برخی قوانین شبکه مورد استفاده قرار می گیرد. اگر بخواهید آدرس فیزیکی کارت شبکه سیستم خود را مشاهده کنید می‌توانید از دستور زیر در ویندوز استفاده نمائید:

```
C:\Ipconfig /all
```

پروتکل تحلیل آدرس(ARP)

پروتکل تحلیل آدرس(Address Resolution Protocol) که توسطRFC 826 منتشر گردیده، وظیفه مشخص نمودن آدرسMAC متناظر با IP مورد نظر را بر عهده دارد.

با توجه به اینکه انتقال بسته‌های دیتا در شبکه‌های محلی (سوئیچینگ) در لایه دو و بر اساس آدرسMAC صورت می گیرد، لذا کلاینت ها جهت ارسال دیتا نیاز به دانستن آدرسMAC متناظر با آدرسIP مقصد مورد نظر را دارند که این وظیفه بر عهده پروتکل ARP می باشد.

سوئیچ ها جهت نگهداری آدرس هایMAC متناظر باIP دارای جدولی به نام ARP Cache بر روی حافظه موقت خود می باشند. برای تکمیل کردن این جدول، سوئیچ آدرسIP مقصد مورد نظر را توسط پیام ARP Request به تمامی تجهیزات متصل به پورت های خود ارسال می نماید. سپس دستگاه دارای آدرسIP مورد نظر توسط پیام ARP Reply آدرس MAC خود را به اطلاع سوئیچ می رساند. از این پس سوئیچ آدرسIP وMAC دستگاه را جهت استفاده های بعدی در جدول ARP خود نگهداری می نماید. با توجه به اینکه این جدول در حافظه RAM ایجاد می گردد، پس از خاموش شدن سوئیچ از بین رفته و فرآیند کشف آدرس هایMAC باید مجددا اجرا گردد.

لازم به ذکر است که علاوه بر سوئیچ ها، تجهیزات متصل به شبکه نیز در حافظه RAM خود دارای جدول ARP می باشند. این جدول که حاوی آدرس هایی است که میزبان تا کنون با آنها در ارتباط بوده، می تواند باعث افزایش کارایی شبکه گردد.

---

[1] Hexadecimal

پروتکل ARP در لایه اول مدل TCP/IP یا لایه دوم مدل OSI کار می کند. وظایف این پروتکل در IPv6 توسط پروتکل کشف همسایه (NDP)[1] انجام می گیرد.

پروتکل DHCP

پروتکل پیکربندی پویای میزبان (Dynamic Host Control Protocol)، وظیفه اختصاص آدرس IP به کلاینت های شبکه را بر عهده داشته و در RFC 2131 تعریف گردیده است.

در شبکه های بزرگ دارای تعداد زیاد کلاینت، تخصیص آدرسIP بصورت دستی توسط مدیر شبکه کاری طاقت فرسا و مشکل‌آفرین خواهد بود. چراکه مدیر شبکه جهت پیکربندی رابط شبکه کلاینت‌ها، ضمن به همراه داشتن لیست بزرگی از آدرس‌هایی که تا کنون اختصاص داده شده، مجبور به حضور فیزیکی در کنار هر کلاینت نیز می باشد.

پروتکلDHCP کار اختصاص آدرس را آسان نموده و سربار مدیریتی ناشی از آن را حذف می‌نماید. با راه اندازی یکDHCP Server، پیام های درخواست کاربران که بصورت Broadcast در شبکه ارسال می شود، با یک آدرسIP منحصر به فرد در شبکه، پاسخ داده می شود.

پروتکلDHCP، آدرسIP، Subnet Mask، Default Gateway وDNS موجود و قابل اطمینان را بر روی رابط شبکه کلاینت، پیکربندی می نماید. این پروتکل، از پورت UDP 67 برای ارسال درخواست به سرویس دهنده و UDP 68 برای ارسال اطلاعات به سرویس گیرنده استفاده می نماید.

پروتکلDHCP برای استفاده در شبکه های مبتنی برIPv6 درRFC 3315 تعریف گردیده است.

سامانه نام دامنه (DNS)

سامانه نام دامنه (Domain Name System)، سیستمی سلسله مراتبی جهت نام گذاری منابع متصل به شبکه مثل کامپیوترها می باشد که توسط RFC 1034 تعریف گردیده است.

برای دسترسی به منابع روی شبکه و یا اینترنت، باید از آدرسIP استفاده نمایید. استفاده از آدرسIP توسط کاربر امری ناخوشایند و البته فراموش شونده است. تصور کنید که شما مجبور باشید برای بازدید از سایتهای مورد نظرتان در اینترنت، آدرس هایIP آنها را به خاطر بسپارید! این یادآوری می تواند لذت استفاده از اینترنت را از شما بگیرد.

[1] Neighbor Discovery Protocol

سامانه DNS یک بانک اطلاعاتی شامل آدرس هایIP منابع روی شبکه یا اینترنت می باشد که هر کدام آنها متناظر با یک نام ملموس و مرتبط ثبت گردیده است. شما فقط کافیست سایت مورد نظر را بر اساس نام آن درخواست کنید تا سامانه DNS زحمت تبدیل آن به آدرس IP را بکشد.

ثبت نام تجهیزات درون شبکه‌های خصوصی در سرور DNS همان شرکت و توسط مدیر شبکه انجام می پذیرد. اما ثبت نام برای سایتهای موجود در اینترنت توسط شرکت های دارای مجوز از سازمان IANA انجام می گیرد.

سامانهDNS برای انتقال اطلاعات به صورت معمول از پورت ۵۳ پروتکلUDP و در مواقع خاص از پورت ۵۳ پروتکلTCP استفاده می نماید. به عنوان مثال اگر DNS درخواستی را دریافت کند که حجم جواب آن بزرگتر از۵۱۲ بایت باشد، درخواست را به مبدا بازگردانده و از او می‌خواهد که درخواستش را مجددا بر روی پروتکل TCP ارسال نماید.

پروتکل انتقال فایل (FTP)

پروتکل انتقال فایل (File Transfer Protocol)، توسط RFC 959 تعریف گشته و وظیفه انتقال مطمئن فایل بین دو دستگاه انتهایی (End-to-End) را بر عهده دارد.

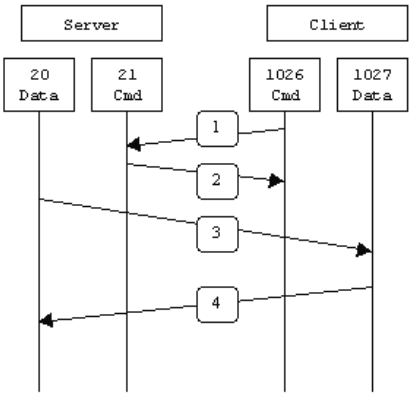
پروتکلFTP یکی از پرکاربردترین پروتکل‌ها در شبکه‌های کامپیوتری می‌باشد. از این پروتکل برای جابه‌جایی فایل بین سیستم ها و از طریق شبکه استفاده می شود. بدلیل اینکه FTP از پروتکلTCP استفاده می کند، دارای قابلیت انتقال مطمئن فایل می باشد. همچنین با تنظیم نام کاربری و کلمه عبور می توان تاحدی امنیت را هم در دسترس داشت.

FTP برای ایجاد کانال کنترلی از پورت TCP 21 سرویس دهنده و ایجاد کانال دیتا از پورت TCP 20 سرویس دهنده استفاده می نماید. پورت کلاینت نیز پورتی تصادفی و بزرگتر از ۱۰۲۴ می باشد.

پروتکل FTP جهت برقراری کانال دیتا دارای دو حالت زیر می باشد:

۱- **حالت فعال (Active FTP)**

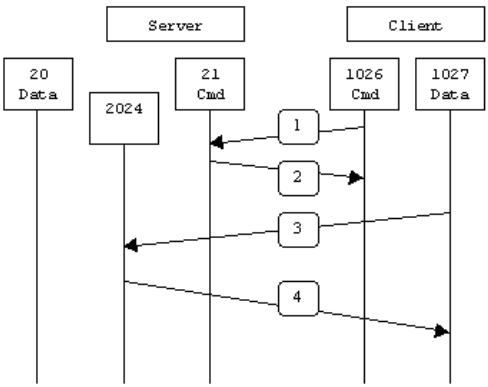
در حالت FTP فعال، ایجاد کانال دیتا از سمت سرویس دهنده شکل می گیرد. به این صورت که ابتدا سرویس گیرنده بر روی پورت ۲۱ یک ارتباط کنترلی با سرویس دهنده برقرار می نماید. پس از آنکه سرویس گیرنده درخواستی را از طریق خط کنترلی برای سرور FTP ارسال کند، سرویس دهنده از طریق پورت ۲۰ خود با یک پورت تصادفی بزرگتر از ۱۰۲۴ بر روی سرویس گیرنده، ارتباط برقرار کرده و اطلاعات مورد نظر را ارسال می نماید.



مراحل کار Active Mode

۲- حالت غیر فعال (Passive FTP)

در حالت FTP غیرفعال، برقراری کانال دیتا از سمت سرویس گیرنده شکل می گیرد. به این صورت که ابتدا سرویس گیرنده از طریق پورت ۲۱ یک کانال کنترلی با سرویس دهنده برقرار می کند و با ارسال دستور PASV درخواست برقراری سرویس Passive FTP می نماید. سپس سرویس دهنده، یک پورت تصادفی بزرگتر از ۱۰۲۴ را جهت ایجاد کانال دیتا انتخاب نموده و به اطلاع سرویس گیرنده می رساند. در نهایت سرویس گیرنده از طریق پورت معرفی شده، یک کانال دیتا با سرویس دهنده برقرار نموده و اقدام به جا به جایی اطلاعات می نماید.



مراحل کار Passive Mode

پروتکل انتقال ساده فایل (TFTP)

پروتکل انتقال ساده فایل(Trivial File Transfer Protocol)، جهت انتقال فایل به روش ساده ولی نامطمئن توسط RFC 1350 منتشر گردیده است.

با توجه به اینکه پروتکلTFTP ازUDP استفاده می‌کند، انتقال فایل توسط این پروتکل بصورت نامطمئن انجام می شود. هرچند درTFTP بر خلافFTP از اطمینان در صحت عملکرد انتقال فایل خبری نیست ولی از نظر سرعت انتقال، TFTP سریعتر از همتای قابل اطمینان خود عمل می کند.

پروتکل TFTP از پورت UDP 69 استفاده می نماید. همچنین این پروتکل قابلیت پشتیبانی از نام کاربری و کلمه عبور را نیز در اختیار ندارد.

پروتکل زمان شبکه (NTP)

پروتکل زمان شبکه(Network Time Protocol)، توسطRFC 1305 تعریف گشته و وظیفه هماهنگ سازی زمان بین تجهیزات موجود در شبکه را بر عهده دارد.

در مواقعی که زمان از اهمیت بالایی برخوردار است، NTP می تواند نقش بسیار مهمی جهت هماهنگ سازی ساعت در مناطق مختلف و بوسیله یک سرورNTP را انجام دهد.

ثبت دقیق رویدادها، اعمال سیاست های شبکه در زمان مشخص، تهیه نسخه پشتیبان[1] و یا استفاده از یک نسخه پشتیبان بر اساس زمان مورد نظر، از جمله مواردی هستند که یکپارچگی زمان نقش مهمی در اجرای درست آنها دارد.

پروتکل NTP برای انجام عملیات خود از پورت UDP 123، استفاده می نماید.

پروتکل ICMP

پروتکل پیام کنترل اینترنت(Internet Control Message Protocol) یا پیام های کنترل شبکه که تحت RFC 792 منتشر گردیده، شامل پیام هایی می باشد که در جهت کنترل و اشکال یابی[2] منابع مختلف شبکه مورد استفاده قرار می گیرند.

پروتکلICMP جزء پروتکل های اصلیTCP/IP بوده و در لایه سوم این مدل مورد استفاده قرار می گیرد. این پروتکل شامل انواع مختلف پیام برای انجام وظایف کنترلی و اشکال یابی می‌باشد که از جمله می توان به موارد زیر اشاره نمود:

---

[1] Backup
[2] Troubleshooting

- پیام Echo Request، جهت بررسی در دسترس بودن رابط شبکه
- پیام Echo Reply، جواب بررسی در دسترس بودن رابط شبکه
- پیام Destination Unreachable، به معنی در دسترس نبودن مقصد
- پیام Time Exceeded، اعلام اتمام عمر بسته[1]

پروتکل TCP/IP دارای ۲ دستور اصلی به شرح زیر می باشد:

۱- دستور Ping

دستور ping دارای پارامترهای متعدد و کارایی‌های متفاوت می باشد. ولی متداول ترین استفاده از این دستور جهت بررسی در دسترس بودن منابع شبکه می باشد.

به عنوان مثال جهت بررسی در دسترس بودن رابط شبکه از طریق سیستم عامل ویندوز می توانیم به یکی از دو صورت زیر عمل کنیم:

با استفاده از آدرس IP

C:\ping 192.168.12.1

و یا بر اساس نام میزبان

C:\ping Microsoft.com

خروجی دستور Ping ممکن است بصورت زیر باشد:

```
C:\>ping 192.168.200.1

Pinging 192.168.200.1 with 32 bytes of data:
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.200.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

برای تغییر پارامترهای پیش فرض دستور ping، می‌توان از سوئیچ ?/ در ویندوز کمک گرفت و یا در تجهیزات سیسکو از حالت Extended بهره برد.

[1] Time To Live (TTL)

```
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t            Ping the specified host until stopped.
                  To see statistics and continue - type Control-Break;
                  To stop - type Control-C.
    -a            Resolve addresses to hostnames.
    -n count      Number of echo requests to send.
    -l size       Send buffer size.
    -f            Set Don't Fragment flag in packet (IPv4-only).
    -i TTL        Time To Live.
    -v TOS        Type Of Service (IPv4-only. This setting has been deprecated
                  and has no effect on the type of service field in the IP Header).
    -r count      Record route for count hops (IPv4-only).
    -s count      Timestamp for count hops (IPv4-only).
    -j host-list  Loose source route along host-list (IPv4-only).
    -k host-list  Strict source route along host-list (IPv4-only).
    -w timeout    Timeout in milliseconds to wait for each reply.
    -R            Use routing header to test reverse route also (IPv6-only).
    -S srcaddr    Source address to use.
    -4            Force using IPv4.
    -6            Force using IPv6.
```

خاطره: ☺

در حال اشکال یابی شبکه یک سازمان بزرگ! بودم، گفتند آقای مهندس فلانی مسئول IT استان فلان، مشکل دارند و از من خواستند که با ایشان تلفنی صحبت کنم!

مهندس فلانی: آقای روغنی من نمی تونم از سرور FTP تهران استفاده کنم.

من: مهندس جان، شما Ping سرور FTP را دارید؟

مهندس فلانی: والا من که خبر ندارم، ولی اگر داشته باشیم هم پیش مدیر مالیمونه!!!

من: 😐 😐 😐

۲- دستور Traceroute

از این دستور جهت ردیابی مسیر ارتباطی، اشکال یابی و پیدا کردن نقطه بروز اشکال در مسیر مورد نظر استفاده می شود.

دستور Traceroute دارای پارامترهایی جهت کارآیی بهتر می باشد که شبیه دستور ping می توان در ویندوز و تجهیزات سیسکو از آن بهره برد.

برای مثال جهت بررسی مسیر ارتباطی سیستم خود با سایت مایکروسافت بصورت زیر عمل می کنیم:

C:\tracert[1] Microsoft.com

همچنین پروتکل ICMP برای IPv6 نیز توسط RFC 2463 تعریف شده است.

پروتکل IGMP

پروتکل مدیریت گروهی اینترنت(Internet Group Management Protocol)، وظیفه ایجاد گروه های چند پخشی بر روی شبکه را بر عهده دارد. این پروتکل دارای ۳ ورژن بوده که به ترتیب توسط RFC 1112، RFC 2236 و RFC 3376 تعریف شده است.

عملیات IGMP بین کلاینت و روتر محلی چند پخشی انجام می پذیرد. این پروتکل در لایه سوم مدل TCP/IP عمل می نماید.

ازIGMP می توان برای مواردی که امکان استفاده از پیام های چند پخشی وجود دارد(مثل ویدئوی آنلاین و بازی)، در شبکه استفاده نمود. IGMP با ایجاد گروه هایی متشکل از اعضای درخواست کننده یک سرویس مشترک(مثل ویدئوی آنلاین) و ارسال چند پخشی دیتا از یک فرستنده به تمامی اعضای گروه، باعث مدیریت استفاده از منابع شبکه می گردد.

در IPv6، پروتکلMLD[2] وظیفه IGMP را انجام می دهد.

Telnet

پروتکل Telnet که توسط RFC 854 منتشر گردیده، جهت برقراری ترمینال مجازی[3] بین تجهیزات و میزبان‌ها در شبکه مورد استفاده قرار می گیرد.

---

[1] دستور Traceroute در سیستم عامل ویندوز، بصورت tracert نوشته می شود.

[2] Multicast Listener Discovery

[3] Virtual Terminal

پروتکلTelnet بر روی پورتTCP 23 و در لایه چهارم مدلTCP/IP کار می کند. این پروتکل با ایجاد یک ترمینال مجازی، دستورات را بصورت متنی(Text) منتقل می نماید.

پروتکل Telnet برای مدیریت و پیکربندی تجهیزات راه دور، مورد استفاده قرار می گیرد. جهت برقراری اتصال Telnet، می توان کاربر را توسط نام کاربری و کلمه عبور مورد شناسایی قرار داد. این پروتکل توسط تمامی سیستم عامل‌ها و تجهیزات مدیریتی شبکه پشتیبانی می گردد.

Rlogin

پروتکلRemote Login برنامه‌ایست تحت سیستم عامل یونیکس که توسط RFC 1282 جهت دسترسی راه دور به تجهیزات شبکه، منتشر گردیده است.

پروتکلRlogin جهت برقراری اتصال از پورت TCP 513 استفاده می کند. این پروتکل وظایف و عملکردی شبیه به پروتکل Telnet دارد، با این تفاوت که نحوه تشخیص هویت کاربر در این دو پروتکل متفاوت است.

در Rlogin زمانیکه کاربر قصد اتصال به یک دستگاه دیگر را دارد، نام کاربری را همان نام کاربر سیستم مبدا که قصد برقراری ارتباط دارد در نظر گرفته شده و فقط کلمه عبور از کاربر پرسیده می شود. همچنین می توان با پیکربندی Rlogin، بدون نیاز به کلمه عبور، به کاربر مورد نظر اجازه برقراری اتصال داد.

هرچندRlogin بر اساس سیستم عامل یونیکس ایجاد گردیده، اما نرم افزارهایی جهت اجرای این پروتکل بر روی سیستم عامل ویندوز ارائه گردیده است.

حداکثر واحد انتقال (MTU)

حداکثر واحد انتقال (Maximum Transfer Unit)، مشخص کننده حداکثر سایز قابل قبول جهت اندازه بسته دیتای ارسالی می باشد.

در سیستم های ارتباطی با توجه به بستر شبکه و خطوط مخابراتی استفاده شده، بسته های دیتا باید دارای سایزی متناسب جهت امکان انتقال، باشند. حداکثر سایز یک بسته را با MTU نمایش می دهند.

☑ مبحث دوم

اصطلاحات و نرم افزارها

رابط خط فرمان (CLI)

رابط خط فرمان (Command Line Interface) راهی برای تعامل انسان با ماشین می باشد. این رابط که بصورت متنی و بدون هیچ ابزار گرافیکی می‌باشد، درخواست‌های کاربر را بصورت دستورهایی با پارامترهای مشخص دریافت کرده و اطلاعات خروجی را نیز بصورت متن ساده نمایش می دهد.

سیستم عامل هایی مثل DOS و Unix صرفا توسط رابط خط فرمان با کاربر در تماس بودند. البته سیستم عامل های جدیدتر و دارای رابط گرافیکی[1] مثل ویندوز و لینوکس نیز همچنان از CLI برای اجرای برخی از دستورات پیشرفته‌تر خود استفاده می کنند.

به دلیل آنکه CLI از محیط گرافیکی استفاده نمی کند، برای اجرای دستورات از منابع کمتری در شبکه استفاده نموده و دارای سرعت عمل به مراتب بیشتری نسبت به رابط گرافیکی می باشد.

هر مقدار که رابطCLI برای کاربران معمولی نامأنوس و خسته کننده است، به همان اندازه برای کاربران حرفه‌ای خوشایندتر و پرکاربردتر می باشد.

TCPdump

نرم افزاری تحت Unix، جهت آنالیز ترافیک شبکه و بر اساس خط فرمان می باشد. این نرم افزار قابلیت مانیتور کردن دیتای ورودی و خروجی به یک رابط شبکه را دارد.

نرم افزار TCPdump قابلیت نمایش دیتا را بر اساس پروتکل، پورت، آدرس IP و مدت زمان جابه‌جایی دارد. همچنین این نرم افزار دارای دستوراتی جهت سفارشی کردن خروجی و ذخیره آن بصورت فایل متنی می باشد. این نرم افزار می تواند کمک خوبی برای کارشناسان جهت اشکال‌یابی در شبکه باشد. این نرم افزار معمولا بر روی برخی تجهیزات شبکه که سیستم عامل آنها بر پایه یونیکس می باشد در دسترس است.[2]

---

[1] Graphic User Interface (GUI)

[2] http://www.tcpdump.org

مدارهای مجتمع با کاربرد خاص (ASIC)

مدارهای مجتمع با کاربرد خاص (Application–Specific Integrated Circuit) که به اختصار ASIC[1] نامیده می شود، مدارهای مجتمعی هستند که برای انجام عملیات خاصی طراحی و بهینه سازی شده اند.

این ICها برای کاربردهای همه جانبه در نظر گرفته نشده و فقط برای انجام عملیات خاصی طراحی و مورد استفاده قرار می گیرند. این نوع طراحی باعث بهینه سازی استفاده از منابع تجهیزات، ضمن ارتقاء کارایی و صرفه جویی در هزینه می گردد.

از ASICها بطور گسترده‌ای در سوئیچ و روترها برای عملیات سوئیچینگ و مسیریابی استفاده می گردد.

Wireshark

Wireshark نرم افزاری متن باز، جهت آنالیز ترافیک شبکه می باشد. این نرم افزار در هر دوحالت خط فرمان و رابط گرافیکی اجرا شده و قابلیت هایی شبیه TCPdump دارد، با این تفاوت که Wireshark علاوه بر اجرا در محیط سیستم عامل های Unix و Linux، دارای نسخه قابل اجرا بر روی سیستم عامل ویندوز نیز می باشد.

نسخه های مختلف Wireshark برای سیستم عامل های مختلف و همچنین متن کد این نرم افزار در آدرس http://www.wireshark.org، قابل دریافت می باشد.

بهترین شیوه (Best Practice)

بهترین شیوه(Best Practice)، روش یا تکنیکی است که بهترین روال انجام یک کار خاص را توصیف می نماید.

تجربه موفق انجام یک کار خاص که توسط گروه های مختلف و در محیط های متنوع برای رسیدن به مطلوب ترین نتیجه، بارها انجام گرفته و امتحان شده، به عنوان Best Practice معرفی می گردد.

Best Practice بهترین شیوه حفظ کیفیت در اجرا و استفاده از محصولات بوده که می تواند جایگزین مناسبی برای وضع استانداردهای اجباری باشد. به عبارت دیگر Best Practice را می‌توان استاندارد و معیار استفاده از تجهیزات و پروتکل ها در شرایط خاص دانست.

---

[1] به اختصار اِی سیک /ˈeɪsɪk/ ASIC تلفظ می گردد.

معمولا شرکت های بزرگ تولید کننده تجهیزات شبکه، بهترین شیوه های اجرایی طرح های مختلف را تحت عنوان Best Practice در اختیار کاربران محصولات خود قرار می دهند. البته ممکن است با توجه به خواسته ها و وضعیت موجود شرکت شما، نیاز یا توان اجرای دقیق طرح مورد نظر امکانپذیر نباشد، ولی Best Practice می تواند برای مهندسین شبکه در این شرایط هم مبنای انجام یک کار موفق قرار گیرد.

کتابخانه زیرساخت فناوری اطلاعات (ITIL)

کتابخانه‌زیرساخت‌فناوری‌اطلاعات(Information Technology Infrastructure Library)، استانداردی غیررسمی شامل طیف گسترده‌ای از Best Practiceهای مدیریت صنعت IT بوده که جهت تسهیل کسب و کار، ایجاد تحول و رشد در زمینه IT مورد استفاده قرار می گیرد.

خاستگاه اولیهITIL کشور انگلیس بوده و برای مدیریت خدمات IT ادارات دولتی در این کشور بنیان گذاری گردید. اما این مجموعه به دلیل قابلیت های خوب اجرایی خیلی سریع توانست مورد استفاده اکثر کشورهای جهان، از جمله ایران نیز قرار گیرد. همچنین ITIL، سه مدرک بین المللی برای دانش آموختگان دوره های تخصصی ITIL پس از کسب موفقیت در آزمون ارائه می نماید.

از مزایای استفاده ITIL، می توان به موارد زیر اشاره کرد:

- بهبود خدمات فناوری اطلاعات
- کاهش هزینه
- رضایت مشتری از طریق روش های حرفه ای تر ارائه خدمات
- بهبود بهره وری
- استفاده بهتر از مهارت ها و تجربه ها
- بهبود ارائه خدمات شخص ثالث[1]

مجموعه ITIL با جزئیات کامل در پنج بخش اصلی، جهت ارائه رویکرد سیستماتیک و حرفه ای برای مدیریت خدمات فناوری اطلاعات در جهت قادر ساختن سازمان برای ارائه خدماتی مناسب، مداوم و مورد اطمینان، بصورت زیر منتشر گردیده است:

۱- استراتژی خدمات (Service Strategy)

۲- طراحی خدمات (Service Design)

[1] Third Party Service

۳- تغییر خدمات (Service Transition)

۴- بهره برداری خدمات (Service Operation)

۵- بهبود مستمر خدمات (Continual Service Improvement)

بخشهای تشکیل دهنده ITIL

تا کنون ITIL در سه ورژن ارائه گردیده است. شما می توانید برای آشنایی کامل با ITILv3 از آدرس http://www.itil-officialsite.com، استفاده نمایید.

بخش دوم

سخت افزار شبکه

فصل چهارم

شبکه‌های محلی

- ☑ مبحث اول: شبکه محلی
- ☑ مبحث دوم: شبکه محلی مجازی
- ☑ مبحث سوم: پروتکل درخت پوشا
- ☑ مبحث چهارم: Inter-VLAN Routing

☑ مبحث اول

شبکه محلی

معمول ترین نوع شبکه که در دسترس ترین نوع آن نیز می‌باشد، شبکه‌های محلی (Local Area Network) یا LAN می‌باشند. شبکه‌های محلی می‌توانند از دو تا صدها کامپیوتر تشکیل شده باشند. همچنین شبکه‌های محلی ممکن است شامل تجهیزات دیگری که قابلیت اتصال به شبکه را دارند مانند پرینت سرور، دوربین تحت شبکه[1]، تلفن تحت شبکه[2] و نظایر آن نیز باشند.

شبکه های محلی در شرکت های کوچک که شامل تعداد کمی گره[3] شبکه است براحتی قابل راه اندازی است. بطوریکه با اختصاص دستی چند آدرسIP به کارت شبکه سیستم ها و اتصال آنها به یک هاب یا سوئیچ ارزان قیمت، شبکه مورد نظر شکل می گیرد. اما همچنان که تعداد سیستم های متصل به شبکه زیاد تر شده و شبکه نیز گسترده تر می شود، نیاز به داشتن دانش بالاتر و امکانات بیشتر نیز محسوس تر می شود. در ادامه تجهیزات مورد نیاز برای راه اندازی شبکه محلی و نحوه عملکرد آنها معرفی می‌گردند.

هاب (Hub)

شبکه‌های مبتنی بر توپولوژی Star، دارای یک نقطه مرکزی جهت اتصال کلاینت های شبکه می‌باشند. اولین دستگاهی که برای نقطه مرکزی شبکه استفاده شد، تجهیزاتی به نام هاب بودند. هاب در لایه اول مدل OSI کار می کند.

هاب دارای پورتهایی جهت اتصال تجهیزات شبکه می باشد که تعداد پورت ها بر حسب مدل می‌تواند مختلف باشد. برای مثال یک هاب ۱۶ پورت، قابلیت اتصال ۱۶ دستگاه تحت شبکه را بر اساس توپولوژی Star ایجاد می نماید.

هاب دستگاه هوشمندی نبوده و قادر به خواندن اطلاعات فریم‌های دریافتی نمی باشد. لذا پیامی که توسط یک کلاینت به آن می رسد را بر روی تمام پورتهای موجود باز پخش می نماید.

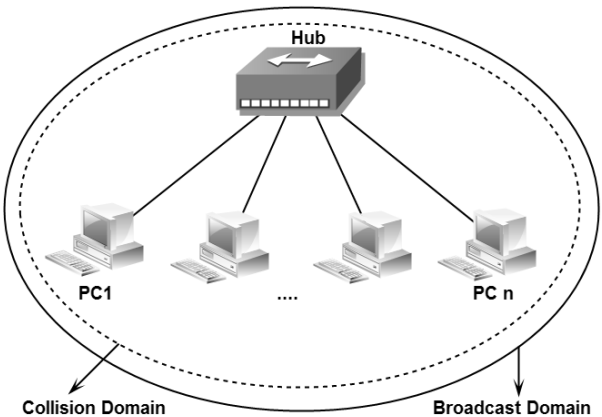
---

[1] IP Camera
[2] IP Phone
[3] Node

پس از آنکه پیام توسط تمام کلاینت‌های متصل به هاب دریافت گردید، کلاینت‌ها آدرس MAC مقصد فریم دریافتی را با آدرسMAC خود مقایسه می نمایند. در صورتیکه آدرس MAC کلاینت و مقصد فریم یکسان باشد، کلاینت پیام را مربوط به خود دانسته و آنرا دریافت می نماید و در غیر اینصورت پیام را دور می اندازد.

دستگاه هایی که به هاب متصل می شوند عضو یک حوزه تصادم (Collision Domain) یکسان هستند. یعنی هر برخوردی که بین فریم های دو دستگاه موجود در یک Collision Domain بوجود می آید، بر روی ارسال دیتای تمام تجهیزات آن حوزه اثر گذار خواهد بود.

همچنین دستگاه های متصل به هاب عضو یک حوزه پخش همگانی (Broadcast Domain) یکسان نیز هستند. به این معنی که پیام Broadcastای که توسط یک دستگاه در یک Broadcast Domain ارسال می گردد، توسط تمام تجهیزات موجود در آن حوزه قابل دریافت می باشد.



استفاده از هاب مشکلاتی نظیر: تصادم در شبکه، سرعت کم مبادلات دیتا و امنیت بسیار پایین را ایجاد می نماید. به همین دلیل استفاده از هاب تقریبا منسوخ شده و امروزه کمتر تجهیزاتی را در بازار می توان یافت که خصوصیت عملکردی آن شبیه هاب باشد.

پُل (Bridge)

پل سخت افزاری است در لایه دوم مدل OSI که در جهت گسترش شبکه و یا برای اتصال دو شبکه به یکدیگر مورد استفاده قرار می گیرد.

پل ها عملیات تقویت سیگنالها را مثل تکرار کننده ها انجام داده و فارغ از پروتکل استفاده شده در لایه دو، اقدام به انتقال اطلاعات می نمایند. به همین دلیل می توان برای اتصال دو شبکه که دارای پروتکل های مختلفی در لایه دوم هستند نیز از پل بهره برد.

پل باعث مجزا شدن حوزه برخورد (Collision Domain) دو شبکه ای که به یکدیگر متصل کرده، شده ولی شبکه ها عضو یک حوزه پخش همگانی (Broadcast Domain) یکسان خواهند بود. هر چند که حوزه پخش همگانی بین دو شبکه متصل شده توسط Bridge یکسان می باشد ولی پل از انتقال دیتایی که مربوط به سگمنت دیگر نباشد جلوگیری به عمل می آورد.

پل دارای جدولی به نام Bridge Table می باشد که حاوی آدرس MAC تجهیزات موجود در شبکه و پورت متناظر Bridge جهت دسترسی به آنها می باشد.

سوئیچ (Switch)

تجهیزات پیشرفته‌تری که در نقطه مرکزی شبکه های Star مورد استفاده قرار می گیرند، سوئیچ ها هستند. سوئیچ نیز همانند هاب دارای پورت هایی جهت اتصال کلاینت های شبکه می‌باشد و تقریبا ظاهری شبیه آن نیز دارند. سوئیچ در لایه دوم مدل OSI کار می کند.

برخلاف هاب، سوئیچ ها تجهیزاتی هوشمند بوده و قابلیت یادگیری نیز دارند. با توجه به اینکه سوئیچ ها می توانند اطلاعات فریم های دریافتی را بخوانند، قادر به یادگیری اطلاعات مربوط به تجهیزات متصل به خود هستند.

سوئیچ دارای جدولی به نام CAM[1] Table می باشد که قادر است آدرس MAC متناظر با تجهیزات متصل شده به هر پورت خود را پس از یادگیری در آن ذخیره کرده و در صورت نیاز، به آن مراجعه نماید.

یادگیری، ثبت و استفاده از جدول CAM Table در سوئیچ ها توسط چهار عمل Learning، Flooding و Filtering and Forwarding انجام می پذیرد.

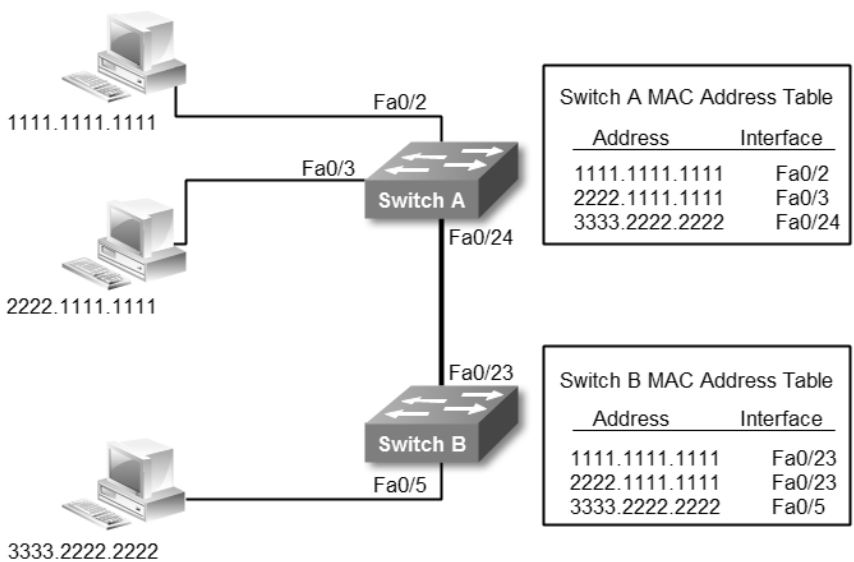
نحوه عملکرد سوئیچ بدین صورت است که ابتدا یک کلاینت دیتای خود را جهت رسیدن به مقصد، تحویل سوئیچ می دهد. سوئیچ با خواندن اطلاعات فریم دریافتی می تواند آدرس MAC مبدا و مقصد فریم را متوجه شود. سوئیچ با توجه به پورتی که اطلاعات را از آن دریافت نموده و خواندن آدرس MAC مبدا فریم، می تواند اطلاعات مربوط به دستگاه ارسال کننده را یاد گرفته و آنرا در جدول CAM Table موجود بر روی حافظه RAM خود ثبت نماید. این عمل را Learning می گویند.

[1] Content Addressable Memory

حال سوئیچ آدرس دستگاه متصل به یکی از پورتهای خود را یاد گرفته ولی با توجه به اینکه سوئیچ هنوز آدرس MAC مقصد فریم دریافتی را فرا نگرفته است، لذا شبیه هاب عمل کرده و یک پیام با آدرس MAC مقصد فریم دریافتی را بر روی تمام پورت ها بجز پورت ارسال کننده، پخش می نماید که این عمل را Flooding می گویند. در این صورت کامپیوتری که آدرس MAC متناظر را دارد به پیام سوئیچ جواب داده و سوئیچ می تواند آدرس MAC و پورت مورد نظر را در جدول CAM Table خود ذخیره نماید. حالا سوئیچ می تواند براحتی پیام را به آدرس مورد نظر ارسال نماید.

مراحل فوق فقط یکبار به ازاء یادگیری هر آدرس، توسط سوئیچ اجرا می گردد. در صورتیکه آدرس MAC مقصد در حافظه سوئیچ موجود باشد، بدون طی مراحل فوق سوئیچ اقدام به ارسال فریم به پورت مورد نظر نموده که این عمل را Filtering and Forwarding می نامند.

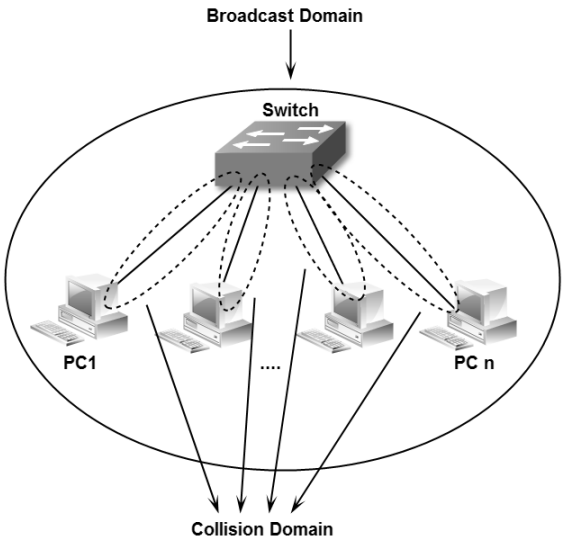
شکل زیر نحوه ثبت آدرس در جدول CAM Table سوئیچ را نشان می دهد.



سوئیچ ها برای جلوگیری از انباشت بیهوده اطلاعات و همچنین جهت بروز نگه داشتن CAM Table خود، در صورت استفاده نکردن از یک رکورد پس از مدت زمان مشخصی که به آن Aging یا سال خوردگی گفته می شود، اقدام به حذف آن آدرس از داخل جدول می نمایند.

با توجه به اینکه جدول CAM Table در حافظه موقتی (RAM) سوئیچ ذخیره می گردد، پس از قطع برق تمام اطلاعات از روی حافظه سوئیچ پاک شده و پس از راه اندازی مجدد، مراحل ثبت رکوردها در جدول باید دوباره انجام پذیرد.

سوئیچ همانند هاب دارای حوزه پخش همگانی(Broadcast Domain) یکسان بوده، ولی درباره حوزه تصادم(Collision Domain) متفاوت از هاب عمل می کند. سوئیچ به ازاء هر دستگاه متصل به خود، یک Collision Domain مستقل ایجاد می کند. محدود شدن Collision Domain بین هر کامپیوتر و پورت سوئیچ، باعث کاهش تصادم و افزایش سرعت انتقال اطلاعات در سوئیچ گردیده است.



روش های سوئیچینگ

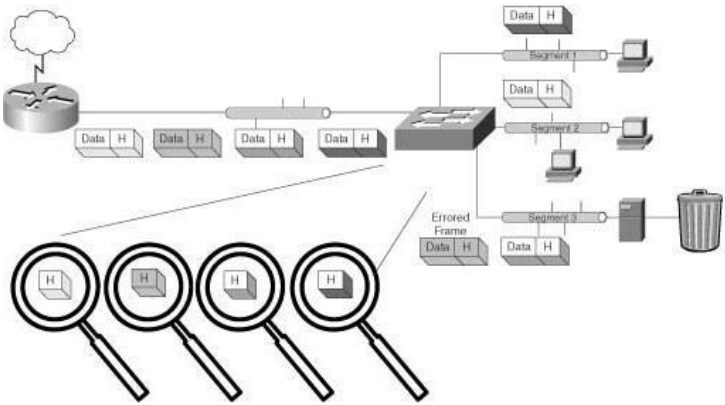
سوئیچ‌ها برای ارسال فریم های دریافتی به مقصد مورد نظر از سه روش مختلف استفاده می‌نمایند:

۱- **Cut-through**

در این روش سوئیچ به محض دریافت۶ بایت اول بسته، آدرس MAC مقصد را در حافظه خود ذخیره کرده و در حین دریافت، اقدام به ارسال فریم به سمت مقصد مورد نظر می نماید.

این روش دارای سرعت بیشتری نسبت به روش های دیگر می باشد ولی امکان بررسی خطای فریم دریافتی را ندارد. سیسکو بهترین نقطه استفاده از این روش را در سوئیچ های واقع در Core شبکه پیشنهاد می نماید.

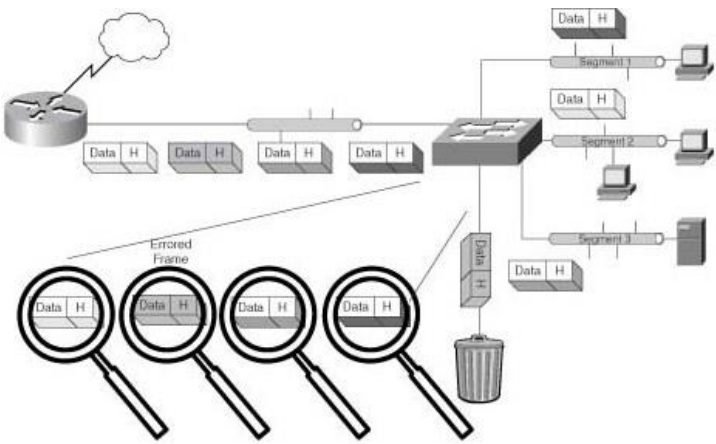
همانطور که در تصویر زیر نشان داده شده است، این روش بدون توجه به خطا فریم ها را به مقصد ارسال کرده و حذف فریم دارای خطا بر عهده دریافت کننده می باشد.



۲- **Store-and-forward**

در این روش سوئیچ ابتدا اقدام به دریافت کامل بسته نموده و پس از چک کردن CRC[1] بسته، در صورتیکه هیچ خطایی مشاهده نگردد، بسته را به مقصد ارسال نموده و در غیر اینصورت بسته را حذف می نماید. سیسکو بهترین نقطه استفاده از این روش در شبکه را استفاده در سوئیچ های Access می داند.

همانطور که در تصویر زیر مشاهده می کنید در این روش فریم های دارای خطا توسط سوئیچ حذف شده و فقط فریم های بدون خطا به مقصد مورد نظر تحویل داده خواهد شد.



[1] Cyclic Redundancy Check

۳- **Fragment-free**

این روش ترکیبی از دو روش Cut-through و Store-and-forward بوده و برای حل مشکل Late-collision ارائه گردیده است.

اجرای عملیات Fragment-free شبیه به Cut-through می باشد با این تفاوت که در این روش قبل از ارسال، سوئیچ اقدام به ذخیره ۶۴ بایت اول بسته می نماید. به دلیل اینکه اغلب اشکالات بسته های دیتا در ۶۴ بایت اول آن قابل تشخیص می باشد، امکان بررسی خطا شبیه روش Store-and-forward نیز در این روش وجود دارد.

انواع پورت سوئیچ

سوئیچ های امروزی بر اساس پروتکل Ethernet کار کرده و دارای پورت هایی با سرعت 10Mb تا 10Gb می‌باشند. علاوه بر سوئیچ هایی با سخت افزار ثابت (Fixed Switches)، سوئیچ های پیشرفته‌تر ماژولار (Modular Switches) که قابلیت پیکربندی سخت افزاری بر اساس نیازهای استفاده کننده را دارند نیز توسط شرکت های تولید کننده، ارائه می گردد.

سوئیچ ها دارای پورتهای فیزیکی مختلفی جهت اتصال تجهیزات به سوئیچ و یا اتصال سوئیچ ها به یکدیگر می باشند که در زیر به توضیح تعدادی از رایج ترین آنها خواهیم پرداخت.

- **پورت RJ45** [1]

رایج ترین پورت فیزیکی مورد استفاده برای پروتکل ایترنت، پورت RJ45 می باشد. این پورت شبیه پورتهای تلفن ولی بزرگتر و دارای تعداد کانکتور بیشتری می باشد. این پورت برای اتصال کلاینت ها توسط انواع کابل های مسی زوج به هم تابیده به سوئیچ مورد استفاده قرار می گیرد.

- **پورت SFP** [2]

جهت اتصال کابل‌های فیبر نوری به سوئیچ از پورتهای SFP استفاده می گردد. کابل‌های فیبر نوری دارای کانکتور مخصوص جهت اتصال به پورتهای SFP می باشند. ماژول های SFP مورد استفاده برای مسافت های مختلف، از لحاظ فیزیکی شبیه هم ولی از لحاظ مدل و کارایی متفاوت می باشند.

---

[1] Registered Jack
[2] Small Form-Factor Pluggable

- **پورت Stack**

از این پورت جهت اتصال سوئیچ ها به یکدیگر و یکپارچه سازی آنها استفاده می کنند. به عنوان مثال اگر دو سوئیچ ۱۲ پورت با قابلیت Stack داشته باشید می توانید با اتصال این دو سوئیچ از طریق پورت Stack به یکدیگر، یک سوئیچ منطقی[1] یکپارچه ۲۴ پورتی داشته باشید.

توجه داشته باشید که برای استفاده از این پورت، سوئیچ ها باید در یک محیط فیزیکی نزدیک به هم قرار داشته باشند.

- **پورت Console**

پورت کنسول که از نظر شکل و ابعاد، ظاهری دقیقا شبیه به RJ45 دارد جهت اتصال کابل سریال مخصوص اعمال مدیریتی به سوئیچ مورد استفاده قرار می گیرد. کاربرد این پورت در پیکربندی سوئیچ می باشد.

نکته: لازم به ذکر است کاربرد پورتهای ایترنت، SFP و کنسول صرفا در سوئیچ ها نبوده، بلکه دیگر تجهیزات شبکه از جمله مودم ها، روتر ها و فایروالها نیز نسبت به مدل و مورد استفاده، از این پورت ها بهره می برند.

انواع استاندارد Ethernet

همانطور که گفتیم، ایترنت گسترده ترین پروتکل مورد استفاده سوئیچ ها در شبکه های محلی می باشد. این پروتکل در لایه اول مدل TCP/IP و در لایه اول و دوم مدل OSI کار می کند. استاندارد ایترنت توسط گروه کاری802.3 در سازمان IEEE گسترش یافته است. این گروه استاندارد ایترنت و پروتکل‌های وابسته را در قالب استانداردهای زیر مجموعه IEEE 802.3x ارائه نموده است. پر استفاده ترین این پروتکل ها در زیر آمده است.

- **Ethernet**

در استاندارد IEEE802.3i تعریف گشته و دارای سرعت 10Mbps[2] می باشد. این پروتکل از پورت فیزیکی RJ45 و کابل مسی زوج به هم تابیده جهت برقراری ارتباط استفاده می کند.

---

[1] Logical
[2] Megabit per second (Mbps)

- **Fast Ethernet**

توسط استانداردIEEE 802.3u توسعه یافته و از سرعت‌هایMbps 10/100 پشتیبانی می نماید. این پروتکل نیز از کابل مسی و RJ45 جهت ارتباطات فیزیکی خود استفاده می نماید.

- **Gigabit Ethernet**

برای پشتیبانی از سرعت 1000Mbps یا به عبارتی دیگر 1Gbps تعریف گردیده است. این پروتکل امکان اجرا بر روی هر دو نوع کابل مسی و فیبر نوری را دارد. استاندارد IEEE802.3ab برای سرعت 1Gbps بر روی بستر کابل مسی و استاندارد IEEE802.3z برای سرعت 1Gbps بر روی بستر فیبر نوری ارائه گردیده است.

- **10 Gigabit Ethernet**

پروتکل 10Gig توسط استاندارد IEEE802.3ae برای پشتیبانی از سرعت 10Gbps ارائه گردیده است. این پروتکل برای اتصالات فیزیکی خود از کابل فیبر نوری و پورت فیزیکی SFP استفاده می نماید.

در این کتاب جهت آشنایی با موارد عملی در بخش های مورد نیاز، مثالی را از طریق طرح سناریوی مرتبط با موضوع، حل می نماییم. در این قسمت نیز برای آشنایی با عملکرد سوئیچ در یک شبکه محلی کوچک، از سناریو زیر استفاده می کنیم.

سناریو(۱)؛ یک شبکه محلی کوچک

طرح مسئله:

شما به عنوان کارشناس، مسئول راه اندازی شبکه یک آژانس هواپیمایی هستید. این آژانس هواپیمایی دارای ۱۶ کامپیوتر، یک سرور جهت برنامه رزرو بلیط و یک مودم ADSL جهت اتصال به اینترنت می باشد. آژانس از شما برای برقراری ارتباط بین کامپیوترها و امکان استفاده آنها از اینترنت از شما کمک می خواهد.

نیاز سنجی:

ابتدا شما نیاز به برپایی شبکه از نظر فیزیکی دارید. کامپیوتر ها باید دارای کارت رابط شبکه باشند، که بطور معمول بر روی مادربرد بصورت Onboard وجود دارد.

برای راه اندازی توپولوژیStar نیاز به سوئیچ دارید. برای انتخاب سوئیچ باید تعداد پورت‌ها، سرعت و پهنای باند مورد نیاز را مدنظر قرار دهید. سپس از طریق کابلهای مسیUTP، کامپیوترها را به سوئیچ متصل نمایید.

برای اتصال به اینترنت یک مودمADSL نیز داریم که معمولا این مودم‌ها دارای قابلیت Routing نیز می باشند، لذا برای اتصال کلاینت‌ها به اینترنت همین مودم کفایت می‌کند.

چون شبکه خصوصی است پس می توانیم از رنج آدرس های Private استفاده نماییم. همچنین به دلیل کوچک بودن شبکه نیازی به راه اندازی سرور DHCP نیز نمی باشد.

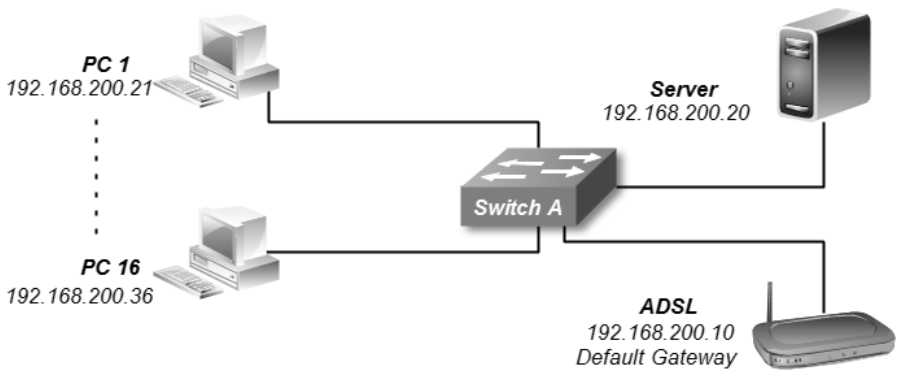
راه حل:

به دلیل اینکه در شبکه‌ای به کوچکی این پروژه، نیازی به راه اندازی سرورDHCP نیست، می‌توان اقدام به تنظیم دستی کارت های شبکه و اختصاص آدرسIP دلخواه از رنج آدرس های Private، نمود.

در اینجا ما از کلاس C آدرس‌های Private و از رنج 192.168.200.0/24 استفاده می کنیم. اگر در فصل دوم مبحث آموزشIP را بخوبی مطالعه کرده باشید، متوجه می شوید که آدرس 192.168.200.0 به عنوان Net ID بوده و 24/ نیز به جای 255.255.255.0 نمایانگر Subnet Mask می باشد. پس ما می توانیم از آدرس 192.168.200.1 تا آدرس 192.168.200.254 را برای اختصاص به کلاینت های شبکه استفاده نماییم. همچنین آخرین آدرس IP، یعنی آدرس

192.168.200.255 نیز قابل اختصاص به کلاینت ها نبوده و به عنوان آدرس Broadcast مورد استفاده قرار می گیرد.

برای اختصاص آدرس Default Gateway به کلاینت‌ها باید از آدرس مودم ADSLتان و برای آدرس DNS نیز از آدرس‌هایی که شرکت خدمات اینترنت در اختیار شما قرار داده، استفاده نمایید.



بابت راه اندازی سوئیچ هم هیچ نگرانی به خود راه ندهید. برای راه اندازی سوئیچ در این شبکه، صرفا اتصال به برق و روشن کردن سوئیچ کفایت می کند و نیاز به هیچ پیکربندی دیگری ندارید.

نحوه عملکرد:

با توجه به اینکه در شبکه داخلی سرورDNS نداریم، کلاینت‌ها جهت دسترسی به سرور و کامپیوترهای دیگر باید از آدرس های IP استفاده نمایند. کامپیوترها برای اینکه بتوانند با یکدیگر از طریق سوئیچ ارتباط داشته باشند، باید آدرسMAC کامپیوتر مقصد خود را بدانند. در اینجاست که کامپیوترها برای یادگیری آدرسMAC مقصد مورد نظر، از پروتکلARP استفاده می کنند.

کامپیوتر مبدا با ارسال پیامARP، به جستجوی آدرسMAC متناظر با آدرسIP مورد نظر خود می پردازد. سوئیچ پس از دریافت پیام، درخواست را با جدولARP خود مقایسه نموده و در صورت پیدا نکردن متناظر، پیامARP را بصورت پخش همگانی برای تمام تجهیزات متصل به خود ارسال می نماید. کامپیوتر دارای آدرسIP مورد نظر نیز پس از دریافت پیام، آدرسMAC خود را از طریق پروتکلARP، به اطلاع سوئیچ رسانده و سوئیچ نیز آنرا در جدولARP خود ذخیره می نماید. سپس سوئیچ توسط پیامARP آدرسMAC را به اطلاع کلاینت مبدا می رساند.

با توجه به اینکه جدولARP در حافظه موقتی سیستم ها ذخیره می شود، پس از قطع برق یا در صورت راه اندازی مجدد از حافظه پاک خواهد شد. البته لازم به ذکر است که نگهداری جدولARP دارای مدت زمان خاصی می باشد که ممکن است در تجهیزات مختلف، با هم فرق کند. در صورتیکه تا پایان این مدت زمان، کامپیوتر از آدرس موجود در جدول ARP استفاده نکند، آن آدرس از جدول ARP حذف می گردد.

پس از آنکه کامپیوتر مبدا از طریق پروتکلARP، آدرسMAC مقصد را یاد گرفت، با جاسازی آدرس‌های IP وMAC مبدا و مقصد در فریم، آنرا تحویل سوئیچ می دهد.

به دلیل اینکه سوئیچ در لایه دوم مدل OSI کار می کند، برای انتقال فریم ها نیاز به دانستن آدرس‌های MAC تجهیزات متصل به خود را دارد. همانگونه که قبلا توضیح داده شد، سوئیچ دستگاهی با سواد! است که با خواندن فریم‌ها می تواند آدرس های مبدا و مقصد را فراگرفته و در جدول CAM Table خود ذخیره نماید. پورت مربوط به آدرس مبدا که پیام از آن دریافت شده مشخص است، اما برای تشخیص پورت متصل به آدرس مقصد، سوئیچ پیامی حاوی آدرسMAC مقصد را به صورت سیل آسا بر روی تمام پورت های خود ارسال می نماید. پس از دریافت جواب از دستگاه دارای آدرس MAC مورد نظر، سوئیچ آدرسMAC و پورت متناظر را در جدول CAM Table خود ذخیره می نماید. حالا سوئیچ در جدول خود هم پورت متناظر با آدرس مبدا و هم پورت متناظر با آدرس مقصد را دارد.

اما برای استفاده از اینترنت شما دارای سرورDNS نیز هستید. سرورDNS مورد استفاده برای اینترنت می تواند سرورهای مرجع مثل 4.2.2.4 یا سرورهای معرفی شده توسطISP باشند. به هر صورت پس از آنکه شما نام یک وب سایت را در مرورگر خود وارد می نمائید، کامپیوتر نام را برای سرورDNS فرستاده تا از آدرسIP متناظر با آن مطلع گردد. سپس در بسته های دیتا از همان آدرس به عنوان آدرس مقصد استفاده می نماید. اما مطمئنا آدرسIP وب سایت جزء رنج آدرس های عمومی یا Public و متفاوت از آدرس های شبکه داخلی می باشد.

با توجه به اینکه شما آدرسIP مودم را به عنوان Default Gateway بر روی کارت رابط شبکه کامپیوترها تنظیم کرده‌اید، این کارت اطلاعات مربوط به آدرس هایIP که جزء Subnet شبکه موجود نمی باشند را به سمت همان آدرس Default Gateway هدایت می نماید.

به همین راحتی شما یک شبکه محلی کوچک راه اندازی نمودید. حالا با اولین دستمزد کاری شبکه، یک جعبه شیرینی برای خانواده محترم بخرید و برای رسیدن به این موفقیت بزرگ! از ایشان تشکر نمائید.

سناریو(۲)؛ گسترش شبکه محلی

طرح مسئله:

آژانس هواپیمایی مسئله قبل به دلیل کمبود فضا، واحد آپارتمان کناری را هم خریداری کرده و بخش مدیریت و امورمالی خود را به آن مکان انتقال داده است. با توجه به عملکرد خوبتان، مجددا از شما خواسته اند با همان شرایط قبل شبکه را در هر دو واحد گسترش دهید.

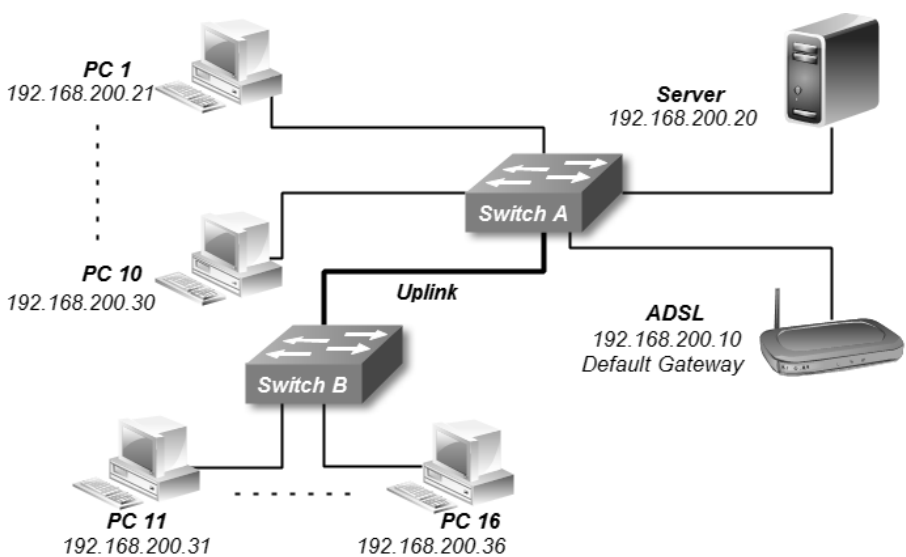
نیاز سنجی:

با توجه به اضافه شدن آپارتمان، نیاز به یک سوئیچ دیگر جهت اتصال کاربران مکان جدید دارید. در ضمن برای یکپارچه شدن شبکه، دو سوئیچ نیز باید به یکدیگر متصل گردند.

با توجه به اینکه قبلا Subnet بزرگی را برای شبکه در نظر گرفته بودید، آدرس IP زیادی برای استفاده دارید. پس مشکلی برای اختصاص IP ندارید.

راه حل:

از توضیح کارهای تکراری صرف نظر می کنیم. برای راه اندازی سوئیچ نیز همچنان نیازی به پیکربندی خاصی نداریم.



برای داشتن شبکه‌ای یکپارچه، سوئیچ‌ها باید به یکدیگر متصل شوند. برخی مدل سوئیچ ها دارای پورتStack می باشند. این پورت باعث می شود هر دو سوئیچ در قالب یک سوئیچ منطقی به نظر آیند. توجه داشته باشید که علاوه بر گرانتر بودن این نوع سوئیچ‌ها، برای استفاده از پورتStack، سوئیچ ها باید از نظر فیزیکی در فاصله کمی از یکدیگر قرار گیرند.

با توجه به اینکه ما می خواهیم سوئیچ دوم را در داخل آپارتمان جدید قرار دهیم پس باید از خاصیت Uplink استفاده نمائیم. بعضی از برندها بر روی سوئیچ های خود دارای پورت مخصوصی به نام Uplink هستند. اما اغلب سوئیچ‌های موجود در بازار قابلیت ارائه خاصیت Uplink را بر روی تمام پورت های خود دارند. به همین دلیل ما پورت های Fa0/1 هر سوئیچ را برای Uplink اختصاص می دهیم.

توجه داشته باشید برای اتصال دو سوئیچ معمولی به یکدیگر باید از کابل Cross استفاده شود. البته سوئیچ‌های جدید اغلب دارای قابلیت تشخیص خودکار نوع کابل[1] بوده و شما را از اجبار در بکار بردن نوع خاص کابل معاف می کنند.

در صورتیکه سوئیچ‌ها دارای پورتSFP باشند، بهتر است از کابل فیبر نوری برای اتصال دو سوئیچ به یکدیگر استفاده نمایید.

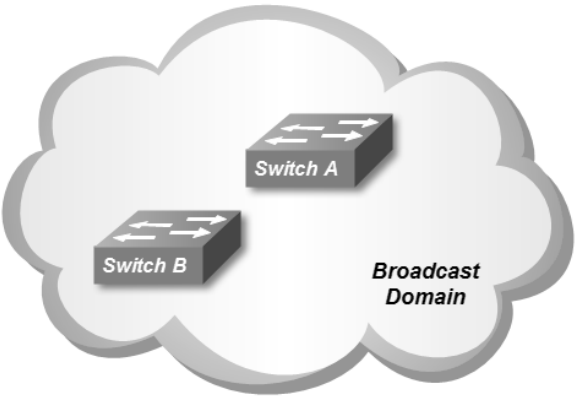
نحوه عملکرد:

نحوه عملکرد هر سوئیچ به طور مجزا و همچنین ارتباط کلاینت هایی که بر روی یک سوئیچ قرار دارند مشابه سناریو اول بوده و همان مراحل نیز برای سوئیچ های A و B در این سناریو نیز رخ می دهد.

در این سناریو با توجه به اینکه شما سوئیچ‌ها را به یکدیگر متصل نموده‌اید، حوزه پخش همگانی (Broadcast Domain) را گسترش داده‌اید. هر دو سوئیچ دارای یک Broadcast Domain یکسان بوده و Collision Domain نیز مثل قبل به ازاء هر کلاینت و پورت سوئیچ برقرار می گردد.

با توجه به اینکه ما حوزه Broadcast را افزایش داده و ارتباطات همچنان در لایه دوم مدل OSI می باشد، اگر کلاینت متصل به سوئیچ A بخواهد با کلاینت متصل به سوئیچ B ارتباط برقرار کند، نیازمند به دانستن آدرس MAC مقصد است. اما به نظر شما با توجه به اینکه هر سوئیچ دارای CAM Table مخصوص به خود است، نحوه به دست آوردن آدرس MAC مقصد چگونه خواهد بود؟

[1] Auto MDI/MDIX



به عنوان مثال فرض کنید کلاینت متصل به سوئیچB قصد ارسال اطلاعات برای سرور متصل به سوئیچ A را دارد. کلاینت با داشتن آدرسIP سرور، با کمک پروتکلARP، آدرس MAC سرور را نیز به دست می آورد. سپس با گنجاندن آدرسMAC سرور به عنوان آدرسMAC مقصد، فریم را تحویل سوئیچ B می دهد.

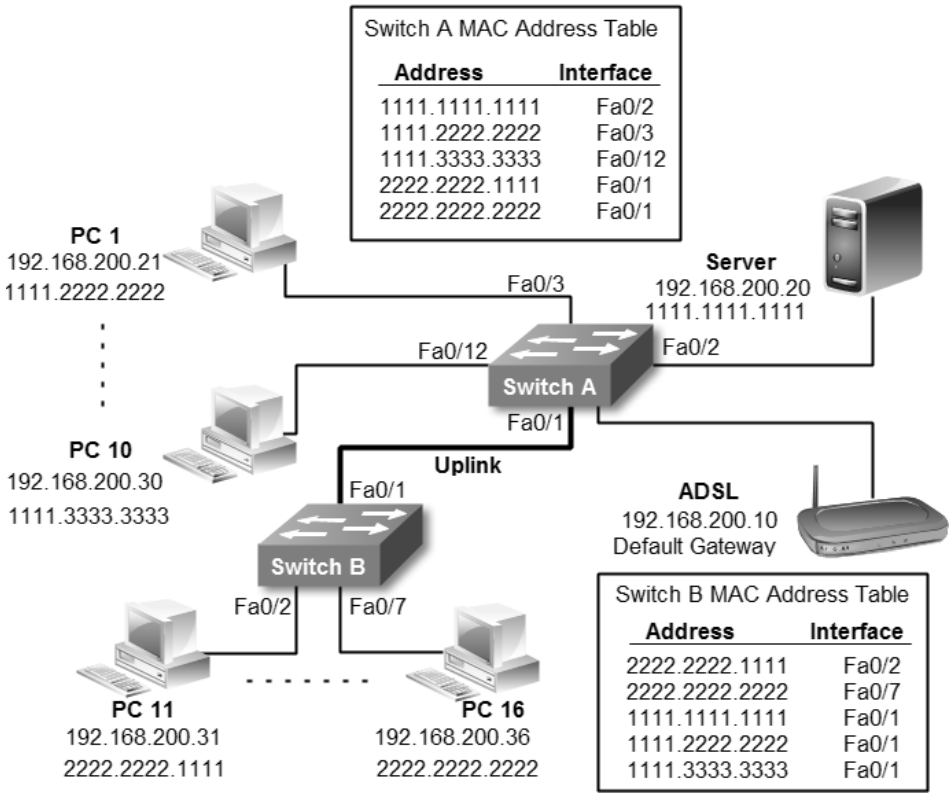
سوئیچ B با توجه به اینکه از پورت متصل به آدرسMAC مقصد فریم اطلاعی ندارد با ارسال پیام به روش Flooding اقدام به پیدا کردن پورت متصل به آدرس MAC مقصد می نماید.

چون هر دو سوئیچ بصورت معمولی به هم متصل شده و عضو یک Broadcast Domain یکسان هستند، پیام Flooding ارسالی سوئیچ B، توسط پورت Fa0/1 متصل به سوئیچ A، در سوئیچ A نیز پخش شده و به سرور مورد نظر می رسد.

سرور پیامAcknowledgment خود را از طریق همان پورت Fa0/1 به اطلاع سوئیچ B می‌رساند. به دلیل اینکه سوئیچ B پیام را از طریق پورت Fa0/1 خود دریافت کرده، در جدول CAM Table خود، پورت متناظر با آدرس MAC سرور را همان پورت Fa0/1 درج کرده و از این پس پیامهایی که آدرس MAC مقصدشان، آدرسMAC سرور است را تحویل پورت Fa0/1 می دهد.

پورت Fa0/1 نیز پیام را تحویل سوئیچ A داده تا سوئیچ A وظیفه رساندن پیام به پورت مقصد را انجام دهد.

پس در صورتیکه شما جدول CAM Table سوئیچ B را ببینید، پورت متناظر تمام کلاینت‌های متصل به سوئیچ A را پورت Fa0/1 مشاهده خواهید نمود. بالطبع این اتفاق در سوئیچ A نیز برای کلاینت های متصل به سوئیچ B رخ خواهد داد.



همانطور که در تصویر فوق ملاحظه می نمائید سوئیچA آدرسMAC کلاینت‌های متصل به سوئیچ B را بر روی پورت Fa0/1 خود نمایش داده و همینطور سوئیچ B نیز آدرس MAC کلاینت‌های متصل به سوئیچA را بر روی پورتFa0/1 خود که متصل به سوئیچA می باشد نمایش می دهد.

☑مبحث دوم

شبکه محلی مجازی (VLAN)

در مبحث قبل برای راه اندازی یک شبکه محلی، به راحتی کامپیوترها را به سوئیچ متصل کرده و با تنظیم آدرسIP، اقدام به برقراری ارتباط بین کامپیوترها نمودیم. خوب این بهترین کاری بود که می توانستیم برای راه اندازی یک شبکه کوچک انجام دهیم. ولی اگر شبکه بزرگتر و دارای تعداد کلاینت بیشتر بود چه کاری باید انجام دهیم؟

همانطور که قبلا گفتیم، کامپیوترها برای انجام بسیاری از کارهای خود ممکن است از طریق ارسال پیام‌های پخش همگانی (Broadcast) اقدام نمایند. حال اگر تعداد کامپیوترها زیاد باشد، این همه پیام Broadcast چه بلایی ممکن است بر سر شبکه بیاورد؟ این تعداد پیام Broadcast می تواند باعث اتلاف منابع شبکه گردد و از آن بدتر تصادم هایی هستند که به دلیل کثرت این پیام ها در شبکه بوجود می آید. پس از هر تصادم، سیستمها موظفند که مجددا پیام خود را ایجاد و منتشر کنند. حال اگر به دلیل تعداد زیاد کلاینت و پیام های Broadcast، تصادم های پی در پی بوجود بیایند، این شبکه عملا از کار افتاده و غیرقابل استفاده می شود.

یکی دیگر از ایرادات این نوع شبکه، کمبود امنیت می باشد. به دلیل اینکه تمام کامپیوتر ها در یک Subnet و Broadcast Domain هستند، دسترسی کامپیوترها به یکدیگر به راحتی امکان پذیر است. به عنوان مثال شما دارای دو بخش مالی و امور اداری در سازمان خود هستید. اگر وضعیت شبکه به همین منوال باشد کاربران می توانند به منابع اشتراک گذاشته بخش های دیگر دسترسی پیدا کنند.

البته در ساده ترین حالت و بدون نیاز به دانش فنی بالا، دسترسی به فایلهای اشتراک گذاشته برای همه امکان پذیر است و در حالت بدتر اگر کاربر باهوش و شیطانی در شبکه داشته باشید براحتی امکان هک دستگاه های قسمت های مهم سازمان را در اختیارش قرار داده‌اید.

برای حل این مشکلات چه راه حلی به نظر شما می آید؟ شاید بگویید برای هر بخش از سوئیچ های مجزا استفاده کنیم. ولی آیا این راه حل بهترین راه حل است؟

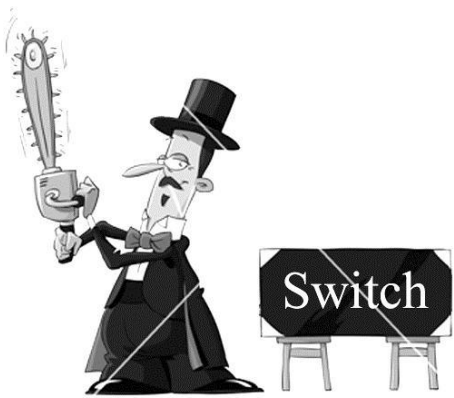
مثلا اگر اتاق اصلی امور مالی سازمان شما در طبقه سوم باشد ولی دو نفر از کارمندان مالی برای نظارت بر انبار در زیر زمین ساختمان مستقر شده باشند، چه کاری انجام می دهید؟

اگر در یک طبقه فقط ۱۵ کارمند داشته باشید که این کارمندها عضو ۳ بخش مختلف سازمان هستند، و برای هر گروه یک سوئیچ استفاده کنید، با پورتهای زیاد باقیمانده، هزینه خرید سوئیچ‌ها و هزینه نگهداری آنها از جمله هزینه برق و Cooling چه می کنید؟

در صورت جدا بودن سوئیچ ها برای به اشتراک گذاشتن منابع عمومی مثل اینترنت و یا پورتال سازمانی چه راه حلی دارید؟ و از همه مهمتر برای مدیریت این شبکه جزیره‌ای و منقطع، چه به روز مسئول شبکه بیچاره خواهدآمد؟

حالا که اشکتان در آمد باید بگویم همان راه حل شما بهترین راه حل است! یعنی استفاده از سوئیچ‌های مجزا برای هر بخش یا گروهی از کارمندان سازمان. البته نه سوئیچ فیزیکی مجزا، بلکه سوئیچ منطقی مجزا!!!

سوئیچ منطقی چیست؟ و چگونه بوجود می‌آید؟ برای ایجاد سوئیچ منطقی مجزا از ویژگی شبکه محلی مجازی (Virtual LAN) که به اختصار VLAN نامیده می شود، استفاده می کنیم. ایجاد شبکه محلی مجازی بر روی سوئیچ، مثل این است که بوسیله اره آهن بر! یک سوئیچ را به چند قسمت مجزا تقسیم کرده باشیم.



شبکه محلی مجازی، باعث تقسیم یک سوئیچ فیزیکی به تعدادی سوئیچ منطقی می گردد. هر سوئیچ منطقی دارای Broadcast Domain مخصوص به خود بوده و همچنین دارای جدول CAM Table مستقل نیز می باشد.

روش های عضوپذیری VLAN

نحوه عضوپذیری شبکه های مجازی یا VLANها به دو صورت زیر انجام می پذیرد:

۱- **بر اساس پورت**[1]

متداول ترین نحوه عضویت در یک VLAN، اختصاص پورت فیزیکی سوئیچ به VLAN مورد نظر می باشد.

در این روش پورت سوئیچ به یک VLAN اختصاص داده شده و مبنای عضویت دستگاه متصل شده به سوئیچ، تنظیمات انجام شده بر روی پورت مربوطه می باشد.

۲- **بر اساس آدرس MAC**

روش دیگر عضویت درVLANها، عضویت بر اساس آدرسMAC کلاینت‌ها می باشد. این روش به دلیل سربار مدیریتی و دشواری اشکال یابی به ندرت مورد استفاده قرار می گیرد.

در این حالت فارغ از اینکه کلاینت از نظر فیزیکی در کجا قرار گرفته و به پورت چه سوئیچی متصل است، بر اساس آدرسMAC درVLAN مربوطه قرار می گیرد.

سیسکو در تجهیزات خود از ویژگیVMPS[2] برای اجرای VLANهای مبتنی بر آدرس MAC پشتیبانی نموده است. در این حالت باید یک سوئیچ را به عنوان VPMS Server قرار داد تا اطلاعات مربوط به آدرس های MAC و VLANهای متناظر را در خود نگهداری نماید. با استفاده از این ویژگی حتی در صورت جابجایی کلاینت و اتصال به یک سوئیچ دیگر، براحتی در VLAN خود قرار می گیرد.

VLAN Database

با ایجاد VLAN و اختصاص پورت های فیزیکی مورد نظر به هر VLAN، می توانید سوئیچ های منطقی مجزا با تعداد پورت‌های دلخواه به وجود آورید. اطلاعات مربوط به VLANها در جدولی به نام VLAN Database بر روی سوئیچ ذخیره می شود. این فایل در سوئیچ سیسکو با نام Vlan.dat و بر روی حافظه Flash قرار دارد.

این فایل حاوی جدولی با فیلدهای شماره ، نام و پورتهای اختصاص داده شده به VLANها می باشد. هر سوئیچ دارای جدول VLAN Database مخصوص به خود می باشد که بر روی حافظه دائمی ذخیره شده و با راه اندازی مجدد سوئیچ از بین نمی رود.

---

[1] Port-Based VLAN
[2] VLAN Membership Policy Server

انواع VLAN

- **Local VLAN**

در صورتی که گستره VLAN فقط محدود به یک سوئیچ فیزیکی باشد و تمام کلاینت های آن نیز به همان سوئیچ متصل باشند، آنرا Local VLAN می نامند.

- **End-to-End VLAN**

یک سوئیچ مجازی می تواند بر روی چندین سوئیچ فیزیکی پخش شده و بر روی سوئیچ های مختلف دارای کلاینت باشد. به این نوع VLANها، End-to-End VLAN گفته می شود.

اتصال Trunk

اگر تمام کلاینت‌های مربوط به یک VLAN بر روی یک سوئیچ فیزیکی باشند، برای ارتباط با یکدیگر مشکلی نخواهند داشت. ولی اگر کلاینت‌های یک شبکه مجازی بر روی چند سوئیچ پراکنده باشند، برای ارتباط بین کلاینت‌ها چه چاره‌ای باید اندیشید؟

با توجه به اینکه پروتکل ایترنت امکان مشخص نمودن VLAN ID را ندارد، در صورتیکه یک VLAN بر روی سوئیچ های مختلف گسترده باشد، باید اطلاعات مربوط به هر VLAN را توسط پروتکل دیگری مشخص نمود تا جریان انتقال اطلاعات در مسیر درست خود قرار بگیرد.

سوئیچ برای نشانه گذاری فریم‌ها جهت مشخص نمودن VLAN ID مربوطه، از پروتکل ISL یا IEEE 802.1q استفاده می‌نماید. همانطور که بیان شد، انتقال فریم های نشانه گذاری شده توسط پورتهای معمولی سوئیچ و تحت پروتکل ایترنت امکان پذیر نمی باشد. به همین دلیل از پورت Trunk برای جابجایی دیتای مربوط به VLANهای مختلف در بین سوئیچ ها استفاده می گردد.

به عبارت دیگر پورت Trunk با کمک پروتکل IEEE 802.1q یا ISL، با Tag زدن فریم‌ها، VLAN ID آنها را قبل از خروج از سوئیچ مشخص می نماید. اتصال Trunk نیز هدایت صحیح جریان اطلاعات مربوط به VLANها را بین سوئیچ های مختلف امکان پذیر می سازد.

اتصالات Trunk در لایه دوم مدل OSI کار کرده و در یکی از سه حالت زیر ممکن است وجود داشته باشد:

- **بین دو سوئیچ**

برای جابه جایی اطلاعات مربوط به End-to-End VLAN ها.

- **بین سوئیچ و روتر(مسیریاب)**

برای برقراری ارتباط بین VLANهای مختلف.

- **بین سوئیچ و سرور**

در برخی موارد نیاز است که سرور از طریق یک کارت شبکه با VLANهای مختلف بصورت مستقیم در تماس باشد. در این حالت برای اینکه سرور امکان ارسال و دریافت فریم های دارای Tag مربوط به VLAN را داشته باشد، از اتصال Trunk بین سوئیچ و سرور بهره گرفته می شود.

انواع پروتکل Trunk

اتصالات Trunk در سوئیچ های سیسکو تحت یکی از دو پروتکل زیر کار می کنند.

۱- پروتکل ISL

پروتکل ISL(Inter-Switch Link Protocol) قبل از استاندارد IEEE، توسط سیسکو معرفی گشته و فقط امکان کار بر روی تجهیزات سیسکو را دارد[1].

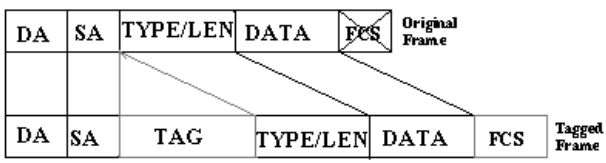
این پروتکل فریم‌های ایترنت را مجددا بسته بندی[2] نموده و در هدر بسته بندی جدید VLAN ID فریم را نیز مشخص می نماید. در این بسته بندی فریم ایترنت اصلی دست نخورده باقی می ماند.

ISL Header	Encapsulation Frame	FCS

۲- پروتکل IEEE 802.1q

پروتکل IEEE 802.1q که آنرا به اختصار dot1q می نامند، پروتکل استانداری است که توسط سازمان IEEE توسعه داده شده و در تمام برندهای تولید کننده تجهیزات شبکه از آن پشتیبانی می شود.

این پروتکل برخلاف ISL اقدام به بسته‌بندی مجدد فریم نکرده و با گنجاندن یک هدر جدید ۴ بایتی در هدر فریم اصلی، VLAN ID مربوطه را نیز مشخص می نماید.



[1] Cisco Proprietary
[2] Encapsulation

پروتکل DTP

پروتکلDTP(Dynamic Trunking Protocol) سوئیچ را قادر می‌سازد تا بصورت اتوماتیک اتصالات Trunk را برقرار نماید. این پروتکل مخصوص سیسکو می باشد.

پروتکلDTP به سوئیچ این امکان را می‌دهد در صورتیکه شرایط برقراری اتصال Trunk با دستگاه مقابل وجود داشته باشد، وضعیت پورت خود را بدون نیاز به پیکربندی و بصورت اتوماتیک به حالت Trunk تغییر دهد.

البته توجه داشته باشید سیسکو توصیه می کند که تنظیم پورت‌ها در هر دو طرف اتصالات Trunk توسط خود شما و بصورت دستی انجام پذیرد.

Native VLAN

همانطور که گفتیم پروتکل dot1q برای انتقال اطلاعات مربوط به VLANهای مختلف، اقدام به Tag زدن فریم ها می نماید که این عمل قالب اصلی فریم ایترنت را تغییر می دهد. برای اینکه بتوان فریم های ایترنت را بدون Tag زدن (Untagged) و با قالب اصلی بین سوئیچ ها منتقل نمود، از Native VLAN استفاده می گردد.

شماره مربوط به شبکه محلی مجازی بومی (Native VLAN)، باید در تمام سوئیچ هایی که توسط اتصالات Trunk به یکدیگر متصل هستند، یکسان باشد. با توجه به اینکه VLAN 1 بصورت پیش فرض بر روی سوئیچ ها وجود دارد، معمولا از همان VLAN 1 به عنوان Native VLAN نیز استفاده می گردد.

نکات تخصیص شماره به VLANها

استاندارد IEEE 802.1q امکان پشتیبانی از رنج 0 تا 4095 را برای شماره گذاری VLANها فراهم می آورد. اما در زمان ایجاد VLAN، جهت تخصیص شماره به آنها باید به نکات زیر توجه داشته باشید:

- VLAN 0 و VLAN 4095 توسط IEEE برای انجام امور خاص رزرو شده است. این VLANها قابل رویت و تغییر توسط کاربر نمی باشند.
- VLAN 1 بصورت پیش فرض بر روی سوئیچ ایجاد شده و امکان حذف آن نیز وجود ندارد. در راه اندازی اولیه تمام پورت های سوئیچ بصورت پیش فرض عضو VLAN 1

می باشند. از این VLAN معمولا به عنوان Native VLAN و Management VLAN نیز استفاده می گردد.

- رنج شماره های 2 تا 1001 را Normal VLANs می نامند. این رنج توسط تمامی تجهیزات سیسکو پشتیبانی می گردد.
- رنج 1005 – 1002 VLAN بصورت پیش فرض بر روی سوئیچ ایجاد شده و قابل پیکربندی و حذف توسط کاربر نمی باشد. این VLANها برای پروتکل های FDDI و Token ring رزرو گردیده است.
- رنج 1006 تا 4094 را Extended VLANs می نامند. قبل از پیکربندی VLANها در این رنج، باید از قابلیت سوئیچ و یا روتر خود در پشتیانی از Extended VLANs مطمئن شوید.

انواع وضعیت پورت سوئیچ

در سوئیچ های قابل مدیریت[1]، پورت ها می توانند در یکی از حالات زیر قرار داشته باشند:

- **Access**

این وضعیت برای پورت‌هایی مورد استفاده قرار می گیرد که جهت دسترسی کاربر نهایی در نظر گرفته شده باشد. در این حالت پورت امکان Trunk را نداشته ضمن آنکه قابلیت تغییر حالت پورت بصورت اتوماتیک نیز وجود ندارد.

بهترین شیوه این است که تمام پورت‌هایی که مورد استفاده قرار نمی گیرند را در این حالت، بصورتShutdown و عضو یک VLAN غیر فعال قرار داد.

- **Dynamic Auto**

تمام پورت های سوئیچ بصورت پیش فرض در این حالت قرار دارند. پورت ها در این حالت قابلیت تغییر بصورت اتوماتیک و بر اساس نوع پورت مقابل خود را دارند. به عنوان مثال اگر پورت مقابل در حالت Trunk باشد، پورت حالت خود را به Trunk تغییر می دهد.

- **Dynamic Desirable**

در این حالت پورت دائما تلاش می کند که با پورت مقابل خود، اتصال Trunk بر قرار نماید. در صورتیکه پورت مقابل در یکی از حالات Trunk، Desirable و یا Auto قرار داشته باشد، این پورت موفق به برقراری اتصال Trunk می گردد.

---

[1] Manageable

- **Trunk**

در این حالت پورت جهت بر قراری اتصالات Trunk مورد استفاده قرار می گیرد. پورت هایی که در وضعیت Trunk قرار دارند سعی می نمایند حالت پورت مقابل خود را نیز به این حالت تغییر دهند.

- **Nonegotiate**

پورتها در این حالت از ایجاد و انتشار پیامهایDTP جلوگیری به عمل می آورند. تنها پورت های Trunk و Access می توانند در این حالت قرار بگیرند.

نکته:

ایجاد VLAN شبیه ایجاد یک شبکه مستقل می باشد که دارای خصوصیات مستقل مربوط به خود است. به همین دلیل در شرایط معمول کلاینت های دو VLAN مختلف امکان برقراری ارتباط با یکدیگر را ندارند، حتی اگر کلاینت‌های هر دو VLAN بر روی یک سوئیچ فیزیکی قرار گرفته باشند.

یکی دیگر از موارد مهمی که باید به آن توجه داشته باشید، Subnet مربوط به هرVLAN می باشد. به دلیل مستقل بودن شبکه‌های مجازی از یکدیگر، جهت اختصاص آدرس IP نیز باید برای هر VLAN یک Subnet جداگانه در نظر بگیرید.

پیکربندی اولیه تجهیزات سیسکو

در ادامه می خواهیم به طرح یک سناریو جهت یادگیری موارد فوق بپردازیم. اما از آنجا که از این به بعد برای اجرای سناریوها شما باید سوئیچ ها را پیکربندی نمائید، لذا قبل از طرح سناریو به تشریح موارد مورد نیاز در پیکربندی سوئیچ های سیسکو می پردازیم.

در گام اول باید با انواع حالت‌های دستوری سوئیچ آشنا شوید. جدول زیر شامل انواع حالت‌ها جهت اعمال دستورات در سوئیچ های سیسکو می باشد:

Mode	Prompt	تشریح حالت
User EXEC	Switch>	از این حالت برای موارد زیر استفاده می شود: • تغییر تنظیمات ترمینال • انجام تست های اولیه • نمایش اطلاعات سیستم

Mode	Prompt	تشریح حالت
Privileged EXEC	Switch#	از این حالت برای بررسی دستورات اعمال شده استفاده می شود. بهتر است برای دسترسی به این حالت از کلمه عبور استفاده شود.
Global configuration	Switch(config)#	از این حالت برای پیکربندی پارامترهایی استفاده می شود که به تمام سوئیچ اعمال می گردند.
Config-vlan	Switch(config-vlan)#	از این حالت برای پیکربندی پارامترهای مربوط به VLANها استفاده می شود.
VLAN configuration	Switch(vlan)#	از این حالت برای پیکربندی پارامتر VLANهای رنج ۱ تا ۱۰۰۵ در VLAN Database استفاده می شود.
Interface configuration	Switch(config-if)#	از این حالت برای پیکربندی پارامترهای مربوط به اینترفیس استفاده می گردد.
Line configuration	Switch(config-line)#	از این روش برای پیکربندی پارامترهای مربوط به خطوط ترمینال استفاده می گردد.

در ادامه به دستورات مورد نیاز جهت اجرای حداقل پیکربندی بر روی سوئیچ های سیسکو می پردازیم:

پیکربندی پارامترهای عمومی		
	Command	Purpose
Step 1	configure terminal Example: Switch> enable Switch# configure terminal	Enters global configuration mode
Step 2	hostname *name* Example: Switch(config)# hostname Switch	Specifies the name for the router.
Step 3	enable secret *password* Example: Switch(config)# enable secret MTR	Specifies an encrypted password to prevent unauthorized access to the switch.

پیکربندی دسترسی به Command-Line		
	Command	Purpose
Step 1	line [aux |console | tty | vty] *line-number* Example: Switch(config)# line console 0	Enters line configuration mode, and specifies the type of line. This example specifies a console terminal for access.

پیکربندی دسترسی به Command-Line		
Step 2	Password *password* Example: Switch(config-line)# password cisco	Specifies a unique password for the console terminal line.
Step 3	login Example: Switch(config-line)# login	Enables password checking at terminal session login.
Step 4	line [aux |console | tty | vty] *line-number* Example: Switch(config-line)# line vty 0 4	Specifies a virtual terminal for remote console access.
Step 5	Password *password* Example: Switch(config-line)# password cisco	Specifies a unique password for the virtual terminal line.
Step 6	login Example: Switch(config-line)# login	Enables password checking at the virtual terminal session login.

سناریو(۳): برقراری VLAN

طرح مسئله:

آژانس هواپیمایی دچار تغییرات در کادر امور مالی خود شده است. مدیر جدید امور مالی نسبت به اطلاعات مالی به شدت حساس بوده و به همه دنیا ظنین است. لذا از آقای رئیس خواسته قسمت ایشان تافته جدا بافته تلقی گردیده و برای امور مالی شبکه‌ای مستقل فراهم آورد. ریاست محترم آژانس نیز طبق معمول دست به دامان حضرتعالی شده تا راه حلی برای خواسته امور مالی ارائه دهید.

لازم به ذکر است که دو نفر از بخش مالی در واحد جدید و عضو سوئیچB بوده و یک نفر هم به همراه سرور مالی در واحد قدیمی و عضو سوئیچ A می باشد.

نیاز سنجی:

برای جدا کردن بخش مالی، مدیر آژانس خود را برای پرداخت هزینه دوباره جهت خرید سوئیچ جدید و کابل کشی مجدد آماده کرده بود. اما از آنجا که مشاور ایشان فرد مهندس و کار بلدی مثل شماست! پس پیشنهاد راه اندازی VLAN را ارائه می کنید. با این کار هم خواسته مالی جهت داشتن شبکه مستقل اجرا شده و هم خرج اضافی روی دست مدیریت محترم نمی گذارید.

اما برای اجرای این کار باید یک Subnet جدید برای امور مالی در نظر بگیرید. به دلیل اینکه Subnet قبلی دارای تعداد زیادی آدرسIP است و شما هم از اسراف بدتان می آید، پس بهتر است Subnet قبلی شبکه را به دو قسمت تقسیم کنید.

کار بعدی هم پیکربندی سوئیچ و عضویت هر کلاینت در VLAN مربوطه می باشد.

راه حل:

ابتدا اقدام به Subnetting کرده و رنج قبلی را به دو قسمت مساوی تقسیم می کنیم. برای این کار یک بیت از بیت های مربوط به Host را کم و به بیت های مربوط به Network اضافه می کنیم. با توجه به اینکه Subnet قبلی در کلاس C بوده است، پس از Subnetting، دو رنج IP به صورت زیر خواهیم داشت:

192.168.200.0 /25	Or	192.168.200.0 255.255.255.128
192.168.200.128 /25	Or	192.168.200.128 255.255.255.128

با توجه به Subnetting فوق ما دارای ۲ شبکه هستیم که هر شبکه قابلیت آدرس دهی به ۱۲۶ کلاینت را دارد. در اینصورت زحمت عوض کردن Subnet Mask جدید بر روی کلاینت ها هم به گردن شما می افتد.

حالا نوبت به پیکربندی سوئیچ ها می رسد. با توجه به اینکه تا کنون هیچ پیکربندی خاصی بر روی سوئیچ ها اعمال نشده است، بهترین راه اتصال، پورت Console می باشد. البته پس از پیکربندی اولیه می توانید از طریق Telnet به سوئیچ ها متصل شوید.

در ابتدا بهتر است پیکربندی اولیه سوئیچ را انجام دهیم. برای پیکربندی اولیه دستورات زیر را از طریق پورت کنسول بر روی سوئیچ ها اجرا می نمائیم:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SwitchA
SwitchA(config)#enable secret cisco
SwitchA(config)#line console 0
SwitchA(config-line)#password cisco
SwitchA(config-line)#login
SwitchA(config-line)#line vty 0 4
SwitchA(config-line)#password cisco
SwitchA(config-line)#login
SwitchA(config-line)#^Z
SwitchA#write
```

دستورات فوق را بر روی سوئیچB نیز اجرا می نمائیم. با این تفاوت که برای Hostname عبارت SwitchB را وارد می نمائیم.

پس از پیکربندی اولیه سوئیچ، در اولین گام اقدام به پیکربندی پورت Trunk نمایید. ما همان اینترفیس(پورت)های Fa0/1 که سوئیچها را به یکدیگر متصل کرده بودند را به عنوان پورت Trunk تنظیم می نماییم.

به صورت پیش فرض پروتکلDTP بر روی سوئیچ در حالت فعال قرار دارد. به همین دلیل در صورتیکه بر روی یکی از سوئیچ ها اقدام به پیکربندی پورت Trunk نمایید، سوئیچ طرف مقابل نیز وضعیت پورت خود را به Trunk تغییر خواهد داد. اما به پیشنهاد سیسکو بهتر است که خودتان اقدام به پیکر بندی پورت Trunk در هر دو طرف اتصال نمائید.

جهت پیکربندی پورت Trunk بر روی سوئیچ ها دستورات زیر را وارد نمایید:

```
SwitchA>enable
SwitchA#configuration terminal
SwitchA(config)#interface fastethernet 0/1
```

```
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#trunk encapsulation dot1q
```

```
SwitchB>enable
SwitchB#configuration terminal
SwitchB(config)#interface fastethernet 0/1
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#trunk encapsulation dot1q
```

حالا نوبت به ایجاد VLANها می رسد. با توجه به اینکه VLAN 1 بصورت پیش فرض وجود داشته و در این VLAN عملیات نشانه گذاری(Tagging) انجام نمی شود، پس شماره VLANهای ما ۲ و ۳ خواهد بود.

برای پرسنل آژانس VLAN 2 را با نام Personnel و برای قسمت امورمالی VLAN 3 را با نامFinance ایجاد می نماییم. توجه داشته باشید که نام VLANها صرفا برای سهولت در امور مدیریتی بوده و از لحاظ فنی هیچ تاثیری بر روی فریم ها نمی گذارد و ملاک تشخیص شبکه همچنان همان VLAN ID می باشد. لازم به ذکر است حتی متفاوت بودن نام VLANها در سوئیچ‌های مختلف نیز هیچ تاثیری بر روی درستی انجام کار نخواهد گذاشت.

```
SwitchA>enable
SwitchA#configuration terminal
SwitchA(config)#vlan 2
SwitchA(config-vlan)#name personnel
SwitchA(config-vlan)#vlan 3
switchA(config-vlan)#name finance
```

```
SwitchB>enable
SwitchB#configuration terminal
SwitchB(config)#vlan 2
SwitchB(config-vlan)#name personnel
SwitchB(config-vlan)#vlan 3
switchB(config-vlan)#name finance
```

حالا نوبت به مشخص نمودن اعضای هر VLAN رسیده است. با توجه به اینکه در این مسئله نظر ما بر اجرای Port-based VLAN می باشد، پس باید اینترفیس(پورت)های مربوط به هر VLAN را مشخص نماییم.

```
SwitchA>enable
SwitchA#configuration terminal
SwitchA(config)#interface range fastethernet0/2 - 14
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 2
```

```
SwitchA(config-if-range)#exit
SwitchA(config)#interface fastethernet0/20
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 3
SwitchA(config-if-range)#exit
SwitchA(config)#exit
SwitchA#write
```

در زمانیکه می‌خواهیم یک پیکربندی را بر روی تعدادی از اینترفیس‌های یک سوئیچ بطور یکسان انجام دهیم، می توانیم بجای اجرای یک به یک دستورات بر روی هر اینترفیس، با استفاده از دستور interface range، پیکربندی را بصورت گروهی انجام دهیم.

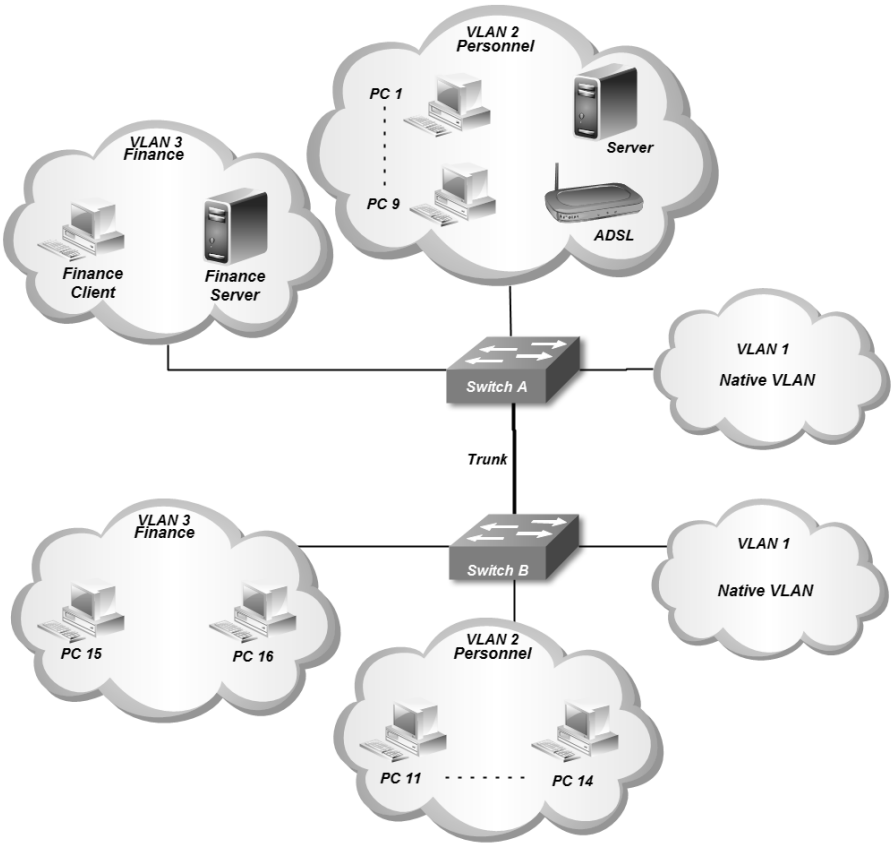
از دستور exit برای بیرون رفتن از Mode کنونی و از دستور end یا کلیدهای Ctrl-Z، برای بازگشت به حالت Privileged EXEC mode استفاده می شود. همچنین از دستور write برای ذخیره پیکربندی در Startup-config استفاده می شود.

```
SwitchB>enable
SwitchB#configuration terminal
SwitchB(config)#interface range fastethernet0/2 - 4
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 2
SwitchB(config-if-range)# interface range fastethernet0/5 - 7
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 3
SwitchB(config-if-range)#end
SwitchB#copy running-config startup-config
```

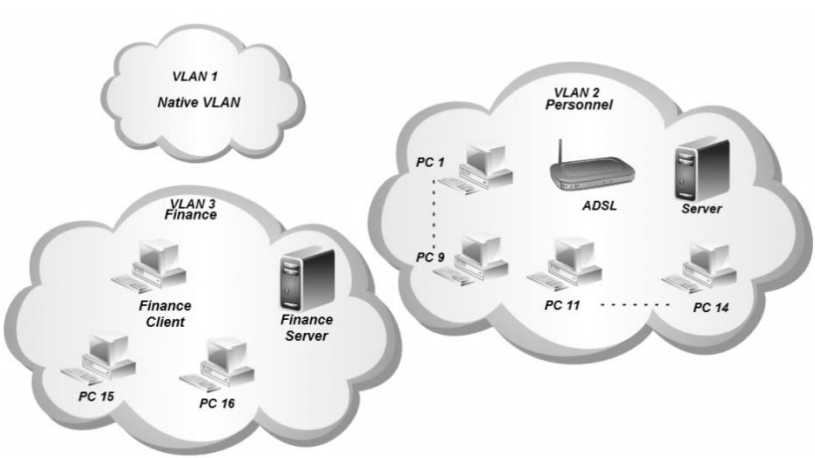
دستور copy running-config startup-config، همان کار دستور write را انجام داده و باعث می‌شود پیکربندی انجام شده که بر روی حافظه موقت قرار دارد، در فایل startup-config موجود بر روی حافظه Flash سوئیچ ذخیره گردد.

لازم به ذکر است که فایل Startup-config حاوی پیکربندی سوئیچ بوده و بر روی حافظه Flash یا دائم سوئیچ ذخیره می شود. هنگامی که سوئیچ Boot می شود فایل Startup-config به حافظه موقت یاRAM سوئیچ انتقال داده شده و نام این فایل موقتی Running-config گذاشته می شود. از این پس تمام تغییرات اعمال شده در این فایل نگهداری می شود. به دلیل اینکه محتویات این فایل پس از راه اندازی مجدد سوئیچ از بین می رود، لذا برای ذخیره تغییرات انجام شده بر روی فایل Startup-config باید از دستور Write یا Copy running-config startup-config بهره ببریم.

تصویر زیر نشان دهنده شبکه پس از پیکربندی سوئیچ‌ها، از نظر فیزیکی می باشد. گستردگی VLANهای End-to-end بر روی سوئیچ های A وB نیز نشان داده شده است.



تصویر زیر نشان دهنده شبکه فوق از نظر منطقی می باشد. در این تصویر اعضای شبکه ها و ارتباطات آنها را نمایش می دهد.

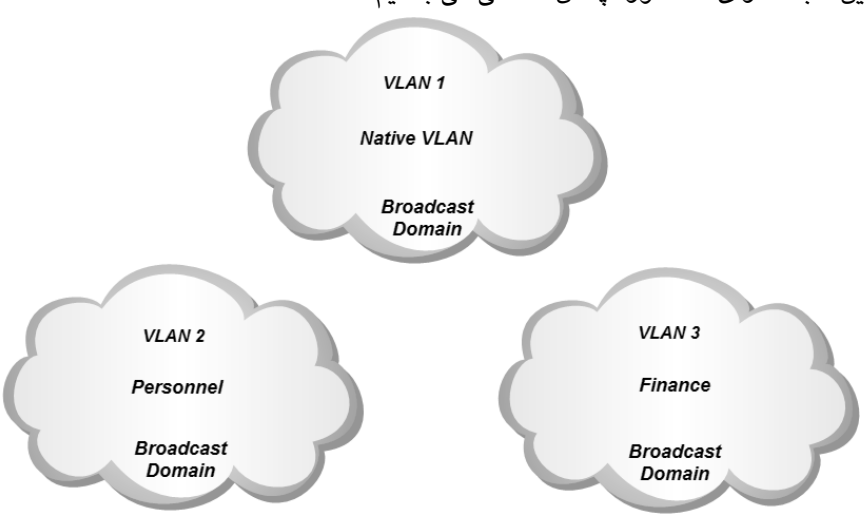


نحوه عملکرد:

عملیات سوئیچینگ را که به یاد دارید! حال اگر کارمند امورمالی که بر روی سوئیچA می‌باشد بخواهد با سیستم مدیر مالی بر روی سوئیچ B، ارتباط برقرار نماید باید آدرس MAC دستگاه مقصد را بیاموزد. همانطور که قبلا گفتیم کلاینت برای یادگیری آدرسMAC بر اساس آدرسIP، از پروتکلARP استفاده می نماید. پروتکلARP نیز برای انجام این کار از پیام‌های پخش همگانی استفاده می نماید. اما پیام Broadcastای که توسط پروتکل ARP بوجود آمده به چه صورت در سوئیچ ها منتشر می گردد؟

سوئیچ A پیام Broadcast را از کلاینت عضو VLAN 3 دریافت می نماید. با توجه به اینکه VLAN 3 یک End-to-End VLAN می باشد پس باید این پیام به اعضای این VLAN که بر روی سوئیچ B قرار دارند نیز ارسال گردد. به همین دلیل این پیام برای ارسال به سوئیچB، تحویل پورت Trunk سوئیچ A می گردد. پورت Trunk توسط پروتکل dot1q اقدام به Tagging فریم مورد نظر جهت مشخص نمودن VLAN ID مربوطه نموده و آنرا تحویل پورتTrunk سوئیچB می‌دهد. پورتTrunk سوئیچB نیز با بررسی فریم بر اساس پروتکلdot1q، متوجهVLAN مربوطه شده و با حذف فیلدهای اضافه شده، فریم ایترنت اصلی را در اختیارVLAN 3 موجود بر روی سوئیچB قرار می دهد. در اینصورت پیام فقط توسط کلاینت‌هایی که عضو VLAN 3 هستند دریافت گردیده و بقیه کلاینت‌ها از وجود آن بی اطلاع خواهند ماند. این عملیات از نظر سخت افزاری توسط ASIC های موجود در سوئیچ انجام می پذیرد.

با توجه به این موضوع که هر VLAN دارای Broadcast Domain مخصوص به خود است، در این شبکه دارای سه حوزه پخش همگانی می باشیم.



سیسکو برای بررسی پیکربندی و مشاهده وضعیت سوئیچ دارای دستوراتی می باشد که با کلمه show آغاز می گردند. برای مثال می توانید جهت مشاهده وضعیت اینترفیس‌ها از دستور show interface و برای مشاهده وضعیت VLANها از دستور show vlan استفاده نمایید.

```
SwitchA#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24

2    Personnel                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14

3    Finance                          active    Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

تمام پورتهای سوئیچ بصورت پیش فرض عضو VALN 1 می‌باشند. به همین دلیل در خروجی دستور show vlan فوق، اینترفیس‌هایی که به عنوان عضو VLAN خاصی انتخاب نشده‌اند، عضو VLAN 1 می باشد.

شماره VLANهای 1002 تا 1005 نیز بصورت پیش فرض در سوئیچ ایجاد شده است. این VLANها برای پروتکل های FDDI و Token ring رزرو شده است.

مرجع دستور Command Reference

Creating or Modifying an Ethernet VLAN		
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.
Step 3	**name** *vlan-name*	(Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size (or other VLAN characteristic).

Creating or Modifying an Ethernet VLAN		
Step 5	**remote-span**	(Optional) Configure the VLAN as the RSPAN VLAN for a remote SPAN session.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 8	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

Assigning Static-Access Ports to a VLAN		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.

Configuring a Trunk Port		
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured for trunking, and enter interface configuration mode.
Step 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode).
Step 4	**switchport access vlan** *vlan-id*	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
Step 5	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN for IEEE 802.1Q trunks.

پروتکل VTP

پروتکل VLAN Trunk Protocol جهت اعمال پیکربندی VLANها بصورت متمرکز بر روی سوئیچ‌ها به کار برده می‌شود. این پروتکل مخصوص سیسکو بوده و تنها در محصولات این شرکت پشتیبانی می گردد.

در سناریوهای قبلی، شما برای ایجاد VLANها مجبور بودید پیکربندی را به ازاء هر سوئیچ بصورت مستقل انجام دهید. اجرای مجزای پیکربندی در مواقعی که شبکه دارای تعداد کمی سوئیچ باشد، شاید ایجاد مشکل ننماید، اما تصور کنید در صورتیکه بخواهید یک شبکه بزرگ با تعداد زیادی سوئیچ را برای پشتیبانی از VLANها پیکربندی کنید چه اتفاقی می افتد؟ شما برای هر تغییر کوچک و بزرگی مثل ایجاد، حذف و یا ویرایش یک VLAN مجبور خواهید بود این عمل را به ازاء هر سوئیچ انجام دهید. به علاوه ی ایجاد سربار مدیریتی و صرف وقت، امکان بوجود آمدن اشکالات در زمان پیکربندی تعداد زیادی سوئیچ نیز به شدت افزایش می یابد.

سیسکو برای حل معضل فوق اقدام به معرفی پروتکلVTP نموده است. با استفاده از این پروتکل شما می‌توانید یک سوئیچ را به عنوان VTP Server در شبکه مشخص نموده و پیکربندی VLANها را بر روی آن انجام دهید، سپس سوئیچ‌های دیگر که به عنوان VTP Client پیکربندی شده‌اند، تنظیمات را بصورت اتوماتیک دریافت و اعمال می نمایند.

لازم به ذکر است کهVTP فقط تنظیمات مربوط به ایجاد، حذف و ویرایش VLANها را انجام می‌دهد و عمل اختصاص پورتهای سوئیچ به VLANهای مختلف، همچنان باید بصورت دستی و بطور مستقیم بر روی هر سوئیچ انجام پذیرد.

پروتکلVTP در لایه دوم مدلOSI کار کرده و امکان ارسال و دریافت بسته‌های خود را بر روی اتصالات Trunk ایجاد شده بر اساس هر دو پروتکل dot1q و ISL را نیز دارد.

نسخه های VTP

پروتکل VTP دارای سه نسخه می باشد که فراگیرترین نسخه آن VTP v2 می باشد. هر چند که VTP v3 دارای امکانات بیشتری نسبت به دو نسخه قبلی خود می‌باشد ولی پشتیبانی نکردن همه IOSهای سیسکو از این نسخه و شرایط خاص استفاده از آن، باعث گردیده که همچنان VTP v2 در عرصه استفاده پیشتاز باشد.

- **VTP v1**

در صورت استفاده ازVTP، نسخه یک این پروتکل بصورت پیش فرض بر روی سوئیچ فعال می گردد. این پروتکل فقط می تواند تا VLAN 1001 را پشتیبانی نماید.

همچنین VTP v1 امکان همکاری با پروتکلToken ring را نیز ندارد.

- **VTP v2**

VTP v2 دارای امکانات بیشتری نسبت به نسخه قبلی خود می باشد. پشتیبانی از Token ring و انتقال پیام های VTP بدون بررسی نسخه آن در حالت Transparent، از جمله ویژگی‌های جدید این نسخه می باشند. در این نسخه نیز همچنان از Extended VLANs پشتیبانی نمی گردد.

- **VTP v3**

نسخه سوم پروتکلVTP دارای امکانات بهبود یافته‌ای نسبت به نسخه‌های قبلی خود است. البتهVTP v3 امکان تعامل با ورژن های قبلی خود را نیز دارد.

از جمله ویژگیهای جدید پشتیبانی شده در این نسخه می توان از Private VLAN، Server Authentication و Extended VLANs نام برد.

انواع وضعیت VTP

سوئیچ‌های شبکه برای راه اندازی پروتکلVTP در یکی از سه حالت زیر پیکربندی می‌گردند:

۱- **VTP Server**

تمام سوئیچ‌ها بصورت پیش فرض در وضعیت VTP Server قرار دارند. در این حالت ایجاد، حذف و ویرایش VLANها بر روی سوئیچ امکان پذیر می‌باشد. تنظیمات ایجاد شده VLANها بر روی سوئیچ VTP Sever در فایلی به نام Vlan.dat و بر روی حافظه دائم (Flash) سوئیچ ذخیره می گردد.

تعیین پارامتر VTP Pruning بر روی این سوئیچ انجام می گردد.

۲- **VTP Client**

در این حالت امکان ایجاد، حذف و ویرایش VLANها امکان پذیر نمی باشد. سوئیچ های Client تنظیمات مربوط به VLANها را از سوئیچ Server دریافت می‌نمایند.

بر روی سوئیچ‌های VTP Client شما فقط می توانید عملیات اختصاص پورت به VLANهای مختلف را انجام دهید. این تنظیمات در حافظه دائم سوئیچ ذخیره می گردد.

۳- **VTP Transparent**

سوئیچی که در حالتVTP Transparent پیکربندی می گردد در پروسه VTP شرکت نمی کند. در این حالت سوئیچ Transparent صرفا مسیری جهت عبور اطلاعات VTP بین سوئیچ‌های متصل به خود بوده و از یکسان سازی اطلاعات خود با VTP و تاثیر

پذیری از آن خودداری می نماید. در این حالت تنظیمات VLAN سوئیچ بصورت مستقل پیکربندی شده و اطلاعات مربوطه را بر روی حافظه دائم خود نگهداری می نماید.

انواع پیام VTP

- **Summary advertisements**

این پیام به صورت پیش فرض هر ۵ دقیقه یکبار توسط سوئیچ VTP Server ارسال می گردد. سوئیچ های Client پس از دریافت این پیام ابتدا اقدام به بررسی نام حوزه (VTP Domain) نموده و در صورتی که پیام مربوط به حوزه مربوطه باشد اقدام به مقایسه Revision Number پیام با پیکربندی خود می کند. اگر عدد پیام رسیده مطابق و یا پایین‌تر از پیکربندی سوئیچ باشد پیام را دور انداخته و در صورتیکه این عدد بزرگتر از پیکربندی اعمال شده بر روی سوئیچ باشد، سوئیچ Client اقدام به ارسال پیام Advertisement request برای سوئیچVTP Server می نماید.

- **Subset advertisement**

این پیام پس از ایجاد، حذف و یا تغییر در پیکربندی VLANها ایجاد و ارسال می گردد. این پیام به ازاء هر VLAN که دچار تغییرات شود ایجاد و ارسال می گردد.

هم زمان با ارسال پیام Subset advertisement، پیام Summary advertisement نیز ارسال می گردد.

- **Advertisement requests**

این پیام توسط سوئیچ VTP Client در یکی از شرایط زیر ارسال می گردد: ۱-سوئیچ راه اندازی مجدد شده باشد. ۲-تغییری در VTP Domain ایجاد شده باشد. ۳-سوئیچ پیامSummary advertisementای را با Revision Number بالاتر از پیکربندی خود دریافت نموده باشد.

حوزه VTP

حوزهVTP یاVTP Domain، شامل مجموعه سوئیچ‌هایی است که دارای خصوصیات پیکربندی مشترکی برای استفاده از VLANها می باشند.

در صورت استفاده از امکانVTP Domain، سوئیچ‌ها فقط اقدام به پذیرش پیام‌هایی می‌نمایند که توسط سوئیچ VTP Serverمربوط به حوزه خودشان ایجاد و منتشر گردیده باشد.

توجه داشته باشید که نام اختصاص داده شده به VTP Domain بر روی تمام سوئیچ‌های حوزه باید بصورت یکسان تعریف گردیده باشد.

VTP Password

با استفاده از امکانVTP Password می‌توان باعث ایجاد امنیت در مورد پخش و قبول پیام‌های VTP در حوزه مربوطه گردید. این ویژگی که از MD5 جهت رمزنگاری اطلاعات استفاده می کند، می‌تواند امنیت انتقال پیام‌ها را تضمین نموده و از شنود اطلاعات توسط افراد غیر جلوگیری به عمل آورد.

توجه داشته باشید عبارت مورد استفاده برای VTP Password در تمامی سوئیچ های عضو حوزه باید بصورت یکسان تعریف گردیده باشد.

شماره اصلاح پیکر بندی

شماره اصلاح پیکربندی(Configuration Revision Number)، عددی است ۳۲ بیتی که نمایانگر سطح تجدید نظر اطلاعات VTP بوده و در غالب پیام های پروتکل VTP وجود دارد.

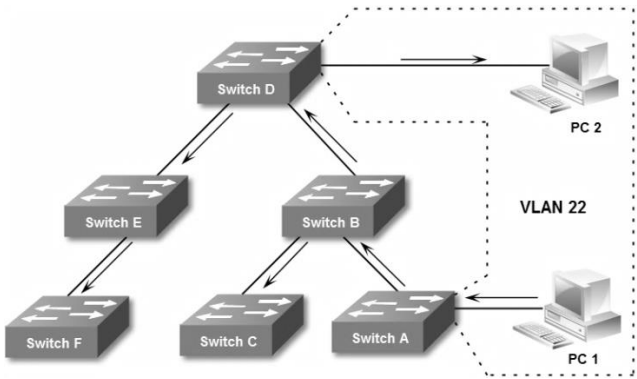
پروتکلVTP از مقایسه عدد Revision Number مربوط به پیام دریافتی با Revision Number پیکربندی اعمال شده بر روی سوئیچ، می تواند تشخیص دهد آیا پیام رسیده جدید است یا خیر. به همین دلیل باید در زمان اضافه نمودن سوئیچ جدید بهVTP Domain از پایین تر بودن این عدد نسبت به سوئیچ VTP Server اطمینان حاصل نموده و یا اقدام به Reset کردن آن عدد نمایید.

این عدد در سوئیچ با پیکربندی Transparent، همواره برابر0 می باشد. به همین دلیل یکی از راه‌هایReset کردنRevision Number سوئیچ، پیکربندی آن در حالتTransparent می‌باشد. همچنین این عدد در زمان تغییر VTP Domain نیز صفر می گردد.

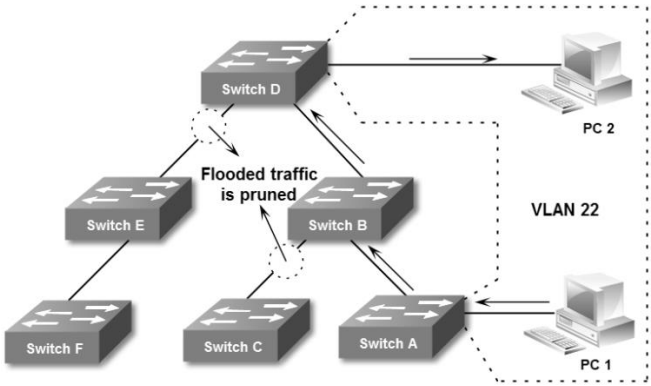
VTP Pruning

از خصوصیتVTP Pruning جهت جلوگیری از انتقال اطلاعات غیر ضروری بین سوئیچ‌ها استفاده می گردد. این خصوصیت که بر روی سوئیچ VTP Server پیکربندی می گردد، باعث می‌شود از انتقال اطلاعات غیر ضروری به سوئیچ هایی که نیازی به آن اطلاعات ندارند جلوگیری به عمل آید.

به عنوان مثال همانطور که در تصویر زیر ملاحظه می نمائید، در حالت معمول پیام‌های Broadcast مربوط به یکVLAN به تمام سوئیچ‌های عضو VTP Domain ارسال می گردند. هرچند که سوئیچ‌هایی که پورت عضو آن VLAN را ندارند از پخش پیام خودداری کرده و آنرا حذف می کنند، ولی انتشار این نوع پیام‌ها باعث استفاده بی مورد از منابع شبکه می گردد.



با استفاده از VTP Pruning می‌توان از ارسال دیتا به سوئیچ‌هایی که هیچ پورت متناظری با VLAN ارسال کننده دیتا ندارند و همچنین در مسیر ترانزیت دیتا به سوئیچ مربوطه نیز نیستند، جلوگیری به عمل آورد.



زمانیکه ویژگی VTP Pruning را بر روی سوئیچ سرور فعال می کنید، چند ثانیه بعد این ویژگی بر روی تمام سوئیچ های عضو آن ناحیه فعال می گردد.

VLAN 1 و VLANهای 1002 تا 1005 از این قاعده مستثنی بوده و VTP Pruning هیچ تاثیری بر روی ترافیک این VLANها نمی گذارد. همچنین VTP Pruning از رنج Extended VLANs نیز پشتیبانی نمی کند.

سناریو(۴)؛ راه اندازی VTP

طرح مسئله:

آژانس هواپیمایی، همان مرغ تخم طلایتان را که یادتان هست. حالا می خواهیم اجرای VTP را بر روی همان شبکه امتحان کنیم. البته در عمل شبکه ای به کوچکی این آژانس نیازی به راه اندازی VTP ندارد. ولی چون تازه کار هستیم راه دیگری برای یادگیری عملی VTP نداریم!

نیاز سنجی:

به جز کمی همت و مطالعه این بخش نیاز دیگری ندارید.

راه حل:

سوئیچ A را به عنوان سوئیچ سرور انتخاب می نماییم. یک نام و کلمه عبور هم برای تنظیمات VTP در نظر می گیریم. ترجیحا از VTP v2 برای این مسئله استفاده می نماییم.

جهت اجرا ابتدا سراغ سوئیچ A رفته و دستورات زیر را اعمال می نماییم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vtp domain MTR
SwitchA(config)#vtp mode server
SwitchA(config)#vtp password cisco
SwitchA(config)#vtp version 2
SwitchA(config)#vtp pruning
```

به دلیل تعلق خاطر بنده به عبارت MTR[1]، نام حوزه را به این صورت انتخاب کردم؛ هر چند که شما هم می توانید از این عبارت برای موفقیت در کارهایتان استفاده کنید! ولی توجه داشته باشید که نام و کلمه عبورVTP را می توانید بر اساس سلیقه خودتان انتخاب نمایید.

با استفاده از دستور درج شده در خط آخر، ویژگی VTP Pruning بر روی سوئیچ سرور فعال گردیده است. همچنین برای غیرفعال نمودن VTP Pruning می توانید از دستور no vtp pruning استفاده نمایید. لازم به ذکر است که برای معکوس کردن اکثر دستورات IOS سیسکو می توانید از عبارت no در ابتدای دستور بهره ببرید.

در گام بعدی سراغ پیکربندیVTP بر روی سوئیچB می رویم:

[1] Mohammad Taghi Roghani

```
SwitchB>enable
SwitchB#configure terminal
SwitchB(config)#vtp domain MTR
SwitchB(config)#vtp password cisco
SwitchB(config)#vtp version 2
SwitchB(config)#vtp mode client
```

اگر به ترتیب اجرای دستورات بر روی سوئیچB توجه نموده باشید، متوجه می‌شوید که Mode مربوط بهVTP به عنوان آخرین دستور وارد گردیده است. به دلیل اینکه پس از تغییر Mode سوئیچ به کلاینت امکان اعمال بعضی از تنظیمات مثل مشخص نمودن نسخه VTP میسر نمی باشد، لذا دستور مربوط به تغییر Mode را ترجیحا به عنوان آخرین دستور به سوئیچ اعمال می کنیم.

پس از دستور vtp mode client، سوئیچ به شما پیام هشداری مبنی بر از دست رفتن اطلاعات مربوط به تنظیمات قبلی VLANها می‌دهد.

برای بررسی طریقه عملکردVTP، می‌توانید پس از اعمال تنظیمات فوق یک تغییر بر روی VLANها در سوئیچ A ایجاد نموده و ظرف چند ثانیه آن تغییر را در سوئیچB نیز مشاهده نمایید.

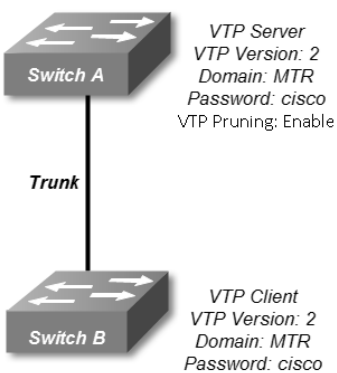
```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vlan 10
SwitchA(config)#name Test
SwitchA(config)#end
SwitchA#write
```

با استفاده از دستور show vlan در سوئیچ B می توانید خروجی زیر را مشاهده نمایید.

```
SwitchB#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21,
                                                Fa0/22, Fa0/23,Fa0/24
2    Personnel                        active    Fa0/2, Fa0/3, Fa0/4
3    Finance                          active    Fa0/5, Fa0/6, Fa0/7
10   Test                             active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

طریقه عملکرد

سوئیچ A به عنوان سرور و سوئیچ B به عنوان کلاینت VTP پیکربندی شده‌اند. سوئیچA هر۵ دقیقه یا پس از اعمال تغییرات در پیکربندی VLANها اقدام به ارسال پیام Summary advertisement به سوئیچ های عضو حوزه خود می نماید. سوئیچ B نیز پس از دریافت پیام ابتدا نام VTP Domain پیام دریافتی را بررسی می نماید. در صورتیکه پیام برای همان حوزه باشد، سوئیچ B اقدام به مقایسه عدد Revision number پیام دریافتی با مقدار پیکربندی موجود می‌نماید. اگر این عدد کوچکتر یا مساوی عدد Revision number موجود بر روی سوئیچ باشد، سوئیچ پیام دریافتی را نادیده گرفته و آنرا دور می اندازد. ولی اگر این عدد بزرگتر از عدد موجود روی سوئیچ باشد، پروتکل VTP متوجه ایجاد تغییرات جدید می شود. پس سوئیچ B با ارسال پیام Advertisement request به سوئیچ سرور، درخواست خود مبنی بر دریافت پیکربندی جدید را اعلام می دارد. در نهایت اطلاعات پیکربندی جدید به سوئیچ B ارسال شده و بر روی سوئیچ اعمال می گردد.



توجه داشته باشید فایل اصلی پیکربندی VLANها فقط روی سوئیچ سرور و در حافظه دائم آن موجود می باشد. سوئیچ کلاینت پس از راه اندازی مجدد و یا قطع برق، در هنگام Boot شدن اقدام به ارسال پیام Advertisement request می نماید.

ویژگیVTP Pruning نیز اجازه عبور ترافیک را برای اتصالاتTrunk سوئیچ‌هایی صادر می‌نماید که حداقل یک پورت آن سوئیچ عضو VLAN مورد نظر بوده و یا در مسیر ترانزیت دیتا به سوئیچ مورد نظر قرار داشته باشند.

استفاده از ویژگی VTP Password بصورت اختیاری می باشد. ولی در صورت استفاده باعث ایجاد امنیت در ارسال و دریافت پیام های VTP می گردد.

مرجع دستور Command Reference:

Configuring a VTP Server		
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp mode server**	Configure the switch for VTP server mode (the default).
Step 3	**vtp domain** *domain-name*	Configure the VTP administrative-domain name. The name can be from 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 4	**vtp password** *password*	(Optional) Set the password for the VTP domain. The password can be from 8 to 64 characters.
Step 5	**vtp version 2**	Enable VTP version 2 on the switch. VTP version 2 is disabled by default on VTP version 2-capable switches.
Step 6	**vtp pruning**	Enable pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.

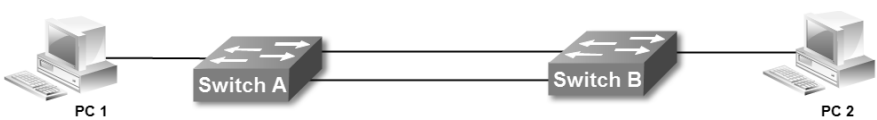
Configuring a VTP Client		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp version 2**	Enable VTP version 2 on the switch.
Step 3	**vtp mode client**	Configure the switch for VTP client mode. The default setting is VTP server.
Step 4	**vtp domain** *domain-name*	(Optional) Enter the VTP administrative-domain name. The name can be from 1 to 32 characters. This should be the same domain name as the VTP server.
Step 5	**vtp password** *password*	(Optional) Enter the password for the VTP domain.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.

☑ مبحث سوم

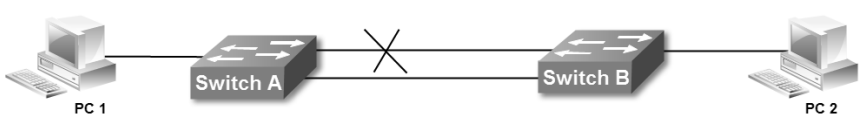
پروتکل درخت پوشا (STP)

پروتکل درخت پوشا(Spanning Tree Protocol)، وظیفه مدیریت لینک‌ها را جهت فراهم آوردن افزونگی[1] مسیر در عین جلوگیری از ایجاد حلقه[2] لایه دو بر عهده دارد.

وجود مسیرهای چندگانه فعال بین دو ایستگاه کاری، باعث ایجاد حلقه لایه دو در شبکه می‌گردد، لذا برای عملکرد درست شبکه فقط باید یک مسیر فعال بین دو ایستگاه کاری وجود داشته باشد. از طرف دیگر نبود لینک‌های اضافه باعث کاهش پایداری[3] شبکه گردیده و در صورت قطع شدن یک لینک، ممکن است نیمی از شبکه از کار بیافتد. به همین دلیل است که مدیران شبکه اقدام به راه اندازی چند مسیر بین سوئیچ‌ها نموده تا امکان افزونگی را در شبکه خود فراهم آورند. اما برای حل مشکل فوق و داشتن ویژگی افزونگی ضمن جلوگیری از ایجاد حلقه می بایست از پروتکل STP بهره برد.



پروتکلSTP وظیفه خود را توسط الگوریتمSTA[4]، انجام می‌دهد. این الگوریتم با شناسایی مسیرهای موجود بین سوئیچ‌ها اقدام به فعال نگاه داشتن یک مسیر و غیرفعال نمودن مسیرهای دیگر می نماید. اما پروتکل STP همچنان لینک ها را تحت نظر دارد تا در صورت از کار افتادن لینک فعال و یا تغییر هزینه[5] آن، اقدام به فعال کردن مسیر جایگزین نموده و از قطع شدن ارتباط جلوگیری به عمل آورد.



[1] Redundancy
[2] Loop
[3] Stability
[4] Spanning Tree Algorithm
[5] Cost

پروتکلSTP توسط سازمانIEEE و تحت استانداردهای 802.1D، 802.1w و 802.1s توسعه داده شده است. البته سیسکو در این زمینه نیز دارای پروتکلهای مخصوص به خود می باشد.

سوئیچ ریشه[1](Root Switch)

پروتکلSTP برای اجرای الگوریتم خود، نیاز به مشخص نمودن یک سوئیچ مرکزی به عنوان سوئیچ ریشه(Root Switch) دارد. پروتکلSTP مدیریت مسیرهای موجود بین سوئیچ‌های شبکه را بر اساس سوئیچ ریشه انجام می دهد، به صورتیکه از هر نقطه در شبکه فقط باید یک مسیر فعال تا سوئیچ ریشه وجود داشته باشد.

انتخاب سوئیچ ریشه بر اساس پارامترBridge ID صورت می گیرد. هر چه این عدد کوچک‌تر باشد امکان انتخاب سوئیچ به عنوان سوئیچ ریشه بیشتر است.

BID هشت بایت بوده که شامل دو بایت Priority و شش بایت MAC Address می باشد. در بعضی از نسخه های STP، ۲ بایت Priority به دو قسمت با عنوان‌های Priority با ۴ بیت و Extended System ID با ۱۲ بیت، تقسیم گردیده است. بسته به پروتکل مورد استفاده، مقدار Extended System ID، ممکن است حاوی شماره VLAN و یا شماره پروسه STP باشد.

نحوه انتخاب سوئیچ ریشه

پروتکلSTP برای انتخاب سوئیچ ریشه از پیام هایBPDU استفاده می‌نماید. پارامترهایی که این پیام‌ها برای انتخاب سوئیچ ریشه انتقال می دهند عبارتند ازPriority و MAC Address. سوئیچ‌ها با دریافت پارامترهای فوق اقدام به مقایسه آنها با مقادیر موجود بر روی خود می‌نمایند. این مقایسه در یکی از حالتهای زیر منجر به انتخاب سوئیچ ریشه می شود:

۱- در ابتدا تمام سوئیچ‌ها با ارسال متناوب پیامBPDU، خود را به عنوان سوئیچ ریشه معرفی می‌نمایند.

۲- سوئیچ دریافت کننده پیام، اقدام به مقایسهPriority پیام رسیده با مشخصات خود می‌نماید. در صورتیکهPriority پیام دریافتی بزرگتر از مقدارPriority سوئیچ دریافت

[1] در برخی متون فنی ازRoot Switch با عنوان Root Bridge نیز نام برده می شود.

کننده باشد، سوئیچ از مقایسه آدرسMAC صرف نظر کرده، پیام را نادیده گرفته و با ارسال پیامBPDU خود را به عنوان سوئیچ ریشه معرفی می کند.

۳- در صورتیکه مقدارPriority پیام رسیده کوچکتر ازPriority سوئیچ دریافت کننده باشد، بدون مقایسه آدرسMAC، اقدام به پذیرش سوئیچ معرفی شده به عنوان Root Switch نموده و این انتخاب را به اطلاع سوئیچ ریشه می‌رساند.

۴- اگر مقدارPriority پیام رسیده با سوئیچ دریافت کننده برابر باشد، سوئیچ اقدام به مقایسه آدرسMAC خود با آدرسMAC سوئیچ ارسال کننده پیام می‌نماید. در صورتیکه آدرسMAC پیام بزرگتر باشد، پیام را دور انداخته و طی ارسال پیامBPDU خود را به عنوان سوئیچ ریشه معرفی می نماید.

۵- اگرPriority سوئیچ و پیام یکسان بوده و آدرسMAC پیام رسیده کوچکتر از آدرس MAC سوئیچ دریافت کننده باشد، سوئیچ معرفی شده را به عنوان سوئیچ ریشه قبول کرده و با ارسال پیام، این اقدام را به اطلاع سوئیچ ریشه می‌رساند.

هر سوئیچ ارسال پیام خود بزرگ بینی "من ریشه هستم" را تا زمانی ادامه می دهد که تمام سوئیچ‌های دیگر آنرا به عنوان ریشه قبول کرده باشند و یا خودش، مجبور به قبول سوئیچ دیگری به عنوان سوئیچ ریشه شده باشد.

در صورت از مدار خارج شدن سوئیچ ریشه و یا اضافه شدن یک سوئیچ به شبکه، پروتکل STP مجددا مراحل فوق را برای انتخاب سوئیچ ریشه جدید و مشخص نمودن توپولوژی شبکه انجام می دهد.

بصورت پیش فرض مقدارPriority سوئیچ32768 می‌باشد و به دلیل برابر بودن این عدد در سوئیچ‌ها، معمولا کوچکتر بودن آدرسMAC باعث انتخاب سوئیچ ریشه می گردد. ولی در صورتیکه مقدارPriority سوئیچ کوچکتر باشد بدون مقایسهMAC، به عنوان سوئیچ ریشه انتخاب می شود.

شما می‌توانید جهت اعمال پارتی بازی! برای انتخاب سوئیچ دلخواهتان به عنوان Root Switch، اقدام به تغییرPriority سوئیچ نمایید. برای تعیین سوئیچ به عنوان ریشه می توانید از دستور زیر استفاده نمایید. این دستور مقدار Priority را به 24576 تغییر می دهد:

Switch(config)# **spanning-tree vlan** *vlan-id* **root primary**

همچنین می توانید از دستور زیر برای اعطای اولویت دوم جهت انتخاب سوئیچ ریشه اقدام نمایید. این دستور مقدار فیلد Priority سوئیچ را برابر28672 قرار می دهد:

Switch(config)# **spanning-tree vlan** *vlan-id* **root secondary**

پس از مشخص شدن سوئیچ ریشه و نقش پورت ها برای دسترسی به سوئیچ ریشه، می‌توان گفت که شبکه به همگرایی[1] رسیده است.

پیام BPDU

پیامBridge Protocol Data Unit، توسط پروتکلSTP جهت انتقال اطلاعات مربوط به این پروتکل، بین سوئیچ ها استفاده می گردد. پیام‌هایBPDU از آدرسMulticast لایه دو برابر با 01-80-C2-00-00-00 برای انتشار فریم‌های خود در شبکه استفاده می نمایند. مکانیسم اجرای الگوریتم STA که باعث مشخص شدن توپولوژی شبکه و نقش هر سوئیچ در فرایندSTP می گردد توسط این پیام ها انجام می پذیرد.

پیام هایBPDU شامل اطلاعاتی از جمله Root ID، Cost of path، BID و Port ID می باشند.

پیام TCN

پیام اطلاعیه تغییر توپولوژی (Topology Change Notification)، پیام‌هایی هستند که در صورت بروز تغییر در توپولوژی شبکه ایجاد و پخش می گردند. این تغییر می‌تواند شامل فعال یا غیر فعال شدن لینک یا سوئیچ در شبکه باشد.

پیامTCN پس از ایجاد، به اطلاع سوئیچ Designated خود می‌رسد. سوئیچ Designated نیز طی پیامTCA(Topology Change Acknowledgment)، دریافت پیام را به اطلاع سوئیچ ارسال کننده می‌رساند. سپس سوئیچ Designated پیام TCN را به سوئیچ Designated خود ارسال می نماید.

پاس دادن پیام‌هایTCN بین سوئیچ‌هایDesignated تا زمان رسیدن این پیام به سوئیچ ریشه ادامه می‌یابد. در نهایت سوئیچ ریشه از تمام اتفاقات روی داده در شبکه با خبر خواهد بود.

انواع پورت درSTP

پورت‌هایی که برای اتصالات بین سوئیچ‌ها در شبکه مورد استفاده قرار گرفته‌اند، جهت اجرای پروتکلSTP باید در یکی از وضعیت‌های زیر قرار گیرند. مشخص نمودن این وضعیت بر اساس بررسی معیارهای موجود در پیام هایBPDU صورت می گیرد. از جمله این معیارها می توان به فیلدهای Path cost،BID و Port ID موجود در این پیام ها اشاره نمود.

[1] Convergence

- **Root Port**

این پورت نشان‌دهنده بهترین مسیر برای رسیدن به سوئیچ ریشه می‌باشد. هیچگاه پورت‌های سوئیچ ریشه در این وضعیت قرار نمی گیرند.

هر چند که انتخاب نوع پورت با توجه به فیلدهای مربوطه و بصورت اتوماتیک مشخص می شود، اما شما این امکان را دارید که با تغییر پارامترهای مربوط به اینترفیس مورد نظر، باعث انتخاب آن به عنوانRoot Port شوید.

- **Designated Port**

مسئول برقراری ارتباط بین سگمنت خود و سوئیچ ریشه می باشد. همچنین پورت مقابل Root Port همواره Designated Port می باشد.

تمام پورت های سوئیچ ریشه در این حالت قرار می گیرند.

- **Alternate**

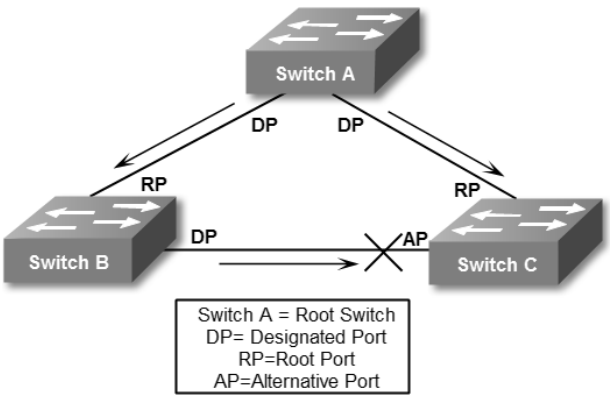
این پورت به عنوان جایگزین پورت Root می باشد. در صورتیکه برای Root Port مشکلی پیش بیاید، از این پورت به عنوان Root استفاده می گردد.

- **Backup**

این پورت به عنوان پشتیبان پورت Designated می‌باشد. در صورتیکه پورت Designated به مشکلی برخورد نماید، از این پورت به عنوان Designated Port استفاده می شود.

پس از انجام مراحل فوق جهت محاسبه بهترین مسیر و تعیین نقش پورت‌ها، پروتکلSTP برای جلوگیری از بوجود آمدن حلقه لایه دو، اقدام به غیر فعال نمودن پورت‌های جایگزین (Alternate و Backup) می‌نماید.

تصویر زیر شامل مثالی جهت نمایش نوع پورت‌ها در فرآیندSTP می باشد:



فرآیند تعیین نقش پورت‌ها

پروتکلSTP برای تعیین نقش پورتهای سوئیچ از پارامترهای کمترینBID، کمترینPath Cost در رسیدن به ریشه و کمترینPort Priority استفاده نموده و در نهایت در صورت برابر بودن همه پارامترهای مذکور، از کمترینPort Number استفاده می نماید.

- **BID**

همانطور که گفته شد پارامترBID(Bridge ID) متشکل از آدرسMAC و مقدارPriority سوئیچ می‌باشد. در صورت وجودVLAN، عددVLAN ID نیز در این پارامتر تاثیر گذار خواهد بود.

- **Path Cost**

هزینه مسیر یا Path Cost، عددی است ۱۶ یا ۳۲ بیتی که محاسبه آن بر اساس پهنای باند اتصالات بین سوئیچ‌ها جهت دستیابی به سوئیچ ریشه انجام می‌پذیرد.

مقدارPath Cost دارای رابطه عکس با پهنای باند بوده و مؤلفه مهمی در زمان اختصاص نقش یک پورت به شمار می‌رود. هر چه مقدارPath Cost کوچکتر باشد، احتمال انتخاب لینک مورد نظر افزایش می‌یابد.

جدول زیر رابطه Path Cost را با پهنای باند نشان می‌دهد:

Bandwidth	STP Cost Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

در صورتیکه بخواهید نقش خاصی را برای یک پورت در جریانSTP در نظر بگیرید، می توانید مقدار Path Cost مربوطه را بصورت دستی تغییر دهید.

- **Port Priority**

این عدد بصورت پیش فرض برابر با 128 می‌باشد. می توانید با تغییر این عدد، در نحوه تخصیص نقش به پورت تاثیرگذار باشید.

- **Port Number**

عدد مربوط به قرار گرفتن پورت بر روی سوئیچ می باشد. به عنوان مثال پورت شماره 20 سوئیچ 2960 بصورت Fastethernet 0/20 نمایش داده می شود. این عدد قابل تغییر نمی باشد.

نسخه‌های STP

پروتکلSTP دارای نسخه‌های استانداردی است که توسطIEEE معرفی گردیده است، ضمن آنکه سیسکو نیز دارای نسخه های STP مخصوص به خود می باشد.

- **STP**

اولین نسخه این پروتکل توسط IEEE و تحت استانداردIEEE 802.1D ارائه گردید. سرعت همگرایی شبکه مبتنی بر پروتکلIEEE 802.1D نامطلوب می باشد. همچنین در زمان ارائه این نسخه هنوز ایده بوجود آمدن VLANها شکل نگرفته بود.

از این نسخه با نام CST (Common STP) نیز یاد می‌شود.

- **PVST**

با توجه به محدودیت‌های استانداردIEEE 802.1D و پشتیبانی نکردن ازVLAN، سیسکو اقدام به معرفی پروتکلPVST(Per VLAN Spanning Tree) نمود. در این استاندارد که مختص سیسکو می باشد، الگوریتمSTA به ازاء هرVLAN بصورت جداگانه اجرا گردیده و هرVLAN دارای Root Switch مخصوص به خود می‌باشد.

- **PVST+**

این پروتکل نسخه بهبود یافته پروتکلPVST بوده و مخصوص تجهیزات سیسکو می‌باشد. به دلیل اینکهPVST دارای ایراداتی از جمله پشتیبانی نکردن از استاندارد IEEE 802.1q بود، سیسکو PVST+ را در جهت رفع ایرادات قبلی معرفی نمود.

- **RSTP**

این پروتکل توسط استاندارد IEEE 802.1w معرفی گردید. پس از معرفی پروتکل‌های سیسکو، سازمانIEEE در جهت اصلاح استانداردهای قبلی خود اقدام به معرفی پروتکل Rapid STP نمود.

با معرفی ویژگی‌هایی از جملهUplinkFast وBackboneFast درRSTP، سرعت همگرایی (Convergence) شبکه در این پروتکل افزایش قابل ملاحظه ای داشت.

- **RPVST+**

در این چشم و هم چشمی بازی‌های تکنولوژیک، سیسکو نیز کم نیاورده و پس از استانداردRSTP اقدام به معرفی استاندارد مخصوص به خود با نام Rapid PVST+ نمود. سیسکو نیز در این پروتکل اقدام به افزایش سرعت همگرایی شبکه نمود.

این پروتکل بصورت پیش فرض در سوئیچ‌های سیسکو بر روی VLAN 1 فعال می‌باشد. همچنین VLANهایی که جدید ایجاد می‌شوند نیز بصورت پیش فرض از پروتکل RPVST+ استفاده می نمایند.

- **MSTP**

این پروتکل که تحت استاندارد IEEE 802.1s انتشار یافت، توانایی گروه‌بندی VLANها و اجرای الگوریتمSTA بر اساس هر گروه را دارد.

در الگوریتمPVST+ به ازاء هرVLAN الگوریتم STA بصورت مستقل اجرا می گردد. این عمل مخصوصا زمانی که تعداد VLANها زیاد باشد می تواند باعث بروز مشکلاتی در شبکه گردد. پروتکلMSTP می‌تواند با گروه‌بندی VLANها، تعداد اجرای الگوریتم STA را به تعداد گروه‌های موجود کاهش دهد. این گروه‌ها کهMST Region نامیده می‌شوند، دارای تنظیماتSTP مشترک می باشند.

این پروتکل با نسخه‌های STP قبلی نیز سازگار بوده و امکان همکاری با آنها را دارد.

توجه داشته باشید پروتکلهایSTP در بعضی از اصطلاحات و ویژگی ها دارای تفاوت‌هایی با یکدیگر هستند. لذا بهتر است قبل از تصمیم گیری جهت اجرای هر کدام از پروتکل‌های فوق به ویژگی‌های آن دقت نمایید.

ویژگی Portfast

ویژگی Portfast به همراه نسخه‌های جدیدترSTP جهت سرعت بخشیدن به پروسه اجرای الگوریتم STA ارائه گردید. فعال شدن این ویژگی بر روی یک پورت، باعث می شود آن پورت از ارسال و دریافت پیام های BPDU خودداری نموده و در پروسهSTP شرکت ننماید.

پورت‌هایی که در پروسهSTP شرکت می نمایند، به مدت زمانی بین ۳۰ تا ۵۰ ثانیه نیاز دارند تا نقش خود را در سوئیچ مشخص نمایند؛ به همین دلیل شرکت نکردن یک پورت در STP باعث آماده به کار شدن سریعتر سوئیچ می گردد.

توجه داشته باشید این خصوصیت باید بر روی پورتهای Access که امکان بوجود آمدن حلقه توسط آنها وجود ندارد، فعال گردد.

سناریو شماره(۵)؛ راه اندازی STP

طرح مسئله:

بله، درست حدس زدید! میریم سراغ آژانس هواپیمایی. بعد از همکاری آژانس با شما، خدا را شکر وضع آژانس روز به روز بهتر می شود. آژانس یک بخش جدید با نام امور گردشگری به مجموعه خود اضافه نموده است. امور گردشگری در واحد شماره ۳ همان برج و در جوار دو واحد قبلی قرار گرفته است. رئیس محترم آژانس از شما خواسته که برای شبکه این واحد نیز فکری کنید!

نیاز سنجی:

برای راه اندازی شبکه در واحد جدید نیاز به خرید یک سوئیچ و دیگر ملزومات گفته شده در سناریوهای قبلی دارید. همچنین ایجاد یکVLAN جدید و اختصاص یک رنج آدرسIP را هم برای بخش جدید در نظر بگیرید.

برای بالابردن پایداری شبکه ما قصد داریم هر سه سوئیچ را به یکدیگر متصل کنیم. اما به دلیل اتصال هر سه سوئیچ به یکدیگر، امکان بروز حلقه لایه دو در شبکه می باشد. لذا برای جلوگیری از این اتفاق ناخوشایند باید اقدام به راه اندازی پروتکل STP در شبکه نماییم.

راه حل:

برای این شبکه طبق روال‌های قبل که در آن استاد شده‌اید عمل کنید. پس از انجام تنظیمات اولیه، سوئیچ جدید را با Revision Number پایین تر در شبکه قرار داده و آن را به عنوان کلاینت در پروتکلVTP پیکربندی نمایید.

می‌توانید برای اطمینان از صفر شدن Revision ابتدا سوئیچ را در حالت Transparent قرار دهید. همزمان پیکربندیVTP و پورت Trunk را بر روی سوئیچ C انجام می‌دهیم:

```
SwitchC>enable
SwitchC#configure terminal
SwitchC(config)#vtp domain MTR
SwitchC(config)#vtp password cisco
SwitchC(config)#vtp version 2
SwitchC(config)#vtp mode client
SwitchC(config)#interface range fastethernet0/23 - 24
SwitchC(config-if-range)#switchport mode trunk
SwitchC(config-if-range)#switchport trunk encapsulation dot1q
```

```
SwitchC(config-if-range)#end
SwitchC#write
```

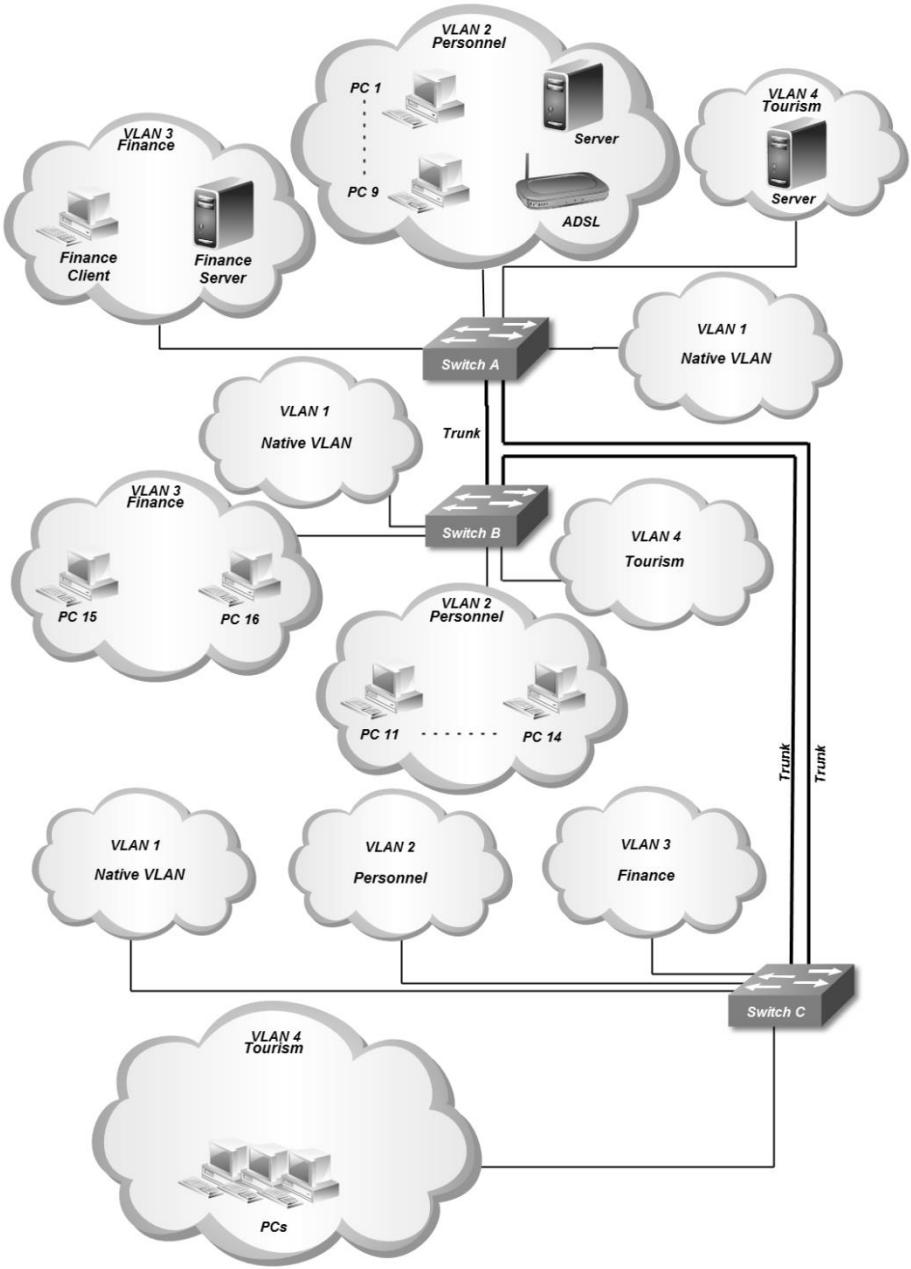
باید برای گروه جدید نیز یکVLAN اختصاصی بوجود آورید. با توجه به اینکه از نظر فیزیکی قصد داریم سرور این گروه را کنار سرور قبلی قرار دهیم، پس این VLAN بر روی سوئیچ های A وC گسترده خواهد بود. برای ایجادVLAN جدید، باید سراغ سوئیچA که به عنوان VTP Server عمل می نماید، برویم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vlan 4
SwitchA(config-vlan)#name tourism
SwitchA(config-vlan)#end
SwitchA#
```

پس از ایجادVLAN جدید، پورتTrunk و پورت متصل به سرور امور گردشگری را نیز بر روی سوئیچ A پیکربندی می نماییم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#interface fastethernet0/24
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#Description  ***Connected to Switch C***
SwitchA(config-if)#Interface fastethernet0/15
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 4
SwitchA(config-if)#Description ***Connected to Server 2***
SwitchA(config-if)#end
SwitchA#write
```

از دستورDescription می توانید برای نوشتن توضیحات در مورد اینترفیس مورد نظر استفاده نمایید. استفاده از این دستور جهت سهولت در مدیریت شبکه و بصورت اختیاری بوده و تاثیری در روند عملیاتی سوئیچ‌ها ندارد.


VLAN 2
Personnel
PC 1
PC 9
Server
ADSL
VLAN 4
Tourism
Server
VLAN 3
Finance
Finance
Client
Finance
Server
Switch A
VLAN 1
Native VLAN
VLAN 1
Native VLAN
Trunk
VLAN 3
Finance
Switch B
VLAN 4
Tourism
PC 15
PC 16
VLAN 2
Personnel
PC 11
PC 14
Trunk
Trunk
VLAN 1
Native VLAN
VLAN 2
Personnel
VLAN 3
Finance
Switch C
VLAN 4
Tourism
PCs

پس از ایجاد VLAN امور گردشگری، می توانید پورتهای مورد نظر سوئیچ C را برای اتصال به این VLAN مشخص نمایید.

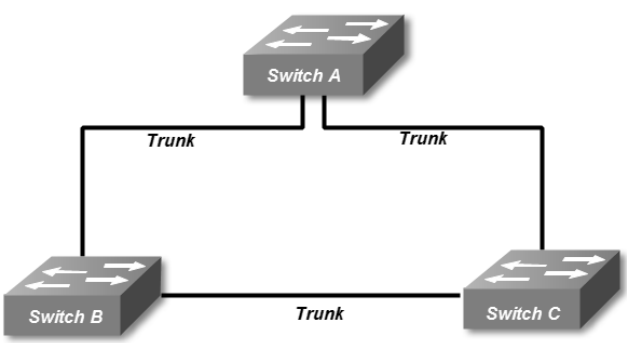
```
SwitchC>enable
SwitchC#configure terminal
SwitchC(config)#interface range fastethernet0/1 - 10
SwitchC(config-if-range)#switchport mode access
SwitchC(config-if-range)#switchport access vlan 4
SwitchC(config-if-range)#end
SwitchC#write
```

یک پورتTrunk نیز بر روی سوئیچB جهت برقراری ارتباط با سوئیچC پیکربندی می نماییم.

```
SwitchB>enable
SwitchB#configure terminal
SwitchB(config)#interface fastethernet0/24
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk encapsulation dot1q
SwitchB(config-if)#Description  ***Connected to Switch C***
SwitchB(config-if)#end
SwitchB#write
```

در این سناریو برای ما نحوه اتصال سوئیچ ها به یکدیگر اهمیت دارد. ما میخواهیم با داشتن افزونگی لینک‌ها ضمن برقراری ارتباط بین سوئیچ‌های شبکه، پایداری شبکه را نیز افزایش دهیم. به همین دلیل است که هر سه سوئیچ را با پورت های Trunk به یکدیگر متصل نموده‌ایم.

به دلیل اتصال هر سه سوئیچ به یکدیگر، بوجود آمدن حلقه لایه دو در شبکه اجتناب ناپذیر می‌باشد. در اینجاست که برای جلوگیری از این اتفاق ناخوشایند اقدام به راه اندازی پروتکل STP در شبکه می‌نماییم.



یکی از مرسوم‌ترین پروتکل‌هایSTP که توسط کارشناسان سیسکو نیز مورد استفاده قرار می‌گیرد، پروتکلRPVST+ می‌باشد. این پروتکل بصورت پیش فرض بر روی سوئیچ‌های سیسکو فعال می باشد. لذا در این سناریو ما هم از RPVST+ استفاده می کنیم.

هر چند که مشخص نمودن سوئیچ ریشه بصورت دستی، اختیاری است اما از آنجا که پارتی بازی لذت بخش است و نمی توان از این گزینه صرف نظر نمود! در گام اول اقدام به مشخص نمودن سوئیچ ریشه نموده و پیکربندی مربوط به آن را انجام می دهیم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#spanning-tree mode rapid-pvst
SwitchA(config)#spanning-tree vlan 1
SwitchA(config)#spanning-tree vlan 2
SwitchA(config)#spanning-tree vlan 3
SwitchA(config)#spanning-tree vlan 4
SwitchA(config)#spanning-tree vlan 1  root primary
SwitchA(config)#spanning-tree vlan 2  root primary
SwitchA(config)#spanning-tree vlan 3  root secondary
SwitchA(config)#spanning-tree vlan 4  root secondary
SwitchA(config)#interface range fastethernet 0/2 – 23
SwitchA(config-if-range)#spanning-tree portfast
SwitchA(config-if-range)#end
SwitchA#write
```

همانطور که می دانید پروتکل RPVST+ به ازاء هرVLAN یک سوئیچ ریشه انتخاب نموده و الگوریتمSTA را بر اساس همان سوئیچ برایVLAN مورد نظر اجرا می نماید. در زمان پیکربندی STP، شما می توانید به ازاء هرVLAN یکی از سوئیچ های شبکه را به عنوان سوئیچ ریشه انتخاب نمایید.

اگرسوئیچ ریشه برای هرVLAN متفاوت باشد، در نتیجه نقش پورتهای برقرار کننده اتصالات Trunk نیز به ازاء هر پروسهSTA متفاوت خواهد بود. این تفاوت نقش پورت‌ها باعث بوجود آمدن امکان استفاده همزمان از تمام لینک‌ها گردیده و خاصیت Load Balancing را در اختیار شما قرار می دهد.

برای اینکه ما نیز از Load Balancing بی نصیب نمانیم، اختصاص سوئیچ ریشه VLANها را بین سوئیچ A و B تقسیم می نماییم.

همچنین با استفاده از دستور portfast می توانیم پورت‌هایی که به عنوانAccess مورد استفاده قرار می گیرند را از پروسهSTP حذف نموده و باعث افزایش سرعت آماده به کار شدن سوئیچ گردید.

```
SwitchB>enable
SwitchB#configure terminal
SwitchB(config)#spanning-tree mode rapid-pvst
SwitchB(config)#spanning-tree vlan 1
SwitchB(config)#spanning-tree vlan 2
SwitchB(config)#spanning-tree vlan 3
SwitchB(config)#spanning-tree vlan 4
SwitchB(config)#spanning-tree vlan 3  root primary
SwitchB(config)#spanning-tree vlan 4  root primary
SwitchB(config)#spanning-tree vlan 1  root secandary
SwitchB(config)#spanning-tree vlan 2  root secondary
SwitchA(config)#interface range fastethernet 0/2 – 23
SwitchA(config-if-range)#spanning-tree portfast
SwitchB(config-if-range)#end
SwitchB#write
```

همانطور که گفتیم Rapid PVST+ بصورت پیش فرض بر روی VLAN 1 و تمام VLANهایی که توسط شما ایجاد می گردد فعال است. لذا اجرای دستورات فوق جهت آشنایی شما با فرآیند اجرای پروتکل STP می باشد.

توسط دستور root primary، سوئیچ B را به عنوان سوئیچ ریشه VLAN 3&4 انتخاب نمودیم. در ضمن با دستور root secondary، سوئیچ را به عنوان پشتیبان VLAN 1&2 در نظر گرفتیم. در صورت از مدار خارج شدن سوئیچ A، سوئیچ B به عنوان سوئیچ ریشه برای VLANهای 2 و 1 انتخاب می شود.

سوئیچ C را نیز بصورت زیر پیکربندی می نماییم.

```
SwitchC>enable
SwitchC#configure terminal
SwitchC(config)#spanning-tree mode rapid-pvst
SwitchC(config)#spanning-tree vlan 1
SwitchC(config)#spanning-tree vlan 2
SwitchC(config)#spanning-tree vlan 3
SwitchC(config)#spanning-tree vlan 4
SwitchA(config)#interface range fastethernet 0/1 – 22
SwitchA(config-if-range)#spanning-tree portfast
SwitchC(config-if-range)#end
SwitchC#write
```

در سوئیچ C نیز اقدام به راه اندازی پروتکل Rapid PVST+ و مشخص کردن اینترفیس‌های Portfast می‌نمائیم.

با توجه به اینکه هر سه سوئیچ با پهنای باند یکسان و توسط پورتهای Fast Ethernet به یکدیگر متصل شده و شرایط خاصی هم مد نظر ما نیست، نیازی به تغییر Path Cost و Port ID در این سناریو دیده نمی شود.

طریقه عملکرد:

با توجه به اینکه ما توسط پارتی بازی سوئیچ ریشه را مشخص کردیم، سوئیچ B وC با دریافت پیام "من ریشه هستم" از سوئیچ A، با توجه به عدد Priority آن و بدون بررسی آدرس MAC، سوئیچ A را به عنوان سوئیچ ریشه برای VLANهای 1 و 2 قبول کرده و خود را از دور رقابت بر سر ریشه شدن بیرون می کشند.

اما برای VLANهای 3 و4 همین اتفاق برای سوئیچB صورت می‌پذیرد. و در این گردونه ریشه شدن، فقط سر سوئیچ C بی کلاه می ماند!

در صورتیکه سوئیچ ریشه را مشخص نمی کردیم، مقدار عدد Priority بصورت پیش فرض باقی مانده و در همه سوئیچ ها برابر می بود، به همین دلیل انتخاب ریشه بر اساس آدرس MAC سوئیچ انجام می گرفت.

پس از مشخص شدن ریشه باید تمام سوئیچ‌های دیگر با مشخص کردن نقش پورت‌های خود، مسیر رسیدن به ریشه را انتخاب نموده و لینک‌های اضافی که باعث بوجود آمدن چرخه لایه دو می شوند را غیر فعال کنند.

به دلیل اینکه عمل فوق به ازاء هرVLAN انجام می پذیرد و ما نقش ریشه را بین دو سوئیچ تقسیم کردیم، می توانیم از لینک‌ها برای VLANهای مختلف در نقش‌های مختلف استفاده نموده و باعث ایجاد LoadBalancing در کنار Redundancy شویم.

با توجه به اینکه ما به ازاء VLANهای مختلف دارای سوئیچ ریشه متفاوت هستیم، پس به ازاء VLANهای مختلف نقش سوئیچ ها را بررسی می نماییم.

نقش پورت ها برای VLAN 1 & 2

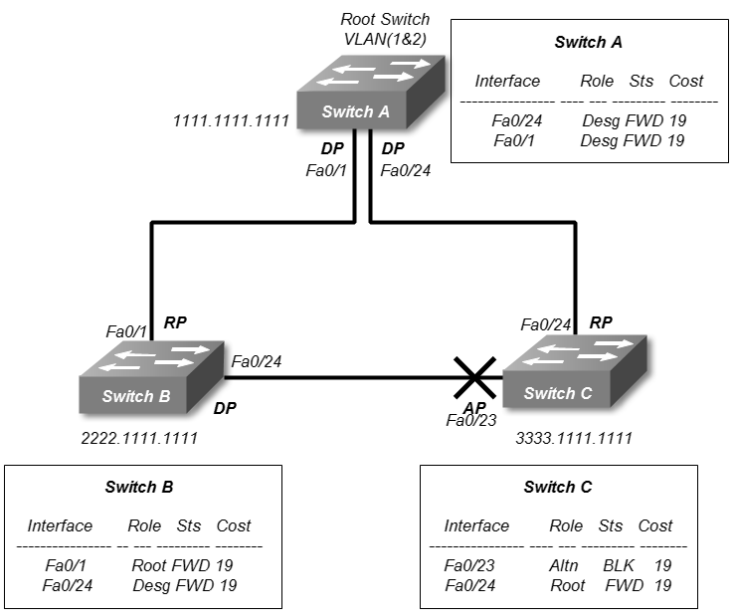
برای VLANهای 1 و2 سوئیچA به عنوان Root Switch بوده و با توجه به اینکه تمام لینک‌ها بر روی پورتFastethernet می‌باشند و هیچ پارتی بازی هم توسط ما برای نقش پورت‌ها انجام نگرفته، پس نقش پورت‌ها با توجه به معیارهای گفته شده مشخص خواهد شد.

تمام پورتهای سوئیچ ریشه که به دیگر سوئیچ ها متصل است، در وضعیتDP قرار می‌گیرند. البته اگر دو پورت سوئیچ ریشه به یک سوئیچ متصل باشد یک پورت به عنوانDP و پورت دیگر به عنوانBackup انتخاب می شود.

سوئیچ‌های B وC دارای یک لینک مستقیم و Path Cost برابر به سوئیچ ریشه می باشند. پس بهترین مسیر برای رسیدن به ریشه برای هر دو سوئیچ لینک‌های مستقیم بوده و این پورت‌ها به دلیل برقراری اتصال با سوئیچ ریشه، به عنوانRP انتخاب می گردند.

به‌دلیل اینکه سوئیچB دارایMAC آدرس کوچکتر و در نتیجهBID کوچکتری نسبت به سوئیچ C می باشد، پورت‌های برقرار کننده لینک بین سوئیچB وC برای سوئیچ B به عنوان DP و برای سوئیچC به دلیل بهترین مسیر جایگزین برای رسیدن به سوئیچ ریشه، در نقش AP قرار می‌گیرد.

در تصویر زیر وضعیت سوئیچ‌ها، نقش پورت‌ها و همچنین خروجی دستور show spanning-tree را مشاهده می نمایید.



نقش پورت ها برای VLAN 3 & 4

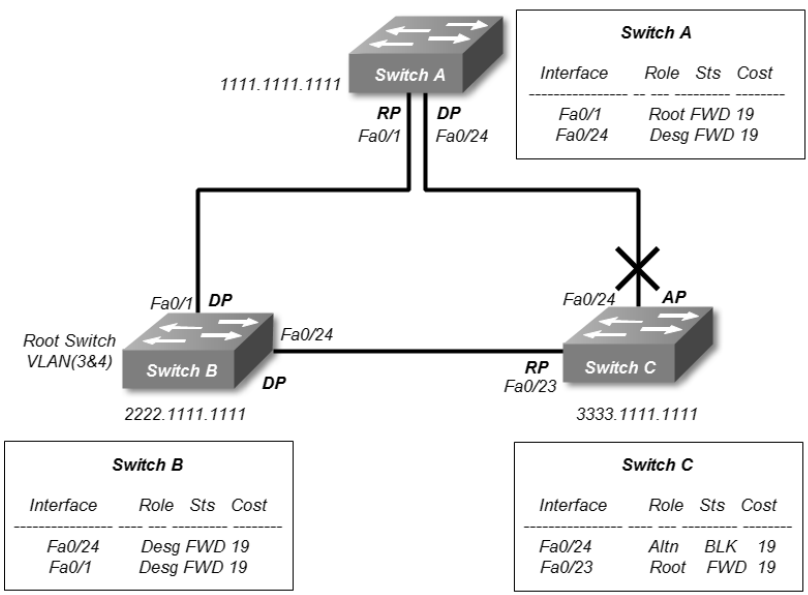
برای VLANهای 3 و4 سوئیچ ریشه، سوئیچ B بوده و با توجه به اینکه تمام لینک‌ها بر روی پورت Fastethernet می باشد و هیچ پارتی بازی هم توسط ما برای نقش پورت‌ها انجام نگرفته است پس نقش پورت‌ها با توجه به معیارهای گفته شده مشخص خواهد شد.

تمام پورتهای سوئیچB که سوئیچ ریشه بوده و به دیگر سوئیچ ها متصل است، نقشDP را به عهده می گیرد.

پورتهای سوئیچA وC که دارای اتصال مستقیم با سوئیچ ریشه می‌باشند، به عنوانRP تعیین می گردند.

با توجه به آدرس MAC سوئیچ A که باعث بوجود آمدنBID کوچکتری نسبت به سوئیچC می‌گردد، نقش پورتهای برقرار کننده اتصال بین این دو سوئیچ نیز تعیین می گردد. پورت سوئیچ C به عنوان AP و بهترین مسیر جایگزین دسترسی به ریشه و پورت سوئیچ A به عنوان DP مشخص می گردد.

در تصویر زیر وضعیت سوئیچ‌ها، نقش پورت‌ها و همچنین خروجی دستور show spanning-tree را مشاهده می نمایید.



نکته حائز اهمیت در دو تصویر فوق این است که در صورت وجود چند سوئیچ ریشه در شبکه، یک پورت می‌تواند برای عبور ترافیک یکVLAN در حالت غیرفعال و برای عبور ترافیک VLAN دیگر در حالت فعال قرار داشته باشد. این اتفاق می تواند ویژگی LoadBalancing را برای شبکه ما به ارمغان آورد.

منبع دستورات Command Reference:

Enabling Rapid PVST+		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **spanning-tree mode rapid-pvst**	Enables Rapid PVST+ on the switch. Rapid PVST+ is the default spanning tree mode.

Enabling Rapid PVST+ per VLAN		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **spanning-tree** *vlan-range*	Enables Rapid PVST+ (default STP) on a per VLAN basis. The *vlan-range* value can be 2 through 4094

Disable Rapid PVST+ per VLAN		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **no spanning-tree** *vlan-range*	Disables Rapid PVST+ on the specified VLAN.

Configuring the Root Bridge ID		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]	Configures a software switch as the primary root bridge. The *vlan-range* value can be 2 through 4094 (except reserved VLAN values.) The *dia* default is 7. The *hello-time* can be from 1 to 10 seconds, and the default value is 2 seconds.

secondary root bridge		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]	Configures a software switch as the secondary root bridge. The *vlan-range* value can be 2 through 4094 (except reserved VLAN values.) The *dia* default is 7. The *hello-time* can be from 1 to 10 seconds, and the default value is 2 seconds.

Configuring the Rapid PVST+ Port Priority		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **interface** *type slot/port*	Specifies the interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority*	Configures the port priority for the LAN interface. The *priority* value can be from 0 to 224. The lower the value, the higher the priority. The priority values are 0, 32, 64, 96, 128, 160, 192, and 224. All other values are rejected. The default value is 128.

Configuring the Rapid PVST+ Pathcost Method and Port Cost		
	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **spanning-tree pathcost method** {**long** | **short**}	Selects the method used for Rapid PVST+ pathcost calculations. The default method is the short method.
Step 3	switch(config)# **interface** *type slot/port*	Specifies the interface to configure, and enters the interface configuration mode.
Step 4	switch(config-if)# **spanning-tree** [**vlan** *vlan-id*] **cost** [*value* | **auto**]	Configures the port cost for the LAN interface. The cost value, depending on the pathcost calculation method, can be as follows: • short—1 to 65535 • long—1 to 200000000 **Note** You configure this parameter per port on access ports and per VLAN on trunk ports. The default is **auto**, which sets the port cost on both the pathcost calculation method and the media speed.

☑مبحث چهارم

Inter-VLAN Routing

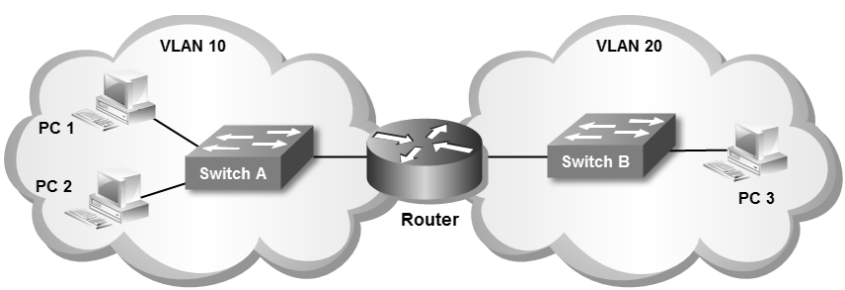
عملیات مسیریابی بین شبکه‌های مجازی را Inter-VLAN Routing می‌نامند. همانطور که قبلا گفته شد ایجادVLAN مثل اره نمودن سوئیچ‌ها بوده و همانگونه که کلاینت‌های دو سوئیچ فیزیکی مجزا امکان برقراری ارتباط با یکدیگر را ندارند، کلاینت‌های VLANهای مختلف هم حتی اگر روی یک سوئیچ فیزیکی قرار داشته باشند امکان برقراری ارتباط با یکدیگر را نخواهند داشت.

برقراری ارتباط بین دو شبکه با رنج آدرسIP مختلف، در لایه دوم مدل OSI امکان پذیر نیست. با توجه به اینکه سوئیچ‌ها بطور معمول در لایه دو کار می کنند، پس برای برقراری ارتباط بین دو شبکه با آدرسIP مختلف نیاز به تجهیزاتی با قابلیت مسیریابی در لایه سوم مدل OSI را داریم. وظیفه مسیریابی در لایه سوم را می توان توسط یک روتر و یا یک سوئیچ Multilayer انجام داد.

به دلیل اینکه تجهیزات لایه ۳ از عبور پیام‌هایBroadcast جلوگیری به عمل می‌آورند، با اضافه شدن این تجهیزات جهت برقراری ارتباط بین VLANها، هیچ تغییری در محدوده حوزه پخش همگانی و حوزه تصادم نسبت به حالت قبل رخ نمی دهد.

توپولوژی پایه Inter-VLAN Routing

توپولوژی پایه که جهت اجرای Inter-VLAN Routing می‌توان در نظر گرفت، عضویت مستقل هر اینترفیس روتر در یکVLAN می‌باشد. در اینصورت پورت‌های مسیریاب امکان برقراری ارتباط بین زیر شبکه‌ها را فراهم می‌آورند.



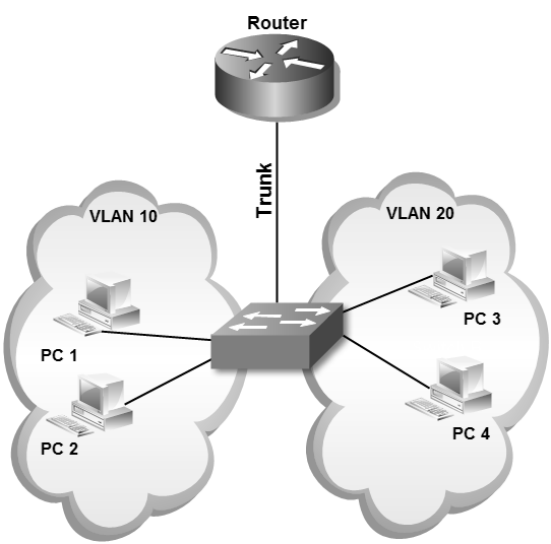
زمانی که PC1 در VLAN 10 می‌خواهد با PC2 در همان VLAN ارتباط برقرار نماید، Switch A بدون آنکه به مسیریاب نیاز داشته باشد می‌تواند وظیفه انتقال اطلاعات را بین دو کلاینت انجام دهد. اما زمانی که PC1 در VLAN 10 قصد برقراری ارتباط با PC3 در VLAN 20 را داشته باشد، سوئیچ اقدام به ارسال بسته به همان اینترفیس مسیریاب که مسئول هدایت ترافیک VALN 10 است، می‌نماید. روتر با بررسی اطلاعات بسته دریافتی بر اساس جدول مسیریابی خود، اقدام به ارسال بسته به اینترفیس موجود در VLAN مورد نظر بر روی سوئیچ B می‌نماید. در نهایت Switch B بسته را به PC3 تحویل می دهد.

Inter-VLAN Routing بر روی یک اتصال Trunk

در حالت قبل به‌دلیل اختصاص هر اینترفیس مسیریاب به یک VLAN، اجباری در Trunk بودن لینک‌های بین مسیریاب وسوئیچ نبوده و می توانستید با عضویت اینترفیس در VLAN مورد نظر، ارتباط بین کلاینت های VLANها را برقرار نمایید.

اشکال حالت قبل در مواقعی مشخص می شود که تعداد VLANها زیاد باشد. با توجه به اینکه معمولا تعداد اینترفیس‌های روتر محدود می باشد، اختصاص هر اینترفیس به یک VLAN باعث افزایش هزینه‌های اجرای شبکه می گردد.

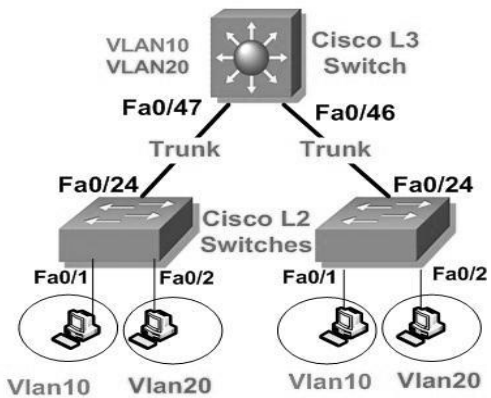
برای حل مشکل فوق، می‌توان با پیکربندی یک اینترفیس مسیریاب بصورت Trunk و اتصال آن به پورت Trunk سوئیچ، اطلاعات چندین VLAN مختلف را بصورت همزمان بر روی یک اینترفیس انتقال داد.



در اینصورت باید به ازاء هرVLAN یکSubinterface بر روی پورتTrunk مسیریاب ایجاد نمود تا به عنوان رابط لایه سه، امکان مسیریابی بین شبکه‌های مختلف را میسر نماید.

Inter-VLAN Routing توسط سوئیچ Multilayer

امکان راه اندازیInter-VLAN Routing توسط سوئیچ‌هایی که قابلیت مسیریابی در لایه ۳ را دارند، نیز میسر می‌باشد. در صورت وجود سوئیچ‌هایMultilayer در شبکه می‌توان ضمن استفاده از آنها به عنوان سوئیچ مرکزی، عملیات مسیریابی را نیز بر عهده آنها گذاشت.



ایجاد اینترفیس مجازی SVI(Switch Virtual Interface) به ازاء هرVLAN در سوئیچ Multilayer، باعث برقراری ارتباط بینVLANها می‌گردد. در این حالت همچنان لینک ارتباطی بین سوئیچMultilayer با دیگر سوئیچ های شبکه نیز بصورتTrunk خواهد بود.

انواع پورت لایه ۳ در سوئیچ Multilayer

سوئیچ‌هایMultilayer دارای سه نوع پورت با قابلیت کار در لایه سه می باشند. قابلیت‌های ارائه شده توسط هر نوع پورت متفاوت بوده و مورد استفاده مخصوص به خود را دارند. هر چند تمام سوئیچ هایMultilayer قابلیت کار در لایه ۳ را دارند ولی پشتیبانی از سه پورت زیر نسبت به مدل سوئیچ ها، ممکن است متفاوت باشد.

۱- **Routed Port**

در واقع Routed Port یک پورت فیزیکی لایه۳ شبیه به پورت های مسیریاب می باشد. برخلاف پورتهای معمولی سوئیچ، Routed Port عضوی از یک VLAN نمی باشد.

همچنین کاربرد این پورت کاملا بصورت فیزیکی بوده و ایجاد Subinterface بر روی آن امکان پذیر نیست.

پورتهای سوئیچMultilayer بصورت پیش فرض در وضعیت لایه۲ قرار دارند، لذا برای فعال ساختن یک پورت به عنوانRouted Port، باید دستورno switchport را برروی اینترفیس مورد نظر که قابلیت کار در لایه ۳ را دارد، اعمال نمود.

۲- اینترفیس مجازی سوئیچ (SVI)

اینترفیس مجازی(Switch Virtual Interface)، جهت ارائه امکانات پایه‌ای لایه ۳ بر روی سوئیچ ایجاد گردیده است.

اینترفیس مجازی صرفا جهت برقراری ارتباط بین VLANها می‌باشد. به‌دلیل اینکه هر SVI بر اساس شمارهVLAN قابل دسترسی می‌باشد، قبل از ایجاد SVI باید از وجود شماره VLAN متناظر در VLAN Database سوئیچ اطمینان حاصل نمایید.

اگر چه این ویژگی جهت فراهم کردن امکانات لایه ۳ بر روی سوئیچ ارائه گردیده، ولی نباید انتظار داشت این اینترفیس‌ها تمام خصوصیت‌های موجود در اینترفیس‌های یک روتر را در اختیار شما قرار دهند. محدودیت‌های SVI در پشتیبانی از خصوصیت‌های لایه ۳، در نسخه های مختلف IOS سیسکو متفاوت می باشد.

آدرس شبکه این اینترفیس‌ها در جدول مسیریابی[1] سوئیچ لایه ۳، بصورت Directly Connected قرار گرفته و نیازی به راه اندازی پروتکل مسیریابی و یا وارد کردن دستور اضافی جهت درج در جدول مسیریابی ندارند.

۳- اینترفیس مجازی پل (BVI)

اینترفیس مجازی پل(Bridge Virtual Interface)، جهت ایجاد پل ارتباطی بین دو اینترفیس لایه ۳ کاربرد دارد.

زمانی که اقدام به برقراری پل بین دو اینترفیس لایه ۳ می‌نمایید، این پورت‌ها عمل بررسی بسته‌ها را انجام نداده و همانند سوئیچ صرفا اقدام به انتقال اطلاعات می‌نمایند. در این زمانBVI که با عضویت اینترفیس‌های مورد نظر ایجاد گردیده، به عنوان اینترفیس لایه ۳، عهده دار انجام امور لایه ۳ مربوط به بسته‌ها می شود.

[1] Routing Table

سوئیچینگ لایه ۳

سوئیچ‌هایMultilayer سیسکو جهت انجام عملیات سوئیچینگ و مسیریابی ضمن استفاده از ASIC، با ارائه تکنیک‌هایی نیز سرعت عمل خود را افزایش داده‌اند. از جمله روشهای استفاده شده در سوئیچ‌هایMultilayer بهره‌گیری از دو جدول مجزا برای انجام سریعتر عملیات مربوط به لایه‌های دو و سه می‌باشد.

- **CAM Table**

سوئیچ جهت انجام عملیات سوئیچینگ دارای جدولی به نام Content Addressable Memory می‌باشد. این جدول حاوی شماره پورت متناظر با آدرسMAC تجهیزات متصل شده به سوئیچ می باشد.

- **TCAM Table**

سوئیچ‌هایMultilayer سیسکو جهت انجام عملیات مسیریابی دارای جدولی به نام Ternary Content Addressable Memory می‌باشند. این جدول حاوی QoS[1]، ACL [2] و دیگر اطلاعات مربوط به لایه ۳ می‌باشد.

نحوه عملکرد جدولTCAM را توسط اصطلاحVMR توصیف می‌نمایند. اصطلاحVMR بر گرفته از کلماتValue, Mask, Result است که مراحل انجام کار درTCAM را ذکر می‌کند. Value به انطباق با الگو اشاره دارد. از جمله پارامترهایی که توسطValue مورد بررسی قرار می‌گیرد می‌توان به آدرسIP، پورت‌ها و مقدارDSCP اشاره نمود. Mask نیز مشخص کنندهPrefix آدرس است. و در نهایتResult بیانگر اعمال Permit یا Deny به دیتا می باشد. این تصمیم گیری بر اساسACL و QoS انجام می پذیرد.

جدولTCAM نقش مهمی در تسریع مسیریابی در سوئیچ‌های Multilayer و روترها ایفا می‌کند.

تکنولوژیCEF

CEF(Cisco Express Forwarding)، یک تکنولوژی پیشرفته سوئیچینگ لایه سوم می باشد. این تکنولوژی مخصوص سیسکو بوده و جهت بهینه‌سازی کارایی[3] و مقیاس پذیری[4] برای شبکه‌هایی با الگوهای ترافیکی بزرگ و پویا استفاده می گردد.

---

[1] Quality of Service
[2] Access List
[3] Performance
[4] Scalability

تکنولوژیCEF برای سرعت بخشیدن به انجام عملیات خود از سخت افزارASIC بهره می‌برد. اگر چه می‌توان ازCEF در هر کجای شبکه استفاده نمود، اما این تکنولوژی معمولا در سوئیچ‌های واقع در ستون فقرات(Backbone) شبکه مورد استفاده قرار می‌گیرد. به همین دلیل این ویژگی روی سری خاصی از سوئیچ‌هایMultilayer و روترها مثل سری‌های 7000، 7200، 7500 و 12000 در دسترس می‌باشد.

اجزای CEF

- **جدول FIB**

FIB(Forwarding Information Base) مفهومی شبیه جداول مسیریابی و پایگاه داده دارد. ضمن نگهداری یک نسخه از اطلاعات موجود در جدول مسیریابی، تمام تغییراتی که در جدول مسیریابی بروز می شوند نیز در جدول FIB منعکس می گردد. به همین دلیل FIB همواره دارای یک نسخه آینه‌ای[1] از اطلاعات موجود در جدول مسیریابی می‌باشد.

همچنینFIB اقدام به نگهداری اطلاعات مربوط به هاب بعدی[2] بر اساس اطلاعات موجود در جدول مسیریابی می‌نماید. از آنجا که یک ارتباط یک به یک بین اطلاعات موجود در FIB با اطلاعات جدول مسیریابی وجود دارد، در نتیجهFIB شامل تمام مسیرهای شناخته شده بوده که با حذف نیاز به نگهداری Route Cache، توانسته باعث افزایش سرعت سوئیچینگ گردد.

- **جدول مجاورت**

جدول مجاورت(Adjacency Table)، وظیفه نگهداری اطلاعات آدرس لایه ۲ مربوط به Next hub را به ازاء تمام مسیرهای موجود در جدول FIB، برعهده دارد.

حالت‌های عملکرد CEF

تکنولوژیCEF را می‌توان در یکی از دو حالت عملکردی زیر مورد استفاده قرار دارد.

---

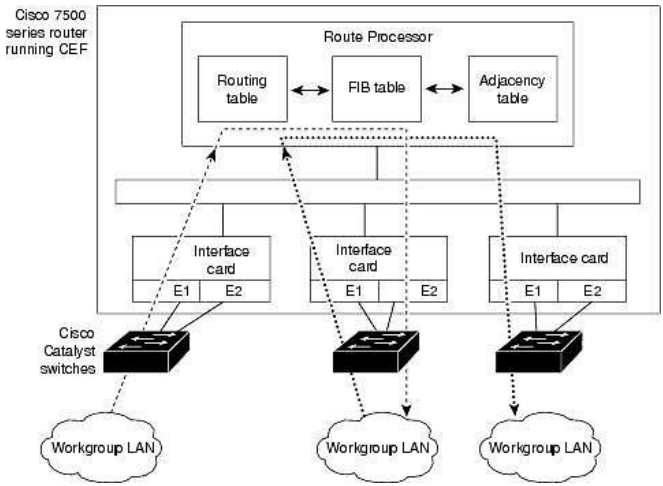
[1] Mirror
[2] Next hub

- **حالت CEF مرکزی**[1]

هنگامی که CEF فعال می گردد، جداول FIB و Adjacency بر روی پردازنده مسیریاب تشکیل می‌گردد. در این حالت بار پردازشی مسیریابی CEF بر روی پردازنده اصلی دستگاه تحمیل می گردد.

این حالت در زمانی که Line Card[۲] در دسترس نباشد و یا هنگامی که قصد استفاده از ویژگی‌های ناسازگار با dCEF را دارید، می تواند مورد استفاده قرار گیرد.

تصویر زیر نشان دهنده روابط بین جداول مسیریابی، FIB و مجاورت در حالت CEF مرکزی می باشد.



- **حالت CEF توزیع شده**[3]

هنگام فعال بودن dCEF، یک نسخه مشابه از محتویات جداول FIB و مجاورت، بر روی Line Card موجود از قبیل VIP[4] و یا GSR[5] نگهداری می‌گردد.

در این حالت عملیات مربوط به CEF بر روی Line Card اجرا شده و بار پردازشی CEF از روی پردازشگر اصلی دستگاه بر روی Line Card مورد نظر منتقل می شود.

---

[1] Central CEF Mode

[۲]. Line Card ها جهت فراهم آوردن اینترفیس و یا سرویس خاصی به تجهیزات شبکه‌ای سیسکو اضافه می گردند.

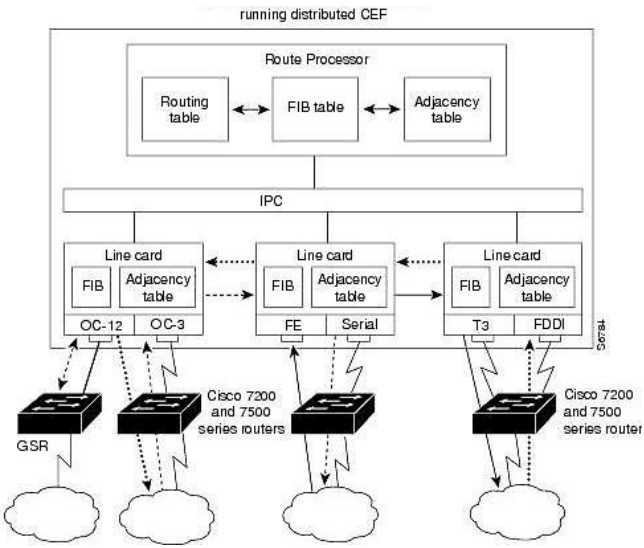
[3] Distributed CEF Mode

[4] Versatile Interface Processor

[5] Gigabit Switch Router

dCEF برای حصول اطمینان از همسان سازی اطلاعات بین Line Card و پردازشگر دستگاه، از مکانیسمی به نامIPC[1] استفاده می نماید.

تصویر زیر نشان دهنده روابط بین پردازشگر و Line Card در حالت dCEF می‌باشد.



نکته: تجهیزات سوئیچ و روتر سیسکو با توجه به مدل، ممکن است فقط امکان راه اندازی یکی از حالت‌های CEF و یا dCEF را داشته باشند.

پشتیبانی رسانه‌ها درCEF

در حال حاضرCEF از رسانههای ارتباطی ATM/AAL5snap، ATM/AAL5mux، ATM/AAL5nlpid، Frame Relay، Ethernet،FDDI،PPP،HDLCوtunnels پشتیبانی می‌نماید.

LoadBalancing در CEF

LoadBalancing امکان بهینه سازی استفاده از منابع شبکه را توسط توزیع ترافیک بر روی مسیرهای متعدد برای ارسال دیتا به یک مقصد خاص، فراهم می نماید. پایه LoadBalancing درCEF بر اساس ترکیبی از اطلاعات موجود در بسته های مبدا و مقصد انجام می گیرد.

[1] Inter Process Communication

در CEF عمل LoadBalancing در یکی از دو حالت زیر انجام می پذیرد.

- **Per-Destination**

این حالت که بصورت پیش فرض در زمان اجرای CEF بر روی دستگاه فعال می باشد، توزیع ترافیک را بر اساس آدرس مقصد مورد نظر انجام می دهد.

در حالت Per-Destination استفاده از لینک‌ها بر اساس هر جفت آدرس منبع و مقصد انجام می‌پذیرد. به عبارت دیگر دستگاه بر اساس هر آدرس مبدا و مقصد که می‌خواهند با یکدیگر ارتباط برقرار نمایند یک لینک را انتخاب نموده و در صورت تغییر هر یک از طرفین، ممکن است لینک مورد استفاده نیز تغییر پیدا کند.

- **Per-Packet**

در این حالت تعادل سازی ترافیک بر اساس تعداد بسته‌ها انجام پذیرفته و توجهی به آدرس مبدا و مقصد نخواهد شد.

Per-Packet از روشRound-Robin برای ارسال اطلاعات استفاده می‌نماید. این روش با ارسال هر بسته بر روی یک لینک، توزیع ترافیک بر روی چند مسیر مختلف را تضمین می‌نماید.

به‌دلیل اینکه در این حالت ارسال اطلاعات بر اساس حجم ترافیک انجام می‌پذیرد، حتی ممکن است بسته‌های دیتا بین یک مبدا و مقصد مشخص از لینک‌های مختلفی ارسال گردند. ارسال پراکنده بسته‌های دیتا می تواند تاثیر نامطلوبی در عملکرد داده‌های وابسته به توالی مثل VoIP ایجاد نماید.

مرجع دستور CEF

جهت راه اندازیCEF می توانید از دستورات زیر استفاده نمایید:

هدف	دستور
جهت فعال شدن حالت CEF	ip cef switch
جهت فعال شدن حالت dCEF	ip cef distributed switch
غیر فعال نمودن CEF	no ip cef switch
غیر فعال نمودن dCEF	no ip cef distributed switch
غیرفعال کردن CEF یا dCEF بر روی یک اینترفیس	no ip route-cache cef
غیرفعال کردن LoadBalancing بر اساس مقصد	no ip load-sharing per-destination
فعال کردن LoadBalancing بر اساس بسته	ip load-sharing per-packet
بررسی وضعیت CEF	show ip cef

سناریو شماره(۶)؛ راه اندازیInter-VLAN Routing توسط روتر

طرح مسئله:

در سناریوهای قبلی با ایجاد VLANهای مختلف در آژانس هواپیمایی، باعث قطع ارتباط کلاینت‌های هر شبکه با دنیای خارج آن شده‌ایم. با این کار نه تنها ارتباط بین پرسنل بخشهای مختلف، بلکه ارتباط آنها با اینترنت نیز قطع شده است. اما یک اصل را فراموش نکنید: پس از هر قطع کردنی یک وصل کردن وجود دارد!

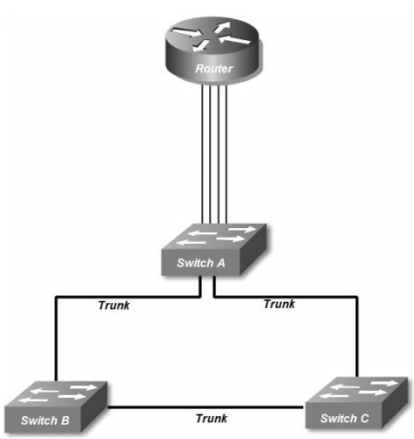
ما برای وصل کردن آمدیم نی برای فصل کردن آمدیم

در حال حاضر آقای رئیس خواستار دسترسی تمام کلاینت‌ها به اینترنت شده و طبق معمول انجام این کار را بر عهده شما گذاشته است.

نیاز سنجی:

برای راه اندازی Inter-VLAN Routing نیاز به تجهیزاتی با قابلیت مسیریابی لایه ۳ داریم. در این سناریو از یک روتر(مسیریاب) برای اجرای عملیات استفاده می‌کنیم. به دلیل اینکه میخواهیم هر اینترفیس مسیریاب در یک VLAN قرار گیرد، نیاز به یک روتر با ۴ عدد اینترفیس ایترنت داریم. به دلیل اینکه در VLAN 1 هیچ کلاینتی نداریم، از اتصال این VLAN به روتر صرف نظر می‌کنیم.

یکVLAN جدید با یک رنجIP هم برای اینترنت نیاز داریم که مودم ADSL را در آن شبکه قرار دهیم. البته روتر توسط کارتADSL می‌تواند نقش مودم را هم بر عهده بگیرد، ولی در این سناریو ما از همان مودم ADSL استفاده می کنیم.



راه حل:

ابتدا یکVLAN جدید با نام اینترنت ایجاد کرده و مودمADSL که به پورت۲۳ سوئیچ A متصل است را در آن شبکه قرار می‌دهیم. همچنین رنج آدرس 192.168.201.128/25 را برای کلاینت های این VLAN در نظر می گیریم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vlan 10
SwitchA(config-vlan)#name internet
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/23
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 10
SwitchA(config-if)#end
SwitchA#write
```

پس از پیکربندی اولیه روتر، اینترفیس‌های روتر را به سوئیچ متصل کرده و هر کدام را عضو یک VLAN قرار می دهیم.

هر چند که می‌توانیم روتر را به هر کدام از سوئیچ‌ها متصل کنیم ولی ترجیحا آنرا به سوئیچ A متصل کرده تا بتوانیم روتر را داخل رک مرکزی قرار دهیم. ۴ پورت شماره های ۱۵ تا ۱۸ سوئیچ A را به VLANهای مختلف اختصاص داده و به اینترفیس‌های روتر متصل می کنیم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#interface fastethernet 0/15
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 2
SwitchA(config-if)#interface fastethernet 0/16
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 3
SwitchA(config-if)#interface fastethernet 0/17
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 4
SwitchA(config-if)#interface fastethernet 0/18
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 10
SwitchA(config-if)#end
SwitchA#write
```

حالا نوبت به آدرس‌دهی اینترفیس‌های روتر می‌رسد. توجه داشته باشید، آدرس IP اختصاص داده شده به اینترفیس‌های روتر به عنوان Default Gateway کلاینت‌های همان VLAN مورد استفاده قرار می گیرند.

اگرچه هر آدرس دلخواه در رنج IP مورد نظر را می‌توان جهت Default Gateway در نظر گرفت، ولی معمولا اولین یا آخرین آدرس IP هر رنج جهت این امر اختصاص می‌یابد.

```
Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.200.1 255.255.255.128
Router(config-if)#description *** Connected to vlan 2 ***
Router(config-if)#no shutdown
Router(config-if)#interface fastethernet 0/1
Router(config-if)#ip address 192.168.200.129 255.255.255.128
Router(config-if)#description *** Connected to vlan 3 ***
Router(config-if)#no shutdown
Router(config-if)#interface ethernet 0/0/0
Router(config-if)#ip address 192.168.201.1 255.255.255.128
Router(config-if)#description *** Connected to vlan 4 ***
Router(config-if)#no shutdown
Router(config-if)#interface ethernet 0/1/0
Router(config-if)#ip address 192.168.201.129 255.255.255.128
Router(config-if)#description *** Connected to vlan 10 ***
Router(config-if)#no shutdown
Router(config-if)#end
Router#write
```

از دستور ip address جهت تخصیص آدرس IP به اینترفیس مورد نظر استفاده می کنیم.

اینترفیس‌های روتر بر عکس سوئیچ، بصورت پیش فرض در حالت shutdown قرار دارند، به همین دلیل جهت فعال کردن آنها باید از دستور no shutdown استفاده نمایید.

شماره مربوط به شاسی روتر همانند سوئیچ از 0 شروع شده ولی شماره اینترفیس‌های روتر بر خلاف سوئیچ از عدد 0 شروع می شوند.

در این سناریو ما از سوئیچ Cisco 1841 استفاده نمودیم که بصورت پیش فرض دارای دو پورت Fastethernet می‌باشد. به دلیل نیاز ما به ۴ پورت ایترنت، اقدام به اضافه نمودن دو کارت cisco wic 1enet که هر کدام دارای یک پورت Ethernet می‌باشند، به روتر نمودیم. به همین دلیل پورت روی شاسی بصورت 0/0 و پورت روی کارت بصورت 0/0/0 آدرس دهی گردیده است.

برای اینکه تمام بسته‌های دیتا که آدرسIP مقصدشان غیر از رنج‌های مشخص شده فوق است را به مودم ADSL مسیردهی نماییم باید آدرسIP مودمADSL را به عنوان Default Gateway روتر مشخص نماییم.

آدرس اختصاص داده شده به مودم 192.168.201.130 می باشد.

```
Router>en
Router#configure terminal
Router(config)# ip routing
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.201.130
Router(config)#end
Router#
```

دستور ip routing باعث فعال شدن عملیات Routing در روتر می گردد.

دستور استفاده شده برای نوشتنDefault Gateway شبیه نوشتن یک روت معمولی می‌باشد، با این تفاوت که جهت آدرس و Subnet مقصد از آدرس 0.0.0.0 استفاده می‌نماییم.

منظور از آدرس 0.0.0.0، هر آدرس مقصدی با هر Subnetای می‌باشد که در جدول Routing ما وجود ندارد. برای نوشتن Default Gateway می توانید از دستور ip default-network نیز استفاده نمایید.

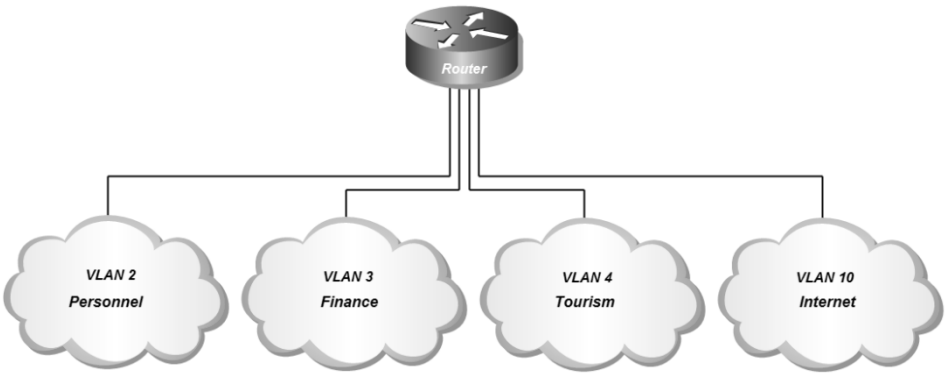
توجه داشته باشید که آدرسIP مربوط به هرVLAN که بر روی اینترفیس روتر تعریف گشته باید به عنوان Default Gateway بر روی کارت شبکه کلاینت‌های همان VLAN تعریف گردد.

پس از انجام مراحل فوق ارتباط بین کلاینت های VLANهای مختلف با یکدیگر برقرار شده و همچنین دسترسی کلاینت ها به اینترنت نیز امکان پذیر می گردد.

البته توجه داشته باشید که همچنان در شبکه‌ها هیچ تغییری در مورد حوزه Broadcast و حوزه Collision نسبت به قبل رخ نداده است.

طریقه عملکرد:

پس از اتصال پورت‌های روتر به هر VLAN، شبکه از نظر منطقی به شکل زیر در خواهد آمد.



همانطور که مشاهده می‌کنید، هر اینترفیس روتر به یکVLAN اختصاص داده شده و به عنوان Default Gateway کلاینت های VLAN مربوطه عمل می کند.

اگر به خروجی دستور show ip route توجه نمایید ملاحظه خواهید کرد که به دلیل اتصال مستقیم اینترفیس‌ها به روتر (directly connected)، بدون نیاز به نوشتن دستور خاصی، روتر تمام شبکه‌های متصل شده را شناسایی نموده است. همچنین Default Route روتر نیز بصورت S* نمایش داده شده است.

```
Router#show ip route
...

    192.168.200.0/25 is subnetted, 2 subnets
C      192.168.200.0 is directly connected, FastEthernet0/0
C      192.168.200.128 is directly connected, FastEthernet0/1
    192.168.201.0/25 is subnetted, 2 subnets
C      192.168.201.0 is directly connected, Ethernet0/0/0
C      192.168.201.128 is directly connected, Ethernet0/1/0
S*   0.0.0.0/0 [1/0] via 192.168.201.130
Router#
```

همانطور که قبلا گفتیم در صورتیکه کلاینت یک شبکه قصد برقراری ارتباط با کلاینت دیگری در همان شبکه را داشته باشد، توسط پروتکلARP آدرسMAC مقصد مورد نظر را به دست آورده و با جایگزینی در فریم، آنرا در اختیار سوئیچ قرار می‌دهد. سوئیچ نیز طبق جدول CAM خود اقدام به تحویل فریم‌ها می نماید.

ولی در صورتیکه کلاینت بخواهد با دستگاهی خارج از Subnet مشخص شده بر روی کارت شبکه خود ارتباط برقرار نماید، آدرسIP مقصد بسته را دقیقا مطابق آدرس مورد نظر در هدر بسته درج نموده ولی در فیلد آدرسMAC مقصد به جای آدرس واقعی از آدرس MAC

اینترفیسی که به عنوان Default Gateway معرفی شده استفاده مینماید. در این صورت سوئیچ پس از بررسی آدرسMAC مقصد، بسته مورد نظر را تحویل اینترفیس روتر که مربوط به همان VLAN می باشد، می‌دهد.

روتر پس از دریافت بسته و بررسی آدرسIP آن، مطابق با جدول مسیریابی خود اقدام به مسیردهی اطلاعات می نماید.

نکته قابل توجه در اینجاست که روتر بدون تغییر در آدرس‌هایIP مبدا و مقصد، آدرسMAC مبدا بسته مورد نظر را به آدرسMAC اینترفیسی که اطلاعات از آن خارج می‌شود تغییر داده و آدرسMAC مقصد را نیز با آدرسMAC اینترفیسی که می‌خواهد بسته را تحویل آن دهد تغییر می‌دهد، سپس اقدام به ارسال اطلاعات می‌نماید.

همانطور که توضیح داده شد روتر با توجه به جدول مسیریابی خود و بر اساس آدرسIP مقصد، اقدام به تحویل بسته به اینترفیس مورد نظر می‌نماید. در صورتیکه آدرسIP مقصد در جدول مسیریابی روتر موجود نباشد، روتر بسته را به دستگاهی که آدرسIP آن به عنوان Default Gateway در روتر مشخص شده ارسال می‌نماید.

بدلیل اینکه در روتر اقدام به معرفی آدرس مودمADSL به عنوان Default Gateway نمودیم، زمانی که روتر بسته‌ای را دریافت نماید که آدرسIP مقصد آن را در جدول مسیریابی خود نداشته باشد، بسته را تحویل مودم ADSL می‌دهد.

با توجه به توضیحات فوق حالا کلاینت‌های بخش‌های مختلف ضمن برقراری ارتباط با اینترنت، امکان برقراری ارتباط با کلاینت‌های دیگر بخشها را نیز دارند. اما اگر یادتان باشد مدیر محترم آژانس، برای قسمت مالی شبکه‌ای ایزوله از شما درخواست کرده بود!

برای حل مشکل فوق دو راه حل دارید. اولین راهکار اینست که با دستور shutdown اقدام به غیرفعال کردن اینترفیس روتر که بهVLAN مالی اختصاص داده شده بود نمایید. در اینصورت اینترنت نیز برای این بخش در دسترس نخواهد بود.

دومین راهکار که بتوانید ضمن ایزوله کردن بخش مالی از دیگر بخشها، امکان دسترسی به اینترنت را برای این بخش فراهم نمایید، استفاده ازAccess List در روتر می‌باشد. مبحث Access List در فصل‌های آتی به طور مفصل تشریح خواهد شد.

مرجع دستور Command Reference

Configuring Fast Ethernet and Gigabit Ethernet Interfaces		
	Command or Action	**Purpose**
Step 1	Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	Router# show ip interface brief	Displays a brief status of the interfaces that are configured for IP. • Learn which type of Ethernet interface is on your router: Fast Ethernet or Gigabit Ethernet.
Step 3	Router# configure terminal	Enters global configuration mode.
Step 4	interface {fastethernet | gigabitethernet} 0/*port* Example: Router(config)# interface fastethernet 0/1 Example: Router(config)# interface gigabitethernet 0/0	Specifies the Ethernet interface and enters interface configuration mode. Note For information on interface numbering, see the quick start guide that shipped with your router.
Step 5	description *string* Example: Router(config-if)# description FE int to 2nd floor south wing	(Optional) Adds a description to an interface configuration. • The description helps you remember what is attached to this interface. The description can be useful for troubleshooting.
Step 6	ip address *ip-address mask* Example: Router(config-if)# ip address 172.16.74.3 255.255.255.0	Sets a primary IP address for an interface.
Step 7	no shutdown Example: Router(config-if)# no shutdown	Enables an interface.
Step 8	Router(config)# end	Returns to privileged EXEC mode.
Step 9	Router# show ip interface brief	Displays a brief status of the interfaces that are configured for IP. • Verify that the Ethernet interfaces are up and configured correctly.

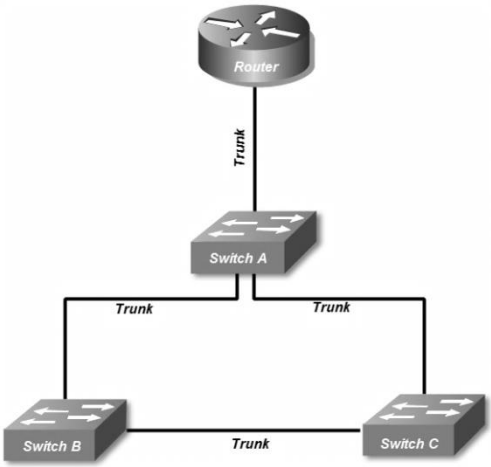
Specifying a Default Route or Gateway of Last Resort		
	Command or Action	**Purpose**
Step 1	Router> enable	Enables privileged EXEC mode.

Specifying a Default Route or Gateway of Last Resort		
		• Enter your password if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# ip routing	Enables IP routing.
Step 4	ip route *dest-prefix mask next-hop-ip-address* [*admin-distance*] [permanent] Example: Router(config)# ip route 192.168.24.0 255.255.255.0 172.28.99.2	Establishes a static route.
Step 5	ip default-network *network-number* or ip route *dest-prefix mask next-hop-ip-address* Example: Router(config)# ip default-network 192.168.24.0 Example: Router(config)# ip route 0.0.0.0 0.0.0.0 172.28.99.1	Selects a network as a candidate route for computing the gateway of last resort. Creates a static route to network 0.0.0.0 0.0.0.0 for computing the gateway of last resort.
Step 6	Router(config)# end	Returns to privileged EXEC mode.
Step 7	Router# show ip route	Displays the current routing table information. • Verify that the gateway of last resort is set.

سناریو شماره(۷)؛ Inter-VLAN Routingتوسط روتر و اتصالTRUNK

طرح مسئله:

طرح مسئله همان طرح سناریوی(۶) می‌باشد. دلیل طرح دوباره مسئله قبل، یادگیری یک راهکار دیگر برای همان مسئله می‌باشد. در این سناریو می خواهیم بجای استفاده از ۴ اینترفیس روتر، از یک اینترفیس و اتصال Trunk استفاده نماییم.



نیاز سنجی:

برای راه اندازی Inter-VLAN Routing نیاز به تجهیزاتی با قابلیت مسیریابی لایه ۳ داریم. در این سناریو از یک روتر(مسیریاب) برای اجرای عملیات استفاده می کنیم. بر عکس سناریوی قبل، این بار از یک اینترفیس روتر برای تبادل ترافیک تمام VLANها استفاده می‌کنیم.

یک VLAN جدید با یک رنج IP هم برای اینترنت نیاز داریم که مودم ADSL را در آن شبکه قرار دهیم. البته روتر توسط کارت ADSL می تواند نقش مودم را هم بر عهده بگیرد. ولی در این سناریو ما از همان مودم ADSL استفاده می کنیم.

راه حل:

ابتدا یکVLAN جدید با نام اینترنت ایجاد کرده و مودمADSL که به پورت۲۳ سوئیچ A متصل است را در آن شبکه قرار می‌دهیم. همچنین رنج آدرس 192.168.201.128/25 را برای کلاینت های این VLAN در نظر می گیریم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vlan 10
SwitchA(config-vlan)#name internet
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/23
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 10
SwitchA(config-if)#end
SwitchA#write
```

در اینجا فقط از یک اینترفیس روتر برای اتصال تمامVLANها استفاده می‌نماییم. در اینصورت پس از برقراری اتصالTrunk بین سوئیچ و روتر، اینترفیسTrunk روتر را به subinterfaceهای مورد نظر تقسیم کرده و هر subinterface را به یک VLAN اختصاص داده و بعنوان Default Gateway از آن استفاده می کنیم.

```
Router>enable
Router#configure terminal
Router(config)#interface fastethernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1q 2
Router(config- subif)#ip address 192.168.200.1 255.255.255.128
Router(config-subif)#description *** Connected to vlan 2 ***
Router(config-subif)#interface fastethernet 0/0.2
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.200.129 255.255.255.128
Router(config-subif)#description *** Connected to vlan 3 ***
Router(config-subif)# interface fastethernet 0/0.3
Router(config-subif)#encapsulation dot1q 4
Router(config-subif)#ip address 192.168.201.1 255.255.255.128
Router(config-subif)#description *** Connected to vlan 4 ***
Router(config-subif)# interface fastethernet 0/0.4
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.201.129 255.255.255.128
Router(config-subif)#description *** Connected to vlan 10 ***
Router(config-subif)# interface fastethernet 0/0.5
Router(config-subif)#encapsulation dot1q 1 native
Router(config-subif)#description *** Native VLAN ***
Router(config-subif)#^Z
Router(config-subif)#end
Router#write
```

برای اینکه قصد داریم از اینترفیس fastethernet 0/0 روتر برای ایجاد subinterfaceها استفاده نماییم، در قدم اول اینترفیس مورد نظر را با دستور no shutdown فعال می نماییم.

با اضافه کردن یک نقطه و سپس عدد مورد نظر، subinterface را بوجود می‌آوریم. عدد subinterface از 1 شروع شده و از نظر فنی هیچ وابستگی به شماره VLANای که قرار است به آن متصل شود ندارد.

با دستورencapsulation توان اضافه و حذف Tag مربوط بهVLANها را به subinterface اعطا می‌کنیم. در دستورencapsulation پس از مشخص کردن پروتکل که می تواند dot1q یا ISL باشد، باید شماره VLAN مورد نظر را نیز مشخص نمایید.

برای مشخص نمودن Native VLAN، پس از درج نوع Encapsulation و شماره VLAN، باید عبارت Native را نیز وارد نمایید.

در نهایت نیز اقدام به اختصاص آدرسIP می‌نمائیم. نحوه تنظیم آدرس بر روی subinterface، تفاوتی با پیکربندی آدرس بر روی اینترفیس‌های معمولی ندارد.

پس از پیکربندی روتر، سراغ سوئیچ می‌رویم. چون می‌خواهیم از سوئیچ A استفاده کنیم، پورت۱۹ سوئیچ را بصورتTrunk پیکربندی کرده و به اینترفیسTrunk روتر متصل می نماییم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#interface fastethernet 0/19
SwitchA(config-if)#switchport mode  trunk
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#end
SwitchA#write
```

برای اینکه تمام بسته های دیتا که آدرسIP مقصدشان غیر از رنج‌های مشخص شده فوق است را به مودمADSL مسیردهی نماییم باید آدرسIP مودمADSL را به عنوان Default Gateway روتر مشخص نماییم.

آدرس اختصاص داده شده به مودم 192.168.201.130 می باشد.

```
Router>en
Router#configure terminal
Router(config)# ip routing
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.201.130
```

دستور ip routing باعث فعال شدن عملیات مسیریابی در روتر می گردد.

دستور استفاده شده برای نوشتنDefault Gateway شبیه نوشتن یک روت معمولی می‌باشد، با این تفاوت که جهت آدرس و Subnet مقصد از آدرس 0.0.0.0 استفاده می نماییم.

منظور از آدرس0.0.0.0، هر آدرس مقصدی با هرSubnetای می‌باشد که در جدول مسیریابی ما وجود ندارد. برای نوشتن Default Gateway می‌توانید از دستور ip default-network نیز استفاده نمایید.

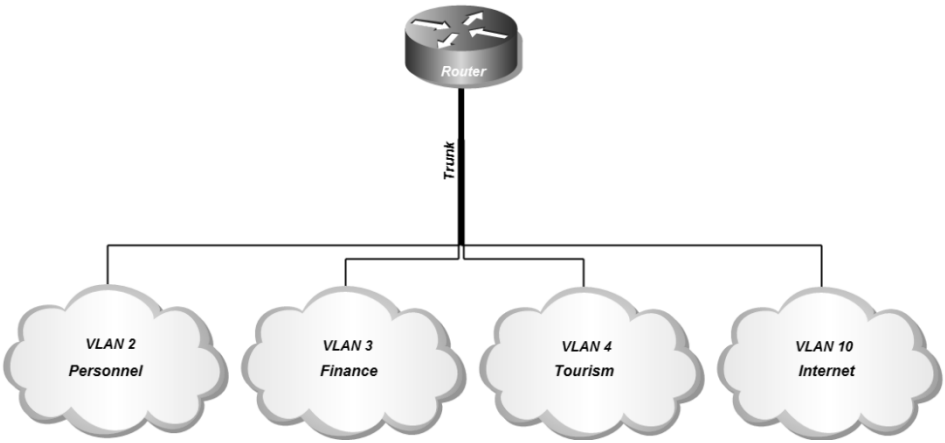
توجه داشته باشید که آدرسIP مربوط به هرVLAN که بر روی subinterface روتر تعریف گشته است باید به عنوانDefault Gateway بر روی کارت شبکه کلاینت‌های همان VLAN تعریف گردد.

پس از انجام مراحل فوق ارتباط بین کلاینت های VLANهای مختلف با یکدیگر برقرار شده و همچنین دسترسی کلاینت ها به اینترنت نیز امکان پذیر می گردد.

البته توجه داشته باشید که همچنان در شبکه ها هیچ تغییری در مورد حوزه Broadcast و حوزه Collision نسبت به قبل رخ نداده است.

طریقه عملکرد:

از نظر منطقی، این شبکه دقیقا مثل شبکه سناریوی قبلی خواهد بود. و تفاوت این دو در استفاده از تعداد پورت فیزیکی برای بر قراری ارتباط بین سوئیچ و روتر است.



در سناریو قبل مجبور بودیم به ازاء هر VLAN یک اینترفیس روتر و یک اینترفیس سوئیچ را درگیر عملیات مسیریابی نماییم. ولی در این سناریو با استفاده از اتصالات Trunk فقط یک اینترفیس روتر و سوئیچ برای انجام عملیات Inter-VLAN Routing مورد نیاز خواهد بود. هر

چند شما می توانید در صورت تعددVLANها، برای داشتن پهنای باند بالاتر از چند لینکTrunk بین سوئیچ و روتر استفاده نمایید.

اگر به خروجی دستورshow ip route توجه کنید، خواهید دید که تغییر خاصی در جدول مسیریابی روتر نسبت به سناریوی قبل به وجود نیامده و تنها تغییر آن، تبدیل اینترفیس به subinterface می باشد.

```
Router#sh ip route
...

    192.168.200.0/25 is subnetted, 2 subnets
C      192.168.200.0 is directly connected, FastEthernet0/0.1
C      192.168.200.128 is directly connected, FastEthernet0/0.2
    192.168.201.0/25 is subnetted, 2 subnets
C      192.168.201.0 is directly connected, FastEthernet0/0.3
C      192.168.201.128 is directly connected, FastEthernet0/0.4
S*   0.0.0.0/0 [1/0] via 192.168.201.130
Router#
```

از نظر عملیاتی تنها تفاوت این حالت با سناریوی قبلی این است که به دلیل استفاده روتر از اتصال Trunk، وظیفه Tag و Untag فریم های ورودی و خروجی به subinterfaceها نیز به وظایف روتر اضافه می گردد.

عملیات مسیریابی نیز همانطور که در سناریوی قبل توضیح داده شده، انجام می پذیرد.

با توجه به توضیحات فوق حالا کلاینت‌های بخش‌های مختلف ضمن برقراری ارتباط با اینترنت، امکان برقراری ارتباط با کلاینت‌های دیگر بخشها را نیز دارند. اما اگر یادتان باشد مدیر محترم آژانس، برای قسمت مالی شبکه ای ایزوله از شما درخواست کرده بود!

برای حل مشکل فوق دو راه حل دارید. اولین راهکار اینست که با دستور shutdown اقدام به غیرفعال کردن subinterface روتر که به VLAN مالی اختصاص داده شده بود نمایید. در اینصورت اینترنت نیز برای این بخش در دسترس نخواهد بود.

دومین راهکار که بتوانید ضمن ایزوله کردن بخش مالی از دیگر بخشها، امکان دسترسی به اینترنت را برای این بخش فراهم نمایید، استفاده از Access List در روتر می باشد. مبحث Access List در فصل‌های آتی به طور مفصل تشریح خواهد شد.

مرجع دستور Command Reference

Ethernet VLAN Subinterface		
	Command or Action	**Purpose**
Step 1	Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	interface *type number* [*name-tag*] Example: Router(config)# interface fastethernet 1/0.1	Configures an interface type and enters interface or subinterface configuration mode.
Step 4	encapsulation dot1q *vlan-id* [native] Example: Router(config-subif)# encapsulation dot1q 10	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.

سناریو شماره(۸)؛ Inter-VLAN Routing توسط سوئیچ Multilayer

طرح مسئله:

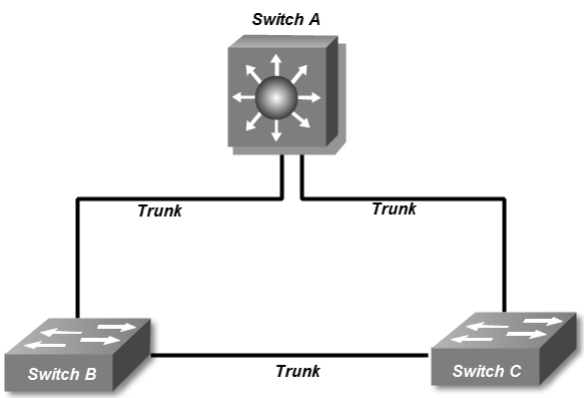
طرح مسئله همان طرح سناریوهای(۶و۷) می‌باشد. دلیل طرح دوباره مسئله، یادگیری یک راهکار دیگر برای همان مسئله می باشد.

در این مسئله سوئیچ A را با یک سوئیچ Multilayer عوض کرده و تمام پیکربندی سوئیچ قبلی را به سوئیچ جدید انتقال می‌دهیم. در صورت استفاده از سوئیچ Multilayer می توانیم بدون نیاز به روتر اقدام به راه اندازی Inter-VLAN Routing نماییم.

نیاز سنجی:

برای راه اندازی Inter-VLAN Routing نیاز به تجهیزاتی با قابلیت مسیریابی لایه ۳ داریم. برخلاف دو سناریوی قبلی این بار از روتر استفاده نمی کنیم. در این سناریو قصد استفاده از یک سوئیچ Multilayer سیسکو را داریم. با توجه به اینکه سوئیچ A یک سوئیچ Multilayer است، دیگر نیازی به خرید تجهیزات اضافی نداریم.

درباره اینترنت و مودم ADSL هم مثل دو سناریو قبل عمل می نماییم.



راه حل:

ابتدا یک VLAN جدید با نام اینترنت ایجاد کرده و مودم ADSL که به پورت ۲۳ سوئیچ A متصل است را در آن شبکه قرار می دهیم. همچنین رنج آدرس 192.168.201.128/25 را برای کلاینت های این VLAN در نظر می گیریم.

```
SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#vlan 10
SwitchA(config-vlan)#name internet
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/23
SwitchA(config-if)#switchport mode  access
SwitchA(config-if)#switchport access vlan 10
SwitchA(config-if)#end
SwitchA#write
```

برخلاف سناریوی قبل، دیگر نیازی به استفاده از پورت‌های فیزیکی برای برقراری ارتباط بین VLANها نداریم. صرف داشتن یک سوئیچMultilayer و برقرار بودن اتصالاتTrunk بین سوئیچ‌ها، برای راه اندازی Inter-VLAN Routing کفایت می کند.

قبل از ایجاد SVI، بایدVLAN متناظر آن در سوئیچ ایجاد شده باشد. در سوئیچ Multilayer به ازاء هرVLAN یک اینترفیس مجازیSVI ایجاد نموده و به عنوانDefault Gateway کلاینت‌های آن VLAN پیکربندی می نماییم.

```
SwitchA#
SwitchA#configure terminal
SwitchA(config)#interface vlan 2
SwitchA(config-if)#ip address 192.168.200.1 255.255.255.128
SwitchA(config-if)#interface vlan 3
SwitchA(config-if)#ip address 192.168.200.129 255.255.255.128
SwitchA(config-if)#interface vlan 4
SwitchA(config-if)#ip address 192.168.201.1 255.255.255.128
SwitchA(config-if)#interface vlan 10
SwitchA(config-if)#ip address 192.168.201.129 255.255.255.128
SwitchA(config-if)#end
SwitchA#write
```

برای ایجادSVI، باید توسط دستورinterface، یک اینترفیس مجازی به ازاء هرVLAN موجود در VLAN Database ایجاد نمایید.

جهت مشخص نمودن مودمADSL به عنوانDefault Route سوئیچMultilayer باید دستورات زیر را اعمال نمایید.

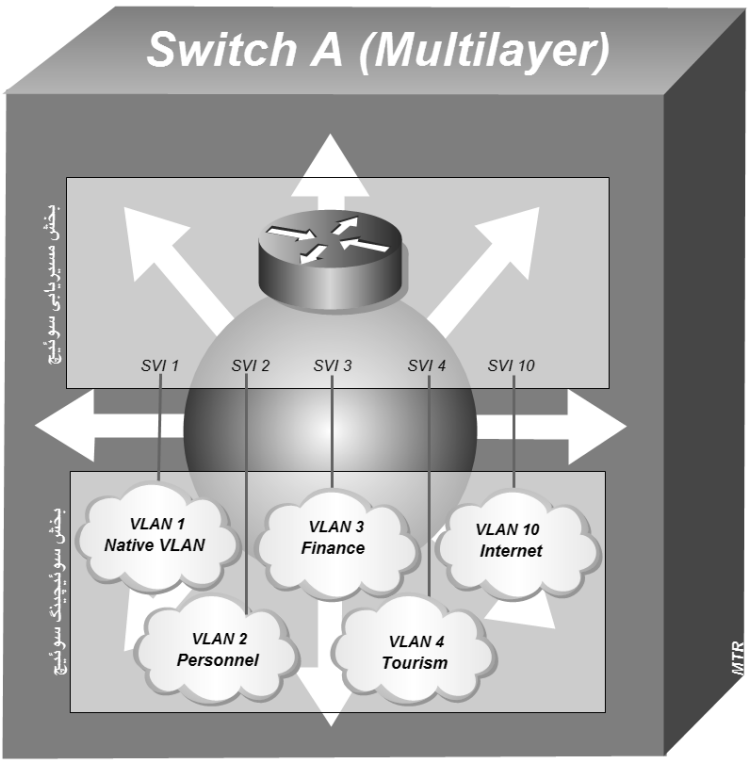
```
SwitchA#
SwitchA#configure terminal
SwitchA(config)#ip default-network 192.168.201.130
```

طریقه عملکرد:

عملکرد سوئیچ Multilayer مثل روتر سناریو قبلی است. تفاوت این دو سناریو در این است که subinterfaceهای سناریو قبل بر روی یک اینترفیس فیزیکی ایجاد شده ولی در سوئیچ Multilayer برای ایجاد SVI نیازی به پورت فیزیکی نمی‌باشد.

سوئیچMultilayer دارای دو قسمت مجزا برای انجام عملیات سوئیچینگ و مسیریابی می‌باشد. تشریح عملیات مسیریابی که در سناریوی قبل برای روتر تشریح داده شد در قسمت مسیریابی سوئیچ Multilayer نیز انجام می پذیرد.

در تصویر زیر اوج خلاقیت! بنده در نشان دادن قسمت سوئیچینگ و مسیریابی سوئیچ Multilayer و اتصال این دو قسمت توسط پورت های مجازیSVI را می توانید مشاهده فرمایید.



خروجی دستور show ip route سوئیچ Multilayer نیز شبیه به خروجی روتر در سناریو قبلی می باشد. فقط توجه داشته باشید هر VLAN باید حداقل یک پورت فعال داشته باشد تا در جدول مسیریابی مشخص گردد.

```
SwitchA#show ip route
...

    192.168.200.0/25 is subnetted, 2 subnets
C     192.168.200.0 is directly connected, Vlan2
C     192.168.200.128 is directly connected, Vlan3
    192.168.201.0/24 is variably subnetted, 3 subnets, 2 masks
C     192.168.201.0/25 is directly connected, Vlan4
C     192.168.201.128/25 is directly connected, Vlan10
S     192.168.201.0/24 [1/0] via 192.168.201.130
```

با توجه به توضیحات فوق حالا کلاینت‌های بخش‌های مختلف ضمن برقراری ارتباط با اینترنت، امکان برقراری ارتباط با کلاینت‌های دیگر بخشها را نیز دارند. اما اگر یادتان باشد مدیر محترم آژانس، برای قسمت مالی شبکه ای ایزوله از شما درخواست کرده بود!

برای حل مشکل فوق دو راه حل دارید. اولین راهکار اینست که با دستور shutdown اقدام به غیرفعال کردن اینترفیس مجازی (SVI) که به VLAN مالی اختصاص داده شده بود نمایید. در اینصورت اینترنت نیز برای این بخش در دسترس نخواهد بود.

دومین راهکار که بتوانید ضمن ایزوله کردن بخش مالی از دیگر بخشها، امکان دسترسی به اینترنت را برای این بخش فراهم نمایید، استفاده از Access List در سوئیچ Multilayer می‌باشد. مبحث Access List در بخش های آتی به طور مفصل تشریح خواهد شد.

مرجع دستور Command Reference

Adding a SVI Interface		
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface vlan** vlan-id	Enter interface configuration mode
Step 3	**description** string	(optional)Add a description for an interface.
Step 4	**ip address** *ip-address mask* Example: Router(config-if)# ip address 172.16.74.3 255.255.255.0	Sets IP address for a SVI.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** interface-id description	Verify your entry.

فصل پنجم

شبکه‌های گسترده؛ مسیریابی

- ☑ مبحث اول: مبانی مسیریابی
- ☑ مبحث دوم: پروتکل RIP
- ☑ مبحث سوم: پروتکل EIGRP
- ☑ مبحث چهارم: پروتکل OSPF
- ☑ مبحث پنجم: پروتکل BGP

☑ مبحث اول

مبانی مسیریابی

گسترش شبکه‌ها به ساختمان‌ها، شهرها و کشورهای دیگر، تقسیم شبکه یک سازمان به زیر شبکه‌های متعدد، ارتباط با شبکه جهانی اینترنت، ارتباط شبکه‌ای بین سازمان‌های مختلف و در یک کلام احتیاج کلاینت به دسترسی دنیای خارج از شبکه خود، نیاز به مسیریابی در شبکه را نمایان ساخته است.

وقتی شبکه‌های مختلف دارایNet Maskهای متفاوت نیاز دسترسی به منابع یکدیگر را دارند، باید یک دستگاه با قابلیت مسیریابی در لایه سوم مدلOSI، مسیریابی بین شبکه‌ها را بر عهده گیرد. این مسیریابی در حالت کوچک و برای چند شبکه مشخص می تواند بصورت Static و در شبکه های گسترده تر بصورت Dynamic انجام پذیرد.

در ادامه این مبحث به معرفی پروتکل‌ها و اصطلاحات مورد نیاز در مسیریابی پرداخته و در مباحث آتی به معرفی جزئی‌تر پروتکل‌های مسیریابی مشهور خواهیم پرداخت.

تفاوت مفهوم Routed Protocol با Routing Protocol

قبل از هر کاری باید تفاوت بین دو مفهوم Routed Protocol و Routing Protocol را بخوبی درک نمایید. آشنایی با این دو مفهوم شما را در یادگیری مسیریابی کمک خواهد کرد.

منظور از Routed Protocol، پروتکل‌هایی هستند که دارای قابلیت مسیریابی می‌باشند. در این حالت قابلیت هدایت بسته اطلاعات به مقصد مورد نظر بین شبکه‌های مختلف میسر می باشد. از جمله Routed Protocolها می توان به پروتکل‌های IPX، AppleTalk و مشهورتر از همه به پروتکلIP اشاره نمود.

اما منظور از Routing Protocol، پروتکل‌هایی هستند که قابلیت تبلیغ و یادگیری مسیر شبکه‌های قابل دسترس را بصورت پویا(Dynamic) دارند. در این حالت، پروتکل‌های مربوطه اقدام به انتقال اطلاعات مورد نیاز جهت شناسایی شبکه‌های قابل دسترس بین روترهای شبکه می نمایند. روترها از این اطلاعات جهت تکمیل جداول مسیریابی خود استفاده می کنند. از جمله پروتکل‌های مسیریابی می توان به RIP، EIGRP و OSPF اشاره نمود.

آدرس‌دهی Classful

همانطور که در فصل دوم گفته شد، پروتکل IP دارای ۵ کلاس آدرس‌دهی استاندارد می‌باشد. اصطلاح Classful زمانی استفاده می‌شود که از آدرس‌های IP در کلاس استاندارد استفاده می‌نماییم. در این حالت طبق جدول تقسیم‌بندی و با توجه به عدد اولین بایت آدرس، می توان Net Mask مورد استفاده را براحتی مشخص نمود.

به دلیل امکان تشخیص کلاس آدرس‌های Classful بر اساس بایت اول آدرس، در این حالت الزام به ذکر Net Mask مربوطه به همراه آدرس IP نمی باشد.

کلاس	رنج اولین بایت مربوط به هر کلاس	تعداد بیت Network	تعداد بیت Host
A	1 to 126	8	24
B	128 to 191	16	16
C	192 to 223	24	8
D	224 to 239	Multicast	
E	240 to 254	Reserved	

پروتکل های مسیریابی که از آدرس دهی Classful استفاده می کنند، Subnet Mask مربوط به آدرس را در پیام خود قرار نداده و فرض را بر Maskهای استاندارد می‌گذارند.

آدرس‌دهی Classless

در مواقعی که برای تغییر در تعداد زیر شبکه، اقدام به قرض دادن بیت‌های Host به بیت‌های Network می‌نماییم، ناگزیر از ایجاد تغییر در Net Mask آدرس مورد نظر خواهیم بود. به رنج آدرس‌های خارج از کلاس استاندارد، در اصطلاح Classless گفته می شود.

برای مشخص کردن بیت‌های مربوط به Host و Network در آدرس‌های Classless، ذکر Subnet Mask به همراه آدرس IP الزامی است.

پروتکل‌های مسیریابی که از آدرس‌دهی Classless پشتیبانی می‌کنند، Subnet Mask مربوط به آدرس‌ها را نیز در پیام‌های خود قرار می‌دهند.

روش CIDR

سازمانIETF با معرفی روشCIDR(Classless Inter-Domain Routing) جایگزینی مناسب برای آدرس‌دهیClassful جهت ایجاد امکان استفاده از رنج آدرس‌های خارج از کلاس استاندارد را در شبکه‌ها فراهم نموده است.

روش CIDR که در برخی از مستندات، Supernetting هم گفته می‌شود امکان خلاصه‌نویسی یا Summarization جداول مسیریابی را نیز فراهم نموده به صورتی که می‌تواند چندین آدرس شبکه را با یک آدرس با Mask بزرگ‌تر و حتی غیر استاندارد آدرس‌دهی نماید. استفاده از این روش باعث کاهش حجم جداول مسیریابی روترها می گردد.

همچنین CIDR باعث انعطاف پذیری در نحوه تخصیص آدرس به زیر شبکه‌ها نیز گردیده است. از طریق این روش می توان رنج آدرس یک شبکه بزرگ مثل کلاسB را به چند زیر شبکه با طول ثابت(مساوی) تقسیم نمود.

روش CIDR طی RFC 1820 توسط سازمان IETF بصورت استاندارد منتشر گردیده است.

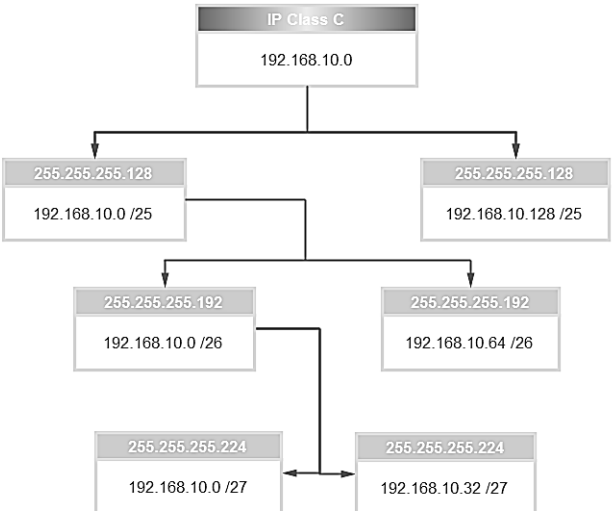
ماسک زیرشبکه با طول متغیر (VLSM)

روش VLSM(Variable Length Subnet Mask)، جهت امکان تقسیم بندی یک Net Mask به چندین زیر شبکه با طول متغیر ایجاد گردیده است.

برای استفاده کارآمدتر از آدرس‌هایIP، ممکن است نیاز به تقسیم یک کلاس استاندارد به چند زیر شبکه با طول متغیر داشته باشیم. با این کار می‌توان به هر بخش تعداد آدرس مورد نیاز را تخصیص داده و از هدر رفتن آدرس‌هایIP جلوگیری به عمل آورد.

به عنوان مثال، بصورت زیر می‌توان یک رنج آدرس کلاسC را به چهار زیرشبکه با Subnet Mask متفاوت تقسیم نمود.

192.168.10.0 /24			
Subnet	**IP Range**	**First/End IP Address**	**Net ID /Broadcast**
1	192.168.10.0 /27	192.168.10.1 192.168.10.30	192.168.10.0 192.168.10.31
2	192.168.10.32 /27	192.168.10.33 192.168.10.62	192.168.10.32 192.168.10.63
3	192.168.10.64 /26	192.168.10.65 192.168.10.126	192.168.10.64 192.168.10.127
4	192.168.10.128 /25	192.168.10.129 192.168.10.254	192.168.10.128 192.168.10.255



پروتکل‌های مسیریابی که امکان گنجاندن Subnet Mask را در پیام‌های خود دارند، می‌توانند از ویژگیVLSM استفاده نمایند..

سازمان IETF طی RFC 1878 جدول مربوط به VLSM را برای IPv4 منتشر نموده است.

ویژگی Subnet-Zero

اگر به یاد داشته باشید، قبلا گفته بودیم به دلیل اینکه اولین آدرس جهت NET ID و آخرین آدرس جهت Broadcast مورد استفاده قرار میگیرد نمی‌توان از آنها جهت آدرس‌دهی استفاده نمود. این اتفاق زمانی که اقدام به Subnetting یک Net Mask می‌نماییم بصورت مشکل بروز کرده و امکان استفاده از اولین و آخرین رنج زیرشبکه ایجاد شده را نمی‌دهد.

مخصوصا این ایراد زمانی تبدیل به یک فاجعه می‌شود که شما بخواهید یک رنج آدرس معتبر[1] اینترنتی که بابت دریافت آن پول پرداخت کرده‌اید را Subnetting نمایید.

برای رفع مشکل فوق و جلوگیری از به هدر رفتن اولین و آخرین رنج آدرس پس از Subnetting، سیسکو اقدام به معرفی ویژگی IP Subnet-Zero نموده است.

برای استفاده از این ویژگی می توان از دستور ip subnet-zero در روترهای سیسکو استفاده نمود. لازم به ذکر است که این ویژگی در IOS های جدید سیسکو بصورت پیش فرض در حالت فعال قرار دارد.

[1] Valid

جدول مسیریابی

جدول مسیریابی یا Routing Table شامل مسیرهای دسترسی به شبکه‌های مختلف به همراه پارامترهای مورد استفاده جهت تشخیص بهترین مسیر می باشد.

روترها با درج مسیرهای شناخته شده در جدول مسیریابی خود، از اطلاعات آن برای هدایت بسته‌های دیتا به مقاصد مورد نظر استفاده می‌کنند. فیلدهای زیر جزء اصلی جداول مسیریابی می باشند:

- **Network**

شامل آدرس شبکه مقصد می باشد.

- **Outgoing Interface**

منظور از Outgoing Interface، اینترفیس خروجی بسته‌ها برای رسیدن به مقصد مورد نظر می باشد. این اینترفیس رابط بین روتر و شبکه مقصد است.

- **Metric**

مشخص کننده اولویت مسیرهای به دست آمده می‌باشد. نحوه محاسبه این پارامتر در پروتکل‌های مسیریابی مختلف، بر اساس مؤلفه‌های متفاوتی انجام می‌پذیرد.

در صورتیکه توسط یک پروتکل مسیریابی چند مسیر برای یک مقصد خاص وجود داشته باشد، اولویت انتخاب مسیر بر اساس Metric اختصاص داده شده به مسیرها انجام می‌پذیرد.

- **Next Hub**

مشخص کننده ایستگاه بعدی بسته دیتا برای رسیدن به مقصد مورد نظر می‌باشد. در بعضی روترها از Next Hub با نام دروازه یا Gateway نیز نام برده می‌شود.

انواع مسیریابی

روترها برای ارسال دیتا به مقصد مورد نظر از سه روش مسیریابی زیر استفاده می نمایند:

۱- **اتصال مستقیم**

به شبکه‌هایی که بطور مستقیم به اینترفیس‌های روتر متصل شده‌اند، اتصال مستقیم گفته می‌شود. در این حالت روتر شبکه‌های متصل به خود را با عنوان Direct Connected در جدول مسیریابی ذخیره می کند.

اطلاعات مربوط به اتصالات مستقیم بدون دخالت مدیر شبکه در جدول مسیریابی درج گردیده و در صورت تغییر نیز بصورت اتوماتیک بروز رسانی می‌گردد.

۲- **مسیریابی Static**

در این حالت مدیر شبکه باید مسیر شبکه‌هایی که مستقیم به روتر متصل نبوده ولی می‌توان توسط روترهای دیگر به آنها دسترسی داشت را بصورت دستی تعریف نماید.

حُسن این روش در استفاده کمتر از منابع شبکه (مثلCPU و پهنای باند) می‌باشد. ولی ایراد این روش در آن است که در صورت تغییرات در شبکه، شناسایی مسیرهای جدید به روتر باید بصورت دستی و توسط مدیر شبکه صورت گیرد.

اطلاعات مربوط بهStatic Route در حافظه دائم روتر ذخیره شده و پس از راه اندازی مجدد از بین نمی‌رود.

استفاده از روشStatic برای شبکه‌های کوچک با تغییرات کم توصیه می‌گردد.

۳- **مسیریابی Dynamic**

در این روش وظیفه شناسایی شبکه‌های قابل دسترس بر عهده پروتکل‌های مسیریابی پویا می‌باشد. در این صورت هر تغییری در شبکه سریعا توسط Routing Protocolها بروز رسانی می‌گردد. همچنین پروتکل‌های مسیریابی امکان Load Balancing را نیز بصورت پویا فراهم می‌آورند.

ایراد این روش در آن است که به علت تولید و پخش پیام‌های مربوط به پروتکل‌های مسیریابی، از منابع شبکه (مثل CPU و Bandwidth) بیشتر استفاده می‌گردد.

اطلاعات مربوط به مسیرهای بدست آمده توسط پروتکل های مسیریابی پویا در حافظه موقت روتر ذخیره شده و پس از راه اندازی مجدد از بین رفته و باید دوباره محاسبه گردند.

استفاده از روش Dynamic در شبکه‌های بزرگ یا شبکه‌هایی که دارای تغییرات زیادی هستند، توصیه می‌شود.

انواع مسیر Static

در صورتیکه نخواهیم از پروتکل های مسیریابی پویا[1] استفاده نماییم و یا اینکه نیاز باشد در کنار مسیرهای پویا مسیرهایی را هم بصورت دستی[2] اضافه کنیم، می‌توانیم مسیرهای مورد نظر را از طریق روش‌های زیر در جدول مسیریابی درج نماییم.

[1] Dynamic Routing Protocol
[2] Manual

۱- **Static Route**

برای درج دستی مسیرهای مورد نظر در داخل جدول مسیریابی، می توان از روش Static Route استفاده نمود. این مسیرها در حافظه دائم روتر ذخیره شده و پس از راه اندازی مجدد از بین نمی‌رود.

پارامتر Administrative Distance در مسیرهای Static بصورت پیش فرض برابر عدد1 می‌باشد، ولی در هنگام نوشتنStatic Route می‌توان جهت اعمال تغییر در اولویت بندی مسیرها، پارامتر فوق را تغییر داد.

۲- **Default Static Route**

در صورت موجود بودن Default Route، اگر برای مقصد پیام رسیده هیچ متناظری در جدول مسیریابی یافت نشود، پیام مورد نظر از بین نرفته و به آدرس Default Route ارسال می گردد.

معمولا در صورت اتصال شبکه به اینترنت و یا اتصال یک شبکه کوچک به یک شبکه بزرگ از Default Route استفاده می‌گردد.

۳- **On Demand Routing (ODR)**

در شبکه‌هایHub and Spoke نیازی به استفاده از پروتکل‌های مسیریابی Dynamic نبوده و همچنین استفاده از مسیرهایStatic نیز باعث افزایش سربار مدیریتی می‌شود.

با استفاده از روشODR می‌توان با پیکربندی یکسان روترهایSpoke اقدام به مسیریابی در این نوع شبکه‌ها نمود.

برای راه اندازی ODR فقط نیاز است تا آنرا بر روی روتر Hub پیکربندی نمایید.

مکانیسمODR برای ارسال آدرس به روترSpoke از پروتکل CDP[1] بهره می‌برد.

۴- **Floating Static Route**

از این روش برای برقراری زندگی مسالمت آمیز بین مسیرهای Static و Dynamic استفاده می‌گردد. در صورتیکه بخواهیم برای مسیرهای Dynamic پشتیبان Static مشخص کنیم از مسیردهی Floating Static استفاده می‌نماییم.

در این حالت به دلیل اینکه می‌خواهیم در صورت در دسترس نبودن مسیرهای پویا، از مسیرهای Static استفاده شود و با توجه به اینکه مسیرهای Static دارای مقدارAD کمتری نسبت به تمام پروتکل‌های مسیریابی پویا می‌باشند، لذا باید با تغییر AD مسیر Static، مقدار آنرا بالاتر از AD پروتکل Dynamic مورد نظر قرار دهیم.

---

[1] Cisco Discovery Protocol

فرآیند انتخاب مسیر توسط روتر

در صورتیکه برای یک مقصد چند مسیر مختلف در جدول مسیریابی روتر موجود باشد، روترهای سیسکو برای انتخاب بهترین مسیر از سه مؤلفه زیر استفاده می‌نمایند.

۱- **Administrative Distance**

مؤلفهAdministrative Distance که به اختصارAD گفته می‌شود، عددی است که بر اساس نوع پروتکل مسیریابی به مسیرهای بدست آمده تخصیص داده می‌شود.

این مؤلفه زمانی کاربرد دارد که از چند پروتکل مسیریابی بصورت همزمان در روتر استفاده کرده باشیم. جدول زیر شامل مقادیر پیش فرض اختصاص داده شده به پروتکل‌های مسیریابی می‌باشد.

Default Administrative Distances	
Connected	0
Static	1
eBGP	20
EIGRP (internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (external)	170
iBGP	200
EIGRP summary route	5

هرچه این عدد کوچکتر باشد، مسیر بدست آمده دارای اولویت بالاتری جهت انتخاب شدن می‌باشد. در صورتیکه بخواهید به یک پروتکل اولویت بالاتری اختصاص دهید، می توانید اقدام به تغییر مقادیر پیش فرض نمایید.

۲- **Metric**

در صورتیکه توسط یک پروتکل مسیریابی چند مسیر به یک مقصد خاص به‌دست آمده باشد، انتخاب بهترین مسیر بر اساسMetric انجام می‌پذیرد. Metric در پروتکل‌های مسیریابی مختلف بر اساس پارامترهای متفاوتی محاسبه می‌گردد. نحوه محاسبه این عدد در قسمت مربوط به هر پروتکل بصورت مشروح توضیح داده خواهد شد.

۳- **Prefix length**

منظور از طول پیشوند(Prefix Length)، تعداد بیت اختصاص داده شده به Network درSubnet Mask می‌باشد. به عنوان مثال در آدرس 192.168.10.0 /25 مقدار Prefix Length برابر عدد 25 می‌باشد.

روتر برای ارسال بسته‌ها به مقصد مورد نظر، مسیری را انتخاب می کند که Mask آن بیشترین طول پیشوند(Prefix Length) را نسبت به مسیرهای مشابه داشته باشد.

الگوریتم‌های مسیریابی پویا

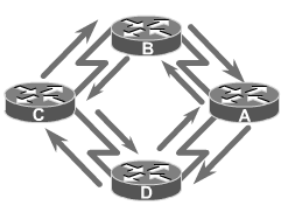
پروتکل‌های مسیریابی پویا بصورت خودکار اقدام به تکمیل جداول مسیریابی خود می‌نمایند. این پروتکل‌ها برای کامل کردن جداول مسیریابی خود از الگوریتم‌های متفاوتی استفاده می‌کنند. این الگوریتم‌ها در دو گروه کلی زیر تقسیم بندی می‌شوند.

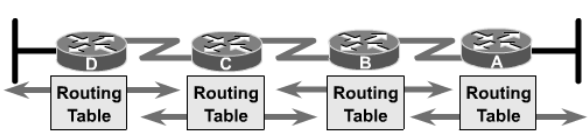
۱- **Distance Vector**

الگوریتم Distance Vector که با نام الگوریتم Bellman-Ford نیز شناخته می‌شود، بر اساس تعداد گام(Hop Count) کار می‌کند. به‌دلیل محدودیت در Hop Count، الگوریتم Distance Vector می‌تواند در شبکه‌ای اجرا گردد که حداکثر دارای ۱۵ عدد روتر یا به عبارتی گام(Hop) باشد.

روتر با ارسال کامل جدول مسیریابی خود در قالب پیام های Broadcast به روترهای همسایه اقدام به کامل کردن اطلاعات آنها می‌نماید.

در الگوریتمDistance Vector روترها فقط دارای شبکه‌های قابل دسترس توسط روترهای همسایه خود بوده و اطلاع جامعی از وضعیت کلی شبکه ندارند.





این الگوریتم برای جلوگیری از ایجاد چرخه لایه سوم در شبکه، از تکنیک‌های Count to infinity، Split horizon، Poison reverse، Hold down timer و Triggered update استفاده می‌نماید.

۲- **Link State**

الگوریتمLink State که با نام الگوریتم Shortest Path First نیز شناخته می‌شود، برای جمع آوری اطلاعات مربوط به شبکه از الگوریتم Dijkstra استفاده می‌نماید.

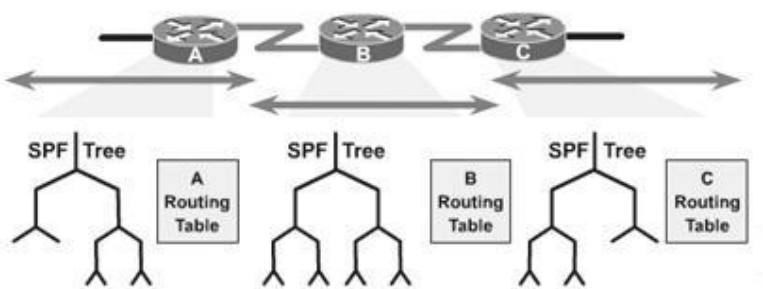
عملیات ارسال پیام در این الگوریتم بصورت مطمئن (Connection Oriented) و در قالب پیام‌های Multicast می‌باشد.

الگوریتمLink State برای شناسایی و بررسی در دسترس بودن روترهای شبکه، اقدام به ارسال متناوب پیام‌های Hello می‌نماید.

در این الگوریتم، روترها فقط یکبار اقدام به ارسال کامل جدول مسیریابی خود کرده و در نوبت های بعدی به ارسال پیام های بروز رسانی افزایشی[1] بسنده می‌نمایند.

در الگوریتم Link State روترهای شبکه دارای اطلاعات جامعی از وضعیت کلی شبکه می‌باشند.

هر چند این الگوریتم دارای خصوصیات بهتری نسبت به Distance Vector می‌باشد، اما برای انجام عملیات خود از منابع روتر و شبکه بیشتر استفاده می‌نماید.



جدول مقایسه الگوریتم‌های مسیریابی

برای درک بهتر تفاوت الگوریتم‌هایLink State وDistance Vector، ویژگی‌های آنها در جدول زیر با یکدیگر مقایسه گردیده است.

[1] Incremental

Distance Vector	Link State
ارسال پیام بصورت Broadcast	ارسال پیام بصورت Multicast
دید روتر به توپولوژی شبکه از منظر روترهای همسایه می‌باشد.	دید روتر به توپولوژی شبکه از منظر خود و بصورت مستقل می‌باشد.
برای بروز رسانی اقدام به ارسال متناوب جدول مسیریابی خود بطور کامل می‌نماید.	پیام‌های بروز رسانی در صورت ایجاد تغییر در شبکه و بصورت پیام‌های افزایشی ارسال می‌گردد.
همگرایی (Convergence) کند	همگرایی (Convergence) سریع
استفاده کم از منابع روتر(CPU, RAM) و شبکه	استفاده زیاد از منابع روتر(CPU, RAM) و شبکه
محدودیت در تعداد روتر	بدون محدودیت در تعداد روتر
امکان ایجاد چرخه لایه سوم	بدون ایجاد چرخه لایه سوم
ارسال پیام بصورت نامطمئن (Connection Less)	ارسال پیام بصورت مطمئن **(Connection Oriented)**
محاسبه بهترین مسیر بر اساس کمترین تعداد Hop بین مبدا و مقصد انجام می‌پذیرد.	محاسبه بهترین مسیر بر اساس پارامترهایی از جمله Bandwidth و Reliability انجام می‌پذیرد.

همگرایی (Convergence)

همگرایی تعریف یک روند کلی است که توسط آن روترهای موجود در شبکه باید سه مرحله زیر را طی نمایند:

۱- متوجه تغییرات بوجود آمده در توپولوژی گردند.

۲- ارتباطات جدید وابسته به این تغییرات را مشخص نمایند.

۳- در نهایت جدول مسیریابی را تغییر داده و اقدام به ثبت بهترین مسیرها در جدول مسیریابی نمایند.

مدت زمان مورد نیاز برای بوجود آمدن همگرایی در شبکه، یکی از مهمترین مؤلفه‌ها جهت مقایسه پروتکل‌های مسیریابی پویا می‌باشد.

سیستم خود مختار (AS)

سیستم خود مختار(Autonomous System)، به گروهی از روترها گفته می‌شود که تحت یک حوزه مدیریتی و در حال اجرای یک پروتکل مسیریابی مشترک می‌باشند.

از منظر AS پروتکل‌های مسیریابی به دو گروه تقسیم می‌شوند.

۱- **Interior Gateway Protocol**

پروتکل‌های مسیریابی که در داخل یکAS یا حوزه مسیریابی اجرا می‌شوند را پروتکل‌های دروازه داخلی IGP(Interior Gateway Protocol) می‌گویند. از جمله این پروتکل‌ها می توان بهRIP وEIGRP اشاره نمود.

۲- **Exterior Gateway Protocol**

پروتکل‌های مسیریابی که بین ASهای مختلف مورد استفاده قرار می‌گیرند را پروتکل دروازه خارجی یا EGP(Exterior Gateway Protocol) می‌گویند. پروتکل‌هایEGP وظیفه کشف مسیر بین حوزه‌های مسیریابی مختلف را بر عهده دارند. تنها نمونه EGP، پروتکلBGP می‌باشد.

Load Balancing

در صورت وجود چند مسیر به یک مقصد مشخص که توسط یک پروتکل مسیریابی به دست آمده باشد، روتر می‌تواند ضمن استفاده همزمان از مسیرها اقدام به توازن بار بر روی آنها نیز نماید. همچنین این امکان وجود دارد که در صورت از دسترس خارج شدن یک مسیر، اطلاعات توسط مسیرهای جایگزین تبادل گردد.

ویژگی Load Balancing نسبت به پروتکل مسیریابی مورد استفاده، در یک یا هر دو حالت زیر ممکن است در دسترس باشد.

۱- **مسیرهای با Metric برابر**

تقریبا تمام پروتکل‌های مسیریابی امکان استفاده از Load Balancing در صورت وجود چند مسیر با Metric برابر به یک مقصد مشخص را دارند. در مستندات فنی به این حالت Equal Cost Path نیز گفته می‌شود.

۲- **مسیرهای با Metric نا برابر**

این حالت که با نامUnequal Cost Path نیز خوانده می‌شود در بعضی از پروتکل‌های مسیریابی پویا در دسترس می‌باشد.

در این حالت امکان Load Balancing بر روی مسیرهای با Metricهای نابرابر نیز وجود دارد.

یک بار دیگر این نکته مهم را متذکر می‌شوم که در هر دو حالت فوق باید مقدار AD مسیرهای به دست آمده برابر باشند.

ویژگی Passive Interface

اینترفیس غیرفعال (Passive Interface)، به اینترفیسی اطلاق می‌گردد که از ارسال و دریافت پیام‌های مربوط به پروتکل‌های مسیریابی خودداری می‌نماید.

در صورتیکه اینترفیس روتر به شبکه داخلی و یا به هر تجهیزات دیگری غیر از روتر متصل باشد، نیازی به ارسال و دریافت پیام‌های مربوط به پروتکل‌های مسیریابی نداشته و می‌توان آنرا از پروسه پروتکل مسیریابی حذف نمود. این کار باعث جلوگیری از اتلاف منابع می گردد.

همچنین ویژگیPassive Interface در امنیت شبکه نیز کاربرد دارد. با فعال کردن این ویژگی بر روی اینترفیس متصل به شبکه خارجی مستقل از مدیریت ما (مثل اینترنت)، می توان از ارسال پیام‌های Update به آن شبکه‌ها که باعث افشای اطلاعات مسیرهای داخل شبکه می‌گردد، جلوگیری به عمل آورد.

البته لازم به ذکر است که پیکربندی یک اینترفیس به عنوان Passive Interface خللی در تبلیغ شبکه‌های متصل به آن ایجاد نمی‌نماید.

در صورتیکه اینترفیسی را به عنوان Passive Interface پیکربندی نماییم، آن اینترفیس از ایجاد، ارسال و دریافت پیام‌های مربوط به پروتکل‌های مسیریابی پویا خودداری نموده و این عمل باعث مصرف بهینه منابع روتر و شبکه می‌گردد.

اینترفیس Loopback

اینترفیس Loopback یک اینترفیس مجازی می‌باشد که همانند اینترفیس‌های فیزیکی روتر پیکربندی می‌شود. این اینترفیس که پس از ایجاد، همواره Up می‌باشد می‌تواند در زمان اشکال‌یابی، کمک قابل توجهی به مدیر شبکه نماید.

استفاده از اینترفیس Loopback در بعضی پروتکل‌های مسیریابی پویا تضمین کننده انجام صحیح پروسه مسیریابی می‌باشد.

اینترفیس Null

اینترفیسNull یک اینترفیس مجازی می‌باشد که می‌تواند جایگزین مناسبی جهت فیلترینگ ترافیک باشد. هر چند که این اینترفیس همواره Up می‌باشد، ولی نمی‌تواند هیچگونه ترافیکی را ارسال و دریافت نماید.

اینترفیسNull به عبارت خودمانی همان "دیوار" است. همانطور که در مواقع خاص دوستان خود را به سمت دیوار Route می‌کنید، وقتی می‌خواهید یک ترافیک خاصی را از بین ببرید بدون آنکه باعث ایجاد سربار برای منابع روتر گردد، می توانید از اینترفیس Null استفاده نمایید.

اینترفیس Null0 بصورت پیش فرض بر روی روتر وجود داشته و امکان حذف آن نیز نمی‌باشد. این اینترفیس قابل پیکربندی بوده و به عنوان مثال شما می توانید بر روی آن، پیام‌های Unreachable را برای ICMP پیکربندی نمایید. ولی به دلیل اینکه اینترفیس Null0 برای از بین بردن بسته‌هایی که به آن ارسال شده، ایجاد گردیده است، لذا نیازی به اعمال پیکربندی خاصی بر روی این اینترفیس نمی‌باشد.

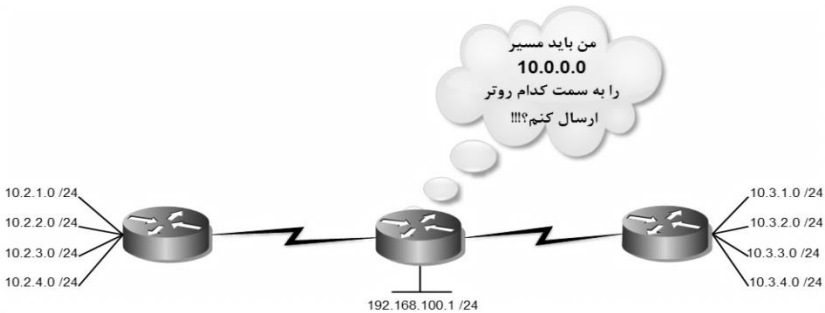
ویژگی Auto-summary

ویژگی خلاصه سازی خودکار (Auto-summary)، جهت خلاصه کردن جداول مسیریابی در بعضی از پروتکل‌های مسیریابی پویا مورد استفاده قرار می‌گیرد.

ویژگی Auto-summary خلاصه نمودن جداول مسیریابی را بر اساس کلاس‌های استاندارد A، B و C انجام داده و به جای تبلیغ تمام زیر شبکه‌ها، فقط آدرس خلاصه شده را تبلیغ می‌نماید.

به دلیل عملکرد این ویژگی در حالت Classful، در صورتیکه برای برخی از مقصدهای خلاصه شده در کلاس استاندارد، مسیر متناظری موجود نباشد، روتر بسته‌های ارسال شده به آن شبکه را به Null0 یا همان دیوار خودمان! تحویل می دهد. به همین دلیل استفاده از Auto-summary در همه شرایط نتیجه مطلوبی به همراه نخواهد داشت.

یکی دیگر از ایرادهای این ویژگی زمانی مشخص می‌شود که یک کلاس استاندارد که به زیر شبکه‌های متعدد تقسیم شده، توسط روترهای مختلفی قابل دسترس باشد. به عنوان مثال اگر در شبکه زیر ویژگیAuto-summary در حالت فعال قرار داشته باشد و روتر خلاصه سازی را بر اساس کلاس استاندارد A انجام دهد، در اینصورت به نظر شما روتر مسیر 10.0.0.0 را به کدامیک از روترها باید مسیردهی نماید تا امکان دسترسی به همه شبکه ها فراهم باشد؟



ترجمه آدرس شبکه (NAT)

ترجمه آدرس شبکه (Network Address Translation) طیRFC 1631، جهت اتصال شبکه‌های دارای آدرس Private با شبکه‌های Public مثل اینترنت، منتشر گردیده است.

عملکرد مکانیسمNAT مثل عملکرد منشی شرکت می‌باشد. منشی ضمن در اختیار داشتن خطوط مخابراتی شرکت، لیست کاملی از شماره‌های داخلی کارمندان را نیز دارد. کارمندان برای برقراری تماس با یکدیگر بدون نیاز به منشی و خطوط مخابرات، توسط شماره‌های داخلی با یکدیگر تماس برقرار می‌نمایند. ولی وقتی یکی از کارمندان می‌خواهد با شخصی بیرون از شرکت تماس بگیرد از منشی درخواست می‌کند شماره موردنظر را توسط خطوط مخابراتی که در اختیار دارد گرفته و به داخلی ایشان متصل نماید. همچنین وقتی شخصی از بیرون شرکت می‌خواهد با یکی از کارمندان تماس تلفنی داشته باشد، اقدام به برقراری تماس با شماره‌های مخابراتی شرکت نموده و از منشی شرکت می خواهد تا ارتباط تلفنی ایشان را با فرد مورد نظر در داخل شرکت برقرار نماید.

مکانیسمNAT نیز وظیفه برقراری ارتباط کلاینت‌های شبکه که از داشتن آدرس Public محروم هستند را با دنیای خارج بر عهده دارد. برای انجام عملیات فوق، روتر دارای جدولی به نام NAT Table می‌باشد که حاوی آدرس های Private متناظر با آدرس های Public اختصاص داده شده، می باشد.

نکته: **امکان استفاده از مکانیسم NAT محدود به برقراری ارتباط بین شبکه های Public و Private نمی باشد. در برخی موارد ممکن است از NAT برای برقراری ارتباط بین دو شبکه Public و یا دو شبکه Private نیز بهره برداری گردد.**

انواع NAT

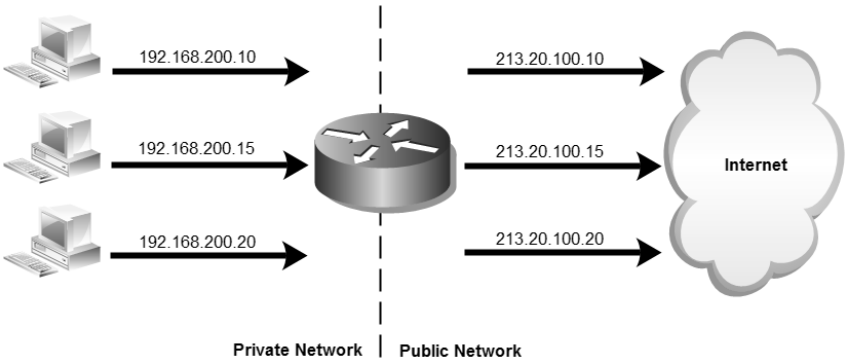
عملیاتNAT با توجه به تعداد آدرس‌های Publicای که در اختیار دارد می‌تواند در شکل‌های مختلفی انجام پذیرد که در ادامه به بررسی آنها می پردازیم.

۱- **Static NAT**

اختصاص[1] یک‌به‌یک آدرس‌هایPrivate به آدرس‌هایPublic راStatic NAT می‌گویند. در این حالت نسبت آدرس‌های Public به Private بصورت ثابت باقی می‌ماند.

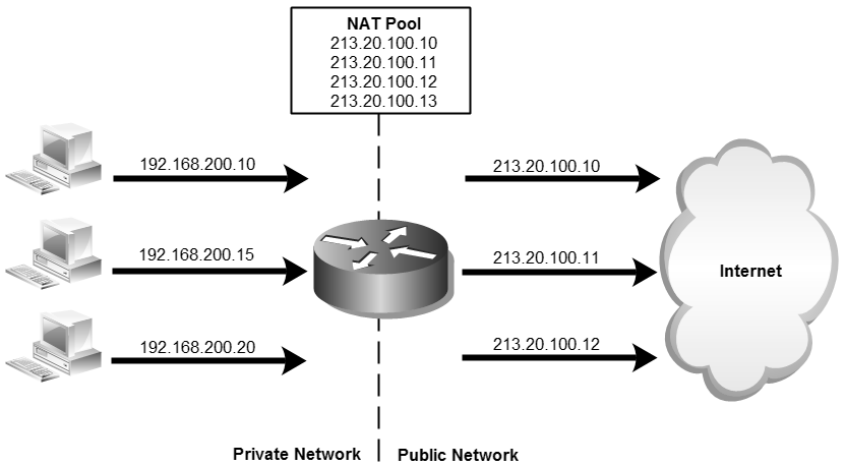
[1] Mapping

این روش مخصوصاً زمانی مورد استفاده قرار می گیرد که بخواهیم یک دستگاه داخل شبکه بطور مستقیم از بیرون شبکه قابل دسترس باشد.



۲- Dynamic NAT

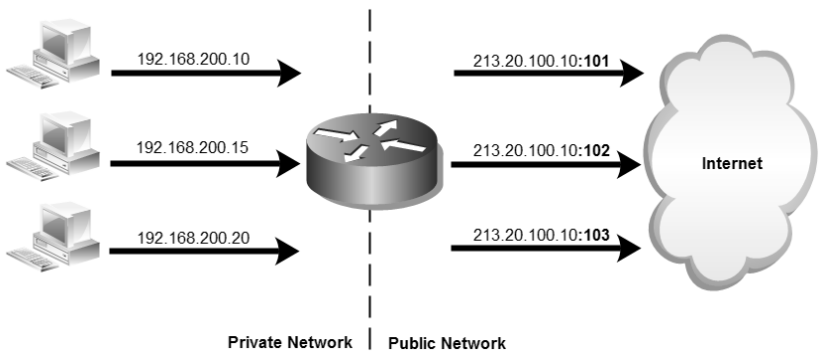
اختصاص پویای یک آدرس Public موجود در NAT Pool، به یک آدرس Private را Dynamic NAT گویند. هر چند که در این حالت همچنان تخصیص آدرس‌ها بصورت یک به یک است ولی این اختصاص پویا بوده و ممکن است در درخواست‌های بعدی کلاینت برای برقراری ارتباط با بیرون شبکه، آدرسPublic متفاوتی به آن اختصاص داده شود.



در این حالت آدرس‌های Public قابل استفاده در NAT Pool به ترتیب در اختیار درخواست کنندگان قرار می‌گیرد.

۳- Overloading

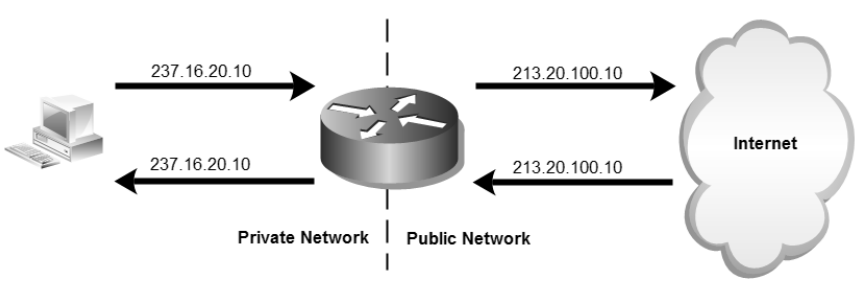
حالتی از Dynamic NAT می‌باشد که وظیفه ترجمه چند آدرس Private به یک آدرس Public را بر عهده دارد. در این صورت به دلیل داشتن فقط یک آدرس Public، تخصیص آدرس به همراه پورت‌های متفاوت به آدرس های Private صورت می‌پذیرد. به دلیل استفاده از پورت‌ها در ترجمه آدرس شبکه، به این روش (Port Address Translation) PAT ، نیز گفته می‌شود.



از این مکانیسم ممکن است در صورت وجود NAT Pool نیز استفاده شود. زمانی که تعداد کلاینت های درخواست کننده بیشتر از تعداد آدرس های موجود در NAT Pool باشد، می توان دو روش Dynamic و PAT را با یکدیگر تلفیق نمود.

۴- Overlapping

ممکن است شبکه‌ای از آدرس‌هایی استفاده کند که در شبکه دیگر مورد استفاده قرار گرفته باشد. مثلا از آدرس های Public بدون دریافت مجوز استفاده کرده و یا اینکه دو شبکه‌ای که می خواهند با یکدیگر ارتباط برقرار کنند، شبیه یکدیگر از آدرس‌های Private استفاده کرده باشند؛ در این صورت برای رفع مشکل در برقراری ارتباط از روش Overlapping استفاده می گردد.



سناریو شماره(۹)؛ Static Route

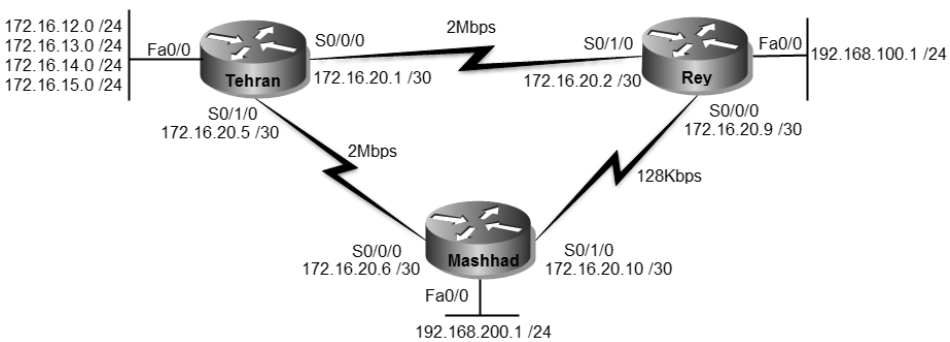
طرح مسئله:

کمپانی MTR Electronics یک شرکت بزرگ است که ساختمان مرکزی آن در تهران بوده و دارای ۲ ساختمان دیگر در شهرری و مشهد مقدس می‌باشد. این شرکت برای برقراری ارتباط بین ساختمان‌های مختلف، از شما کمک خواسته است.

ساختمان تهران دارای ۴ زیر شبکه و ساختمان‌های ری و مشهد هر کدام دارای یک شبکه می‌باشند. لینک‌های مخابراتی بین تهران با شهرری و مشهد دارای 2Mb پهنای باند می‌باشند. همچنین یک لینک مخابراتی پشتیبان نیز بین شهرری و مشهد برقرار می باشد که دارای 128Kb پهنای باند می باشد.

نیاز سنجی:

برای برقراری ارتباط بین ساختمان در شهرهای مختلف، شرکت نیاز به اجاره خطوط مخابراتی و خرید ۳ روتر با کارت های مربوطه دارد.



راه حل:

پس از پیکربندی اولیه روترها، اقدام به پیکربندی روتر تهران می‌نماییم. به دلیل اینکه از یک اینترفیس روتر برای Inter-VLAN Routing استفاده می‌کنیم، باید اینترفیس روتر را به عنوان Subinterface پیکربندی نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface fastEthernet 0/0
Tehran(config-if)#no shutdown
```

```
Tehran(config-if)#interface f0/0.2
Tehran(config-subif)#encapsulation dot1Q  2
Tehran(config-subif)#ip address 172.16.12.1 255.255.255.0
Tehran(config-subif)#inter f0/0.3
Tehran(config-subif)#encapsulation dot1Q  3
Tehran(config-subif)# ip address 172.16.13.1 255.255.255.0
Tehran(config-subif)#inter f0/0.4
Tehran(config-subif)#encapsulation dot1Q  4
Tehran(config-subif)# ip address 172.16.14.1 255.255.255.0
Tehran(config-subif)#inter f0/0.5
Tehran(config-subif)#encapsulation dot1Q  5
Tehran(config-subif)# ip address 172.16.15.1 255.255.255.0
Tehran(config-subif)#end
Tehran#write
```

پس از پیکربندی Subinterface ، خروجی دستور show ip address بصورت زیر خواهد بود:

```
Tehran#show ip route
<... Output Omitted...>

    172.16.0.0/24 is subnetted, 4 subnets
C      172.16.12.0 is directly connected, FastEthernet0/0.2
C      172.16.13.0 is directly connected, FastEthernet0/0.3
C      172.16.14.0 is directly connected, FastEthernet0/0.4
C      172.16.15.0 is directly connected, FastEthernet0/0.5
Tehran#
```

پس از اینترفیس ایترنت، اقدام به پیکربندی پورت سریال روتر که به شهرری و مشهد متصل است می‌نماییم. توجه داشته باشید به دلیل اینکه ما در سناریو اقدام به اتصال مستقیم دو پورت سریال به یکدیگر نموده‌ایم، برای مشخص کردن Clock Rate باید یکی از روترها را باید به عنوان DCE [1] تنظیم نماییم.

البته مشخص کردن Clock Rate در زمان استفاده از برنامه‌های شبیه ساز[2] و یا در لابراتوارها که فاقد مودم هستیم، انجام می‌پذیرد. در غیر اینصورت و در دنیای واقعی، معمولا این مودم‌ها هستند که وظیفه DCE/DTE[3] اتصالات را برعهده می گیرند.

برای تخصیص آدرس به لینک‌های WAN، جهت جلوگیری از به هدر رفتن آدرس‌های IP از Subnet Mask بصورت 255.255.255.252 استفاده میکنیم. با این Subnet Mask هر زیر

[1] Data Circuit-terminating Equipment
[2] Simulator
[3] Data-Terminal Equipment

شبکه دارای ۴ عدد آدرس IP خواهد بود، که اولین و آخرین آدرس برای NET ID و Broadcast اختصاص داده شده و۲ آدرس باقیمانده نیز برای آدرس‌دهی به دو طرف لینک استفاده می شود.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface serial 0/0/0
Tehran(config-if)#no shutdown
Tehran(config-if)#clock rate 2000000
Tehran(config-if)#ip address 172.16.20.1 255.255.255.252
Tehran(config-if)#interface serial 0/1/0
Tehran(config-if)#no shutdown
Tehran(config-if)#clock rate 2000000
Tehran(config-if)#ip address 172.16.20.5 255.255.255.252
Tehran(config-if)#end
Tehran#write
```

حالا می رویم سراغ پیکربندی روتر شهرری و مشهد:

```
Rey>enable
Rey#configure terminal
Rey(config)#interface fastEthernet 0/0
Rey(config-if)#no shutdown
Rey(config-if)#ip address 192.168.100.1 255.255.255.0
Rey(config-if)#interface serial 0/0/0
Rey(config-if)#no shutdown
Rey(config-if)#clock rate 128000
Rey(config-if)#ip address 172.16.20.9 255.255.255.252
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#no shutdown
Rey(config-if)#ip address 172.16.20.2 255.255.255.252
Rey(config-if)#end
Rey#write
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#ip address 192.168.200.1 255.255.255.0
Mashhad(config-if)#interface serial 0/0/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#ip address 172.16.20.6 255.255.255.252
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#ip address 172.16.20.10 255.255.255.252
Mashhad(config-if)#end
```

اگر از روتر تهران هریک از شبکه‌های مشهد یا شهرری را ping کنیم، خروجی بصورت زیر خواهد بود، که به معنی عدم دسترسی به شبکه‌های فوق می‌باشد.

البته این خروجی در زمان ping شبکه های تهران و مشهد توسط روتر شهرری نیز روی خواهد داد. همچنین اگر شبکه های شهرری و تهران را از روتر مشهد ping کنیم، همین جواب را مشاهده خواهیم نمود.

```
Tehran#ping 192.168.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Tehran#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Tehran#
```

همانطور که ملاحظه می کنید، علیرغم اینکه اتصالات برقرار است ولی امکان دسترسی به شبکه ها میسر نمی‌باشد. عدم دسترسی به دلیل این است که هر کدام از روترها از شبکه‌های متصل به روترهای همسایه خود بی اطلاع هستند. لذا برای دسترسی به شبکه‌های دیگر باید اقدام به شناسایی مسیرهای قابل دسترسی از طریق روترهای همسایه به هر یک از روترها نماییم.

```
Tehran#configure terminal
Tehran(config)#ip route 192.168.100.0 255.255.255.0 172.16.20.2
Tehran(config)#ip route 192.168.200.0 255.255.255.0 172.16.20.6
Tehran(config)#ip route 192.168.200.0 255.255.255.0 172.16.20.2 5
Tehran(config)#ip route 192.168.100.0 255.255.255.0 172.16.20.6 5
Tehran(config)#
```

در دو خط اول اقدام به معرفی شبکه هایی که با لینک 2Mbps و بطور مستقیم به روتر تهران متصل هستند، کردیم.

اما به نظر شما اگر یکی از لینک‌های مستقیم تهران با شعب قطع شود، چه اتفاقی می‌افتد؟ جواب ساده است! ارتباط تهران با آن شهر نیز قطع خواهد شد. ولی آیا با وجود لینک بین شهرری و مشهد ما نمی توانیم یک مسیر جایگزین ایجاد کنیم؟ بله ما می‌توانیم با توجه به لینک بین شهرری و مشهد، مسیر جایگزینی برای تهران فراهم آوریم. به همین دلیل مسیر دوم هر

شبکه را از شبکه دیگر ولی با Administrative Distance متفاوت برای روتر تهران مشخص می نماییم. با توجه به اینکه بصورت پیش فرض AD مسیرهای Static برابر1 می باشد، با دادن عدد 5 به AD مسیرهای جایگزین، روتر زمانی از آنها استفاده خواهد کرد که لینک اصلی در دسترس نباشد.

عمل شناسایی شبکه ها را برای روترهای شهرری و مشهد نیز تکرار خواهیم کرد.

```
Rey>enable
Rey#configure terminal
Rey(config)#ip route 172.16.12.0 255.255.252.0 172.16.20.1
Rey(config)#ip route 192.168.200.0 255.255.255.0 172.16.20.1 5
Rey(config)#ip route 172.16.12.0 255.255.252.0 172.16.20.10 5
Rey(config)#ip route 192.168.200.0 255.255.255.0 172.16.20.10
Rey(config)#end
Rey#write
```

با نوشتن آدرس شبکه تهران بصورت 172.16.12.0 255.255.252.0، به جای نوشتن آدرس ۴ شبکه موجود در ساختمان تهران، با تغییر Subnet Mask اقدام به Summarization جدول مسیریابی کرده و فقط با یک خط Route، هر ۴ شبکه را مسیر دهی می‌نماییم.

به دلیل اینکه لینک ارتباط هر شعبه با تهران دارای پهنای باند 2Mbps می باشد، مسیر اصلی را از طریق همان لینک انتخاب نموده و با تغییر AD، از آن به عنوان لینک پشتیبان شهرری و مشهد نیز استفاده می‌نماییم. اما برای ارتباط مستقیم بین شهرری و مشهد، با توجه به حجم کم ترافیک از همان لینک مستقیم 128Kb استفاده می‌کنیم.

اعمال فوق را در روتر مشهد نیز تکرار می نماییم:

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ip route 172.16.12.0 255.255.252.0 172.16.20.5
Mashhad(config)#ip route 192.168.100.0 255.255.255.0 172.16.20.9
Mashhad(config)#ip route 172.16.12.0 255.255.252.0 172.16.20.9 5
Mashhad(config)# ip route 192.168.100.0 255.255.255.0 172.16.20.5 5 Mashhad(config)#end
Mashhad#write
```

حالا در صورت ping هر یک از شبکه‌ها توسط هر کدام از روترها، جواب خوشحال کننده زیر را دریافت خواهیم نمود!

```
Tehran#ping 192.168.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/22 ms

Tehran#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/16 ms

Tehran#
```

علامت ! به معنی در دسترس بودن شبکه، علامت . به معنی انقضای زمان[1] و علامت U به معنی عدم دسترسی[2] می باشد.

طریقه عملکرد:

ابتدا به بررسی جداول مسیریابی روترها می پردازیم. لطفاً به دقت به خروجی دستور show ip route توجه نمایید!

```
Tehran#show ip route
<... Output Omitted...>
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.16.12.0/24 is directly connected, FastEthernet0/0.2
C      172.16.13.0/24 is directly connected, FastEthernet0/0.3
C      172.16.14.0/24 is directly connected, FastEthernet0/0.4
C      172.16.15.0/24 is directly connected, FastEthernet0/0.5
C      172.16.20.0/30 is directly connected, Serial0/0/0
C      172.16.20.4/30 is directly connected, Serial0/1/0
S   192.168.100.0/24 [1/0] via 172.16.20.2
S   192.168.200.0/24 [1/0] via 172.16.20.6
Tehran#
```

```
Rey#show ip route
...
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S      172.16.12.0/22 [1/0] via 172.16.20.1
C      172.16.20.0/30 is directly connected, Serial0/1/0
```

[1] Timed out
[2] Unreachable

```
C     172.16.20.8/30 is directly connected, Serial0/0/0
C   192.168.100.0/24 is directly connected, FastEthernet0/0
S   192.168.200.0/24 [1/0] via 172.16.20.10
```

```
Mashhad#show ip route
…
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S     172.16.12.0/22 [1/0] via 172.16.20.5
C     172.16.20.4/30 is directly connected, Serial0/0/0
C     172.16.20.8/30 is directly connected, Serial0/1/0
S   192.168.100.0/24 [1/0] via 172.16.20.9
C   192.168.200.0/24 is directly connected, FastEthernet0/0
Mashhad#
```

خوب توجه کردید؟ چه چیزی نظر شما را جلب کرد؟ اگر فرد باهوشی باشید که حتما هستید! متوجه شدید که تعداد مسیرهایی که در جدول مسیریابی نمایش داده می‌شوند از تعداد مسیرهایی که ما به روترها معرفی کردیم کمتر است. به عبارت دیگر در خروجی دستور show ip route از مسیرهایی که AD آنها برابر ۵ است، خبری نیست.

خوب، قبل از اینکه اعصاب مبارکتان را بهم بریزید به خروجی دستور show running روترها توجه بفرمایید:

```
Tehran#show running-config
<…Output Omitted…>
!
ip classless
ip route 192.168.100.0 255.255.255.0 172.16.20.6 5
ip route 192.168.200.0 255.255.255.0 172.16.20.2 5
ip route 192.168.100.0 255.255.255.0 172.16.20.2
ip route 192.168.200.0 255.255.255.0 172.16.20.6
!
<…Output Omitted…>
```

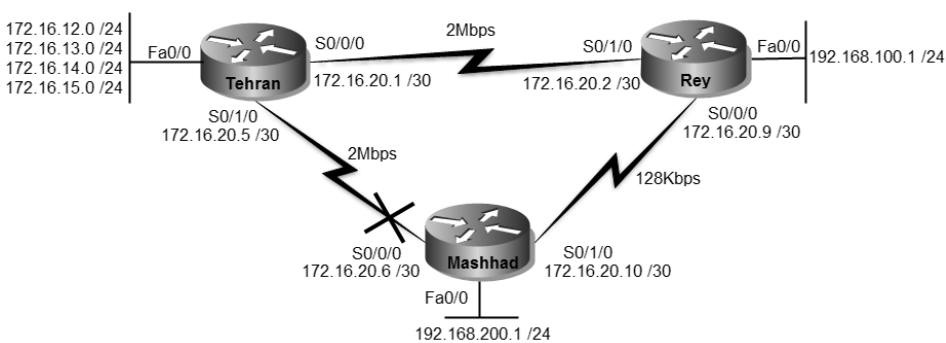
```
Rey#show running-config
<…Output Omitted…>
!
ip classless
ip route 172.16.12.0 255.255.252.0 172.16.20.1
ip route 172.16.12.0 255.255.252.0 172.16.20.10 5
ip route 192.168.200.0 255.255.255.0 172.16.20.10
ip route 192.168.200.0 255.255.255.0 172.16.20.1 5
<…Output Omitted…>
```

```
Mashhad#show running-config
<…Output Omitted…>
!
```

```
ip classless
ip route 172.16.12.0 255.255.252.0 172.16.20.5
ip route 172.16.12.0 255.255.252.0 172.16.20.9 5
ip route 192.168.100.0 255.255.255.0 172.16.20.9
ip route 192.168.100.0 255.255.255.0 172.16.20.5 5
!
<...Output Omitted...>
```

همانطور که مشاهده فرمودید، پیکربندی روترها توسط ما درست انجام شده و مسیرها نیز در فایل پیکربندی روتر موجود می‌باشند. اما دلیل درج نشدن مسیرهای جایگزین در جدول مسیریابی چیست؟ همانطور که قبلا هم گفتیم جدول مسیریابی حاوی بهترین مسیرهای موجود برای دسترسی به شبکه‌های مختلف می‌باشد. چون مسیرهای با اولویت بالاتر در دسترس هستند، روتر اقدام به درج آنها در جدول مسیریابی نموده و در صورت از کار افتادن مسیرهای اصلی، اقدام به جایگزین کردن مسیرهای دارای AD یا Metric بزرگتر در جدول مسیریابی خود خواهد نمود.

برای اینکه توضیح بالا را در عمل به چشم خود ملاحظه بفرمایید ما اقدام به قطع لینک بین تهران و مشهد می نماییم.



حالا به خروجی دستور show ip route روترهای تهران و مشهد دقت بفرمایید:

```
Tehran#sh ip route
<...Output Omitted...>
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C     172.16.12.0/24 is directly connected, FastEthernet0/0.2
C     172.16.13.0/24 is directly connected, FastEthernet0/0.3
C     172.16.14.0/24 is directly connected, FastEthernet0/0.4
C     172.16.15.0/24 is directly connected, FastEthernet0/0.5
C     172.16.20.0/30 is directly connected, Serial0/0/0
S   192.168.100.0/24 [1/0] via 172.16.20.2
```

```
S   192.168.200.0/24 [5/0] via 172.16.20.2
Tehran#
```

```
Mashhad#sh ip route
<…Output Omitted…>
Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S      172.16.12.0/22 [5/0] via 172.16.20.9
C      172.16.20.8/30 is directly connected, Serial0/1/0
S   192.168.100.0/24 [1/0] via 172.16.20.9
C   192.168.200.0/24 is directly connected, FastEthernet0/0
Mashhad#
```

بله! همانطور که ملاحظه می فرمایید مسیرهایی که AD آنها ۵ می باشد جایگزین لینک قطع شده بین تهران و مشهد شده‌اند.

حتما خوشحال شدید؟ ولی این خوشحالی دوامی نخواهد داشت. چراکه اگر اقدام به ping شبکه های تهران از روتر مشهد و یا بالعکس نمایید، نتیجه ای جز در دسترس نبودن شبکه نخواهید داشت.

```
Tehran#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

البته به این نکته توجه داشته باشید هر چند که امکان ping توسط روترها ممکن نیست ولی در صورتیکه توسط یک کلاینت اقدام به ping نمایید، امکان دسترسی فراهم خواهد بود!

یک فوت کوزه گری! دلیل اینکه شبکه‌ها برای کلاینت‌ها قابل دسترس است ولی برای روترها نه، عدم شناسایی آدرس لینک‌ها در تمامی روترهای شبکه می باشد. وقتی شما اقدام به ping یک شبکه از داخل روتر می‌نمایید، آدرس مبدا بسته ping، آدرس اینترفیسی خواهد بود که روتر بسته را توسط آن به سوی شبکه مقصد ارسال می‌نماید. مثلا زمان قطع بودن لینک تهران و مشهد اگر اقدام به ping شبکه مشهد توسط روتر تهران نمایید، آدرس مبدا بسته 172.16.20.1 خواهد بود. آیا شما به روتر مشهد شبکه‌ای که شامل این آدرسIP باشد را معرفی نموده‌اید؟ مسلما جواب نه خواهد بود. پس انتظار جواب از سوی روتر مشهد را نیز نداشته باشید!

در این سناریو برای اینکه بتوانید توسط روتر تهران شبکه مشهد و توسط روتر مشهد شبکه های تهران را ping کنید دو راه حل پیش رو دارید: اول اینکه شروع به معرفی آدرس‌های لینک

بین روترها نمایید. این کار نه تنها نفعی ندارد بلکه باعث اضافه شدن سربار مدیریتی و همچنین استفاده بیشتر از منابع روتر خواهد شد. دومین راه حل این است که از دستور ping بصورت پیشرفته استفاده کنید. به دلیل اینکه ما خیلی حرفه‌ای هستیم! از همین روش استفاده می‌کنیم.

برای استفاده از ping بصورت پیشرفته یا توسعه یافته[1]، باید ابتدا دستور ping را بدون هیچ پارامتر دیگری وارد نمایید. در این صورت ping به ازاء تمام پارامترها از شما نظرخواهی می‌کند. اگر با مقادیر پیش فرض می‌خواهید کار را ادامه دهید، با زدن کلید Enter به گزینه بعدی رفته و در غیر اینصورت می‌توانید مقدار مورد نظر را به پارامتر اختصاص دهید. فقط توجه داشته باشید در جواب سوال Extended commands [n]: حرف y را به معنی "بله" وارد نموده و برای پارامتر Source address or interface: نیز آدرس ای را وارد نمائید که برای روتر مقصد شناخته شده باشد.

```
Tehran#ping
Protocol [ip]:
Target IP address: 192.168.200.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.12.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.12.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/14 ms

Tehran#
```

همانطور که مشاهده می‌کنید اگر آدرس مبدا بستهping ارسالی روتر تهران، شبکه 172.16.12.1 که توسط روتر مشهد شناسایی شده باشد، شبکه برای روتر تهران قابل دسترس خواهد بود.

[1] Extended

طریقه درج مسیرها در جدول مسیریابی را مشاهده نمودید. این جدول نسبت به در دسترس بودن مسیرها و اولویت تخصیص داده شده به آنان، همواره شامل بهترین مسیر قابل استفاده برای مقاصد مختلف خواهد بود.

مرجع دستور Command Reference:

Ping Character Description	
Character	**Description**
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

Ping Command Field Descriptions	
Field	**Description**
Protocol [ip]:	Prompts for a supported protocol. Enter appletalk, clns, ip, novell, apollo, vines, decnet, or xns. The default is ip.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.
Repeat count [5]:	Number of ping packets that are sent to the destination address. The default is 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds). The ping is declared successful only if the ECHO REPLY packet is received before this time interval.
Extended commands [n]:	Specifies whether or not a series of additional commands appears. The default is no.
Source address or interface:	The interface or IP address of the router to use as a source address for the probes. The router normally picks the IP address of the outbound interface to use. The interface can also be mentioned, but with the

Ping Command Field Descriptions	
	correct syntax as shown here: Source address or interface: ethernet 0 **Note:** This is a partial output of the extended **ping** command. The interface cannot be written as e0.
Type of service [0]:	Specifies the Type of Service (ToS). The requested ToS is placed in each probe, but there is no guarantee that all routers process the ToS. It is the Internet service's quality selection. The default is 0.
Set DF bit in IP header? [no]:	Specifies whether or not the Don't Fragment (DF) bit is to be set on the ping packet. If yes is specified, the Don't Fragment option does not allow this packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU), and you will receive an error message from the device that wanted to fragment the packet. This is useful for determining the smallest MTU in the path to a destination. The default is no.
Validate reply data? [no]:	Specifies whether or not to validate the reply data. The default is no.
Data pattern [0xABCD]	Specifies the data pattern. Different data patterns are used to troubleshoot framing errors and clocking problems on serial lines. The default is [0xABCD].
Loose, Strict, Record, Timestamp, Verbose[none]:	IP header options. This prompt offers more than one option to be selected. They are: • **Verbose** is automatically selected along with any other option. • **Record** is a very useful option because it displays the address(es) of the hops (up to nine) the packet goes through. • **Loose** allows you to influence the path by specifying the address(es) of the hop(s) you want the packet to go through. • **Strict** is used to specify the hop(s) that you want the packet to go through, but no other hop(s) are allowed to be visited. • **Timestamp** is used to measure roundtrip time to particular hosts. The difference between using the **Record** option of this command and using the **traceroute** command is that, the **Record** option of this command not only informs you of the hops that the echo request (ping) went through to get to the destination, but it also informs you of the hops it visited on the return path. With the **traceroute** command, you

Ping Command Field Descriptions	
	do not get information about the path that the echo reply takes. The **traceroute** command issues prompts for the required fields. Note that the **traceroute** command places the requested options in each probe. However, there is no guarantee that all routers (or end nodes) process the options. The default is none.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets that are sent. This is used to determine the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Performance problems caused by packet fragmentation is thus reduced. The default is no.
!!!!!	Each exclaimation point (!) denotes receipt of a reply. A period (.) denotes that the network server timed out while waiting for a reply. Refer to ping characters for a description of the remaining characters.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Static Route		
	Command or Action	**Purpose**
Step 1	enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	ip routing Example: Router(config)# ip routing	Enables IP routing.
Step 4	ip route *dest-prefix mask next-hop-ip-address* [*admin-distance*] [permanent] Example: Router(config)# ip route 192.168.24.0 255.255.255.0 172.28.99.2	Establishes a static route.
Step 5	end	Returns to privileged EXEC mode.
Step 6	show ip route Example: Router# show ip route	Displays the current routing table information. • Verify that the gateway of last resort is set.

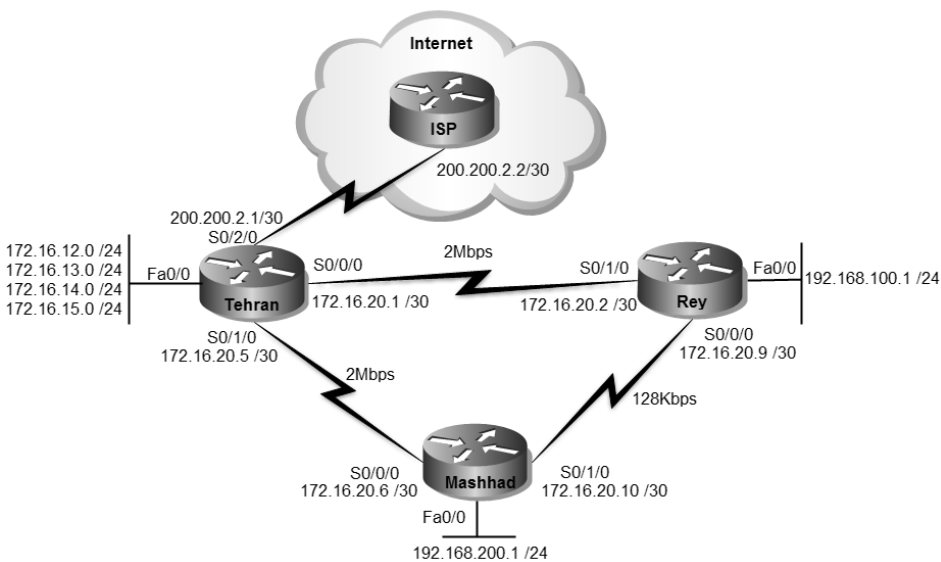
سناریو شماره(۱۰): ترجمه آدرس شبکه

طرح مسئله:

کمپانی MTR Electronics اقدام به اجاره یک اتصال اینترنت در تهران نموده است. شرکت ISP هم یک آدرس Valid به این شرکت اختصاص داده است. مدیران شرکت از شما خواسته‌اند امکان برقراری ارتباط با اینترنت را برای کلاینت‌های هر سه ساختمان این شرکت فراهم آورید.

نیاز سنجی:

با توجه به اینکه در شبکه از آدرس‌های Private استفاده نمودیم برای برقراری ارتباط با اینترنت نیاز به انجام عملیات NAT جهت ترجمه آدرس Private به Public و بالعکس داریم.



به دلیل اینکه ما فقط یک آدرسPublic داریم لذا باید ازNAT در حالت Overloading استفاده نماییم.

راه حل:

ابتدا اقدام به پیکربندی اینترفیس متصل به ISP می نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface serial 0/2/0
Tehran(config-if)#no shutdown
Tehran(config-if)#ip address 200.200.2.1 255.255.255.252
Tehran(config-if)#end
Tehran#write
```

حالا باید اقدام به نوشتن Default Route برای تمام روترها نماییم. با داشتن Default Route اگر بسته‌ای به روتر برسد که آدرس مقصد آن در جدول مسیریابی روتر موجود نباشد، روتر بجای حذف بسته، آنرا به آدرس Default Route ارسال می‌نماید.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#ip route 0.0.0.0 0.0.0.0 200.200.2.2
Tehran(config)#end
Tehran#write
```

```
Rey>enable
Rey#configure terminal
Rey(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1
Rey(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.10 5
Rey(config)#end
Rey#write
```

دلیل نوشتن دوDefault Route باAD مختلف، امکان استفاده از لینک‌هایBackup می باشد.

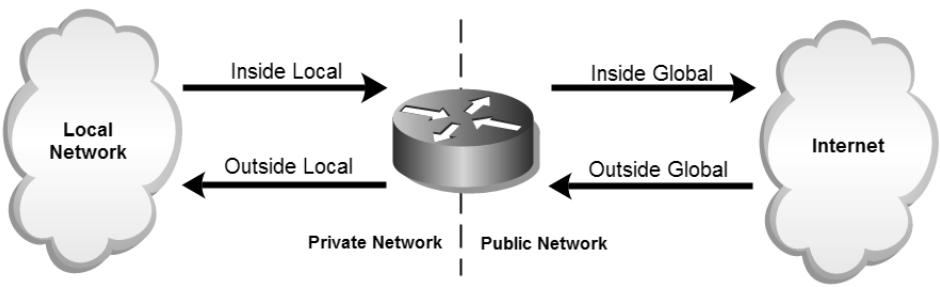
```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.5
Mashhad(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.9 5
Mashhad(config)#end
Mashhad#write
```

پس از انجام مراحل فوق، علیرغم اینکه ما شبکه 200.200.2.0/30 را برای روترهای شهرری و مشهد معرفی نکرده‌ایم، ولی به دلیل وجود Default Route امکان ping آدرس 200.200.2.1 از روترهای شهرری و مشهد فراهم می باشد.

```
Mashhad#ping 200.200.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/23 ms
```

هر چند که امکان ping آدرس 200.200.200.1 فراهم است ولی امکان دسترسی به آدرس‌های اینترنت برای روترها امکان پذیر نمی‌باشد. دلیل عدم دسترسی به اینترنت غیرقابل مسیریابی بودن آدرس Private در اینترنت می‌باشد. به همین علت ما اقدام به راه اندازی NAT بر روی اینترفیس روتر تهران که به ISP متصل است، می نماییم.

قبل از شروع به پیکربندیNAT، به تصویر زیر دقت کنید تا فعالیت‌های روتر در زمان استفاده از مکانیسم NAT را متوجه شوید.



همانطور که ملاحظه می کنید برای مکانیسمNAT در روتر، نیاز به مشخص کردن اینترفیس ورودی به عنوان inside و اینترفیس خروجی به عنوان outside می‌باشد. به همین دلیل اینترفیس متصل به ISP را به عنوان Outside و اینترفیس‌های دیگر روتر را به عنوان inside پیکربندی می کنیم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface range fastEthernet 0/0.2 - fa0/0.5
Tehran(config-if-range)#ip nat inside
Tehran(config-if-range)#interface serial 0/0/0
Tehran(config-if)#ip nat inside
Tehran(config-if)#inter serial 0/1/0
Tehran(config-if)#ip nat inside
Tehran(config-if)#interface serial 0/2/0
Tehran(config-if)#ip nat outside
Tehran(config-if)#end
Tehran#write
```

برای مشخص نمودن شبکه های داخلی مورد نظر جهت اعطای اجازه NAT، اقدام به تعریف Access List و سپس Assign آن به عملیات NAT می نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#ip access-list extended 100
Tehran(config-ext-nacl)#permit ip 172.16.12.0 0.0.3.255 any
Tehran(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 any
Tehran(config-ext-nacl)#permit ip 192.168.200.0 0.0.0.255 any
Tehran(config-ext-nacl)#exit
Tehran(config)#ip nat inside source list 100 interface serial 0/2/0
Tehran(config)#exit
Tehran#
```

در Access List 100 شبکه‌های مورد نظر جهت ترجمه به آدرس Public را مشخص نمودیم. سپس توسط دستور ip nat اقدام به مرتبط ساختن ACL و اینترفیس خروجی جهت مکانیسم NAT نمودیم.

حالا وقت آن رسیده که با استفاده از روش پیشرفته ping اقدام به بررسی ارتباط با وب سرور سیسکو به آدرس 198.133.219.25 بر روی اینترنت نماییم.

```
Mashhad#ping
Protocol [ip]:
Target IP address: 198.133.219.25
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.200.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
```

همانطور که ملاحظه می نمایید ارتباط ما با اینترنت با مکانیسم NAT برقرار شده است. اگر همین حالا با استفاده از دستور show ip nat statistics به بررسی عملیات انجام شده بپردازید، خروجی زیر را مشاهده خواهید نمود.

```
Tehran#show ip nat translations
Pro  Inside global    Inside local      Outside local     Outside global
icmp 200.200.2.1:21   192.168.200.1:21  198.133.219.25:21 198.133.219.25:21
icmp 200.200.2.1:22   192.168.200.1:22  198.133.219.25:22 198.133.219.25:22
icmp 200.200.2.1:23   192.168.200.1:23  198.133.219.25:23 198.133.219.25:23
icmp 200.200.2.1:24   192.168.200.1:24  198.133.219.25:24 198.133.219.25:24
icmp 200.200.2.1:25   192.168.200.1:25  198.133.219.25:25 198.133.219.25:25
```

در جدول فوق می توانید اتفاقاتی که بر روی آدرس IP در زمان عبور از روی اینترفیس‌های inside و outside روی داده است را مشاهده نمایید. برای ۵ پیامی که دستور ping از طریق آدرس 192.168.200.1 به وب سرور سیسکو ارسال نموده است، مکانیسم NAT بر روی روتر تهران ۵ بار اقدام به ترجمه آدرس با پورتهای متفاوت نموده است. ولی به دلیل اینکه آدرس‌های اینترنت در داخل شبکه قابل مسیریابی هستند، آدرس اینترنت در زمان ورود به شبکه هیچ تغییری نکرده و فقط پورت آن بر اساس پورت پیام درخواستی تنظیم شده است.

عمر نگهداری آدرس‌های ترجمه شده در جدول NAT روتر ۲۴ساعت می باشد و پس از مدت زمان فوق اقدام به پاک نمودن اطلاعاتی که هیچ فعالیتی نداشته‌اند، از جدول NAT خود می‌نماید.

طریقه عملکرد:

نوشتن Default Route باعث میگردد روترهای شهرری و مشهد در صورت دریافت بسته‌ای که هیچ متناظری برای آدرس مقصد آن در جدول مسیریابی موجود نباشد، اقدام به ارسال آن به آدرس Default Route نمایند. همچنین روتر تهران نیز بسته‌های با مقصد ناشناخته دریافتی از شبکه‌های متصل به خود و دیگر روترها را به آدرس ISP که به عنوان Default Route معرفی گشته، ارسال می نماید.

شبکه‌های داخلی که میخواهیم اجازه استفاده از مکانیسمNAT داشته باشند را توسط Access List مشخص می نماییم.

اینترفیس‌های روتر که به شبکه داخلی متصل هستند را به عنوان inside و اینترفیس روتر که به شبکه خارجی(مثل اینترنت) متصل است را به عنوان outside معرفی می‌نماییم.

به دلیل اینکه تعدادIP Valid اختصاص داده شده به شرکت از تعداد کلاینت‌هایی که می‌خواهند از اینترنت استفاده کنند کمتر است باید از NAT Overloading استفاده نماییم. به

همین دلیل با استفاده از دستور ip nat اقدام به مرتبط نمودن ACL با اینترفیس خروجی و نوع NAT مورد استفاده می‌نماییم. پس از انجام عملیات فوق خروجی دستور show running-config در روتر تهران بصورت زیر خواهد بود.

```
Tehran#sh running-config
<…Output Omitted…>
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.16.12.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 172.16.13.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 172.16.14.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 172.16.15.1 255.255.255.0
 ip nat inside
!
…
!
interface Serial0/0/0
 ip address 172.16.20.1 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/0
 ip address 172.16.20.5 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/0
 ip address 200.200.2.1 255.255.255.252
 ip nat outside
 !
…
!
ip nat inside source list 100 interface Serial0/2/0 overload
ip classless
ip route 192.168.100.0 255.255.255.0 172.16.20.6 5
ip route 192.168.200.0 255.255.255.0 172.16.20.6
ip route 192.168.200.0 255.255.255.0 172.16.20.2 5
```

```
ip route 192.168.100.0 255.255.255.0 172.16.20.2
ip route 0.0.0.0 0.0.0.0 200.200.2.2
!
!
access-list 100 permit ip 172.16.12.0 0.0.3.255 any
access-list 100 permit ip 192.168.100.0 0.0.0.255 any
access-list 100 permit ip 192.168.200.0 0.0.0.255 any
!
...
Tehran#
```

روتر تهران قبل از ارسال بسته‌ها به اینترفیس outside اقدام به مقایسه آدرس مبدا بسته با ACL مرتبط با NAT می‌نماید. در صورتیکه شبکه مبدا در ACL به عنوان permit تعریف شده باشد، روتر مکانیسم NAT را بر روی بسته انجام داده و سپس اقدام به ارسال بسته می‌نماید و در غیر اینصورت اقدام به حذف بسته می‌نماید.

درNAT Overloading به علت کمبود آدرسIP، مکانیسمNAT به ازاء پیام‌های ارسالی مختلف اقدام به ترجمه آنها به یک آدرس معتبر ولی با پورت‌های متفاوت می‌نماید. سپس آدرس‌های ترجمه شده و پورت‌های متناظر را تا ۲۴ ساعت در جدول NAT نگهداری می‌نماید تا در صورت دریافت جواب از شبکه خارجی (مثل اینترنت) بتواند بسته را تحویل درخواست کننده بدهد.

توجه داشته باشید در این نوع مکانیسم، اطلاعاتی از شبکه خارجی می‌تواند به شبکه داخلی وارد شود که قبلا توسط کلاینت‌های داخلی درخواست و در جدولNAT ثبت شده باشد. به عبارت دیگر در صورت استفاده از مکانیسم‌های پویای NAT (مثل Dynamic NAT و یا NAT Overloading) بطور معمول شبکه خارجی نمی‌تواند مبدا برقراری ارتباط باشد.

در صورتیکه بخواهیم امکان دسترسی به یک کامپیوتر مثل وب سرور در شبکه داخلی را برای شبکه خارجی فراهم نماییم باید از مکانیسم Static NAT استفاده نماییم.

مرجع دستور Command Reference:

Network Address Translation	
Dynamic NAT	**ip nat source** { **list** { *access-list-number* | *access-list-name* } **interface** *type number* | **pool** *name* } [**overload** | **vrf** *name*]
Network Static NAT	**ip nat source static network** *local-network global-network mask* [**extendable | no-alias | no-payload** | **vrf** *name*]
Static NAT	**ip nat source static** { **esp** *local-ip* **interface** *type number* | *local-ip global-ip* } [**extendable | no-alias | no-payload** | **vrf** *name*]

پارامترهای مورد استفاده دستورات فوق، در جدول زیر شرح داده شده است:

Syntax Description	
list *access- list-number*	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access- list-name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
Interface*type*	Specifies the interface type for the global address.
interface*number*	Specifies the interface number for the global address.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
Overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static *local-ip*	Sets up a single static translation. The *local-ip* argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from the RFC 1918, or obsolete.
local-port	Sets the local TCP/UDP port in a range from 1 to 65535.
static*global-ip*	Sets up a single static translation. The *local-ip* argument establishes the globally unique IP address of an inside host as it appears to the outside network.
global-port	Sets the global TCP/UDP port in the range from 1 to 65535.
Extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits as alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
esp *local-ip*	Establishes IPSec-ESP (tunnel mode) support.
Tcp	Establishes the Transmission Control Protocol.
Udp	Establishes the User Datagram Protocol.
network*local-network*	Specified the local subnet translation.
global-network	Specifies the global subnet translation.
Mask	Establishes the IP network mask to be used with subnet translations.

☑ مبحث دوم

پروتکل RIP

پروتکل اطلاعات مسیریابی(Routing Information Protocol)، اولین پروتکل مسیریابی پویا بوده که توسط سازمانIETF به صورت استاندارد منتشر گردیده است. پروتکلRIP در گروه پروتکل‌هایDistance Vector قرار گرفته و از پارامترhop-count برای تشخیص بهترین مسیر استفاده می کند. این پروتکل برای کار در شبکه های مبتنی بر IPv4 دارای دو نسخه می‌باشد.

نسخه اول RIP

اولین نسخه پروتکل RIP با عنوان RIP v1 توسط RFC 1058 منتشر گردیده که خصوصیات اصلی این نسخه بصورت زیر می‌باشد:

- در گروه پروتکل های Distance Vector قرار دارد.
- پروتکلی استClassful که امکان گنجاندنSubnet Mask آدرس هایIP را در پیام‌های مسیریابی ندارد.
- پیام های Update را بصورت Broadcast ارسال می‌نماید.
- محاسبه Metric در این پروتکل بر اساس تعداد گام(hop-count) انجام می پذیرد.
- حداکثر تعداد hop در این پروتکل ۱۵ عدد می باشد. این محدودیت به دلیل جلوگیری از بروز چرخه لایه سه در شبکه است.
- تناوب ارسال پیام‌های Update در این پروتکل بصورت پیش فرض ۳۰ ثانیه می‌باشد.
- امکان Equal Cost Path Load Balancing در این نسخه وجود دارد.

این نسخه امروزه منسوخ شده و جای خود را به نسخه دوم این پروتکل داده است.

نسخه دوم RIP

به دلیل ایرادهای موجود در نسخه اول پروتکلRIP، سازمان IETF اقدام به انتشار نسخه بروز شده این پروتکل با عنوان RIP v2 و تحت استاندارد RFC 1721 نمود. ویژگی‌های این نسخه که اساس آن بر پایه RIP v1 است، بصورت زیر می باشد:

- در گروه پروتکل‌های Distance Vector قرار دارد.
- پروتکلی است Classless که امکان گنجاندن Subnet Mask آدرس‌های IP را در پیام‌های مسیریابی دارد.
- از ویژگی های خلاصه سازی، CIDR و VLSM پشتیبانی می‌کند.
- پیام های Update را بصورت Multicast و به آدرس 224.0.0.9 ارسال می‌نماید.
- محاسبه Metric در این پروتکل بر اساس تعداد گام(hop-count) انجام می پذیرد.
- حداکثر تعداد hop در این پروتکل ۱۵ عدد می‌باشد. این محدودیت به دلیل جلوگیری از بروز چرخه لایه سه در شبکه است.
- امکان استفاده از ویژگی Authentication در این نسخه فراهم گردیده است.
- فیلد آدرس Next Hub در جدول مسیریابی اضافه شده است.
- پروتکلRIP از اتصال UDP و پورت 520، برای ارسال اطلاعات خود استفاده می‌نماید.
- ویژگی Auto-summary در این پروتکل بصورت پیش فرض فعال می‌باشد.
- از ویژگی Equal Cost Path Load Balancing پشتیبانی می‌کند.

طریقه عملکرد RIP

پروتکل RIP، معمولا در شبکه‌های کوچک که دارای تعداد کمی روتر می‌باشند مورد استفاده قرار می‌گیرد. این پروتکل به دلیل استفاده از hop-count دارای محدودیت در تعداد روتر می‌باشد. منظور از Hop-count، تعداد روترهایی می باشد که یک بسته برای رسیدن به مقصد باید از آنها عبور نماید.

پروتکل RIP برای تبادل اطلاعات مسیریابی خود با روترهای همسایه اقدام به ارسال اطلاعات مسیریابی در قالب پیام‌هایAdvertisement می‌نماید. این پیام‌ها توسط پورتUDP 520 هر ۳۰ ثانیه یکبار بصورت Multicast با آدرس224.0.0.9 به روترهای دیگر ارسال می‌نماید.

همگرایی(Convergence) در شبکه‌هایی که از پروتکل مسیریابیRIP استفاده می‌نمایند بصورت کند انجام می پذیرد. بطور مثال در صورت وجود ۱۵ عدد روتر در شبکه و با توجه به

اینکه پیام‌های Advertisement هر ۳۰ ثانیه یکبار تولید و ارسال می گردند، 450=30*15 ثانیه (بیش از ۷ دقیقه) زمان لازم است تا در صورت بوجود آمدن یک تغییر، شبکه به همگرایی برسد.

روترها باید بطور متناوب هر ۳۰ ثانیه پیام Update را از روترهای همسایه خود دریافت نمایند. در صورتی که روتر ۶ برابر مدت زمان معمول ارسال پیام‌ها یعنی ۱۸۰ ثانیه، پیام جدیدی از یک روتر دریافت ننماید، مسیرهای بدست آمده از روتر مورد نظر را در وضعیت غیرقابل استفاده (nonupdating) قرار می‌دهد. اگر مدت زمان تعویق دریافت پیام‌ها ادامه پیدا کرده و به ۸ برابر زمان معمول یعنی ۲۴۰ ثانیه بطول انجامد، روتر اقدام به حذف مسیرهای بدست آمده از طریق روتر مورد نظر خواهد کرد.

مقدار Administrative Distance پروتکل RIP بصورت پیش فرض برابر 120 می‌باشد. همچنین این پروتکل برای تعیین بهترین مسیر بر اساس Metric تصمیم گیری می‌نماید. محاسبه Metric در پروتکلRIP نسبت به تعداد روتر موجود بین مبدا و مقصد انجام می پذیرد. هرچه تعداد روترهای بین مبدا و مقصد بسته کمتر باشد، آن مسیر دارای Metric بهتری نسبت به بقیه مسیرهای بدست آمده خواهد بود، حتی اگر پهنای باند کمتری نسبت به آنها داشته باشد.

برای مشخص کردن Default Network در زمان اجرای پروتکل RIP، می توان آنرا بر روی روتر اصلی متصل به Default Network مشخص نموده و سپس توسط پیام‌های Update آنرا به اطلاع دیگر روترهای شبکه رساند.

پروتکلRIP v2 بواسطه پشتیبانی از Classless و گنجاندن Subnet Mask آدرس‌ها در پیام‌های مسیریابی خود، امکان استفاده از ویژگی‌های خلاصه سازی، CIDR و VLSM را نیز فراهم نموده است.

زمان سنج[1]های RIP

پروتکل مسیریابی RIP برای انجام عملیات خود از چندین پارامتر زمانی مختلف بهره می‌برد. با توجه به شرایط شبکه، ممکن است برای کارایی بهتر نیاز به تغییر برخی مقادیر پیش فرض اختصاص داده شده به این زمان سنج ها، داشته باشید. این زمان سنج‌ها عبارتند از:

۱- **Update**

فاصله زمانی بین ارسال پیام‌های بروز رسانی روترها می‌باشد. مقدار پیش فرض این زمان سنج ۳۰ ثانیه می‌باشد.

[1] Timer

۲- **Invalid Timer**

در صورت عدم دریافت پیام بروز رسانی یک روتر پس از گذشت این زمان که بطور پیش فرض ۱۸۰ ثانیه می‌باشد، مسیرهای بدست آمده از روتر مورد نظر غیر فعال شده ولی از جدول مسیریابی حذف نمی‌شوند.

مقدار این زمان سنج باید حداقل ۳ برابر زمان سنج Update تنظیم شده باشد.

۳- **Hold-down timer**

در صورت از دسترس خارج شدن یک مسیر، روتر با ارسال پیامPoison Route به دیگر روترهای شبکه آنها را از مسیر معیوب آگاه می‌سازد. روتر دریافت کننده پیام Poison Route به مقدار مدت زمان Hold-down Timer پیام را نگه داشته تا شبکه به همگرایی برسد. اگر در خلال این مدت زمان روتر مسیری را برای شبکه مورد نظر دریافت نماید، فرض را بر چرخه[1] لایه سوم گذاشته و آنرا نادیده می‌گیرد.

مقدار این زمان سنج که بصورت پیش فرض۱۸۰ ثانیه می‌باشد باید حداقل ۳ برابر مقدار زمان سنج Update تنظیم شده باشد.

زمان سنج Hold-down Timer توسط سیسکو به پروتکل RIP اضافه گردیده است.

۴- **Flush Timer**

در صورت عدم دریافت پیام بروز رسانی از روتر همسایه پس از گذشت این زمان که بصورت پیش فرض ۲۴۰ ثانیه می‌باشد، روتر اقدام به حذف مسیرهایی می‌نماید که توسط روتر فوق به دست آمده است.

توسط دستور show ip protocols در روترهای سیسکو، می توانید مقدار زمان تخصیص داده شده به زمان سنج های فوق را بررسی نمایید.

تعامل بین RIP v1 و RIP v2

پس از پیکربندیRIP بر روی روتر، بصورت پیش فرض اینترفیس‌های روتر پیام‌های هر دو نسخه RIP v1 و RIP v2 را دریافت نموده ولی صرفا اقدام به ارسال اطلاعات مسیریابی در قالب RIP v1 می‌نمایند. توسط دستورهای زیر می‌توانید امکان ارسال و دریافت نسخه‌های مختلف RIP را بصورت هم زمان و یا انفرادی بر روی اینترفیس مورد نظر پیکربندی نمایید.

[1] Loop

Command	Purpose
Router(config-if)# ip rip send version 1	Configures an interface to send only RIP Version 1 packets.
Router(config-if)# ip rip send version 2	Configures an interface to send only RIP Version 2 packets.
Router(config-if)# ip rip send version 1 2	Configures an interface to send RIP Version 1 and Version 2 packets.

Command	Purpose
Router(config-if)# ip rip receive version 1	Configures an interface to accept only RIP Version 1 packets.
Router(config-if)# ip rip receive version 2	Configures an interface to accept only RIP Version 2 packets.
Router(config-if)# ip rip receive version 1 2	Configures an interface to accept either RIP Version 1 or 2 packets.

به این نکته توجه داشته باشید در صورتی که توسط دستور زیر اقدام به مشخص نمودن نسخه RIP نمایید، روتر تمام ارسال و دریافت‌ها را بر اساس همان نسخه انجام خواهد داد.

Command	Purpose
Router(config-router)# **version** {**1** | **2**}	Configures the software to receive and send only RIP Version 1 or only RIP Version 2 packets.

ویژگی Authentication

یکی از تفاوت‌های اصلی RIP v2 نسبت به نسخه قبلی خود، پشتیبانی از ویژگی تصدیق هویت یا Authentication می‌باشد. با استفاده از این ویژگی روترها قبل از ارسال و دریافت پیام‌های حاوی اطلاعات مسیریابی، اقدام به Authentication روتر مقابل خود می‌نمایند.

پیاده سازی Authentication در یکی از دو حالت زیر امکان پذیر است:

۱- **متن ساده**

در این حالت رشته کلید[1] مورد استفاده جهت Authentication بین روترها بصورت متن ساده[2] تبادل می‌گردد.

[1] Key-chain
[2] Clear Text

۲- MD5[1]

در این حالت رشته کلید (Key-chain) مورد استفاده، بصورت کد در هم ریخته[2] بر اساس الگوریتم MD5، بین روترها منتقل می‌گردد. استفاده از این روش باعث افزایش امنیت و جلوگیری از شنود رشته کلید توسط هکرها می‌گردد.

الگوریتم MD5 که آن را اثر انگشت[3] نیز می‌نامند، توسط RFC 1321 ارائه گردیده است. این الگوریتم عمل کد گذاری اطلاعات را بر اساس Hash کردن آن بصورت ۱۲۸ بیتی انجام می دهد.

[1] Message Digest 5
[2] Hash
[3] Fingerprint

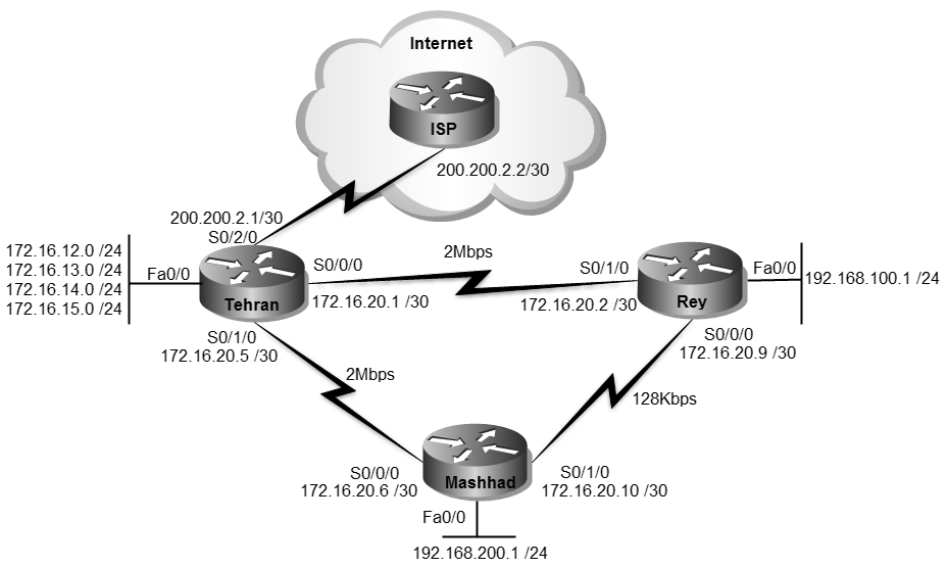
سناریو شماره(۱۱): راه اندازی RIP

طرح مسئله:

همان سناریوی قبلی که در آن اقدام به راه اندازی مسیریابی بصورت Static برای MTR Electronic کرده بودیم را می‌خواهیم این بار با استفاده از پروتکل مسیریابی پویا پیکربندی نماییم.

نیاز سنجی:

با توجه به تعداد کم روترها می‌خواهیم از پروتکل RIP v2 برای این پروژه استفاده کنیم. موارد مورد نیاز دیگر نیز همانند دو سناریوی قبل بوده و از تکرار آن خودداری می نماییم.



راه حل:

در این سناریو پیکربندی روترها بجز در موارد نوشتن مسیر Static همانند سناریوی قبل می‌باشد. لذا جهت جلوگیری از اطاله کلام، از تکرار پیکربندی اولیه روترها که در سناریوهای قبلی به آن ها پرداخته شده خودداری کرده و مستقیما به سراغ پیکربندی RIP می‌رویم.

فقط توجه داشته باشید که اگر میخواهید این سناریو را روی پیکربندی سناریوی قبلی ادامه دهید، حتما قبل از شروع تمام Static Routeها را از روی هر سه روتر حذف نمائید.

ابتدا اقدام به راه اندازی پروتکل RIP بر روی روتر تهران می نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router rip
Tehran(config-router)#version 2
Tehran(config-router)#network 172.16.12.0
Tehran(config-router)#network 172.16.13.0
Tehran(config-router)#network 172.16.14.0
Tehran(config-router)#network 172.16.15.0
Tehran(config-router)#network 200.200.2.0
Tehran(config-router)#default-information originate
Tehran(config-router)#exit
Tehran(config)#ip default-network 200.200.2.0
Tehran(config)#ip route 0.0.0.0 0.0.0.0 200.200.2.2
Tehran(config)#^Z
Tehran#write
```

از دستور router rip برای فعال سازی پروتکل و از دستور version برای مشخص نمودن نسخه مورد نظر استفاده نمودیم.

توسط دستور network شبکه‌هایی که روتر تهران بصورت مستقیم با آنها در ارتباط است را جهت استفاده در پیام‌های Advertisement مشخص می‌نماییم.

در صورت استفاده از دستور Default-network، می‌توانیم مسیر مشخص شده جهت Default Route را توسط پیام‌های بروز رسانی به اطلاع سایر روترها برسانیم. البته باید قبلا توسط دستورdefault-information originate روتر را به عنوان تبلیغ کننده Default Route در شبکه تعیین کرده باشید.

به پیکربندی پروتکل RIP بر روی سایر روترها ادامه می دهیم:

```
Rey>enable
Rey#configure terminal
Rey(config)#router rip
Rey(config-router)#version 2
Rey(config-router)#network 192.168.100.0
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#router rip
Mashhad(config-router)#version 2
Mashhad(config-router)#network 192.168.200.0
```

پس از عملیات فوق، علیرغم اینکه تمام شبکه‌ها را در پروتکل RIP مشخص نمودیم ولی امکان ping شبکه های دیگر را توسط هیچ یک از روترها نخواهیم داشت. نه اشتباه نکنید! حتی ping بصورت Extended هم نمی‌تواند در این مورد کار گشا باشد.

برای درک این اشکال به خروجی دستور show ip protocol توجه نمایید:

```
Rey#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface         Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0     2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
            192.168.100.0
Passive Interface(s):
Routing Information Sources:
            Gateway        Distance      Last Update
Distance: (default is 120)
Rey#
```

در خروجی دستور show ip protocols ضمن مشاهده پروتکل مسیریابی مورد استفاده به همراه زمان سنج‌ها و دیگر تنظیمات آن، می توانید اینترفیس‌هایی که در جریان پروتکل مسیریابی قرار دارند را نیز مشاهده نمایید. همانطور که در قسمت مشخص شده خروجی فوق مشهود است به دلیل اینکه ما توسط دستورnetwork آدرس‌های مربوط به اینترفیس‌های Serial را مشخص نکرده‌ایم، این اینترفیس‌ها در جریان پروتکلRIP قرار نگرفته، لذا ارسال و دریافت پیام‌های بروز رسانی پروتکل RIP توسط این اینترفیس‌ها امکان پذیر نمی‌باشد.

پس به یاد داشته باشید برای اشتراک اینترفیس‌ها در جریان پروتکل مسیریابی، باید آدرس مربوطه را توسط دستور network معرفی نماییم.

```
Rey(config)#router rip
Rey(config-router)#network 172.16.20.0
Rey(config-router)#network 172.16.20.8
```

```
Mashhad(config)#router rip
Mashhad(config-router)#network 172.16.20.4
Mashhad(config-router)#network 172.16.20.8
```

حالا مجددا به خروجی دستور show ip protocols نگاهی بفرمایید:

```
Rey#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       2     2
  Serial0/0/0           2     2
  Serial0/1/0           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        172.16.0.0
        192.168.100.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
        172.16.20.1       120       00:00:00
        172.16.20.10      120       00:00:19
Distance: (default is 120)
Rey#
```

همانطور که ملاحظه می فرمایید، اینترفیس‌های Serial نیز وارد بازی شدند. حالا اگر اقدام به ping هر یک از شبکه ها از طریق هر کدام از روترها بفرمایید، خروجی خوشحال کننده زیر را ملاحظه خواهید نمود:

```
Tehran#ping 192.168.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms

Tehran#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

البته فراموش نکنید که از طریق دیگر روترها هم می توانید به اینترنت دسترسی داشته باشید.

```
Rey#ping
Protocol [ip]:
Target IP address: 198.133.219.25
```

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/7 ms
```

حتما سوال می کنید چرا علیرغم معرفی آدرس اینترفیس‌های Serial، باز هم از ping بصورت Extended استفاده کردیم؟! به این دلیل که در ACL نوشته شده برای NAT به آدرس های فوق اجازه استفاده از NAT داده نشده است. (یعنی تو کتابهای سیسکو هم نمی‌توانید این همه نکته یاد بگیرد!!!)

طریقه عملکرد:

پروتکلRIP v2 شبکه‌های معرفی شده توسط دستور network را در قالب پیام‌های Multicast و آدرس224.0.0.9 به اطلاع روترهای همسایه خود می‌رساند. هر روتر پس از دریافت پیام های update، یک عدد به مقدار Metric آن اضافه کرده و با آدرس‌های موجود در جدول مسیریابی خود مقایسه می‌کند. در صورتیکه مسیری با Metric بهتر برای مقصد مورد نظر در جدول مسیریابی موجود نباشد، مسیر به دست آمده را ثبت کرده و در غیر اینصورت اقدام به نادیده گرفتن آن می نماید.

با توجه به اینکه روترها پیام های خود را هر۳۰ ثانیه ارسال می‌کنند، شبکه ما پس از مدت زمان ۹۰ ثانیه به همگرایی رسیده و روترها از شبکه‌های یکدیگر اطلاع خواهند یافت.

پس از همگرایی شبکه خروجی دستور show ip route روترها بصورت زیر خواهد بود:

```
Tehran#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
     i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
     * - candidate default, U - per-user static route, o - ODR
     P - periodic downloaded static route

Gateway of last resort is 200.200.2.2 to network 0.0.0.0
```

```
    172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
S      172.16.0.0/16 [1/0] via 172.16.12.1
C      172.16.12.0/24 is directly connected, FastEthernet0/0.2
C      172.16.13.0/24 is directly connected, FastEthernet0/0.3
C      172.16.14.0/24 is directly connected, FastEthernet0/0.4
C      172.16.15.0/24 is directly connected, FastEthernet0/0.5
C      172.16.20.0/30 is directly connected, Serial0/0/0
C      172.16.20.4/30 is directly connected, Serial0/1/0
R      172.16.20.8/30 [120/1] via 172.16.20.2, 00:00:18, Serial0/0/0
                [120/1] via 172.16.20.6, 00:00:21, Serial0/1/0
R   192.168.100.0/24 [120/1] via 172.16.20.2, 00:00:18, Serial0/0/0
R   192.168.200.0/24 [120/1] via 172.16.20.6, 00:00:21, Serial0/1/0
    200.200.2.0/24 is variably subnetted, 2 subnets, 2 masks
S      200.200.2.0/24 [1/0] via 200.200.2.2
                [1/0] via 200.200.2.1
C      200.200.2.0/30 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 200.200.2.2
Tehran#
```

همانطور که مشاهده می کنید مسیرهای بدست آمده توسط پروتکل RIP با حرف R در ابتدای مسیر مشخص شده است.

```
Rey#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 172.16.20.1 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
R      172.16.12.0/24 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
R      172.16.13.0/24 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
R      172.16.14.0/24 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
R      172.16.15.0/24 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
C      172.16.20.0/30 is directly connected, Serial0/1/0
R      172.16.20.4/30 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
                [120/1] via 172.16.20.10, 00:00:05, Serial0/0/0
C      172.16.20.8/30 is directly connected, Serial0/0/0
C   192.168.100.0/24 is directly connected, FastEthernet0/0
R   192.168.200.0/24 [120/1] via 172.16.20.10, 00:00:05, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 172.16.20.1, 00:00:22, Serial0/1/0
Rey#
```

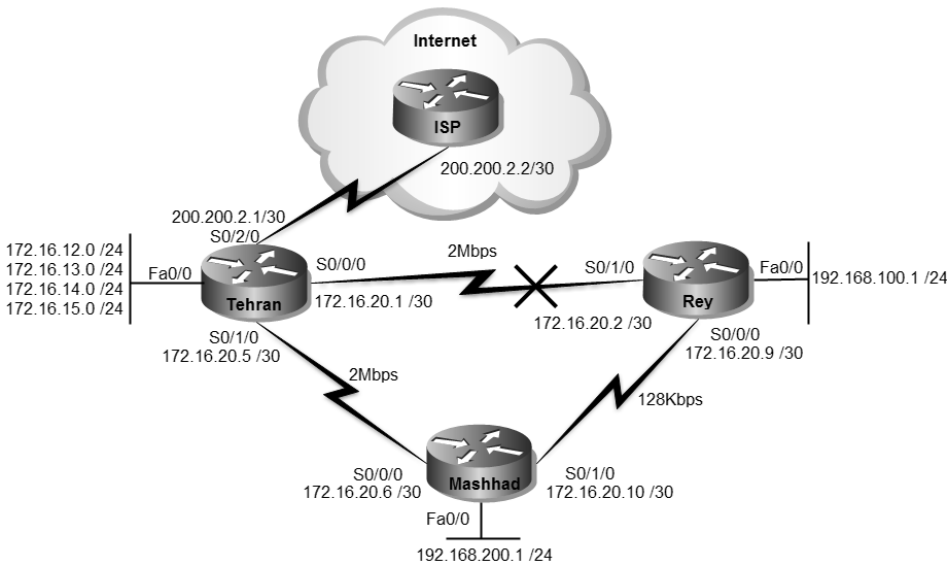
در روترهای شهرری و مشهد، علاوه بر مسیر شبکه های دیگر، مسیر Default Route هم از طریق پروتکل RIP به دست آمده است.

همچنین در عبارت [120/1] ، عدد 120 نشان دهنده مقدار AD پروتکل RIP و عدد 1 مربوط به Metric مسیر به دست آمده می‌باشد. به دلیل اینکه بسته‌ها تا مقصد باید از یک روتر(hop) عبور کنند، عدد Metric برابر 1 قرار گرفته است.

همچنین با استفاده از دستور traceroute می توانید مسیر طی شده بسته ها برای رسیدن به مقصد را مشاهده نمایید:

```
Rey#traceroute 172.16.12.1
Type escape sequence to abort.
Tracing the route to 172.16.12.1

 1  172.16.20.1    6 msec   5 msec   5 msec
Rey#
```

حالا برای بررسی پویا بودن عملیات مسیریابی، اقدام به قطع اتصال مستقیم بین تهران و شهرری می نماییم:



پس از قطع لینک و گذشت ۹۰ ثانیه، خروجی دستور show ip route بصورت زیر خواهد بود:

```
Rey#show ip route
...
Gateway of last resort is 172.16.20.10 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
R     172.16.12.0/24 [120/2] via 172.16.20.10, 00:00:10, Serial0/0/0
R     172.16.13.0/24 [120/2] via 172.16.20.10, 00:00:10, Serial0/0/0
R     172.16.14.0/24 [120/2] via 172.16.20.10, 00:00:10, Serial0/0/0
R     172.16.15.0/24 [120/2] via 172.16.20.10, 00:00:10, Serial0/0/0
R     172.16.20.4/30 [120/1] via 172.16.20.10, 00:00:10, Serial0/0/0
C     172.16.20.8/30 is directly connected, Serial0/0/0
```

```
C   192.168.100.0/24 is directly connected, FastEthernet0/0
R   192.168.200.0/24 [120/1] via 172.16.20.10, 00:00:10, Serial0/0/0
R*  0.0.0.0/0 [120/2] via 172.16.20.10, 00:00:10, Serial0/0/0
Rey#
```

همانطور که ملاحظه می کنید، با قطع لینک مستقیم بین تهران و شهرری، روتر اقدام به جایگزینی مسیرهای با Metric بالاتر جهت دسترسی به شبکه‌های متصل به روتر تهران نموده است.

البته روتر شهرری قبلا هم تبلیغ شبکه‌های تهران را از طریق روتر مشهد دریافت کرده بود، ولی به دلیل بالاتر بودن Metric، از ثبت آنها در جدول مسیریابی خودداری نموده بود.

برای اطمینان از در دسترس بودن شبکه ها، اقدام به ping آنها می نماییم:

```
Rey#ping 172.16.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/12/35 ms

Rey#
```

برای اینکه مسیر طی شده برای رسیدن به شبکه مورد نظر را ببینید، می توانید از دستور Traceroute استفاده نمایید:

```
Rey#traceroute 172.16.12.1
Type escape sequence to abort.
Tracing the route to 172.16.12.1

 1  172.16.20.10   7 msec   8 msec   1 msec
 2  172.16.20.5    12 msec  9 msec   9 msec
Rey#
```

هر چند قبلا برای دسترسی روتر شهرری به شبکه های تهران فقط نیاز به گذشتن از یک hop می بود ولی همانطور که ملاحظه می فرمایید، در حال حاضر به دلیل قطع ارتباط مستقیم تهران و شهرری، پروتکل RIP از طریق روتر مشهد اقدام به برقراری ارتباط با شبکه های متصل به روتر تهران می نماید.

مرجع دستور Command Reference:

Enabling RIP		
	Command	**Purpose**
Step 1	Router(config)# **router rip**	Enables a RIP routing process, which places you in router configuration mode.
Step 2	Router(config-router)# **network** *ip-address*	Associates a network with a RIP routing process.

Specifying a RIP Version	
Command	**Purpose**
Router(config-router)# **version** {**1** | **2**}	Configures the software to receive and send only RIP Version 1 or only RIP Version 2 packets.

Adjusting Timers	
Command	**Purpose**
Router(config-router)# **timers basic** *update invalid holddown flush* [*sleeptime*]	Adjusts routing protocol timers.

Enabling RIP Authentication		
	Command	**Purpose**
Step 1	Router(config-if)# **ip rip authentication key-chain** *name-of-chain*	Enables RIP authentication.
Step 2	Router(config-if)# **ip rip authentication mode** {**text** | **md5**}	Configures the interface to use MD5 digest authentication (or let it default to plain text authentication).

Verify Commands	
Command	**Description**
show ip rip database	Displays the contents of the RIP private database when triggered extensions to RIP are enabled.
debug ip rip	Displays information on RIP routing transactions.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

☑ مبحث سوم

پروتکل EIGRP

شرکت سیسکو به عنوان پیشتاز عرصه تکنولوژی شبکه، دارای پروتکل مسیریابی مختص به خود نیز می‌باشد. به‌دلیل اینکه پروتکل مسیریابی سیسکو دارای خصوصیاتی پیشرفته تر از گروه Distance Vector ولی پایین تر از گروه Link State می‌باشد، نمی‌توان آنرا بطور کامل جزء هیچ کدام از دو گروه فوق دانست. به همین دلیل در مستندات سیسکو، این پروتکل را جزء دسته جدیدی به نام Hybrid [1] و یا Distance Vector پیشرفته ذکر می‌نمایند.

این پروتکل که فقط بر روی تجهیزات سیسکو قابل راه اندازی می‌باشد در دو نسخه با مشخصات زیر ارائه گردیده است.

پروتکل IGRP

اولین نسخه پروتکل مسیریابی سیسکو با نام (Interior Gateway Routing Protocol) IGRP منتشر گردید. این نسخه دارای ویژگی‌های اصلی به شرح زیر می‌باشد.

- در گروه پروتکل‌های Distance Vector قرار می‌گیرد.
- از مفهوم AS پشتیبانی می‌نماید.
- عملکرد این پروتکل بصورت Classful بوده لذا امکان استفاده از ویژگی‌های VLSM، CIDR و خلاصه سازی در این پروتکل موجود نمی‌باشد.
- پیام‌های خود را در قالب Broadcast ارسال می‌نماید.
- پیام‌های Update را بصورت پیش فرض هر ۹۰ ثانیه یکبار ارسال می‌نماید.
- محاسبه Metric بر اساس پارامترهای delay، bandwidth، reliability و load انجام می‌پذیرد.
- نهایت تعداد روترهای موجود در شبکه می تواند ۲۵۵ عدد باشد.
- دارای AD برابر 100 می باشد.

---

[1] به معنی دوگانه

- دارای امکانLoad Balancing در هردو حالتEqual Cost وUnequal Cost می‌باشد.

امروزه این پروتکل نیز همانند نسخه اول RIP منسوخ شده و جای خود را به نسخه بعدی خود داده است.

پروتکل EIGRP

دومین نسخه پروتکل مسیریابی سیسکو با نام (Enhanced Interior Gateway Routing Protocol) EIGRP منتشر گردید. این نسخه که بر پایه پروتکل IGRP توسعه یافته، دارای ویژگی های اصلی به شرح زیر می‌باشد.

- به دلیل خصوصیات بهتر از گروه Distance Vector آنرا جزء گروه Hybrid و یا Advanced Distance Vector می‌دانند.
- از مفهوم AS پشتیبانی می‌نماید.
- از الگوریتم DUAL برای مسیریابی استفاده می‌کند. به همین دلیل عاری از حلقه لایه سوم در شبکه می‌باشد.
- از پیام‌های Hello در قالب Multicast و به آدرس 224.0.0.10 برای بررسی ساختار شبکه استفاده می‌نماید.
- پیام‌هایUpdate را اولین بار بصورت کامل و در دفعات بعد بصورت افزایشی[1] ارسال می‌نماید. این پیام‌ها توسط پروتکلRTP بصورت قابل اطمینان ارسال می‌نماید.
- عملکرد این پروتکل بصورت Classless بوده لذا امکان استفاده از ویژگی‌های VLSM، CIDR و خلاصه سازی را ارائه می‌نماید.
- ویژگی Auto-summary در این پروتکل بصورت پیش فرض فعال می‌باشد.
- محاسبه Metric بصورت پیش فرض توسط فرمولی بر اساس پارامترهای delay و bandwidth انجام می‌پذیرد. اما بصورت اختیاری می توانید از پارامترهای Load و Reliability نیز در محاسبه Metric استفاده نمایید.
- دارای امکان Load Balancing در هر دو حالت Equal Cost وUnequal Cost می‌باشد.
- مقدار AD آن برابر 90 می‌باشد.

[1] Incremental

- از ویژگی Authentication فقط در حالت MD5 پشتیبانی می‌نماید.
- امکان راه اندازی در شبکه‌های مبتنی بر پروتکل‌های لایه سه IP، IPX و AppleTalk را دارد.
- برای مشخص کردن زیر شبکه‌ها از Wildcard Mask استفاده می‌نماید.

پروتکل RTP

از پروتکلRTP(Reliable Transport Protocol)، جهت انتقال قابل اطمینان اطلاعات استفاده می‌گردد. این پروتکل دریافت اطلاعات را بصورت مطمئن تضمین می‌نماید.

پروتکلRTP برای اطمینان از صحت بسته‌ها از Sequence Number استفاده می‌نماید. همچنین این پروتکل با ارسال پیام‌های Acknowledge به فرستنده، دریافت صحیح بسته‌ها را اعلام می‌نماید.

پروتکلEIGRP برای ارسال پیام‌های خود به جای استفاده از پروتکل‌های TCP و UDP، از پروتکل RTP در قالب IP Protocol Type 88 استفاده می‌نماید.

توجه داشته باشید پروتکل انتقال اطلاعات قابل اطمینان (Reliable Transport Protocol) RTP با پروتکل انتقال بلادرنگ RTP(Real-time Transport Protocol) که برای انتقال صوت و تصویر کاربرد دارد، متفاوت می‌باشد.

الگوریتم DUAL

مسیریابی در پروتکلEIGRP بر اساس الگوریتم DUAL(Diffusing Update Algorithm) انجام می پذیرد. این الگوریتم توسط موسسه تحقیقاتی SRI International[1] و بوسیله پروفسور Jose Joaquin Garcia-Luna-Aceves توسعه داده شده است.

الگوریتم DUAL پروتکلEIGRP را قادر می‌سازد تا تشخیص دهد مسیری که توسط روتر همسایه تبلیغ شده به علت ایجاد حلقه لایه سه بوده یا مسیر درستی را دریافت نموده است.

همچنین این الگوریتم می تواند در صورت معیوب شدن یک مسیر، بدون آنکه منتظر پیام های Update بماند، اقدام به انتخاب مسیر جایگزین نماید.

[1] www.sri.com

جداول پروتکل EIGRP

پروتکل EIGRP برای انجام عملیات مسیریابی بر اساس الگوریتم DUAL، دارای سه جدول به شرح زیر می باشد:

- **Neighbor Table**

این جدول، شامل لیست روترهای همسایه می‌باشد. اطلاعات مندرج در این جدول بر اساس پیام‌های Hello مشخص می‌گردند.

- **Topology Table**

حاوی اطلاعات توپولوژی شبکه می‌باشد . این اطلاعات که از روترهای همسایه (که در Neighbor Table قرار دارند) بدست آمده است، شامل تمام مسیرهای مربوط به مقصدهای موجود در AS به همراه Metric هر یک از آنها می‌باشد.

همچنین مشخص نمودن مسیرهای اصلی (Successor) و مسیرهای جایگزین (Feasible Successor) به مقاصد مختلف در شبکه، بر اساس محتویات جدول توپولوژی انجام می پذیرد.

جدول توپولوژی دارای چند فیلد برای نگهداری اطلاعات مورد نیاز می باشد که دو فیلد مهم آن عبارتند از FD و RD.

فیلد FD(Feasible Distance) : شامل Metric محاسبه شده یک مسیر برای رسیدن به یک مقصد مشخص از منظر روتر محلی می‌باشد.

این فیلد به ازاء تمام مقصدهای موجود در AS شامل مسیر می‌باشد.

فیلد RD(Reported Distance) : شامل Metric محاسبه شده برای مقصدی می‌باشد که توسط روتر همسایه محاسبه و تبلیغ شده است. مقدار Metric این مسیرها از منظر روتر همسایه می باشد.

از مقدار این فیلد در زمان محاسبه مقدار FD نیز استفاده می‌گردد.

- **Routing Table**

این جدول، همان جدول مسیریابی روتر می‌باشد. پس از آنکه پروتکل EIGRP بهترین مسیرها را بر اساس دو جدول مخصوص به خود مشخص نمود اقدام به ثبت آنها در جدول مسیریابی روتر می‌نماید.

به این نکته توجه داشته باشید که روتر فارغ از پروتکل مسیریابی اجرا شده، برای انجام عملیات مسیریابی نهایتا بر اساس مسیرهای ثبت شده در Routing Table عمل می‌نماید.

مراحل انتخاب مسیر

پروتکل EIGRP سه مرحله اصلی زیر را برای درج یک مسیر در جدول مسیریابی روتر طی می نماید:

۱- **Neighbor Discovery**

پروتکلEIGRP با ارسال پیام Hello اقدام به کشف روترهای همسایه می‌نماید. روترها پس از دریافت پیام Hello اقدام به بررسی پارامترها نموده تا تشخیص دهند آیا روتر مقابل می تواند به عنوان همسایه در جدول Neighbor Table ذخیره گردد یا خیر.

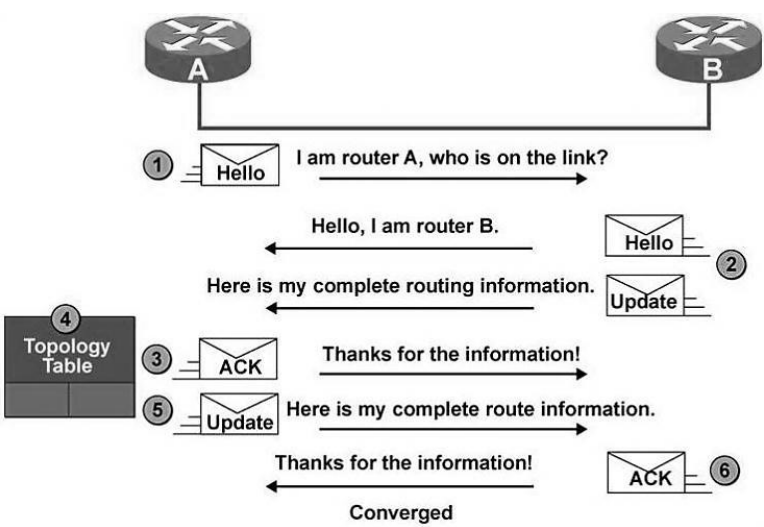
۲- **Topology Exchange**

پس از برقراری رابطه همسایگی، برای بار اول روترها اقدام به تبادل کامل اطلاعات جدول توپولوژی خود در قالب پیام update با روترهای همسایه می‌نمایند ولی در دفعات بعد فقط تغییرات را در قالب پیام‌های افزایشی به اطلاع یکدیگر می‌رسانند.

۳- **Choosing Routes**

پروتکلEIGRP اقدام به بررسی اطلاعات موجود در جدول توپولوژی نموده و مسیر دارای بهترینMetric را جهت دسترسی به شبکه مورد نظر انتخاب و در جدول مسیریابی ثبت می‌نمایند.

انجام مراحل فوق در تصویر زیر نمایش داده شده است.



محاسبه Metric

برای محاسبه Metric در پروتکل EIGRP می توان علاوه بر Delay و Bandwidth از پارامترهای Load و Reliability نیز استفاده نمود.

در صورتی که بخواهید از هر چهار پارامتر فوق در محاسبه Metric بهره ببرید، باید از طریق فرمول زیر اقدام نمایید.

$$\text{Metric}= (k1 \times Bandwidth) + \left(\frac{k2\times Bandwidth}{256-Load}\right) + (k3 \times Delay) \times \left(\frac{k5}{Reliability+k4}\right)$$

همانطور که در فرمول فوق ملاحظه می‌نمایید، در این فرمول دارای ۵ متغیر K هستیم که آنها را K-Values می‌نامند. مقدار مشخص شده برای متغیرهای K1 تا K5 باید در تمام روترهای همسایه بطور یکسان تنظیم گردد.

بصورت پیش فرض مقدار K1=K3=1 و مقدار K2=K4=K5=0 می‌باشد. به همین دلیل است که فقط Bandwidth و Delay در محاسبه Metric تاثیر گذار می‌باشند. در صورتیکه بخواهید پارامترهای دیگر را در محاسبه Metric دخیل نمایید باید به متغیرK2، K4 و K5 عددی غیر از صفر اختصاص دهید.

هر چند که سیسکو امکان استفاده از دو پارامتر اضافی را در محاسبه Metric امکان پذیر ساخته ولی استفاده از آنها را توصیه نمی‌کند. به همین دلیل محاسبه Metric در پروتکل EIGRP بصورت پیش فرض بر اساس Bandwidth و Delay انجام می‌پذیرد.

فرمول محاسبه Bandwidth و Delay بطور جداگانه بصورت زیر می باشد:

$$\text{Bandwidth}=\left(\frac{10^7}{Least\ Bandwidth}\right) \times 256$$

$$\text{Delay}=(Cumulative\ delay) \times 256$$

با توجه به فرمول های مذکور در نهایت فرمول محاسبه Metric بصورت زیر در می آید:

$$\text{Metric} = \left(\left(\frac{10^7}{Least\ Bandwidth}\right) + Cumulative\ delay\right) \times 256$$

تشریح پارامترهای استفاده شده در فرمول فوق به شرح زیر می باشد:

- **عدد ثابت** 10^7

این مقدار بطور ثابت در فرمول قرار می گیرد.

- **Least Bandwidth**

منظور از اصطلاح حداقل پهنای باند، لینکی است که دارای کمترین پهنای باند در طول مسیر مورد نظر می باشد. این مقدار باید بر اساس Kbps در فرمول درج گردد.

به عنوان مثال اگر لینک دارای کمترین پهنای باند در طول مسیر مورد نظر ما، یک لینک ایترنت 10Mbps باشد، مقداری که باید به عنوان Least Bandwidth در فرمول گذاشته شود عدد 10^4 خواهد بود. به دلیل اینکه 10 مگابیت بر ثانیه معادل 10000 کیلوبیت بر ثانیه می‌باشد.

- **Cumulative delay**

منظور از عبارت Cumulative Delay، یعنی مجموع تاخیرها. برای بدست آمدن این مقدار باید تاخیر مربوط به تمام لینک‌های طول مسیر با یکدیگر جمع شوند.

واحد محاسبه این عدد باید بر اساس tens of microseconds (µs) باشد. منظور از tens of microsecond، این است که ابتدا باید مقدار به دست آمده(بر اساس میکرو ثانیه) را بر10 تقسیم نموده و سپس عدد بدست آمده را در فرمول جایگزین نمائید.

- **عدد ثابت 256**

این مقدار همواره بطور ثابت در فرمول قرار می گیرد.

در جدول زیر مقدار Delay و Bandwidth در لینک های پر استفاده نمایش داده شده است.

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 Mbps)
Ethernet	25,600 (1 ms)	256,000 (10 Mbps)
T-1 (1.544 Mbps)	512,000 (20,000 ms)	1,657,856
64 kbps	512,000	40,000,000
56 kbps	512,000	45,714,176

نکته: در بعضی از مستندات سیسکو از MTU نیز به عنوان یکی از پارامترهای موثر در محاسبه Metric نام برده شده است. اما طبق پارامترهای ذکر شده در فرمول فوق، MTU در محاسبه Metric هیچ نقشی نداشته و صرفا به عنوان فیلدی در پیام های بروز رسانی EIGRP ذکر می شود. این مسئله در آخرین کتاب منتشر شده سیسکو درباره مسیریابی با عنوان CCNP Route 642-902 نیز بیان گردیده است.

انواع پیام‌ها در EIGRP

پروتکل EIGRP برای انجام پروسه مسیریابی خود، دارای ۵ نوع پیام به شرح زیر می‌باشد:

۱- **Hello**

پروتکلEIGRP از این پیام برای شناسایی روترهای همسایه استفاده می‌نماید. روتر این پیام را بصورت Multicast از طریق اینترفیس‌هایی که EIGRP بر روی آنها فعال گردیده، ارسال می‌نماید.

۲- **Acknowledgment**

پیام Acknowledgment همان پیام Hello ولی بدون هیچ داده‌ای می‌باشد. این پیام بصورت Unicast در جواب پیام‌هایی داده می‌شود که نیاز به تائید دریافت دارند.

روترها در تائید دریافت پیام‌هایUpdate،Queryو Reply از پیامAcknowledgment استفاده می‌نمایند.

۳- **Update**

از پیامUpdate برای انتقال اطلاعات مربوط به مسیر شبکه‌های قابل دسترس استفاده می گردد. پس از کشف یک همسایه جدید، پیام های Update بصورت Unicast به آن روتر ارسال می گردد تا پروتکل EIGRP بتواند جدول توپولوژی خود را کامل نماید.

البته در موارد دیگر مثل زمانی که Metric یک مسیر تغییر می‌کند، پیام‌های Update بصورت Multicast ارسال می‌گردد.

پیام‌های Update همواره بصورت قابل اطمینان ارسال گردیده و شامل Prefix، Prefix Length، پارامترهای مورد نیاز در Metric (مثل Bandwidth و Delay) و پارامترهای غیر موثر در Metric (hop-count و MTU) می‌باشد.

۴- **Query**

پیام Query در زمانی ارسال می‌گردد که یک مقصد دارای مسیر جایگزین (Feasible Successor) نباشد. این پیام که جهت درخواست مسیر جایگزین می‌باشد در قالب پیام‌های Multicast و بصورت قابل اطمینان ارسال می‌گردد.

۵- **Reply**

پیام Reply در جواب پیام‌های درخواست[1] جهت معرفی مسیر جایگزین و بصورت Unicast برای درخواست کننده ارسال می شود.

این پیام بصورت قابل اطمینان ارسال می گردد.

---

[1] Query

زمان سنج‌های پروتکل EIGRP

۱- **Hello Timer**

پیام Hello بصورت پیش فرض در شبکه‌های پر سرعت مثل اینترنت هر۵ ثانیه و در اتصالات کم سرعت مثل لینک‌های WAN، هر ۶۰ ثانیه بصورت متناوب ارسال می‌گردد.

۲- **Hold-down Timer**

در صورتیکه پس از گذشت ۳ برابر مدت زمان Hello، روتر پیام Hello دیگری مبنی بر در دسترس بودن روتر همسایه دریافت نکند فرض را بر معیوب بودن آن گذاشته و اقدام به حذف روتر مذکور از جدول Neighbor Table می‌نماید.

مقدار این زمان سنج که آنرا Hold-down Timer می‌نامند، بصورت پیش فرض در اتصالات پر سرعت ۱۵ ثانیه و در اتصالات کم سرعت ۱۸۰ ثانیه می‌باشد.

نکته: **بر خلاف پروتکل‌های مسیریابی که تا کنون با آنها آشنا شده ایم، پروتکل EIGRP پیام های Update را بصورت متناوب ارسال نمی‌نماید. ارسال پیام Update در این پروتکل فقط در دو صورت انجام می‌پذیرد: ۱- هنگام مشخص شدن یک همسایه جدید ۲- در زمان ایجاد تغییر در توپولوژی.**

Load Balancing در EIGRP

پروتکل EIGRP ویژگی Load Balancing را به هر دو صورت Equal و Unequal امکان پذیر ساخته است. برای پیکربندی ویژگی فوق می توان از پارامترهای زیر بهره برد:

۱- **Maximum Path**

پروتکل EIGRP بصورت پیش فرض امکان Load Balancing بر روی ۴ مسیر با Metric برابر را دارد. ولی می توان با استفاده از دستور Maximum-path تعداد این مسیرها را نهایتا به ۶ مسیر افزایش داد.

در صورتیکه بخواهید امکان Load Balancing را بر روی روتر غیر فعال نمایید، باید مقدار 1 را به این متغییر اختصاص دهید.

۲- **Variance**

پروتکل EIGRP علاوه بر امکان Load Balancing بر روی مسیرهای Equal، امکان استفاده از مسیرهای Unequal را نیز دارد. برای فعال کردن این ویژگی باید از پارامتر Variance جهت مشخص نمودن ضریب متغیر استفاده نماییم.

سناریو شماره(۱۲): راه اندازی EIGRP

طرح مسئله:

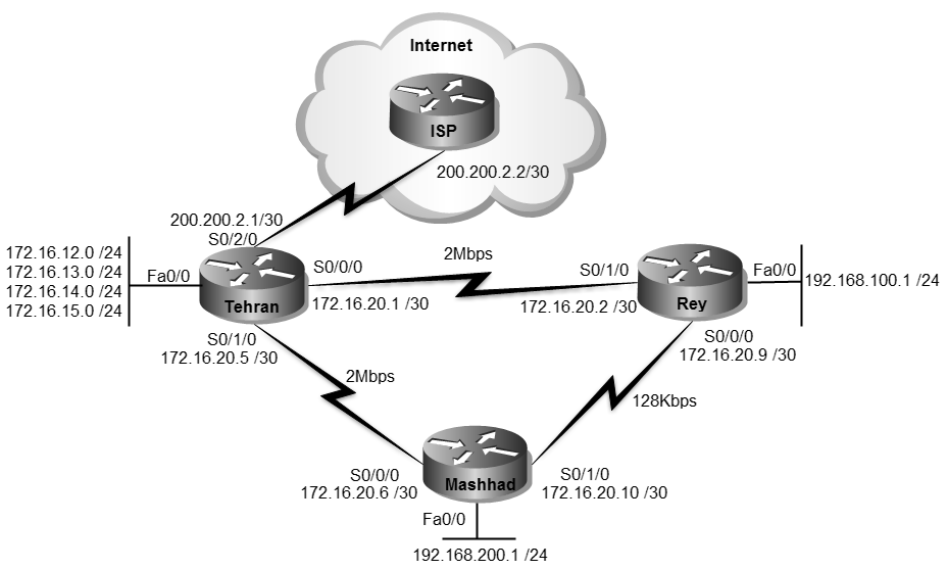
عملیات مسیریابی را برای همان سناریوی قبلی شبکه شرکت MTR Electronic، ولی این بار بر اساس پروتکل EIGRP انجام می‌دهیم.

نکته: در صورت استفاده از روترهای سناریوی قبل، باید برای غیر فعال کردن پروتکل RIP، دستور زیر را بر روی هر سه روتر اجرا نمایید:

Router(config)#no router rip

نیاز سنجی:

برای راه اندازی پروتکل EIGRP تجهیزات خاصی مورد نیاز نمی باشد. فقط درک مطالب گفته شده، برای انجام این سناریو کفایت می نماید.



راه حل:

با توجه به اینکه فرض را بر انجام شدن پیکربندی اولیه روترها گذاشته‌ایم، مستقیما سراغ راه اندازی پروتکل EIGRP می‌رویم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router eigrp 110
Tehran(config-router)#network 172.16.12.0 0.0.3.255
Tehran(config-router)#network 172.16.20.0
Tehran(config-router)#network 172.16.20.4
Tehran(config-router)#network 200.200.2.0
Tehran(config-router)#no auto-summary
Tehran(config-router)#exit
Tehran(config)#ip default-network 200.200.2.0
Tehran(config)#ip route 0.0.0.0 0.0.0.0 200.200.2.2
Tehran(config)#^Z
Tehran#write
```

```
Rey>enable
Rey#configure terminal
Rey(config)#router eigrp 110
Rey(config-router)#network 192.168.100.0
Rey(config-router)#network 172.16.20.0
Rey(config-router)#network 172.16.20.8
Rey(config-router)#no auto-summary
Rey(config-router)#^Z
Rey#write
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#router eigrp 110
Mashhad(config-router)#network 192.168.200.0
Mashhad(config-router)#network 172.16.20.8
Mashhad(config-router)#network 172.16.20.4
Mashhad(config-router)#no auto-summary
Mashhad(config-router)#^Z
Mashhad#write
```

در پیکربندی EIGRP و در حین فعال کردن این پروتکل بر روی روتر باید شماره AS مورد نظر را نیز مشخص نماییم. توجه داشته باشید که شماره AS برای تمام روترهای موجود در شبکه باید بصورت یکسان تنظیم گردد.

توسط دستور network اقدام به معرفی شبکه‌هایی نمودیم که می‌خواهیم روتر آنها را تبلیغ نماید. این شبکه‌ها باید توسط روتر تبلیغ کننده در دسترس باشند.

همانطور که ملاحظه می‌نمایید در پروتکل EIGRP برای معرفی کردن زیر شبکه‌ها باید از Wildcard Mask استفاده نماییم.

با توجه به اینکه شبکه های محلی متصل به روتر تهران را می‌توانیم با کمک Wildcard Mask بصورت خلاصه آدرس دهی نماییم، با نوشتن تنها یک خط Route بصورت network 172.16.12.0 0.0.3.255، هر چهار شبکه را آدرس دهی نمودیم.

به دلیل اینکه پروتکل EIGRP مسیریابی را بطور پیش فرض بصورت Classful انجام می‌دهد، با نوشتن دستور no auto-summary، امکان استفاده از ویژگی Classless را توسط این پروتکل فعال می‌نماییم.

لینک‌های WAN در پروتکل EIGRP بصورت پیش فرض T1 محسوب شده و برای آنها پهنای باند 1.544Mbps در نظر گرفته می‌شود. لذا با توجه به اینکه پهنای باند لینک‌های شبکه ما متفاوت از T1 می‌باشد، توسط دستور Bandwidth اقدام به مشخص نمودن مقدار واقعی آنها می نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface s0/0/0
Tehran(config-if)#bandwidth ?
  <1-10000000>  Bandwidth in kilobits
Tehran(config-if)#bandwidth 2000
Tehran(config-if)#interface s0/1/0
Tehran(config-if)#bandwidth 2000
Tehran(config-if)#^Z
Tehran#write
```

همانطور که در دستورات فوق مشاهده میکنید، مقدار پهنای باند را باید بر حسب Kbps مشخص نمایید.

```
Rey>enable
Rey#configure terminal
Rey(config)#interface serial 0/0/0
Rey(config-if)#bandwidth 128
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#bandwidth 2000
Rey(config-if)#^Z
Rey#write
```

```
Mashhad>enable
Mashhad#configure terminal
```

```
Mashhad(config)#interface serial 0/0/0
Mashhad(config-if)#bandwidth 2000
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#bandwidth 128
Mashhad(config-if)#^Z
Mashhad#write
```

پس از اعمال دستورات فوق، خروجی دستور show ip route بر روی روتر ری و مشهد به صورت زیر خواهد بود:

```
Mashhad#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D       172.16.12.0/24 [90/1794560] via 172.16.20.5, 00:10:05, Serial0/0/0
D       172.16.13.0/24 [90/1794560] via 172.16.20.5, 00:10:05, Serial0/0/0
D       172.16.14.0/24 [90/1794560] via 172.16.20.5, 00:10:05, Serial0/0/0
D       172.16.15.0/24 [90/1794560] via 172.16.20.5, 00:10:05, Serial0/0/0
D       172.16.20.0/30 [90/2304000] via 172.16.20.5, 00:10:05, Serial0/0/0
C       172.16.20.4/30 is directly connected, Serial0/0/0
C       172.16.20.8/30 is directly connected, Serial0/1/0
D    192.168.100.0/24 [90/2306560] via 172.16.20.5, 00:10:05, Serial0/0/0
C    192.168.200.0/24 is directly connected, FastEthernet0/0
     200.200.2.0/30 is subnetted, 1 subnets
D       200.200.2.0 [90/21024000] via 172.16.20.5, 00:10:05, Serial0/0/0
Mashhad#
```

مسیرهای دریافت شده توسط پروتکل EIGRP با علامت D نمایش داده شده است. ولی همانطور که ملاحظه می کنید از Default Network خبری نیست.

```
Rey#show ip route
<<… Output Omitted…>>
Gateway of last resort is not set
     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D       172.16.12.0/24 [90/1794560] via 172.16.20.1, 00:08:43, Serial0/1/0
D       172.16.13.0/24 [90/1794560] via 172.16.20.1, 00:08:43, Serial0/1/0
D       172.16.14.0/24 [90/1794560] via 172.16.20.1, 00:08:43, Serial0/1/0
D       172.16.15.0/24 [90/1794560] via 172.16.20.1, 00:08:43, Serial0/1/0
C       172.16.20.0/30 is directly connected, Serial0/1/0
D       172.16.20.4/30 [90/2304000] via 172.16.20.1, 00:08:43, Serial0/1/0
C       172.16.20.8/30 is directly connected, Serial0/0/0
C    192.168.100.0/24 is directly connected, FastEthernet0/0
D    192.168.200.0/24 [90/2306560] via 172.16.20.1, 00:08:43, Serial0/1/0
     200.200.2.0/30 is subnetted, 1 subnets
D       200.200.2.0 [90/21024000] via 172.16.20.1, 00:08:43, Serial0/1/0
```

علیرغم اینکه پارامتر ip default-network را در روتر تهران پیکربندی نموده‌ایم، ولی طبق خروجی‌های فوق، پروتکلEIGRP از تبلیغ Default Network خودداری نموده است. این اتفاق به دلیل این است که پروتکلEIGRP فقط در حالت Classful اقدام به تبلیغ Default network می‌نماید و ما با اعمال دستور no auto-summary، باعث جلوگیری از این اتفاق شده‌ایم.

برای رفع این مشکل دو راه حل داریم: اول آنکه در تمام روترها بصورت دستی اقدام به نوشتن Default Route نماییم. دوم اینکه در صورتی که محدودیت نداشته باشیم از اعمال دستور no auto-summary در روتری که به شبکه خارجی متصل است، صرف نظر نماییم.

با توجه به اینکه در این سناریو ما به مشکلی برنمی‌خوریم! از اعمال دستور no auto-summary در روتر تهران صرف نظر می نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router eigrp 110
Tehran(config-router)#auto-summary
Tehran#
```

پس از دستور فوق خروجی show ip route روترهای ری و مشهد به صورت زیر خواهد بود:

```
Rey#show ip route
<<… Output Omitted…>>

Gateway of last resort is 172.16.20.1 to network 200.200.2.0

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D      172.16.12.0/24 [90/1794560] via 172.16.20.1, 00:16:35, Serial0/1/0
D      172.16.13.0/24 [90/1794560] via 172.16.20.1, 00:16:35, Serial0/1/0
D      172.16.14.0/24 [90/1794560] via 172.16.20.1, 00:16:35, Serial0/1/0
D      172.16.15.0/24 [90/1794560] via 172.16.20.1, 00:16:35, Serial0/1/0
C      172.16.20.0/30 is directly connected, Serial0/1/0
D      172.16.20.4/30 [90/2304000] via 172.16.20.1, 00:16:35, Serial0/1/0
C      172.16.20.8/30 is directly connected, Serial0/0/0
C   192.168.100.0/24 is directly connected, FastEthernet0/0
D   192.168.200.0/24 [90/2306560] via 172.16.20.1, 00:16:35, Serial0/1/0
D*   200.200.2.0/24 [90/21024000] via 172.16.20.1, 00:16:35, Serial0/1/0
Rey#
```

```
Mashhad#show ip route
<<… Output Omitted…>>

Gateway of last resort is 172.16.20.5 to network 200.200.2.0

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D      172.16.12.0/24 [90/1794560] via 172.16.20.5, 00:17:40, Serial0/0/0
```

```
D      172.16.13.0/24 [90/1794560] via 172.16.20.5, 00:17:40, Serial0/0/0
D      172.16.14.0/24 [90/1794560] via 172.16.20.5, 00:17:40, Serial0/0/0
D      172.16.15.0/24 [90/1794560] via 172.16.20.5, 00:17:40, Serial0/0/0
D      172.16.20.0/30 [90/2304000] via 172.16.20.5, 00:17:40, Serial0/0/0
C      172.16.20.4/30 is directly connected, Serial0/0/0
C      172.16.20.8/30 is directly connected, Serial0/1/0
D   192.168.100.0/24 [90/2306560] via 172.16.20.5, 00:17:40, Serial0/0/0
C   192.168.200.0/24 is directly connected, FastEthernet0/0
D*   200.200.2.0/24 [90/21024000] via 172.16.20.5, 00:17:40, Serial0/0/0
Mashhad#
```

همانطور که مشاهده می‌کنید، با صرف نظر از no auto-summary در روتر تهران، امکان تبلیغ Default Network نیز فراهم گردید.

اگر به خروجی‌های فوق دقت نموده باشید، متوجه خواهید شد که علیرغم اینکه شهرری و مشهد دارای لینک مستقیم با یکدیگر هستند اما مسیری که در جدول Routing Table این دو روتر برای ارتباط با یکدیگر قرار گرفته است، از طریق مسیر تهران می‌باشد. انتخاب این مسیر به دلیل پهنای باند و زمان تاخیر بهتر لینک مستقیم تهران با شعب، نسبت به لینک مستقیم شهرری و مشهد با یکدیگر می‌باشد. اگر به یاد داشته باشید این اتفاق در سناریو قبلی که بر اساس RIP بود اتفاق نیافتاد؛ چراکه Metric در RIP بر اساس تعداد hop به دست می‌آید و مقدار پهنای باند در آن تاثیری ندارد.

برای بررسی مسیر ارتباط شهرری و مشهد با یکدیگر، از دستور Traceroute استفاده می‌نماییم:

```
Rey#traceroute 192.168.200.1
Type escape sequence to abort.
Tracing the route to 192.168.200.1

 1  172.16.20.1    42 msec   1 msec    7 msec
 2  172.16.20.6    8 msec    8 msec    14 msec
Rey#
```

```
Mashhad#traceroute 192.168.100.1
Type escape sequence to abort.
Tracing the route to 192.168.100.1

 1  172.16.20.5    3 msec    7 msec    8 msec
 2  172.16.20.2    15 msec   11 msec   10 msec
Mashhad#
```

حالا به خروجی دستور show ip eigrp topology دقت نمایید:

```
Rey#show ip eigrp topology
IP-EIGRP Topology Table for AS 110
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
     r - Reply status

P 192.168.100.0/24, 1 successors, FD is 28160
       via Connected, FastEthernet0/0
P 172.16.20.8/30, 1 successors, FD is 20512000
       via Connected, Serial0/0/0
P 172.16.20.0/30, 1 successors, FD is 1792000
       via Connected, Serial0/1/0
P 172.16.20.4/30, 1 successors, FD is 2304000
       via 172.16.20.1 (2304000/1792000), Serial0/1/0
       via 172.16.20.10 (21024000/1792000), Serial0/0/0
P 192.168.200.0/24, 1 successors, FD is 2306560
       via 172.16.20.1 (2306560/1794560), Serial0/1/0
       via 172.16.20.10 (20514560/28160), Serial0/0/0
P 172.16.12.0/24, 1 successors, FD is 1794560
       via 172.16.20.1 (1794560/28160), Serial0/1/0
P 172.16.13.0/24, 1 successors, FD is 1794560
       via 172.16.20.1 (1794560/28160), Serial0/1/0
P 172.16.14.0/24, 1 successors, FD is 1794560
       via 172.16.20.1 (1794560/28160), Serial0/1/0
P 172.16.15.0/24, 1 successors, FD is 1794560
       via 172.16.20.1 (1794560/28160), Serial0/1/0
P 200.200.2.0/24, 1 successors, FD is 21024000
       via 172.16.20.1 (21024000/20512000), Serial0/1/0
Rey#
```

همانطور که ملاحظه می کنید، روتر شهرری در جدول توپولوژی خود دارای دو مسیر با دو Metric متفاوت برای رسیدن به شبکه مشهد می‌باشد. و از آنجا که Metric مسیر تهران برای رسیدن به شبکه مشهد بهتر از مسیر مستقیم آنها می‌باشد، همان مسیر در جدول مسیریابی قرار گرفته است.

اما اگر به یاد داشته باشید، قبلا گفتیم که EIGRP امکان Load Balancing بر روی مسیرهای با Metric نابرابر را هم دارد. حالا اگر بخواهیم از لینک مستقیم شهرری و مشهد نیز بصورت همزمان با لینک تهران استفاده کنیم، می توانیم از دستور Variance کمک بگیریم.

```
Rey>enable
Rey#configure terminal
Rey(config)#router eigrp 110
Rey(config-router)#variance 10
Rey(config-router)#^Z
Rey#
```

پس از اعمال دستور فوق، خروجی جدول مسیریابی روتر شهرری به صورت زیر در می‌آید:

```
Rey#show ip route
…
<<… Output Omitted…>>
```

```
Gateway of last resort is 172.16.20.1 to network 200.200.2.0

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D      172.16.12.0/24 [90/1794560] via 172.16.20.1, 00:02:58, Serial0/1/0
D      172.16.13.0/24 [90/1794560] via 172.16.20.1, 00:02:58, Serial0/1/0
D      172.16.14.0/24 [90/1794560] via 172.16.20.1, 00:02:58, Serial0/1/0
D      172.16.15.0/24 [90/1794560] via 172.16.20.1, 00:02:58, Serial0/1/0
C      172.16.20.0/30 is directly connected, Serial0/1/0
D      172.16.20.4/30 [90/2304000] via 172.16.20.1, 00:02:58, Serial0/1/0
                [90/21024000] via 172.16.20.10, 00:02:58, Serial0/0/0
C      172.16.20.8/30 is directly connected, Serial0/0/0
C    192.168.100.0/24 is directly connected, FastEthernet0/0
D    192.168.200.0/24 [90/2306560] via 172.16.20.1, 00:02:58, Serial0/1/0
                [90/20514560] via 172.16.20.10, 00:02:58, Serial0/0/0
D*   200.200.2.0/24 [90/21024000] via 172.16.20.1, 00:02:58, Serial0/1/0
Rey#
```

در حال حاضر پروتکل EIGRP با توجه به امکان Unequal Load Balancing امکان استفاده از هر دو ارتباط شهرری و مشهد را بصورت همزمان برقرار نموده است.

اگر دوبار پشت سر هم اقدام به Traceroute شبکه مشهد از طریق روتر شهرری نمایید، خواهید دید که ارتباط یک بار از طریق مسیر تهران و بار دیگر از طریق لینک مستقیم، با شبکه مشهد برقرار می شود.

```
Rey#traceroute 192.168.200.1
Type escape sequence to abort.
Tracing the route to 192.168.200.1

  1  172.16.20.1    34 msec   1 msec    1 msec
Rey#traceroute 192.168.200.1
Type escape sequence to abort.
Tracing the route to 192.168.200.1

  1  172.16.20.10   12 msec   6 msec    5 msec
Rey#
```

طریقه عملکرد:

پروتکلEIGRP با ارسال متناوب پیام Hello در قالب Multicast به آدرس 224.0.0.10 اقدام به شناسایی روترهای همسایه می‌نماید. روترهای دریافت کننده پیام Hello اقدام به بررسی شماره AS پیام نموده و در صورتیکه پیام برای همان ASای باشد که روتر در آن وجود دارد، اقدام به پذیرش آن نموده و در غیر اینصورت پیام را نادیده می گیرند.

روتر پس از شناسایی همسایه‌های خود و برقراری رابطه مجاورت[1] با آنها، اقدام به ثبت روترهای همسایه و اینترفیس‌های مربوطه در جدول Neighbor Table خود می‌نماید.

توسط دستور show ip eigrp neighbors ، می توانید روترهایی را که به عنوان همسایه در جدول Neighbor Table ثبت شده را ملاحظه نمایید.

```
Rey#show ip eigrp neighbors
IP-EIGRP neighbors for process 110
H   Address        Interface     Hold Uptime   SRTT   RTO   Q   Seq
                                 (sec)         (ms)       Cnt  Num
0   172.16.20.1    Se0/1/0        14  00:21:25  40    1000  0   34
1   172.16.20.10   Se0/0/0        13  00:21:25  40    1000  0   63
```

پس از ثبت روتر در جدول Neighbor Table، برای بار اول روترها اقدام به ارسال کامل جدول توپولوژی خود در قالب پیام Update به یکدیگر می‌نمایند. این پیام‌های Update بصورت Unicast و به آدرس روتر موجود در جدول ارسال می‌شود. روترهای همسایه نیز در صورت دریافت پیام Update، با ارسال پیام Acknowledge درستی دریافت پیام را به اطلاع روتر ارسال کننده می‌رسانند.

پس از این مرحله هر سه روتر تهران، شهرری و مشهد مقدس، دارای جدول توپولوژی کامل با آگاهی از شبکه‌های قابل دسترس در AS مورد نظر می‌باشند.

جدول توپولوژی روتر شامل تمام مسیرهای موجود جهت دسترسی به شبکه های تبلیغ شده می‌باشد. روتر پس از کامل شدن جدول Topology Table خود، اقدام به بررسی مسیرهای موجود در این جدول نموده و بر اساس AD و Metric، بهترین مسیرهای موجود را مشخص نموده و در جدول Routing Table درج می‌نماید.

مسیرهای موجود در Topology Table ممکن است دارای Metric متفاوت باشند. مثلا برای روتر شهرری دو مسیر به شبکه مشهد وجود دارد. یک مسیر از طریق روتر تهران و یک مسیر هم بطور مستقیم. ولی به علت پهنای باند بهتر و مدت تاخیر کمتر لینک تهران، این مسیر به عنوان Successor مشخص شده و لینک مستقیم بین ری و مشهد نیز به عنوان Feasible Successor مشخص گردیده است. مسیر یا مسیرهایSuccessor در جدول مسیریابی روتر ثبت شده و مسیرهایFeasible Successor نیز به عنوان مسیرهای جایگزین در جدول توپولوژی باقی می‌مانند. در صورت از دست رفتن لینک Successor، الگوریتم DUAL بدون نیاز به دریافت پیام‌های Update جدید، با رجوع به جدول توپولوژی، مسیری را که قبلا به عنوان Feasible Successor مشخص شده بود را در جدول مسیریابی روتر ثبت می‌نماید.

[1] Adjacency

همانطور که قبلا گفتیم، روتر اقدام به ارسال پیام‌های متناوبHello و همچنین پیام‌های Update در زمان مورد نیاز می‌نماید. این پیام‌ها از طریق اینترفیس‌هایی ارسال و دریافت می‌شوند که آدرس آنها قبلا توسط دستورNetwork به پروتکل مسیریابی معرفی شده باشند. اگر بر روی روتر دستور show ip eigrp interface را اجرا نماییم، می توانیم اینترفیس‌هایی را که در پروسه پروتکل مسیریابی دخیل هستند را مشاهده نماییم. برای مثال این دستور را بر روی روتر مشهد اجرا می‌نماییم:

```
Mashhad#show ip eigrp interfaces
IP-EIGRP interfaces for process 110

                Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface       Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0           0      0/0    1236     0/10        0        0
Se0/0/0          1      0/0    1236     0/10        0        0
Se0/1/0          1      0/0    1236     0/10        0        0
Mashhad#
```

همانطور که مشاهده می نمایید، اینترفیس Fa0/0 نیز در پروسه پروتکل EIGRP حضور دارد. اما با توجه به اینکه این اینترفیس به شبکه داخلی متصل بوده و نیازی به ایجاد، ارسال و دریافت پیام های Hello و Update ندارد، می توانیم این اینترفیس را به عنوان Passive Interface پیکربندی نموده تا ضمن جلوگیری از به هدر رفتن منابع روتر، باعث افزایش امنیت شبکه نیز شویم.

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#router eigrp 110
Mashhad(config-router)#passive-interface fastEthernet 0/0
Mashhad(config-router)#^Z
Mashhad#
```

پس از اعمال دستور فوق، خروجی show ip eigrp interface روتر مشهد به شکل زیر خواهد بود:

```
Mashhad#show ip eigrp interfaces
IP-EIGRP interfaces for process 110

                Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface       Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0/0          1      0/0    1236     0/10        0        0
Se0/1/0          1      0/0    1236     0/10        0        0
Mashhad#
```

توجه داشته باشید که پیکربندی اینترفیس Fa0/0 هیچ خللی در تبلیغ شبکه‌های متصل به آن، ایجاد نمی‌نماید.

این عمل را می‌توانید بر روی اینترفیس‌های Fastethernet روترهای تهران و شهرری نیز تکرار نمایید. البته از همه مهمتر اینکه، اینترفیس متصل به شبکه خارجی را حتما باید به عنوان Passive-interface پیکربندی نمایید. در غیر اینصورت پیام‌های حاوی مشخصات شبکه شما به خارج از شبکه راه یافته و ممکن است امنیت شبکه را به مخاطره اندازد.

برای بررسی زمان سنج‌ها، مقادیر اختصاص داده شده به K-Values و دیگر تنظیمات پروتکل EIGRP می توانید از دستور show ip protocols استفاده نمایید:

```
Tehran#show ip protocols

Routing Protocol is "eigrp  110 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 110
  Automatic network summarization is in effect
  Automatic address summarization:
    200.200.2.0/24 for FastEthernet0/0.2, FastEthernet0/0.3, FastEthernet0/0.4, FastEthernet0/0.5, Serial0/0/0, Serial0/1/0
      Summarizing with metric 20512000
    172.16.0.0/16 for Serial0/2/0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.12.0/22
    172.16.20.0/30
    172.16.20.4/30
    200.200.2.0
  Passive Interface(s):
    FastEthernet0/0
    Serial0/2/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.20.6     90            5572
    172.16.20.2     90            5696
  Distance: internal 90 external 170

Tehran#
```

همانطور که در خروجی فوق ملاحظه می کنید، تعداد hop-count در پروتکل EIGRP برابر 100 می باشد. شما می توانید این مقدار را تا 255 افزایش دهید.

همچنین بصورت پیش‌فرض maximum-path=4 می‌باشد. این عدد نشان دهنده تعداد مسیری است که در Load Balancing مورد استفاده قرار می‌گیرد. تعداد مسیرهای Load Balancing در پروتکل EIGRP می تواند، حداکثر تا ۶ مسیر پیکربندی گردد.

مرجع دستور Command Reference:

Enable EIGRP		
Step	**Command**	**Purpose**
1	**router eigrp** *autonomous-system* Example: Router(config)#router eigrp 110	Enable an EIGRP routing process in global configuration mode.
2	**network** *network-number wildcard-mask* Router(config-router)#network 10.10.10.0 0.0.0.255	Associate networks with an EIGRP routing process in router configuration mode.

Monitor and Maintain EIGRP	
Command	**Purpose**
show ip eigrp interfaces *[interface] [as-number]*	Display information about interfaces configured for EIGRP.
show ip eigrp neighbors *[type number]*	Display the EIGRP discovered neighbors.
show ip eigrp topology *[autonomous-system-number | [[ip-address] mask]]*	Display the EIGRP topology table for a given process.
show ip eigrp traffic *[autonomous-system-number]*	Display the number of packets sent and received for all or a specified EIGRP process.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

Adjust the Interval between Hello Packets and the Hold Time	
Command	**Purpose**
ip hello-interval eigrp *autonomous-system-number seconds*	Configure the hello interval for an EIGRP routing process.
ip hold-time eigrp *autonomous-system-number seconds*	Configure the hold time for an EIGRP routing process.

EIGRP Command (Optional)	
Command	**Description**
auto-summary Example: Router(config-router)#auto-summary	The behavior of this command is enabled by default (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).
metric weights *tos k1 k2 k3 k4 k5* Example: Router(config-router)# metric weights 0 1 0 1 0 0	Constants that convert an IGRP or EIGRP metric vector into a scalar quantity. Tos= Type of service must always be zero.
passive-interface *{*interface-type interface-number*}* Example: Router(config-router)# passive-interface fastethernet 0/0	To disable sending routing updates on an interface, use the passive-interface command in router configuration mode. To reenable the sending of routing updates, use the no form of this command.
bandwidth *value(Kbps)* Example: Router(config-if)#bandwidth 128	Sets a bandwidth value for an interface.

Configure EIGRP Route Authentication		
Step	**Command**	**Purpose**
1	**interface** *type number*	Configure an interface type and enter interface configuration mode
2	**ip authentication mode eigrp** *autonomous-system* **md5**	Enable MD5 authentication in EIGRP packets.
3	**ip authentication key-chain eigrp** *autonomous-system key-chain*	Enable authentication of EIGRP packets.
4	**exit**	Exit to global configuration mode.
5	**key chain** *name-of-chain*	Identify a key chain. (Match the name configured in Step 1.)
6	*key number*	In key chain configuration mode, identify the key number.
7	*key-string text*	In key chain key configuration mode, identify the key string.
8	**accept-lifetime start-time** *{infinite | end-time | duration seconds}*	Optionally specify the time period during which the key can be received.
9	**send-lifetime start-time** *{infinite | end-time | duration seconds}*	Optionally specify the time period during which the key can be sent.

☑ مبحث چهارم

پروتکل OSPF

پروتکل مسیریابی OSPF(Open Shortest Path First)، یک پروتکل استاندارد بوده که توسط سازمان IETF بصورت استاندارد منتشر گردیده است.

پروتکل OSPF برای IPv4 دارای دو نسخه می‌باشد. اما نسخه‌ای که بصورت عملیاتی مورد استفاده قرار گرفت OSPF v2 بوده که در قالب استاندارد RFC 2328 منتشر گردیده است.

خصوصیات کلی پروتکل OSPF v2 را می توان بصورت زیر نام برد:

- عضو گروه پروتکل‌های مسیریابی Link State می‌باشد.
- از مفهوم AS پشتیبانی می‌نماید.
- از ویژگیArea پشتیبانی می‌نماید. استفاده از Area در این پروتکل، باعث کاهش سایز جداول مسیریابی شده و به همین دلیل است که OSPF قابلیت اجرا در شبکه‌های بسیار بزرگ را دارد.
- از مدل سلسله مراتبی[1] استفاده می‌نماید.
- از الگوریتمDijkstra [2] برای مسیریابی استفاده می‌نماید. این الگوریتم به‌ازاء هر منطقه(Area) بطور مستقل اجرا می‌گردد.
- دارای سرعت همگرایی سریعتر از پروتکل‌های Distance Vector می‌باشد.
- از پارامتر هزینه مسیر (Path Cost) برای محاسبه Metric استفاده می‌نماید.
- عملکرد این پروتکل بصورت Classless بوده و امکان پشتیبانی از خلاصه سازی، VLSM و CIDR را دارد.
- امکان استفاده از Authentication در هر دو حالت Simple و MD5 را دارد.
- برای برقراری رابطه مجاورت اقدام به ارسال متناوب پیام Hello می‌نماید.

---

[1] Hierarchical Model

[2] در برخی مستندات فنی از این الگوریتم با عنوان SPF نیز نام برده می شود.

- پیام های Update را هر ۳۰ دقیقه یکبار ارسال می‌نماید. این پیام‌ها برای اولین بار بصورت کامل و در دفعات بعد حاوی خلاصه‌ای از جدول LSDB می‌باشند.
- از پیام‌های Multicast به آدرس 224.0.0.5 (برای روترهای OSPF) و آدرس 224.0.0.6 (برای روترهای DR)، استفاده می‌نماید.
- ارسال پیام‌ها بصورت قابل اطمینان و توسط پروتکل IP Protocol Type 89 انجام می‌پذیرد. (پروتکل OSPF همانند EIGRP از پروتکل های TCP/UDP استفاده نمی کند.)
- عدد AD اختصاص داده شده به این پروتکل 110 می‌باشد.
- به دلیل استفاده از الگوریتم Dijkstra، شبکه عاری از حلقه لایه سوم می‌باشد.
- امکان Load Balancing بر روی مسیرهای با Metric برابر (Equal) را نهایتا بر روی ۶ مسیر دارد.
- خلاصه سازی فقط بصورت دستی و بر روی روترهای ABR امکان پذیر است.

انواع پیام‌های OSPF

پروتکل OSPF برای انجام عملیات مسیریابی از ۵ نوع پیام به شرح زیر استفاده می‌نماید:

۱- Hello

از پیام Hello برای کشف روترهای همسایه، برقراری رابطه مجاورت و مشخص کردن وضعیت روتر استفاده می گردد.

همچنین با توجه به اینکه پیام Hello شامل Router ID می‌باشد، در پروسه انتخاب روترهای DR [1] و BDR [2] نیز مورد استفاده قرار می‌گیرد.

این پیام بصورت پیش فرض در شبکه‌های Broadcast مثل اترنت هر۱۰ ثانیه و در شبکه‌های Non-Broadcast هر۳۰ ثانیه یکبار در قالب Multicast و به آدرس 224.0.0.5 ارسال می‌گردد.

در صورتی که روتر ۴ برابر مدت زمان پیام Hello، هیچ پیامی از روتر همسایه دریافت ننماید، فرض را بر معیوب شدن آن روتر گذاشته و وضعیت آنرا به Down تغییر می‌دهد. مقدار این زمان سنج که Dead Interval نامیده می شود، بصورت پیش فرض در شبکه های Broadcast، ۴۰ ثانیه و در شبکه های Non Broadcast، ۱۲۰ ثانیه می‌باشد.

---

[1] Designated Router
[2] Backup Designated Router

۲- **Database Description**

هر بسته Database Description شامل شرح مختصری از تمام LSA های موجود در دیتابیس روتر می‌باشد. وقتی روتر همسایه این بسته را دریافت می‌نماید، محتویات دیتابیس خود را با آن مقایسه نموده و متوجه کاستی‌های دیتابیس خود می‌شود.

روترها از این پیام که به اختصار DD و یا DBD نیز نامیده می‌شود برای هماهنگ سازی[1] اطلاعات دیتابیس خود با دیگر روترهای همان AS، استفاده می‌نمایند.

به فرآیند ارسال و دریافت بسته‌های DBD، "فرآیند تبادل دیتابیس"[2] می‌گویند. در طی این فرآیند دو روتر اقدام به برقراری رابطه Master/Slave با یکدیگر می‌نمایند.

۳- **Link-State Request**

این پیام شامل لیست شناسه مربوط به پیام‌های LSA مورد نیاز درخواست کننده، برای کامل کردن اطلاعات جدول LSDB خود می‌باشد. بطور معمول روتر این لیست را از مقایسه پیام DBD دریافت شده با دیتابیس خود به دست می‌آورد.

پیام Link-State Request بصورت اختصار، LSR نامیده می شود.

۴- **Link-State Update**

این پیام که شامل جزئیات کامل LSAها می‌باشد، بطور معمول در جواب پیام‌های درخواست (LSR) ارسال می‌گردد.

۵- **Link-State Acknowledgement**

پیام LSAck، جهت تایید دریافت پیام هایLSU ارسال می‌گردد.

انواع پیام های LSA

روترهایی که پروتکلOSPF بر روی آنها اجرا گردیده است، باید دارای اطلاعات کاملی از مسیرها و شبکه‌های مربوط به Area خود باشند. این اطلاعات در جدولی به نام LSDB ذخیره می‌گردد. جداولLSDB باید بر روی تمام روترهای همان Area با یکدیگر هماهنگ باشند.

پروتکلOSPF برای تبادل اطلاعات مورد نیاز جدولLSDB از پیام‌های (Link-State Advertisement) LSA استفاده می‌نماید. این پیام‌ها حاوی یک شماره ترتیب[3] به طول ۳۲ بیت، جهت تشخیص جدید یا قدیمی بودن پیام‌ها و همچنین توالی صحیح دریافت آنها می باشد. جدول LSDB دارای فیلد Age برای مشخص نمودن زمان مفید نگهداری پیام های LSA می‌باشد.

---

[1] synchronous
[2] Database Exchange Process
[3] Sequence Number

پیام های LSA برای انجام وظایف خود دارای انواع مختلفی پیام می‌باشد که هر کدام آنها توسط یک شماره مشخص می‌شوند. شرح این پیام ها در ادامه آمده است.

- **LSA Type 1**

این نوع پیام را Router LSA نیز می‌نامند. روترها با ارسال این پیام، لیست لینک‌های خود را که به روتر و یا شبکه‌های دیگر در همان Area متصل است، به همراه Metric آنها برای تمام روترهای Area خود ارسال می‌نماید.

- **LSA Type 2**

این پیام توسط روترDR برای تمام روترهای همان حوزه ارسال می‌گردد. این پیام شامل لیست Cost مسیرها و روترهایی می‌باشد که روتر ارسال کننده پیام، توسط آنها به عنوان DR پذیرفته شده است.

از پیام LSA Type 2 با عنوان Network LSA نیز نام برده می‌شود.

- **LSA Type 3**

این پیام توسط روتر ناحیه مرزی (ABR) ایجاد شده و به داخل یک Area پخش می‌گردد. این پیام حاوی اطلاعات مربوط به مسیر شبکه‌های قابل دسترس در Areaهای دیگر می‌باشد.

نام دیگر این پیام، Network Summary LSA است.

- **LSA Type 4**

این پیام که توسط روترهای ABR به داخل یک ناحیه ارسال می‌گردد، شامل هزینه دسترسی به روتر ASBR می‌باشد.

پیام LSA Type 4 را با عنوان ASBR Summary LSA نیز می‌نامند.

- **LSA Type 5**

این پیام توسط روتر ASBR به تمام نواحی حوزه OSPF ارسال می‌گردند. پیام LSA Type 5 که با عنوان AS External LSA نیز نام برده می‌شود، حاوی اطلاعات مسیرهای دسترسی به شبکه‌های خارجی از طریق روتر ASBR می‌باشد.

- **LSA Type 6**

این پیام که Multicast Group Membership نیز نامیده می‌شود، در عمل به سرانجام مشخصی نرسیده و توسط روترهای سیسکو نیز پشتیبانی نمی‌گردد.

- **LSA Type 7**

این پیام به جای پیام LSA Type 5 توسط روترASBR در ناحیهNSSA ارسال می‌گردد.

از پیام LSA Type 7 با عنوان NSSA External نیز نام برده می‌شود.

جداول پروتکل OSPF

پروتکلOSPF نیز همانند پروتکل‌های مسیریابی دیگر، برای انجام عملیات خود دارای ۳ جدول به شرح زیر می‌باشد.

- **Neighbor Table**

جدول همسایه (Neighbor Table) شامل روترهای همسایه می‌باشد که اقدام به برقراری رابطه مجاورت با روتر نموده‌اند.

روترها برای کشف، مشخص نمودن و بررسی وضعیت روترهای همسایه از ارسال متناوب پیام های Hello استفاده می‌نمایند.

- **Link-State Database**

جدول Links-State Database را به اختصار LSDB می‌نامند. طریقه عملکرد جدول LSDB نیز شبیه جدول توپولوژی بوده، به همین دلیل در برخی مستندات فنی از این جدول با نام Topology Table نیز یاد می‌شود.

جدول LSDB شامل آدرس تمام روترهای موجود در همان Area و شبکه‌های متصل به آنها به همراه Metric مسیرها می‌باشد. البته توجه داشته باشید که محاسبه Metric برای مسیرهای به دست آمده، بر اساس الگوریتم Dijkstra و بصورت مستقل در هر روتر انجام می‌پذیرد.

پروتکل OSPF برای درج اطلاعات در جدول LSDB از پیام های LSA استفاده می‌نماید.

- **Routing Table**

پروتکل OSPF با بررسی جداول LSDB و Neighbor، بهترین مسیرهای منتهی به مقصدهای مختلف را مشخص کرده و در جدول Routing Table درج می‌نماید.

روتر در نهایت برای انجام عملیات مسیریابی بر اساس محتویات این جدول اقدام می‌نماید.

ناحیه (Area)

توسط پروتکلOSPF می توان یک شبکه را به زیر دامنه‌های کوچکتری به نام ناحیه (Area) تقسیم بندی نمود. یک Area، مجموعه‌ای منطقی از شبکه‌ها، روترها و اتصالاتی است که دارای یک شناسه ناحیه شبیه به یکدیگر می‌باشند.

نواحی باعث محدود شدن دامنه توزیع اطلاعات مربوط به مسیرها می‌شوند. هر روتر باید اطلاعات کامل Topology مربوط به ناحیه‌ای را نگهداری نماید که به آن تعلق دارد. این روترها

نیازی به نگهداری اطلاعات دقیق توپولوژی مربوط به سایر نواحی را در دیتابیس خود نداشته و فقط از Rout Summarization مربوط به آنها با خبر می‌باشند لذا سایز جداول مسیریابی آنها کاهش می‌یابد.

اطلاعات موجود در دیتابیس LSDB(Link State Database) روترهای موجود در یک ناحیه باید همواره با یکدیگر هماهنگ شده و دقیقا شبیه به یکدیگر باشند. همچنین به یاد داشته باشید که امکان فیلترینگ اطلاعات مربوط به پیام‌های Update در داخل یک ناحیه امکان پذیر نمی‌باشد.

در نهایت می توان گفت مهمترین مزیت ایجاد نواحی، کاهش تعداد مسیرهای انتشار داده شده می باشد که این امر با فیلترینگ و خلاصه سازی مسیرها بوجود می‌آید.

حداکثر ۵۰ عدد روتر می تواند در هر ناحیه OSPF قرار داشته باشد.

انواع Area

ناحیه‌های مورد استفاده در پروتکل OSPF به ۵ قسمت زیر تقسیم می شوند:

۱- **Backbone**

برای اجرای پروتکل OSPF، حداقل نیاز به وجود یک ناحیه با نام ناحیه ستون فقرات (Backbone Area) می‌باشد. با توجه به اینکه ناحیه‌ها توسط عدد اختصاص داده شده به آنها (Area ID)، قابل شناسایی هستند، ناحیه ستون فقرات را Area 0 نیز می‌نامند. این Area باید با تمام Areaهای موجود در شبکه، بطور مستقیم در ارتباط باشد. به همین دلیل، ساختار OSPF را ساختار درختی و یا سلسله مراتبی می‌نامند.

۲- **Standard**

ناحیه Standard یک ناحیه معمولی است که به ناحیه ستون فقرات متصل بوده و شرایط خاصی بر آن حاکم نمی‌باشد.

۳- **Stub**

ناحیه Stub، به شبکه ای کوچک اطلاق می شود که نیازی به دریافت تبلیغات روترهای خارجی[1] را نداشته و به دلیل کوچک بودن می‌تواند با یک Default Route ساده، با شبکه های خارجی[2] ارتباط برقرار نماید.

جلوگیری از ورود تبلیغ شبکه‌های خارجی به ناحیه Stub، باعث کوچک شدن جداول مسیریابی روترهای این ناحیه می گردد.

---

[1] External Routers

[2] منظور از شبکه های خارجی، شبکه های موجود در ASهای دیگر می باشد.

هر چند که ناحیه Stub از ورود اطلاعات روترهای خارجی جلوگیری می‌نماید، اما اطلاعات تبلیغ شده توسط نواحی دیگر همان دامنه OSPF را دریافت می‌نماید.

۴- **Totally Stub**

این ناحیه نیز شبیه ناحیهStub می‌باشد با این تفاوت که علاوه بر عدم دریافت اطلاعات مربوط به شبکه‌های خارجی، از پذیرش اطلاعات مربوط به نواحی دیگر همان دامنه OSPF نیز خودداری می‌نماید. روترهای این ناحیه فقط دارای LSDB مخصوص به خود بوده و دیگر شبکه‌ها را بر اساس Default Route مسیر دهی می‌نماید.

این ناحیه توسط سیسکو معرفی گردیده و فقط در تجهیزات سیسکو قابل پیکربندی می‌باشد.

۵- **NSSA**

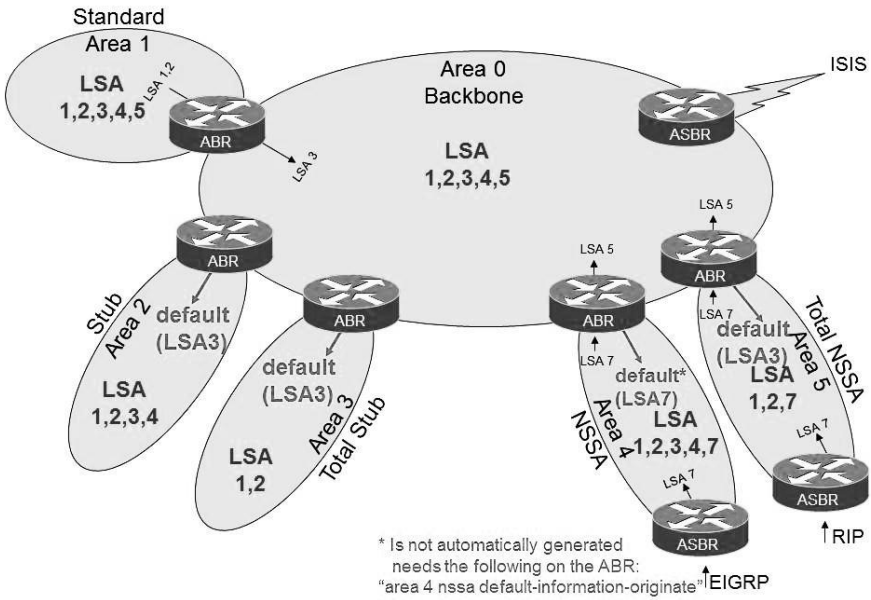
ناحیه NSSA(Not-So-Stubby Area) که توسط استاندارد1587 RFC منتشر گردیده، عملکردی شبیه ناحیه Stub داشته ولی دارای انعطاف پذیری بیشتری نسبت به آن می‌باشد. توسط این ناحیه‌ها که در مرز[1] شبکهOSPF واقع می‌شوند، می‌توان مسیرهای خارجی را به حوزه مسیریابیOSPF وارد نمود. در نتیجه توسط ناحیه NSSA می توان سرویس تبادل اطلاعات را با حوزه‌های کوچک مسیریابی که جزئی از حوزه OSPF نمی‌باشند، نیز بوجود آورد.

۶- **Totally NSSA**

ناحیه Totally NSSA، توسط سیسکو معرفی گشته و عملکردی شبیه ناحیه NSSA دارد. تفاوت این ناحیه با NSSA در استفاده نکردن از پیام های LSA نوع4 و3 می‌باشد.

در تصویر زیر انواع ناحیه های OSPF و نوع پیام‌های LSA مورد استفاده در آنها نمایش داده شده است.

[1] Edge



قوانین استفاده از Area

در زمان راه اندازی پروتکلOSPF، برای استفاده صحیح از ویژگی Area، باید سه قانون زیر را رعایت نمایید.

۱- برای راه اندازی پروتکلOSPF، حداقل باید یک ناحیه با عنوان ناحیه ستون فقرات یا Area 0 ایجاد گردد.

۲- تمام نواحی غیر از ستون فقرات، حتما باید دارای یک اتصال مستقیم با ناحیه ستون فقرات باشند.

البته در شرایطی که امکان اتصال مستقیم یک ناحیه با ناحیه ستون فقرات وجود نداشته باشد، می توان از ویژگی Virtual Link بهره برد.

۳- ناحیه ستون فقرات تحت هیچ شرایطی (مثل خراب شدن یک لینک یا روتر) نباید به قسمت های کوچکتری تقسیم شود.

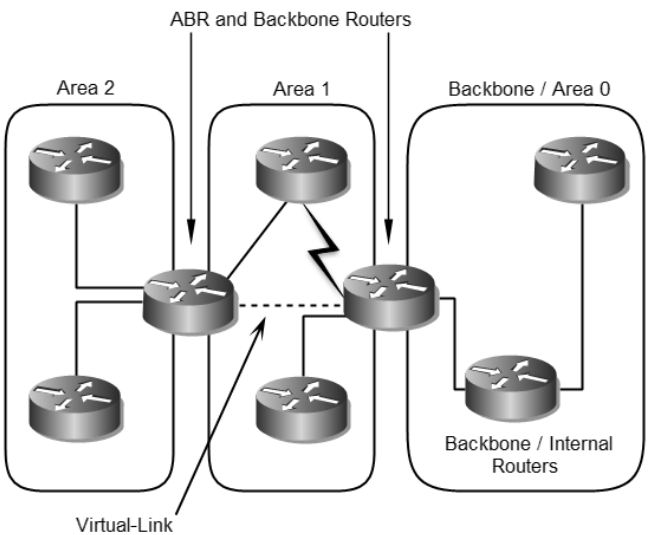
ویژگی Virtual-Link

Virtual-Link یک لینک مجازی بوده که از طریق یک منطقه ثالث، ناحیه ستون فقرات را به یک ناحیه دیگر در همان حوزه OSPF متصل می‌نماید.

همانطور که قبلا گفتیم، تمام حوزه‌های موجود در ناحیهOSPF باید بصورت فیزیکی دارای ارتباط مستقیم با ناحیه ستون فقرات (Backbone Area) باشند. در برخی موارد که ایجاد اتصال مستقیم امکان پذیر نبوده و یا لینک مستقیم دچار خرابی شده باشد، می توان از ویژگی Virtual-Link استفاده نمود.

همچنین دیگر کاربرد Virtual-Link زمانی است که بخواهیم قسمت‌های منقطع ناحیه ستون فقرات را به یکدیگر متصل نماییم.

به ناحیه‌ای که عهده‌دار برقراری Virtual-Link می‌شود، منطقه حمل و نقل (Transit) گفته می‌شود. منطقه حمل و نقل نمی تواند به عنوان حوزه Stub مورد استفاده قرار گیرد.



طبقه بندی روترها

روترهایی که پروتکلOSPF را در شبکه اجرا می‌نمایند، بر اساس نحوه قرار گرفتن در Area و نقشی که در پروسه مسیریابی بر عهده می‌گیرند، به چهار گروه زیر طبقه بندی می‌شوند:

۱- **Internal Routers**

روترهای داخلی (Internal Routers)، روترهایی هستند که تمام اینترفیس‌های آنها متصل به شبکه‌های متعلق به همان ناحیه می‌باشد.

بر روی این روترها یک کپی یکسان از الگوریتم مسیریابی درحال اجرا بوده و دارای یک جدول LSDB مشابه می‌باشد.

۲- **Area Border Routers**

روتر ناحیه مرزی(ABR)، به روترهایی اطلاق می‌شود که همزمان به مناطق مختلفی متصل باشند. البته حداکثر ۳ ناحیه می‌تواند به روتر ABR متصل باشد.

بر روی روترهای ناحیه مرزی چندین کپی از الگوریتم مسیریابی در حال اجرا می‌باشد. تعداد این کپی‌ها بستگی به تعداد نواحی متصل شده به روتر دارد.

روترهای ناحیه مرزی حاوی اطلاعات توپولوژی تمام نواحی متصل به خود بوده و به ازاء هریک از آنها دارای یک جدول LSDB جداگانه می‌باشد. روترهای ABR وظیفه ارسال این اطلاعات را به ناحیه Backbone داشته و ناحیه Backbone نیز بالطبع آن را به اطلاع نواحی دیگر می‌رساند.

۳- **Backbone Routers**

روتر ستون فقرات(BR) به روتری گفته می شود که حداقل دارای یک اتصال مستقیم به ناحیه ستون فقرات باشد.

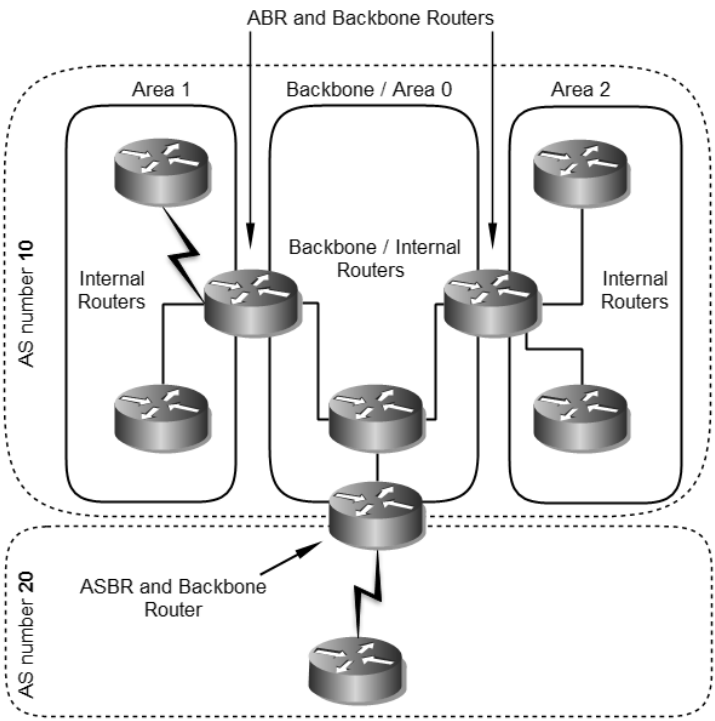
این حالت می‌تواند شامل تمام روترهایی گردد که یک اینترفیس آنها متصل به ناحیه دیگری می‌باشد، مثل روترهای ناحیه مرزی (ABR). ولی به هر حال نیازی نیست که یک روتر ستون فقرات عملکردی شبیه یک روتر ناحیه مرزی داشته باشد و می تواند تمام اینترفیس‌های آن به ناحیه ستون فقرات متصل باشد.

۴- **AS Boundary Routers**

روترهای مرزی AS که بطور اختصار آنرا ASBR نیز می‌نامند، به روترهایی گفته می‌شود که اقدام به تبادل اطلاعات مسیریابی خود با روترهای واقع در یک AS دیگر می‌نمایند. این روترها باید حداقل دارای یک اتصال مستقیم به شبکه‌ای با شناسه AS متفاوت باشند.

توجه داشته باشید که این طبقه بندی کاملا مستقل از دیگر طبقه بندی‌ها می‌باشد. یک روتر ASBR ممکن است همزمان نقش یک روتر داخلی (Internal Router) یا یک روتر ABR و یا یک روترBR را نیز بر عهده داشته باشد.

با دقت در تصویر زیر می توانید با نقش روترها در پروتکل OSPF بهتر آشنا شوید:



طریقه محاسبه Metric

پروتکل OSPF برای محاسبه Metric از هزینه مسیر (Path Cost) استفاده می‌نماید. مقدار Cost دارای رابطه عکس با پهنای باند می باشد. هر چه مقدار پهنای باند بیشتر باشد، مقدار Cost کمتر خواهد بود. در نهایت مسیرهایی برای درج در جدول Routing Table انتخاب می شوند که دارای مقدار Cost کمتری نسبت به مسیرهای دیگر به مقصد مورد نظر باشند.

پروتکل OSPF برای محاسبه Cost مسیرهای به دست آمده، از فرمول زیر استفاده می نماید:

$$\text{Cost} = \frac{Reference\ Bandwidth}{Configured\ Bandwidth}$$

تشریح پارامترهای استفاده شده در فرمول فوق بصورت زیر می باشد:

۱- **Reference Bandwidth**

مرجع پهنای باند (Reference Bandwidth) مقدار پهنای باندی است که می خواهیم مقدار Cost لینک‌های شبکه بر اساس آن محاسبه گردد.

بصورت پیش فرض مقدار این پارامتر بر اساس اتصالات 100Mbps تعیین گردیده است. اما در چند سال اخیر با توجه به فراگیری استفاده از لینک‌های پر سرعت مثل 1Gbps یا 10Gbps، در صورتیکه مرجع پهنای باند همان مقدار پیش فرض باشد، مقدار Cost به دست آمده برای تمام لینک های با سرعت برابر و بالاتر از 100Mbps با یکدیگر هیچ فرقی نخواهد داشت.

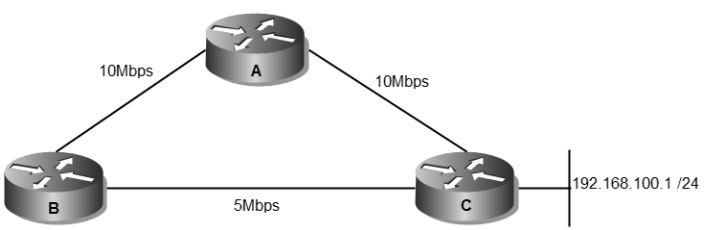
برای رفع ایراد فوق می توانید مقدار Reference Bandwidth را بصورت دستی تعیین نمایید. برای تغییر مقدار پیش فرض در روترهای سیسکو از دستور زیر استفاده نمایید.

Router(config-router)#**auto-cost reference-bandwidth** *Value*

۲- **Configured Bandwidth**

مقدار پهنای باند لینک مورد نظر برای محاسبه Cost می باشد.

برای درک بهتر نحوه محاسبه Cost به مثال زیر دقت نمایید.

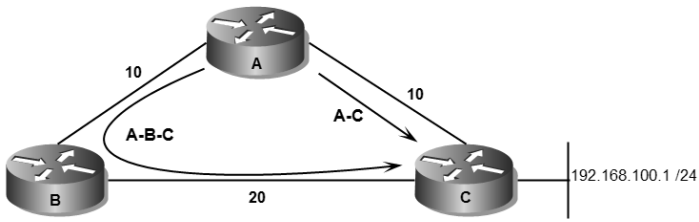


پروتکل OSPF ابتدا Cost مربوط به هر لینک را محاسبه می‌نماید. با توجه به اینکه مقدار پیش فرض برای پارامتر Reference Bandwidth برابر 100Mbps می‌باشد، مقدار Cost هر لینک بصورت زیر محاسبه می‌گردد.

AtoB= $\frac{100\ Mbps}{10}$=10 AtoC= $\frac{100\ Mbps}{10}$=10 BtoC= $\frac{100\ Mbps}{5}$=20

پس از محاسبه Cost، پروتکل OSPF لینک ها را به چشم Cost آنها می بیند!

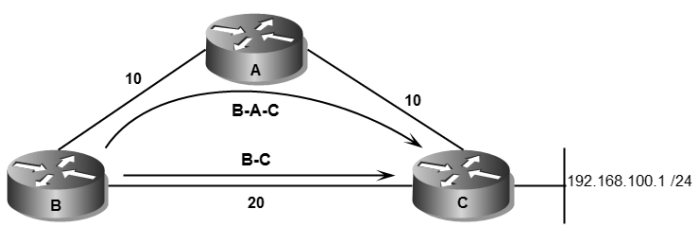
حال اگر روتر A بخواهد به شبکه 192.168.100.0 /24 دسترسی داشته باشد، دارای ۲ مسیر می باشد. محاسبه Cost مسیرها به شکل زیر انجام می گیرد:



A-C = 10
A-B-C = 10+20 = 30

همانطور که مشاهده می‌نمایید، روتر برای محاسبه Cost هر مسیر اقدام به محاسبه مجموع Cost تمام لینک‌های طول مسیر می‌نماید. با توجه به اینکه مسیر مستقیم روتر A به C دارای Cost پایین‌تری می‌باشد، پروتکلOSPF مسیر اول را در جدول مسیریابی روتر ثبت خواهد نمود.

اما اگر بخواهیم از طریق روتر B به شبکه 192.168.100.0 /24 دسترسی داشته باشیم، دارای دو مسیر با Cost زیر خواهیم بود.



B-C = 20
B-A-C = 10+10 = 20

در اینصورت ما دارای دو مسیر با Cost برابر برای دسترسی روتر B به شبکه 192.168.100.0 /24 هستیم. به توجه به اینکه پروتکل OSPF امکان Load Balancing بر روی مسیرهای Equal را دارد، پس هر دو مسیر فوق در جدول مسیریابی روتر ثبت خواهد گردید.

نکته: پهنای باند لینک های Serial در پروتکل OSPF بطور پیش فرض برابر لینک های T1 در نظر گرفته می شود.

نحوه انتخاب روتر DR و BDR

پروتکلOSPF برای برقراری رابطه مجاورت در شبکه‌های Broadcast و Non-Broadcast از ویژگی Designated Router استفاده می‌نماید. در این حالت روترهای موجود در شبکه به جای برقراری رابطه مجاورت با یکدیگر، با روتری که به عنوان DR تعیین گشته رابطه مجاورت برقرار نموده و اقدام به تبادل پیام‌های مسیریابی خود با روترDR می‌نمایند. روتر DR نیز وظیفه دارد اطلاعات به دست آمده را به اطلاع سایر روترهای شبکه برساند. در این صورت پیام‌ها بصورت بهینه ارسال و دریافت شده و از به هدر رفتن منابع شبکه جلوگیری به عمل می‌آید.

برای اینکه در صورت غیرفعال شدن روتر DR خللی در عملکرد شبکه وارد نگردد یک روتر جهت پشتیبانی روتر DR با عنوان Backup Designated Router مشخص می‌گردد.

روترDR وBDR براساس Priority تخصیص داده شده به اینترفیس دخیل در پروسه انتخاب، مشخص می‌گردد. با توجه به اینکه بصورت پیش فرض مقدارPriority اینترفیس روتر1 می‌باشد، معمولا انتخاب روترهای DR/BDR بر اساس Router ID انجام می‌شود. اگر پارامتر Router ID هم بر روی روترهای شبکه بصورت پیش فرض باشد، مقدار آن بر اساس بزرگترین آدرسIP اختصاص داده شده به اینترفیس مجازی Loopback و یا اینترفیس فیزیکی روتر تعیین می‌گردد.

نحوه انتخاب روترهای DR/BDR بی شباهت با انتخاب سوئیچ ریشه در پروتکل STP نیست. روترها با گنجاندن Priority یا Router ID در پیام های Hello و ارسال آن به یکدیگر، سعی می‌کنند نقش DR را بر عهده بگیرند. اما در نهایت روترها با مقایسه پارامتر پیام‌های رسیده، اقدام به انتخاب روترهای DR/BDR می‌نمایند. توجه داشته باشید که تبادل پیام های Update پس از برقراری رابطه مجاورت و مشخص شدن روترهای همسایه انجام می‌پذیرد.

پس از مشخص شدن نقش DR/BDR، روترهای شبکه فقط اقدام به برقراری رابطه مجاورت با آنها نموده و از این پس پیام‌های Update خود را در قالب Multicast و آدرس 224.0.0.6 به روترهای DR/BDR ارسال می‌نمایند. روتر DR نیز پس از دریافت پیام Update، آنرا در قالب Multicast و آدرس 224.0.0.5 به اطلاع سایر روترهای موجود در شبکه می‌رساند. روتر BDR نیز همواره از تمام اطلاعات روتر DR با خبر بوده و به محض از دسترس خارج شدن آن، نقش DR را بر عهده می‌گیرد.

انواع شبکه در OSPF

روترهای پروتکلOSPF برای برقراری رابطه مجاورت در شبکه‌های مختلف، دارای عملکردی متفاوت می‌باشد. لذا پروتکلOSPF، شبکه‌ها را به گروه‌های مختلفی تقسیم‌بندی می‌نماید.

۱- **Point-to-Point**

منظور از شبکه Point-to-Point، شبکه ای متشکل از اتصال یک جفت روتر با یکدیگر می‌باشد.

اتصال سریال یک نوع شبکه Point-to-Point می‌باشد.

۲- **Broadcast**

منظور از شبکه Broadcast، شبکه‌هایی هستند که در آنها بیش از دو روتر توسط توپولوژی های Full Mesh یا Partial Mesh به یکدیگر متصل شده و قابلیت استفاده از پیام‌های Broadcast را نیز داشته باشند. از جمله شبکه‌های Broadcast می‌توان از شبکه‌های Ethernet نام برد.

انتخاب روترهای DR و BDR در این نوع شبکه ها ضروری می‌باشد. روترهای موجود در شبکه Broadcast، به جای برقراری رابطه مجاورت با یکدیگر، فقط اقدام به برقراری رابطه مجاورت با روترهای DR و BDR می‌نمایند.

روترها در این نوع شبکه، برای ارسال پیام های Hello علاوه بر Multicast از ظرفیت های ارسال پیام بصورت Broadcast نیز بهره می‌برند.

۳- **Non-Broadcast**

شبکه Non-Broadcast، به شبکه‌هایی اطلاق می‌شود که دارای بیش از دو روتر در شبکه می‌باشند ولی قابلیت امکان استفاده از ظرفیت‌های پیام Broadcast را ندارند. در این نوع شبکه‌ها برقراری رابطه مجاورت بر اساس پیام های Hello انجام می پذیرد ولی به دلیل عدم امکان استفاده از پیام های Broadcast، پیکربندی بیشتری نسبت به حالت قبل برای کشف روترهای همسایه مورد نیاز می‌باشد.

پروتکل OSPF در شبکه‌های Non-Broadcast بطور معمول از پیام های Multicast برای رابطه با روترهای همسایه استفاده می‌نماید.

انتخاب روترهای DR و BDR در این نوع شبکه ضروری است. پروتکل OSPF بر روی شبکه‌های Non-Broadcast در یکی از دو حالت Point-to-Multipoint یا Non-Broadcast Multi Access اجرا می‌گردد.

شبکه X.25 PDN ، مثالی از شبکه های Non-Broadcast می‌باشد.

۴- **Point-to-Multipoint**

حالت Point-to-Multipoint، رفتار شبکه Non-Broadcast را بر روی شبکه‌ای متشکل از مجموعه‌ای از لینک‌های Point-to-Point، اجرا می‌نماید.

۵- **Non-Broadcast Multi Access**

حالتNBMA، عملکرد پروتکلOSPF در شبکه Broadcast را شبیه‌سازی می‌نماید.

مقایسه شبکه های فوق را می توانید در جدول زیر ملاحظه نمایید:

نوع شبکه	نیاز به انتخاب روتر DR/BDR ؟	زمان سنج پیش فرض ارسال Hello	نیاز به مشخص شدن Neighbor ؟	اجازه داشتن بیش از ۲ روتر در یک زیر شبکه؟
Point-to-Point	خیر	10	خیر	خیر
Broadcast	بله	10	خیر	بله
NBMA	بله	30	بله	بله
Point-to-Multipoint	خیر	30	خیر	بله
Non-Broadcast Multi Access	خیر	30	بله	بله

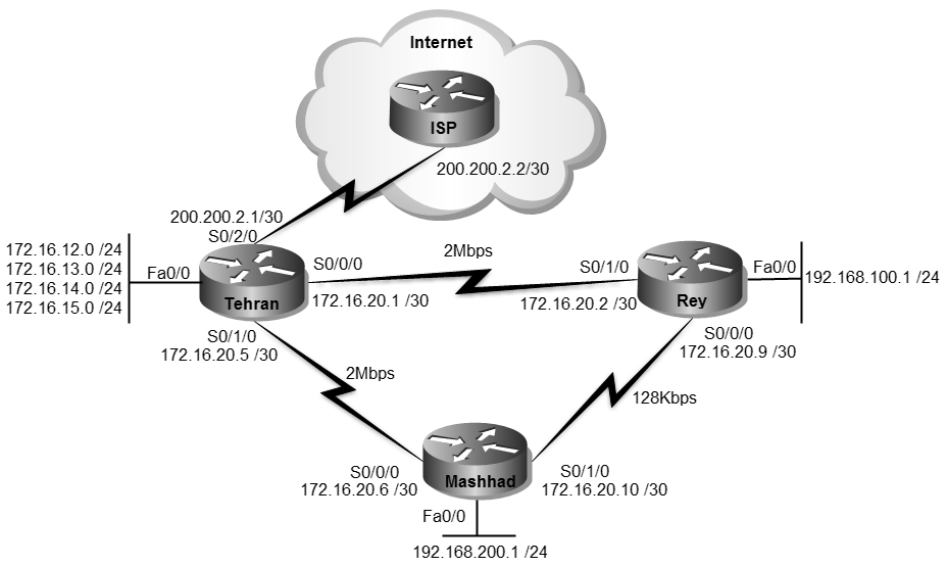
سناریو شماره(۱۳)؛ راه اندازی OSPF

طرح مسئله:

می‌خواهیم عملیات مسیریابی را برای شبکه شرکت MTR Electronic، بر اساس پروتکل OSPF انجام می‌دهیم.

نیاز سنجی:

تجهیزات سخت افزاری دیگری برای راه اندازی پروتکل مسیریابی OSPF بر روی شبکه مورد نیاز نمی‌باشد.



راه حل:

با توجه به کوچک بودن شبکه، راه اندازی پروتکلOSPF را در قالب یک ناحیه (Area 0) انجام می‌دهیم. هر چند که با وجود یک ناحیه، نیازی به پیکربندی روتر ABR نخواهیم داشت، ولی روتر تهران به دلیل ارتباط با اینترنت باید نقش ASBR را بر عهده بگیرد.

اگر از روترهای سناریوی قبل استفاده می‌کنید، در قدم اول باید پروتکل EIGRP را بر روی روترها غیرفعال کنید.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#no router eigrp 110
Tehran(config)#no ip default-network 200.200.2.0
Tehran(config)#no ip route 0.0.0.0 0.0.0.0 200.200.2.2
Tehran(config)#^Z
Tehran#
```

```
Rey(config)#no router eigrp 110
```

```
Mashhad(config)#no router eigrp 110
```

برای راه اندازی پروتکل OSPF بر روی روترها دستورات زیر را وارد می‌نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router ospf 110
Tehran(config-router)#network 172.16.12.0 0.0.3.255 area 0
Tehran(config-router)#network 172.16.20.0 0.0.0.3 area 0
Tehran(config-router)#network 172.16.20.4 0.0.0.3 area 0
Tehran(config-router)#^Z
Tehran#write
Tehran#
```

با اعمال دستور router ospf، پروتکلOSPF را بر روی روتر فعال می‌کنیم. عدد 110 نیز مشخص کننده شماره Process ID مربوط به پروتکل OSPF می‌باشد. توجه داشته باشید که Process ID در پروتکل OSPF را با AS در پروتکل EIGRP اشتباه نگیرید! شناسه Process ID فقط در همان روتر مورد بررسی قرار گرفته و تفاوت آن در روترهای مختلف هیچ خللی در عملکرد پروتکل OSPF در یک شبکه وارد نمی‌کند.

در پروتکلOSPF، برقراری رابطه مجاورت بر اساس Area اختصاص داده شده در دستور network انجام می پذیرد.

همانطور که می دانید توسط دستور Passive-interface، می توان از ارسال و دریافت پیام های مربوط به پروتکل مسیریابی توسط اینترفیس‌های مورد نظر جلوگیری نمود. معمولا این دستور برای اینترفیس‌هایی به کار برده می‌شود که علیرغم معرفی برای تبلیغ در پروتکل مسیریابی، نیازی به مشارکت آنها در ارسال و دریافت پیام‌های پروتکل مسیریابی نمی‌باشد.

```
Tehran(config-router)#passive-interface fastEthernet 0/0.2
Tehran(config-router)#passive-interface fastEthernet 0/0.3
Tehran(config-router)#passive-interface fastEthernet 0/0.4
```

```
Tehran(config-router)#passive-interface fastEthernet 0/0.5
```

```
Rey>enable
Rey#configure terminal
Rey(config)#router ospf 110
Rey(config-router)#network 192.168.100.0 0.0.0.255 area 0
Rey(config-router)#network 172.16.20.0 0.0.0.3 area 0
Rey(config-router)#network 172.16.20.8 0.0.0.3 area 0
Rey(config-router)#^Z
Rey#
```

استفاده از Wildcard Mask در دستور Network برای معرفی زیر شبکه‌ها به OSPF ضروری می‌باشد. همچنین به ازاء هر دستور Network باید Area مورد نظر جهت تبلیغ شبکه را نیز مشخص نماییم.

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#router ospf 110
Mashhad(config-router)#network 192.168.200.0 0.0.0.255 area 0
Mashhad(config-router)#network 172.16.20.4 0.0.0.3 area 0
Mashhad(config-router)#network 172.16.20.8 0.0.0.3 area 0
Mashhad(config-router)#^Z
Mashhad#write
```

پس از اعمال دستورات فوق، شبکه های تهران، شهرری و مشهد از طریق هر سه روتر قابل دسترس می‌باشند. اما دسترسی به اینترنت هنوز امکان پذیر نیست.

برای برقراری ارتباط با اینترنت، روتر تهران که متصدی برقراری ارتباط با خارج از شبکه می باشد باید نقش روتر ASBR را بر عهده بگیرد.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router ospf 110
Tehran(config-router)#default-information originate
Tehran(config-router)#exit
Tehran(config)#ip route 0.0.0.0 0.0.0.0 200.200.2.2
Tehran(config)#^Z
Tehran#write
```

دستور default-information originate، مشخص می‌نماید که این روتر می‌تواند Default Route را توسط پروتکل مسیریابی به دیگر روترهای شبکه تبلیغ نماید.

با دستور ip route 0.0.0.0 0.0.0.0 200.200.2.2، روتر تمام شبکه‌های ناشناخته را به آدرس 200.200.2.2 ارسال می‌کند.

پس از اعمال دستور فوق، خروجی show ip route بر روی روترهای شهرری و مشهد بصورت زیر خواهد بود.

```
Rey#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.20.1 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O       172.16.12.0/24 [110/51] via 172.16.20.1, 00:11:50, Serial0/1/0
O       172.16.13.0/24 [110/51] via 172.16.20.1, 00:11:50, Serial0/1/0
O       172.16.14.0/24 [110/51] via 172.16.20.1, 00:11:50, Serial0/1/0
O       172.16.15.0/24 [110/51] via 172.16.20.1, 00:11:50, Serial0/1/0
C       172.16.20.0/30 is directly connected, Serial0/1/0
O       172.16.20.4/30 [110/100] via 172.16.20.1, 00:11:50, Serial0/1/0
C       172.16.20.8/30 is directly connected, Serial0/0/0
C    192.168.100.0/24 is directly connected, FastEthernet0/0
O    192.168.200.0/24 [110/101] via 172.16.20.1, 00:01:27, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.1, 00:11:50, Serial0/1/0
Rey#
```

```
Mashhad#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.20.5 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O       172.16.12.0/24 [110/51] via 172.16.20.5, 00:12:52, Serial0/0/0
O       172.16.13.0/24 [110/51] via 172.16.20.5, 00:12:52, Serial0/0/0
O       172.16.14.0/24 [110/51] via 172.16.20.5, 00:12:52, Serial0/0/0
O       172.16.15.0/24 [110/51] via 172.16.20.5, 00:12:52, Serial0/0/0
O       172.16.20.0/30 [110/100] via 172.16.20.5, 00:12:52, Serial0/0/0
C       172.16.20.4/30 is directly connected, Serial0/0/0
C       172.16.20.8/30 is directly connected, Serial0/1/0
O    192.168.100.0/24 [110/101] via 172.16.20.5, 00:03:13, Serial0/0/0
C    192.168.200.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.5, 00:12:52, Serial0/0/0
Mashhad#
```

همانطور که ملاحظه می‌کنید Gateway of last resort روترها، اینترفیس متصل به روتر تهران را نشان می‌دهند.

مسیرهای به دست آمده توسط پروتکل OSPF نیز با درج حرف O در ابتدای هر مسیر مشخص شده است. مسیر Default Route به دست آمده از طریق این پروتکل نیز با درج عبارت O*E2 مشخص گردیده است. در این عبارت، حرف E به معنای External Route در جدول مسیریابی درج گردیده است.

طریقه عملکرد:

با توجه به اینکه در این سناریو شبکه ما دارای تعداد کمی روتر می باشد، پروتکل OSPF را فقط با ناحیه Backbone یا همان Area 0 پیکربندی می‌نماییم.

روتر تهران به شبکه خارجی متصل بوده و وظیفه برقراری ارتباط شبکه با اینترنت را بر عهده دارد. لذا نقش ASBR به این روتر تعلق گرفته و با ارسال یک Default Route، ارتباط تنها Area موجود را با محیط خارج برقرار می‌نماید.

```
Tehran#show ip ospf database
        OSPF Router with ID (200.200.2.1) (Process ID 110)

            Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
200.200.2.1     200.200.2.1     1404        0x8000000a 0x00a7cd 8
192.168.200.1   192.168.200.1   1404        0x80000006 0x00e3f4 5
192.168.100.1   192.168.100.1   1394        0x80000006 0x00dbce 5

            Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         200.200.2.1     1414        0x80000001 0x00b38a 1
Tehran#
```

همچنین شما می توانید توسط دستور زیر از وجود روترهای ABR و ASBR در داخل شبکه مطلع گردید.

```
Mashhad#show ip ospf border-routers
OSPF Process 110 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 200.200.2.1 [50] via 172.16.20.5, Serial0/0/0, ASBR, Area 0, SPF 50
Mashhad#
```

همانطور که در خروجی فوق ملاحظه می نمایید، روتر تهران به دلیل داشتن یک اینترفیس در شبکه خارجی، به عنوان روتر ASBR در شبکه شناخته شده و وظیفه ارتباط با اینترنت را نیز بر عهده گرفته است.

با توجه به نحوه اتصال روترها به یکدیگر، شبکه ما از نظر OSPF یک شبکه Point-to-Point می‌باشد. در این نوع شبکه نیازی به مشخص کردن روترهای DR/BDR نمی‌باشد. همچنین با توجه به اینکه روترها توسط لینک Point-to-Point به یکدیگر متصل شده‌اند، نیازی به مشخص نمودن روترهای همسایه بصورت دستی نیز نمی‌باشد. هر روتر با روترهای همسایه خود که دارای Area ID یکسان بر روی اینترفیس‌های متصل به هم باشند، رابطه مجاورت برقرار کرده و آنرا به عنوان همسایه خود در جدول Neighbor Table ثبت می‌نماید.

پس از مشخص شدن روترهای همسایه و درج آنها در جدول Neighbor Table، روترها اقدام به تبادل پیام های DBD با یکدیگر می‌نمایند. این پیام ها جهت هماهنگ سازی جداول توپولوژی یا LSDB تمام روترهای همسایه، ارسال و دریافت می‌گردند.

پس از دریافت پیام‌های DBD، روترها محتویات پیام را با جدول LSDB خود مقایسه کرده و طی ارسال پیام LSR، نیازهای اطلاعاتی خود را جهت تکمیل جدول LSDB به اطلاع روتر همسایه می‌رساند. پس از هماهنگ شدن جدول LSDB روتر با جدول LSDB روتر همسایه، وضعیت آن روتر در جدول Neighbor Table در حالت Full قرار می گیرد.

```
Tehran#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.1     0   FULL/  -         00:00:39    172.16.20.2     Serial0/0/0
192.168.200.1     0   FULL/  -         00:00:30    172.16.20.6     Serial0/1/0
Tehran#
```

روترها توسط پیام هایLSA، محتویات جدول LSDB مربوط به Area مورد نظر را در اختیار یکدیگر قرار می‌دهند. پس از تبادل اطلاعات روترها با یکدیگر، پروتکل OSPF بر روی هر روتر بصورت مستقل اقدام به راه اندازی الگوریتم Dijkstra نموده تا توپولوژی، مسیرها و Cost آنها را از دیدگاه خود روتر نسبت به شبکه مشخص نموده و در جدول LSDB ذخیره نماید.

پس از تکمیل جدولLSDB پروتکلOSPF مقایسهMetric یا Cost مسیرهای موجود به یک مقصد مشخص را شروع کرده و مسیرهای با Metric بهتر را در جدول مسیریابی روتر درج می‌نماید. در صورتیکه مسیرهایی با Metric برابر به یک مقصد مشخص در جدول LSDB وجود داشته باشد، پروتکلOSPF جهت Load Balancing تمام آنها را در جدول مسیریابی ثبت می‌کند. تعداد این مسیرها بصورت پیش فرض ۴ عدد است اما می‌توان آن را تا ۶ مسیر افزایش داد.

به عنوان مثال اگر به خروجی دستور show ip route بر روی روتر مشهد و شهرری توجه نمایید، می‌بینید که علیرغم وجود یک لینک مستقیم بین شهرری و مشهد، مسیر ارتباطی این دو شبکه با یکدیگر از روتر تهران می گذرد. این اتفاق به دلیل بالاتر بودن Cost لینک مستقیم نسبت به مسیر جایگزین می‌باشد.

```
Rey#show ip route

<... Output Omitted...>

Gateway of last resort is 172.16.20.1 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.12.0/24 [110/51] via 172.16.20.1, 00:22:16, Serial0/1/0
O      172.16.13.0/24 [110/51] via 172.16.20.1, 00:22:16, Serial0/1/0
O      172.16.14.0/24 [110/51] via 172.16.20.1, 00:22:16, Serial0/1/0
O      172.16.15.0/24 [110/51] via 172.16.20.1, 00:22:16, Serial0/1/0
C      172.16.20.0/30 is directly connected, Serial0/1/0
O      172.16.20.4/30 [110/100] via 172.16.20.1, 00:22:16, Serial0/1/0
C      172.16.20.8/30 is directly connected, Serial0/0/0
C   192.168.100.0/24 is directly connected, FastEthernet0/0
O   192.168.200.0/24 [110/101] via 172.16.20.1, 00:11:53, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.1, 00:22:16, Serial0/1/0
Rey#
```

طبق خروجی فوق، مجموع Cost لینک Rey-Tehran-Mashhad عدد 101 شده است. (این عدد همان 100 می باشد که روتر یک عدد به آن اضافه نموده است.)

همانطور که قبلا گفته بودیم، پروتکل OSPF فقط امکان Load Balancing بر روی مسیرهای با Metric برابر را دارد. ولی ما می توانیم با تغییر دستی Cost لینک Rey-Mashhad، امکان Load Balancing روی لینک های Unequal را در پروتکل OSPF نیز فراهم نماییم.

هر چند که من تغییر دستی Cost در پروتکل مسیریابی را توصیه نمی‌کنم! اما می توانید این کار را بصورت زیر انجام دهید:

```
Rey>enable
Rey#configure terminal
Rey(config)#interface serial 0/0/0
Rey(config-if)#ip ospf cost 100
Rey(config-if)#^Z
```

پس از اعمال دستور فوق، خروجی show ip route به شکل زیر در خواهد آمد:

```
Rey#show ip route
<... Output Omitted...>

Gateway of last resort is 172.16.20.1 to network 0.0.0.0
```

```
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O     172.16.12.0/24 [110/51] via 172.16.20.1, 00:32:17, Serial0/1/0
O     172.16.13.0/24 [110/51] via 172.16.20.1, 00:32:17, Serial0/1/0
O     172.16.14.0/24 [110/51] via 172.16.20.1, 00:32:17, Serial0/1/0
O     172.16.15.0/24 [110/51] via 172.16.20.1, 00:32:17, Serial0/1/0
C     172.16.20.0/30 is directly connected, Serial0/1/0
O     172.16.20.4/30 [110/100] via 172.16.20.1, 00:32:17, Serial0/1/0
C     172.16.20.8/30 is directly connected, Serial0/0/0
C   192.168.100.0/24 is directly connected, FastEthernet0/0
O   192.168.200.0/24 [110/101] via 172.16.20.10, 00:02:12, Serial0/0/0
                     [110/101] via 172.16.20.1, 00:02:12, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.16.20.1, 00:32:17, Serial0/1/0
Rey#
```

به دلیل اینکه مسیرهای به دست آمده توسط پروتکلOSPF می‌باشد، مقدار AD آنها با یکدیگر برابر می‌باشد. همچنین با تغییر دستی Cost مربوط به لینک مستقیم شهرری و مشهد، مقدار Metricمسیرها نیز با هم برابر شده و در نهایت هر دو مسیر در جدول مسیریابی قرار گرفته‌اند.

برای بررسی صحت عملکرد Load Balancing می‌توانیم از دستور traceroute استفاده نماییم:

```
Rey#traceroute 192.168.200.1
Type escape sequence to abort.
Tracing the route to 192.168.200.1

 1  172.16.20.10   20 msec   4 msec   8 msec

Rey#traceroute 192.168.200.1
Type escape sequence to abort.
Tracing the route to 192.168.200.1

 1  172.16.20.1    8 msec   8 msec   6 msec
Rey#
```

مرجع دستور Command Reference:

Enable OSPF		
Step	**Command**	**Purpose**
1	**router ospf** *process-id*	Enable OSPF routing, which places you in router configuration mode.
2	**network** *address wildcard-mask* **area** *area-id*	Define an interface on which OSPF runs and define the area ID for that interface.

Configure OSPF Interface Parameters	
Command	**Purpose**
ip ospf cost *cost*	Explicitly specify the cost of sending a packet on an OSPF interface.
ip ospf retransmit-interval *seconds*	Specify the number of seconds between link state advertisement retransmissions for adjacencies belonging to an OSPF interface.
ip ospf transmit-delay *seconds*	Set the estimated number of seconds it takes to transmit a link state update packet on an OSPF interface.
ip ospf priority *number*	Set priority to help determine the OSPF designated router for a network.
ip ospf hello-interval *seconds*	Specify the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.
ip ospf dead-interval *seconds*	Set the number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPF router down.
ip ospf authentication-key *key*	Assign a password to be used by neighboring OSPF routers on a network segment that is using OSPF's simple password authentication.
ip ospf message-digest-key *keyid* **md5** *key*	Enable OSPF MD5 authentication.
ip ospf authentication[**message-digest** | **null]**	Specifies the authentication type for an interface.

Configure OSPF Network Type	
Command	**Purpose**
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] }**}** *Example:* Router(config-if)#ip ospf network point-to-point	Configure the OSPF network type for a specified interface.

Generate a Default Route	
Command	**Purpose**
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]	Force the autonomous system boundary router to generate a default route into the OSPF routing domain.

Control Default Metrics	
Command	**Purpose**
ospf auto-cost reference-bandwidth *ref-bw*	Differentiate high bandwidth links.

Monitor and Maintain OSPF	
Command	**Purpose**
show ip ospf [process-id]	Display general information about OSPF routing processes.
show ip ospf [process-id area-id] database **show ip ospf** [process-id area-id] database [router] [link-state-id] **show ip ospf** [process-id area-id] database [router] [self-originate] **show ip ospf** [process-id area-id] database [router] [adv-router [ip-address]] **show ip ospf** [process-id area-id] database [network] [link-state-id] **show ip ospf** [process-id area-id] database [summary] [link-state-id] **show ip ospf** [process-id area-id] database [asbr-summary] [link-state-id] **show ip ospf** [process-id] database [external] [link-state-id] **show ip ospf** [process-id area-id] database [database-summary]	Display lists of information related to the OSPF database.
show ip ospf border-routers	Display the internal OSPF routing table entries to Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).
show ip ospf interface [interface-name]	Display OSPF-related interface information.
show ip ospf neighbor [interface-name] [neighbor-id] detail	Display OSPF-neighbor information on a per-interface basis.
show ip ospf request-list [nbr] [intf] [intf-nbr]	Display a list of all LSAs requested by a router.
show ip ospf retransmission-list [nbr] [intf] [intf-nbr]	Display a list of all LSAs waiting to be retransmitted.
show ip ospf virtual-links	Display OSPF-related virtual links information.

☑ مبحث پنجم

پروتکل BGP

کسانی که پایه اینترنت را بنا نهادند، هیچ گاه تصور نمی‌کردند روزی برسد که این شبکه دنیا را به تسخیر خود در آورده و به چنین گستردگی برسد.

گسترش شبکه اینترنت به‌حدی است که بقای بسیاری از بنگاه‌های تجاری به در دسترس بودن شبکه اینترنت وابسته شده است. از طرفی گستردگی و پراکندگی این شبکه نیاز به یک مسیریابی دقیق و پیچیده را بوجود آورده است.

شبکه اینترنت مجموعه‌ای از ASهای بهم پیوسته است که هر کدام از آنها دارای سیاست‌های مسیریابی مستقل به خود می‌باشد. برای بوجود آوردن یک شبکه یکپارچه به نام اینترنت، نیاز به پروتکلی برای مسیریابی بین ASهای مختلف می‌باشد. این وظیفه را پروتکلی به نام (Border Gateway Protocol)BGP در محیط اینترنت انجام می‌دهد.

پروتکلBGP تا کنون در ۴ نسخه مختلف منتشر گردیده است. نسخه نهایی و مورد استفاده این پروتکل BGP v4 می‌باشد که طی استاندارد RFC 4271 منتشر گردیده است. نسخه‌های قبلی این پروتکل به علت اشکالاتی از جمله Classful بودن، دوام چندانی نداشته و خیلی زود نسخه چهار این پروتکل به عمومیت رسید.

به دلیل مسیریابی بین ASهای مختلف، پروتکل BGP در گروه پروتکل‌های (Exterior Gateway Protocol)EGP دسته‌بندی می‌شود. پروتکل‌هایی نظیر RIP، EIGRP و OSPF که وظیفه مسیریابی درون ASها را بر عهده دارند، عضو گروه (Interior Gateway Protocol) IGP بوده و پروتکلBGP تنها پروتکل مسیریابی موجود در گروه EGP می‌باشد. هرچند که این پروتکل امکان انجام عملیات مسیریابی برای ASها را هم به صورت داخلی (IBGP) و هم بصورت خارجی (EBGP) نیز فراهم می‌نماید.

مقدار پیش فرض اختصاص داده شده به AD مسیرهای IBGP برابر 200 و AD مسیرهای به دست آمده از طریق EBGP برابر 20 می‌باشد.

پروتکل BGP تنها پروتکل مسیریابی می باشد که امکان استفاده از پروتکلTCP برای تبادل اطلاعات مربوط به مسیریابی را دارد. به دلیل استفاده از پروتکلTCP، تبادل اطلاعات بصورت قابل اطمینان انجام می‌گیرد. همانطور که می دانید پروتکل TCP دارای مکانیسم اطمینان از صحت

عملکرد خود بوده و فارغ از نوع پروتکل استفاده کننده، وظیفه خود را جهت تبادل قابل اطمینان اطلاعات انجام می‌دهد. به همین دلیل پروتکل BGP بر خلاف پروتکل‌های EIGRP و OSPF نیازی به مکانیسم مستقل جهت تایید صحت تبادل اطلاعات، نخواهد داشت.

استفاده از پروتکلTCP در کنار مزیت‌هایی که دارد، محدودیت‌هایی را نیز برای یک پروتکل مسیریابی به وجود می‌آورد. پروتکلBGP به علت استفاده ازTCP، امکان بهره برداری از پیام‌های Broadcast و Multicast را ندارد. به همین دلیل امکان کشف اتوماتیک روترهای همسایه وجود نداشته و حتما باید آدرس Neighbor بصورت دستی در این پروتکل پیکربندی گردد.

پروتکل BGP از منظر محاسبهMetric در گروه پروتکلPath-vector قرار می گیرد. پروتکل Path-vector عملکردی شبیه به پروتکل Distance-vector دارد. با این تفاوت که پروتکل Distance-vector برای مسیریابی درون ASها و پروتکلPath-vector برای مسیریابی بین ASها کاربرد دارد. همچنین پروتکلPath-vector برای محاسبه Metric، از پارامترهایی به نام Attribute نیز استفاده می‌نماید.

عملکرد پروتکلBGP بصورت Classless بوده و امکان گنجاندن Subnet Mask در پیام های خود را دارد. به همین دلیل امکان استفاده از ویژگی های VLSM و CIDR در این پروتکل فراهم گردیده است.

نحوه تخصیص شماره AS

همانطور که قبلا گفتیم، سیستم خود مختار(Autonomous System)، به گروهی از روترها گفته می‌شود که تحت یک حوزه مدیریتی و در حال اجرای یک پروتکل مسیریابی مشترک می‌باشند.

سازمانIANA طبق استانداردRFC 1930 اقدام به تخصیص شمارهAS ID به شبکه‌های موجود در سرتاسر اینترنت می‌نماید. این شناسه ها باید همانند آدرس IP، بصورت یکتا بر روی اینترنت موجود باشند.

رنج شناسه AS، اولین بار بصورت یک عدد ۱۶ بیتی منتشر شد که از عدد 1 شروع شده و به عدد 65535 خاتمه می‌یافت. اما پس از آنکه سازمان IANA متوجه شد که این عدد ۱۶ بیتی کفاف اختصاص ID به تمام ASها را نخواهد داد، در گام دوم اقدام به گسترش آن به صورت یک عدد ۳۲ بیتی نمود. سازمان IANA رنج 1 تا 65535 را برای همان عدد ۱۶ بیتی کنار گذاشته و از مابقی این آدرس ها (65536 - 4294967295) برای اختصاص به سایر AS ها استفاده نمود.

بطور مثالID اختصاص داده شده به سیسکوAS109 وID اختصاص داده شده به شرکت مایکروسافت AS3598 می‌باشد.

همچنین سازمان IANA رنج شناسه 64512 الی 65534 را همانند آدرس های IP Private، برای استفاده های شخصی مشخص نموده است.

لیست کامل AS IDهای اختصاص داده شده توسط IANA را می‌توانید در آدرس‌های زیر مشاهده نمایید:

http://www.iana.org/assignments/as-numbers/as-numbers.xml
http://bgp.potaroo.net/cidr/autnums.html

انواع عملکرد پروتکل BGP

پروتکلBGP از منظر نحوه برقراری ارتباط با روتر همسایه به دو کلاسIBGP وEBGP تقسیم بندی می‌گردد.

- **Internal BGP**

در این حالت پروتکلBGP بصورت داخلی و برای مسیریابی درون AS مورد استفاده قرار می‌گیرد. زمانی که هر دو روتری که قصد برقراری رابطه مجاورت با یکدیگر را دارند در یک AS قرار گرفته باشند، پروتکل BGP در کلاس IBGP عمل می‌نماید.

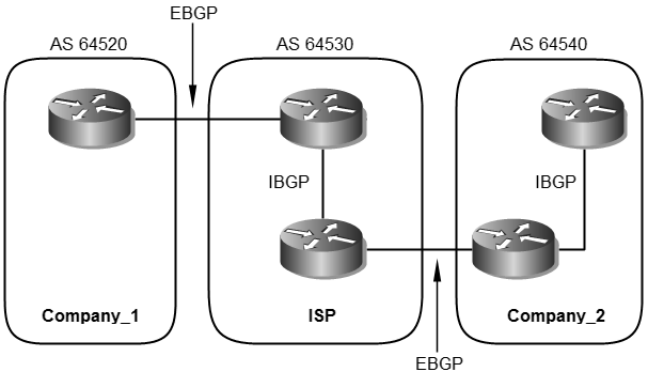
روترهایی که در کلاس IBGP عمل می‌نمایند، برای برقراری رابطه مجاورت نیازی به برقراری اتصال مستقیم با یکدیگر ندارند. در این حالت صرفا در دسترس بودن روتر همسایه توسط جدول مسیریابی، جهت برقراری رابطه مجاورت کفایت می کند.

- **External BGP**

اگر رابطه مجاورت بین روترهایی برقرار شود که در ASهای متفاوتی قرار دارند، پروتکلBGP در کلاسEBGP عمل می‌نماید. در این حالت پروتکل BGP برای مسیریابی بین ASهای مختلف مورد استفاده قرار می گیرد.

برای برقراری رابطه مجاورت در حالت EBGP، روترها حتما باید دارای لینک مستقیم با یکدیگر باشند.

در تصویر زیر روترهای BGP در هر دو حالت IBGP و EBGP نمایش داده شده است.



انواع پیام‌های BGP

پروتکلBGP برای انجام عملیات مسیریابی خود از چهار نوع پیام استفاده می‌نماید. این پیام‌ها توسط پروتکلTCP و پورت 179 بصورت قابل اطمینان ارسال می‌گردند.

- **Open**

اولین پیامی که پس از برقراری یک اتصالTCP بین روترها تبادل می‌گردد، پیام Open می‌باشد. اگر پیام Open توسط روتر مقابل پذیرفته شود یک پیام Keepalive در جهت تایید دریافت پیام Open ارسال می‌نماید.

از جمله فیلدهای موجود در پیام Open می توان به Version، AS و Hold Time اشاره نمود.

- **Update**

از پیام های Update برای انتقال اطلاعات مسیریابی بین روترهای همسایه درBGP استفاده می‌شود. از اطلاعات موجود در پیام های Update می توان برای ساخت یک گراف که توصیف کننده روابط بین ASهای مختلف می‌باشد، استفاده نمود. با این کار پروتکل BGP ایجاد حلقه یا بعضی رفتارهای ناهنجار که ممکن است در مسیریابی بین ASها بوجود بیاید را تشخیص داده و از شبکه حذف می‌نماید.

- **Keepalive**

مکانیسم مورد استفاده پروتکلBGP برای بررسی در دسترس بودن روترهای همسایه، استفاده از پیام های Keepalive می باشد.

این پیام بصورت متناوب هر ۶۰ ثانیه یکبار به روترهای همسایه ارسال می گردد تا در دسترس بودن خود را به اطلاع آنها برساند. پیام Keepalive از انقضای زمان سنج Hold-time، جلوگیری به عمل می‌آورد.

- **Notification**

پیام Notification پس از تشخیص یک وضعیت خطا (Error) ارسال می‌گردد. اتصال BGP بلافاصله پس از دریافت این پیام بسته می‌شود.

فیلدهای این پیام شامل Error Code، Error Subcode و Data می‌باشد.

اصطلاحات روترها در BGP

- **BGP Speaker**

اصطلاح BGP Speaker به روتری اطلاق می شود که پروتکل BGP بر روی آن راه اندازی گردیده است.

- **BGP Peer**

بر خلاف سایر پروتکل‌های مسیریابی، پروتکل BGP امکان کشف خودکار روترهای همسایه را ندارد. به همین دلیل باید روترهای همسایه بصورت دستی برای روتر Speaker معرفی گردند. به روترهایی که جهت برقراری رابطه مجاورت به روتر Speaker معرفی شده‌اند، BGP Peer گفته می‌شود.

روترها به دو صورت داخلی(IBGP) و خارجی (EBGP) اقدام به برقراری رابطه مجاورت با یکدیگر می نمایند.

روترهای همسایه داخلی که در یک AS قرار دارند، نیازی به اتصال مستقیم با یکدیگر ندارند. ولی روترهای همسایه خارجی که دارای AS متفاوت می‌باشند، برای برقراری رابطه مجاورت باید حتما دارای اتصال مستقیم با یکدیگر باشند.

در برخی مستندات فنی از اصطلاح BGP Neighbor هم برای BGP Peer استفاده می‌شود.

- **BGP Peer-Group**

یک Peer-Group شامل دو یا چند روترBGP Peer می باشد که دارای سیاست‌های مشترکی در بروز رسانی اطلاعات می‌باشند.

- **BGP Session**

هنگامی که دو روتر Speaker به عنوان Peer به یکدیگر معرفی می‌شوند، برای تبادل اطلاعات مسیریابی با یکدیگر اقدام به برقراری BGP Session می‌نمایند.

روترها برای برقراری BGP Session از پروتکل TCP و پورت 179 استفاده می‌نمایند.

- **BGP Route**

یک BGP Route از دو قسمت تشکیل شده است: Prefix و Path-Attributes.

البته در بیشتر مواقع از اصطلاح Path به جای BGP Route در مستندات فنی استفاده می‌شود. ولی از لحاظ فنی، Path فقط یکی از دو قسمت تشکیل دهنده BGP Route می‌باشد.

انواع وضعیت روتر در BGP

روترهای BGP برای برقراری رابطه مجاورت با روتر همسایه، مراحل زیر را طی می نمایند. اگر همه چیز خوب پیش برود، در نهایت وضعیت روترهای همسایه در حالت Established قرار گرفته و می توانند اقدام به تبادل پیام های Update با یکدیگر نمایند.

اما اگر برقراری رابطه مجاورت به هر دلیلی برقرار نشود، روترها مراحل زیر را بصورت دوره ای تکرار می کنند تا موفق به برقراری رابطه مجاورت با یکدیگر گردند.

- **Idle**

روتر زمانی در حالت Idle قرار می‌گیرد که روند BGP توسط administratively down متوقف شده و یا روتر در انتظار تلاش بعدی برای برقراری ارتباط است.

- **Connect**

در این حالت روتر منتظر کامل شدن برقراری اتصال TCP می‌باشد. در این حالت شما نمی‌توانید مشخص نمایید که آیا اتصال TCP می تواند کامل شود یا خیر؟

- **Active**

در این حالت اتصال TCP برقرار شده است ولی هنوز هیچ پیام BGP بین روترهای همسایه تبادل نگردیده است.

- **Opensent**

اتصال TCP برقرار شده است و پیام BGP Open به روتر همسایه ارسال گردیده است. ولی هنوز روتر همسایه اقدام به ارسال پیام Open نکرده است.

- **Openconfirm**

در این حالت هر دو روتر همسایه اقدام به ارسال و دریافت پیام BGP Open نموده‌اند. گام بعدی دریافت پیام Keepalive جهت تایید درستی پارامترهای دریافتی و یا پیام Error جهت ارسال کد خطای پیش آمده می باشد.

- **Established**

در این حالت تمام پارامترهای روتر همسایه تطبیق داده شده است. رابطه مجاورت برقرار شده و در حال حاضر روترها می توانند اقدام به تبادل پیام های Update با یکدیگر نمایند.

با استفاده از دستورهای show ip bgp summary و show ip bgp neighbor *Address* می توانید از وضعیتی که روترها در آن قرار دارند مطلع شوید.

پایگاه اطلاعات مسیریابی(RIB)

روترهایBGP Speaker برای نگهداریBGP Routeهای خود، از پایگاه اطلاعات مسیریابی RIB(Routing Information Base) استفاده می‌نمایند.

یک RIB از سه بخش زیر تشکیل شده است:

۱- **Adj-RIBs-In**

این بخش شامل اطلاعات مسیریابی می‌باشد که روتر توسط پیام‌های Update دریافتی از دیگر روترهای Speaker یاد گرفته است.

به عبارتی دیگر، این بخش شامل اطلاعات دریافتی پردازش نشده می باشد.

۲- **Loc-RIB**

این بخش شامل مسیرهایی می باشد که روتر Speaker بر اساس سیاست های محلی خود از بین مسیرهای موجود در Adj-RIBs-In انتخاب نموده است.

مسیرهای موجود در Loc-RIB توسط روتر Speaker و بصورت محلی مورد استفاده قرار می‌گیرند. همچنین مشخص نمودن Next-hop مسیرهای موجود در این بخش، بر اساس جدول Routing Table محلی روتر Speaker انجام می شود.

۳- **Adj-RIBs-Out**

این بخش شامل مسیرهایی می باشد که روترSpeaker قصد دارد آنها را در قالب پیام های Update به روترهای همسایه خود تبلیغ نماید.

Path Attributes

پروتکلBGP یک پروتکلPath Vector بوده و برای محاسبه Metric عملیات مسیریابی خود از Path Attributes استفاده می‌نماید. به عبارت دیگرPath Attributes همان Metric پروتکل مسیریابیBGP هستند.

مؤلفه های Path Attributes در یک تقسیم بندی کلی، طبق جدول زیر گروه بندی می شوند:

BGP Attributes	**Well-Known**	**Mandatory**	Origin
			AS-Path
			Next hop
		Discretionary	Local Preference
			Atomic Aggregate
	Optional	**Transitive**	Aggregator
		Non-Transitive	Multi Exit Discriminator (MED)

➢ در اولین گام، BGP Attributes به دو دسته تقسیم بندی می شوند:

- **Well-Known**

باید توسط همه اجرا کنندگان به رسمیت شناخته شود. تمامAttribute های زیر مجموعه این گروه به روترهای همسایه منتشر می‌شوند.

روترهایBGP peer پس از دریافت پیام‌هایUpdate شامل Well-Known Attributes، باید این Attributeها را در هر پیام Updateای که به روترهای همسایه ارسال می کنند، گنجانده باشند.

- **Optional**

نیازی به رسمیت شناختن توسط همه اجراکنندگان ندارد. و می‌تواند بصورت Private اجرا گردد.

هر Path می تواند علاوه برWell-Known Attributeها، شامل یک یا چند Optional Attribute نیز باشد. اما نیاز نیست و انتظار هم نمی‌رود که اجرا کنندگان BGP، از تمامOptional Attributeها پشتیبانی کنند.

➢ بخش Well-Known به دو قسمت زیر تقسیم می شود:

- **Mandatory**[1]

همانطور که از نام این گروه پیداست، استفاده ازAttributeهای زیر مجموعه گروه Mandatory، اجباری بوده و باید در تمام پیام‌های Update که حاویNLRI است، وجود داشته باشند.

---

[1] اجباری

- **Discretionary**[1]

استفاده از Attributeهای زیر مجموعه Discretionary، اختیاری می‌باشد. اما این Attribute ها نیز می‌توانند طی پیام‌های Update خاص، ارسال شوند.

➢ بخش Optional نیز به دو گروه تقسیم بندی می‌شود:

- **Transitive**

اگر روترSpeaker دریافت کننده Attributeهای زیر مجموعه این گروه، حتی متوجه اینAttribute هم نشود، بدون اعمال تغییر آنرا به روترهای همسایه خود ارسال می‌نماید.

نحوه اجرای Transitive در یکی از دو حالت زیر انجام می شود:

i. **Recognized Transitive**

اگرPath دارای این Attribute، توسط روتر پذیرفته شده و برای سایر روترها نیز ارسال گردد، در صورتی که برای Flag مربوط به این Attribute توسط ASهای قبلی، مقدار"1" تعیین شده باشد، این مقدار نباید توسط AS حاضر به "0" تغییر نماید.

ii. **Unrecognized Transitive**

اگرPath دارای اینAttribute توسط روترها پذیرفته شده و به اطلاع سایر روترهای همسایه نیز رسانده شود، در اینصورت مقدار بیتFlag مربوط به Attribute، مقدار "1" تعیین خواهد شد.

- **Non-Transitive**

اگر روترSpeaker دریافت کننده Non-Transitive Attribute، متوجه آن نشود اقدام به حذف Attribute از داخل پیام Update می‌نماید.

➢ گروه Well-Known Mandatory، شامل سه Attribute زیر می باشد.

- **Origin**

Origin Attribute توسط روترBGP Speakerای که منشا اطلاعات مسیریابی می‌باشد، تولید می‌شود. مقدار Origin توسط هیچ روتر Speaker دیگری نباید تغییر داده شود.

---

[1] احتیاطی

اگر مسیرOrigin توسط یک پروتکل مسیریابی داخلی(IGP) به دست آمده باشد با حرف " i " ، اگر توسط یک پروتکل مسیریابی خارجی(EGP) به دست آمده باشد با حرف " e " و اگر از راه های دیگری نظیر Redistribute به دست آمده باشد توسط علامت " ? " مشخص می گردد.

- **AS-Path**

از این ویژگی برای شناسایی‌ASهای مسیر انتقال اطلاعات مسیریابی، استفاده می‌شود. به عبارت دیگرAS-Path شامل لیست ASهایی می‌باشد که پیام Update در طول مسیر انتقال از آنها عبور کرده است.

روتر Speaker قبل از انتشار پیام Update دریافتی، شماره AS خود را به لیست AS-Path اضافه می‌نماید. این عمل باعث جلوگیری از به وجود آمدن چرخه در شبکه می‌گردد.

- **Next hop**

ویژگیNext hop مشخص کننده آدرسIP مربوط به روتری می‌باشد که باید به عنوان hop بعدی جهت رسیدن پیام Update به مقصد، مورد استفاده قرار گیرد.

➢ گروه Well-Known Discretionary ، شامل دو Attribute به شرح زیر می باشد.

- **Local Preference**

روترSpeaker بر اساس سیاست های پیکربندی محلی خود اقدام به محاسبه درجه اولویت برای مسیرهای خارجی به دست آمده می نماید. این Attribute در داخل پیام های Updateای گنجانده می شود که روترSpeaker به روترهای همسایه داخلی (IBGP) خود ارسال می‌نماید.

روترهای Speaker نباید اقدام به ارسال خصوصیت Local Preference به روترهای همسایه خارجی خود نماید. همچنین روترSpeaker نیز پارامتر Local Preference دریافتی از همسایه های خارجی خود را نادیده می گیرد. (البته بجز در موارد مستثنی شده در RFC3065)

هر چه مقدار Local Preference بالاتر باشد، احتمال انتخاب آن مسیر توسط روتر بیشتر می شود.

- **Atomic Aggregate**

وقتی که یک روترSpeaker دارای مجموعه‌ای از مسیرها برای تبلیغ به یک همسایه خاص می‌باشد، AS-Path آن شامل لیست بزرگی از ASهایی خواهد بود که این Updateها در طول مسیر از آنها عبور کرده‌اند.

در بسیاری از موارد مدیر شبکه می تواند تشخیص دهد که آیا با حذف قسمتی از لیست AS-Path از درون پیام Update ارسالی به یک همسایه خاص! اتفاق بدی مثل حلقه لایه سوم در شبکه اتفاق می افتد یا خیر؟

در صورتیکه مدیر شبکه به این نتیجه برسد، می تواند حذف قسمتی از لیستAS-Path را با درج Atomic Aggregate Attribute در پیام هایUpdate به اطلاع روتر همسایه خود برساند.

➢ گروه Transitive Optional Attribute، شامل یک Attribute به شرح زیر می‌باشد.

- **Aggregator**

فرآیندی است که بتوان با ترکیب ویژگی‌های چندین مسیر مختلف، آنها را فقط توسط یک مسیر تبلیغ نمود.

این تجمیع مسیرها می تواند باعث کاهش مقدار اطلاعاتی باشد که باید بین روترهای Speaker تبادل گردد.

مسیرهای دارایMED Attributeهای مختلف، نباید از این خصوصیت استفاده نمایند.

➢ گروه Non-Transitive Optional Attribute، شامل یک Attribute به شرح زیر می باشد.

- **Multi Exit Discriminator (MED)**

در صورت وجود چندین نقطه ورودی و خروجی به یک ASهمسایه، از این Attribute برای تخصیصMetric به مسیرها استفاده می‌شود. هر چه عدد اختصاص یافته به Metric کوچکتر باشد، احتمال انتخاب آن مسیر افزایش می‌یابد.

اگر پارامترMED بر رویEBGP دریافت شود، ممکن است درIBGP نیز منتشر شده و به روترهایSpeaker در همان AS ارسال گردد.

ولی اگر پارامترMED از یک روتر همسایه در همانAS دریافت شود(بصورتIBGP)، نباید به روترهای همسایه در AS های همجوار ارسال گردد.

در نهایت RFC 4271، بر اساس نوع عملکرد پروتکل BGP، الزام استفاده از Attributeها را طبق جدول زیر مشخص نموده است:

Attribute	EBGP	IBGP
Origin	Mandatory	Mandatory
AS-Path	Mandatory	Mandatory
Next hop	Mandatory	Mandatory
Local Preference	ignored (except in RFC3065)	Required
Atomic Aggregate	Discretionary	Discretionary
Aggregator	Discretionary	Discretionary
Multi exit discriminator	Discretionary	Discretionary

پارامتر Weight

علاوه بر Attributeهای مذکور، سیسکو برای پروتکل BGP یک پارامتر دیگر به نام Weight معرفی نموده است. این پارامتر مخصوص سیسکو بوده و فقط در تجهیزات سیسکو قابل دسترسی می‌باشد.

مقدار این پارامتر از رنج 0 تا $2^{16} - 1$ توسط روتر در زمان دریافت Updateها برای مسیرهای دریافتی تعیین می‌شود. پارامتر Weight فقط توسط خود روتر و بصورت محلی استفاده شده و به روترهای دیگر ارسال نمی‌گردد.

هر چه مقدار تخصیص یافته به این پارامتر بزرگ تر باشد، احتمال انتخاب آن مسیر افزایش می یابد. بصورت پیش فرض مقدار Weight برای مسیرهای به دست آمده از طریق سایر روترها عدد 0 و برای مسیرهای به دست آمده محلی عدد 32768 می‌باشد.

برای تخصیص مقدار Weight بصورت دستی به روترهای همسایه می‌توانید از دستور زیر استفاده نمایید. در اینصورت مسیرهای بدست آمده توسط آن روتر با مقدار Weight مورد نظر ذخیره می شوند.

Router(config-router)# **Neighbor** *ip-address* **weight** *value*

الگوریتم انتخاب بهترین مسیر در BGP

فرآیند تصمیم گیری انتخاب بهترین مسیر در پروتکل BGP توسط مراحل زیر انجام می‌پذیرد. البته لازم به ذکر است که این جدول برگرفته از کتاب CCNP-Route 642-902 می‌باشد و ممکن است با RFC کمی تفاوت داشته باشد.

شاید شروع مراحل با گام 0 کمی عجیب به نظر آید ولی به دلیل منطق به کار رفته در این جدول، مراحل با گام 0 شروع شده است.

در گام 0 روتر به بررسی مسیر BGP پرداخته و آدرس Next-hop آنرا با مسیرهای موجود در جدول مسیریابی مقایسه می‌نماید. اگر روتر نتواند آدرس Next-hop را با آدرس‌های جدول مسیریابی تطابق دهد، قاعدتا نخواهد توانست اطلاعات مورد نظر را به آن آدرس خاص ارسال نماید. پس BGP شروع به طی ۸ مرحله زیر برای دستیابی به بهترین مسیر برای مقصد مورد نظر خواهد نمود. فکر کنم حالا منطق شروع با گام 0 را دریافته باشید! گام 0 همان شرط شروع مراحل می‌باشد.

گام	حرف	عبارت خلاصه شده	کدام بهتر است؟
0	N	آیا Next-hop قابل دسترسی است؟	اگر هیچ مسیری برای دسترسی به Next-hop وجود ندارد، پس روتر نمی تواند از این مسیر استفاده نماید.
1	W	Weight	مقدار بزرگتر
2	L	Local-Preference	مقدار بزرگتر
3	L	Locally injected routes	اولویت مسیرهایی که بصورت محلی یاد گرفته از مسیرهای بدست آمده توسط IBGP/EBGP بهتر است.
4	A	AS-Path Length	مقدار کوچکتر
5	O	Origin	ترجیح I بر E ترجیح E بر ?
6	M	MED	مقدار کوچکتر
7	N	Neighbor Type	ترجیح EBGP بر IBGP
8	I	IGP Metric to next-hop	مقدار کوچکتر

اگر پس از مراحل فوق، همچنان توفیق انتخاب بهترین مسیر نصیب روتر نشده باشد، سه مرحله زیر را در ادامه طی خواهد نمود:

گام نهم: قدیمی ترین مسیر شناخته شده EBGP.

گام دهم: انتخاب بر اساس پایین ترین RID[1] روتر همسایه.

گام یازدهم: انتخاب براساس پایین ترین آدرس IP روتر همسایه.

[1] Router ID

انواع توپولوژی دسترسی به اینترنت

شاید شما فکر کنید که یادگیری پروتکل BGP فقط برای کارشناسانی مفید است که در ISPها کار کرده و یا قصد کار درISP دارند. اما یکی از مزیت‌های مهم BGP، استفاده از آن برای مسیریابی خارجی جهت سازمان های بزرگ است.

همانطور که گفته شد، به دلیل گستردگی اینترنت و نفوذ آن در کسب و کار بنگاه های تجاری، در دسترس بودن اینترنت برای این سازمانها امری حیاتی محسوب می‌شود. به همین دلیل سازمان ها تمایل به دریافت چند لینک اینترنت از یک ISP و یا چند لینک از چند ISP مختلف دارند.

هر چند که می توان با نوشتن یک Default Route ساده، امکان دسترسی به اینترنت را برای شبکه فراهم نمود. یا حتی در صورت داشتن چند لینک می توان از چند Default Route با Metric برابر یا متفاوت استفاده نمود. اما همیشه داشتن Default Route متضمن انتخاب بهترین مسیر به مقصد مورد نظر در اینترنت نمی‌باشد. همچنین داشتن چند Default Route با Metric برابر به اینترنت، ممکن است اثر نا مطلوبی بر روی بعضی از برنامه‌های کاربردی داشته باشد.

انتخاب نحوه دسترسی به اینترنت، یکی از تصمیمات مهم مدیر شبکه است. استفاده از Default Route در کنار مزایا ممکن است دارای معایبی نیز باشد. این امر در مورد استفاده از BGP هم صادق است. اگر پروتکل BGP به درستی پیکربندی نگردد، ممکن است شبکه شما را به شبکه Transit بین دوISP تبدیل نماید. همچنین راه اندازیBGP می‌تواند استفاده از منابع روترهای شبکه شما را تا حد قابل ملاحظه ای افزایش دهد.

این نکته را نیز فراموش نکنید: این شما نیستید که همواره باید به اینترنت دسترسی داشته باشید، بلکه در صورتی که شما سرور یا سرورهایی را روی اینترنت Publish کرده باشید، دسترسی از اینترنت به شبکه شما نیز برای ادامه کسب و کارتان، حیاتی خواهد بود. در این صورت است که استفاده از BGP، می تواند بهترین گزینه ممکن باشد.

در این قسمت به بررسی انواع مختلف اتصال یک سازمان بزرگ به اینترنت می‌پردازیم. همچنین مزایا و معایب استفاده از BGP یا Static Default Route را به ازاء هر مورد بررسی می‌کنیم.

- **یک ISP با یک لینک (Single homed)**

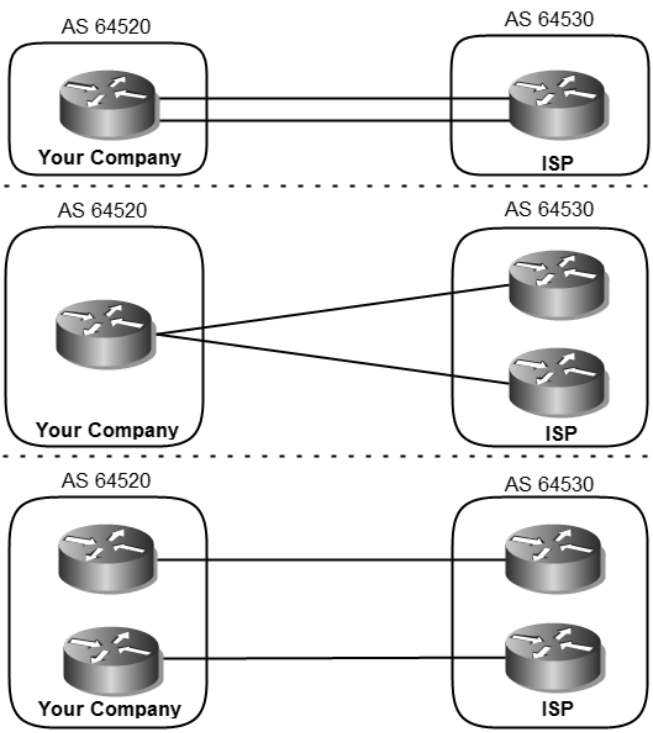
در طراحی Single Homed، شما تنها به یک لینک از یکISP نیاز خواهید داشت. با این نوع طراحی، برای دسترسی به هر مقصدی در اینترنت فقط یک راه وجود دارد. در

نتیجه مهم نیست که شما ازBGP استفاده کنید یا خیر؛ در هر حال فقط یک خروجی برای دسترسی به اینترنت برای شبکه شما وجود دارد.

اگر چه در صورت استفاده ازBGP، می توانید آنرا طوری پیکربندی نمایید که فقط Default Route را به شبکه شما ارسال نماید. ولی در این حالت استفاده از Static Default Route بهترین انتخاب خواهد بود.

- **یک ISP با دو لینک (Dual homed)**

در این حالت شبکه شما دارای دو یا چند لینک به اینترنت می‌باشد، ولی تمام لینک‌ها تنها از طریق یکISP تامین می گردد. طراحی این نوع اتصال می تواند به یکی از سه روش زیر انجام پذیرد.



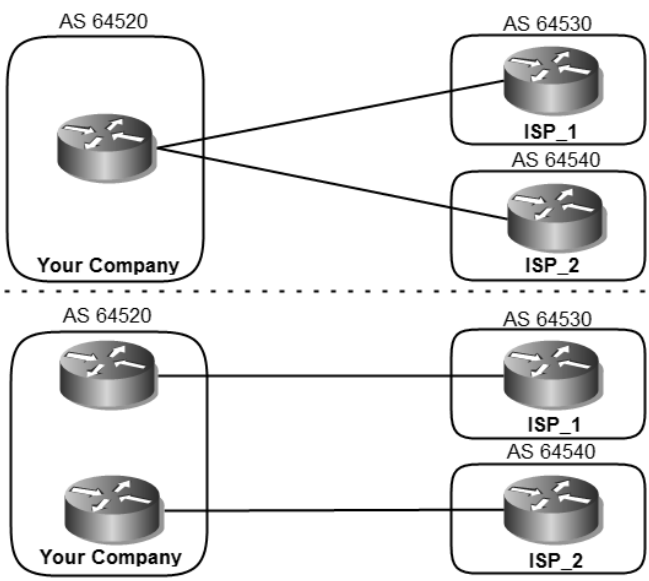
هر یک از موارد فوق می تواند دارای مزیت‌هایی باشد. اگر بخواهید از Static Default Route در این نوع طراحی استفاده کنید، می توانید دو Default Route با Metric برابر برای استفاده از ویژگی Load Balancing و یا Metric متفاوت جهت Failover داشته و توسط پروتکل مسیریابی داخلی، Default Routeها را به اطلاع سایر روترهای شبکه نیز برسانید. به هر حال چه Metric ها برابر باشند یا نباشند، در صورت قطع شدن یک لینک، تمام ترافیک بر روی لینک دیگر ارسال شده و ارتباط سازمان با اینترنت قطع نخواهد شد.

اما با توجه به داشتن دو لینک و استفاده از دو روتر در هر طرف (طرح سوم)، بهتر است طرحی را پیاده سازی نمایید که ویژگی Redundancy را نیز برای شما فراهم آورد. در اینصورت استفاده از BGP گزینه بهتری خواهد بود.

- **دو ISP، هر کدام با یک لینک (Single multihomed)**

توپولوژی Single Multihomed، به این معنی است که شبکه داخلی با حداقل دوISP در ارتباط بوده و به ازاء هر ISP یک لینک اتصال به اینترنت داشته باشد.

در این صورت شبکه ما طبق یکی از طرح های زیر خواهد بود.

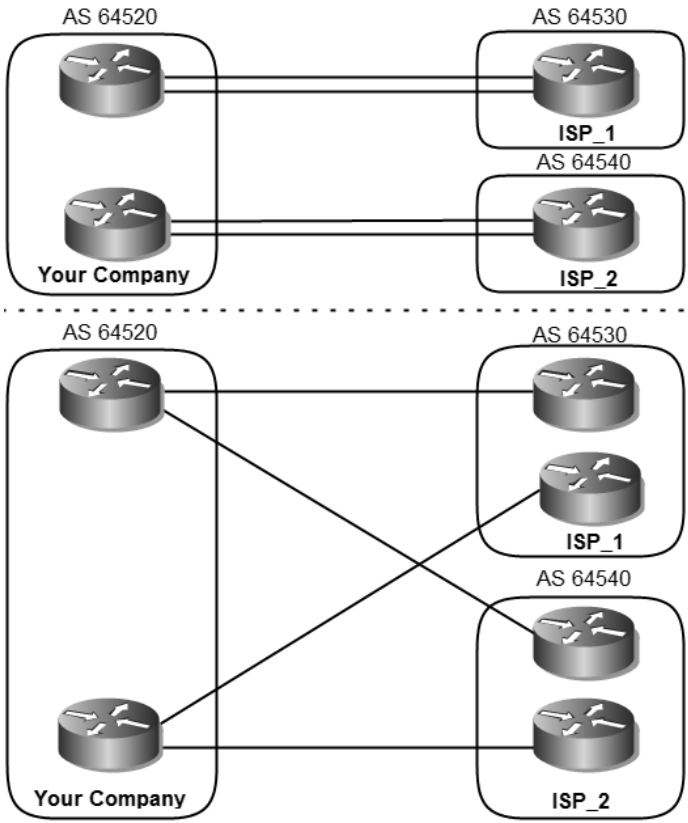


هر چند که در این حالت نیز می توانیم از Static Default Route با Metricهای برابر یا متفاوت استفاده نماییم، اما با توجه به وجود دو ISP مختلف استفاده از BGP راه حل بهتری خواهد بود.

با توجه به وجود دوISP مختلف، مطمئنا شبکه‌هایی در اینترنت هستند که دسترسی به آنها از طریق یکی ازISPها به صرفه‌تر خواهد بود. در این صورت استفاده از پروتکل BGP می تواند تاثیر قابل توجهی در مسیریابی اینترنت برای شبکه داخلی فراهم آورد. همچنین اگر دسترسی از طریق اینترنت به شبکه داخلی نیز برای شما مهم باشد، استفاده از BGP مخصوصا در حالت دوم تصویر فوق، می تواند بهترین گزینه باشد.

- **دو ISP، هر کدام با دو لینک (Dual Multihomed)**

در این حالت شبکه دارای دو(یا بیشتر) ISP بوده که با هر کدام از آنها دارای حداقل دو لینک ارتباطی می باشد. بعضی از حالت های ممکن در این نوع طراحی در شکل زیر نشان داده شده است.



تمام حالت هایی که می تواند اتفاق بیافتد در شکل فوق نشان داده نشده است. اما با توجه به وجود حداقل دوISP با حداقل دو لینک به ازاء هر یک از آنها، بهتر است طراحی شبکه به صورتی شکل پذیرد کهRedundancy را بطور کامل در اختیار داشته باشیم.

استفاده از پروتکلBGP مخصوصا در حالت دوم تصویر فوق می تواند یک گزینه ایده‌آل برای دسترسی شبکه به اینترنت باشد.

هنگام استفاده از روش دوم تصویر فوق کهRedundancy نیز به بهترین شکل در آن صورت گرفته است، مخصوصا در زمانی که دسترسی از اینترنت به شبکه امری حیاتی محسوب می گردد، بهترین زمان استفاده از پروتکل BGP خواهد بود.

انواع ارسال Update

در صورتی که برای برقراری ارتباط سازمان خود با اینترنت از پروتکل BGP استفاده نمایید، برای دریافت جداول مسیریابی اینترنت می‌توانید پروتکلBGP را در یکی از سه حالت زیر پیکربندی نمایید.

۱- **فقط Default Route**

در این حالت ISP توسط پروتکل BGP فقط اقدام به ارسال Default Route برای شبکه شما نموده و از ارسال اطلاعات دیگر خودداری می‌نماید.

۲- **Full Update**

در این حالت ISP جدول BGP خود را بصورت کامل برای شبکه شما ارسال می‌نماید. استفاده از روشFull Update بار پردازشی زیادی به روترهای شبکه شما تحمیل می‌نماید.

۳- **Partial Update**

در این حالتISP به جای ارسال کامل جدولBGP، فقط Update مسیرهایی را به شبکه شما ارسال می نماید که احتمال می دهد بهترین راه دسترسی به آنها، خود ISP باشد. همچنین علاوه بر مسیرهای فوق، یک Default Route نیز جهت دسترسی به سایر شبکه هایی که در پیام Update موجود نیست، به شبکه شما ارسال می‌نماید.

برای استفاده از این ویژگی باید ازBGP Filtering در پیکربندی روترها استفاده نمایید.

BGP Filtering

برای کنترل ارسال و دریافت پیام هایUpdate در پروتکلBGP چند راه مختلف وجود دارد. شما از این راه‌ها می توانید جهت مشخص نمودن نوع ارسال Update در حالت BGP Multi-homing نیز بهره ببرید. این حالت ها که به سه گروه زیر تقسیم می‌شوند، از نظر نتیجه شبیه به یکدیگر می‌باشد. آنچه که باعث می شود یکی از این روشها را بر روش های دیگر ترجیح داده شود، نوع پیکربندی و سیاست های اعمال شده در شبکه مورد نظر می باشد.

- **Route Filtering**

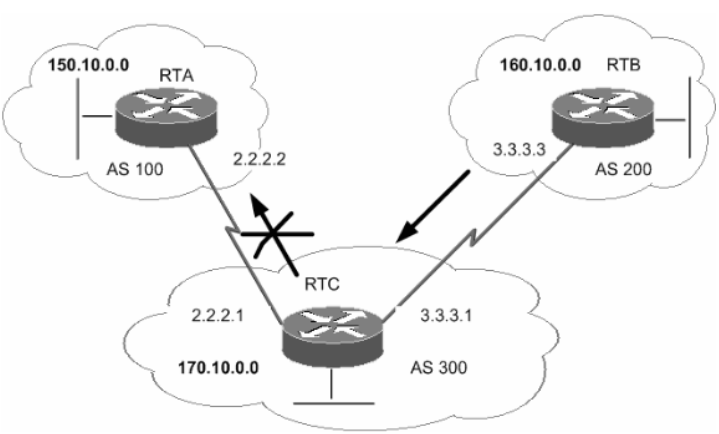
به منظور محدود نمودن اطلاعات مسیریابی که توسط روتر یاد گرفته شده و یا تبلیغ می‌شود، می‌توان اطلاعاتBGP را با کنترل Routing Updateهای دریافتی و ارسالی مربوط به یک روتر همسایه خاص، فیلتر نمود.

در این روش توسط Access List، اقدام به محدود کردن مسیرهایی که توسط روتر یاد گرفته و یا تبلیغ شود، می‌نماییم.

با استفاده از دستور زیر می توان اقدام به استفاده از ویژگی Route Filtering نمود:

neighbor {*ip-address* **|** *peer-group-name***} distribute-list** *access-list-number* **{in | out}**

به عنوان مثال، اگر بخواهیم از ارسالBGP Update شبکه 160.10.0.0 توسط روترRTC به روترRTA جلوگیری نماییم؛ باید پس از نوشتن ACL، آنرا به روتر همسایه مورد نظر اختصاص دهیم.



در اینصورت خروجی دستور show running-config بر روی روترRTC بصورت زیر خواهد بود:

```
RTC# show running-config

<...Output Committed...>

router bgp 300
network 170.10.0.0
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 distribute-list 1 out

access-list 1 deny 160.10.0.0 0.0.255.255
access-list 1 permit 0.0.0.0 255.255.255.255
```

اگر به ACLها توجه نمایید، متوجه خواهید شد که فقط Update مربوط به شبکه 160.10.0.0 /16 فیلتر شده و مابقی شبکه ها از طریق AS 300 به AS 100 تبلیغ خواهند شد.

- **Path Filtering**

در این روش می‌توان با استفاده از اطلاعات موجود درAS Path، اقدام به فیلتر نمودن هر یک از Updateهای ورودی و خروجی روتر نمود.

در اینصورت می‌توان شماره AS مورد نظر را جهت ارسال و یا دریافت پیام Update مشخص نمود.

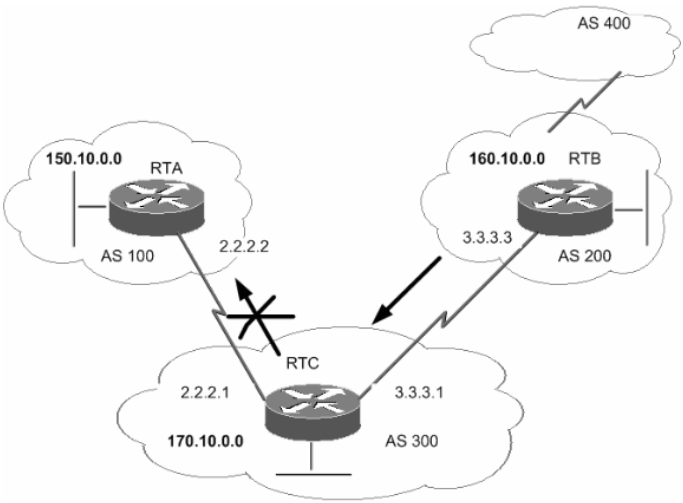
برای این منظور ابتدا باید توسط دستور زیر اقدام به ایجاد ACL بر اساس AS Path نماییم.

ip as-path access-list *access-list-number* **{permit | deny}** *as-regular-expression*

سپس توسط دستور زیر، ACL ایجاد شده را به همسایه مورد نظر اختصاص می دهیم:

neighbor {*ip-address* **|** *peer-group-name***} filter-list** *access-list-number* **{in | out}**

به عنوان مثال با استفاده ازPath Filter در شبکه زیر، از تبلیغ شبکه‌های مربوط به AS 200 توسط روتر AS 300 به AS 100 جلوگیری نموده ولی در عین حال اطلاعات مربوط به دیگرASها (مثل AS 400) توسط روترAS 300 به AS 100 تبلیغ خواهد شد.



در نهایت خروجی دستور show running-config بر روی روتر RTC به صورت زیر خواهد بود:

```
RTC# show running-config

<…Output Committed…>

router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 filter-list 1 out


ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
```

حتما با دیدن as-path access-list فوق متعجب شده‌اید! در نوشتنACL برای-AS Path از کاراکترهای خاصی استفاده می‌شود که برخی از آنها در جدول های زیر شرح داده شده‌اند.

اولین قسمت این عبارت را Atom می نامند. Atom یک کاراکتر تک است که در جدول زیر بعضی از این کاراکترها شرح داده شده است:

کاراکتر	شرح	مثال
.	در صورت تطبیق با هر کاراکتر به تنهایی هر "." به ازاء یک کاراکتر	0.0 با 0x0 و 020 تطابق دارد. همچنین t..t با text یا test تطابق دارد ولی با trust تطابق ندارد.

کاراکتر	شرح	مثال
^	در صورت تطبیق با شروع رشته ورودی	^123 با 1234 تطابق دارد ولی با 0123 تطابق ندارد.
$	در صورت تطبیق با پایان رشته ورودی	$123 با 0123 تطابق دارد ولی با 1234 تطابق ندارد.
\	در صورت تطبیق با کاراکترهایی که بعد از \ می آیند.	..\1.\172 با 172.1.10.10 تطابق دارد ولی با 172.12.0.0 تطابق ندارد.
_	کاراکتر _ در طول رشته می تواند با کاما(,)، کروشه چپ({)، کروشه راست(})، شروع رشته ورودی(^)، انتهای رشته ورودی($) یا یک Space جایگزین شود.	_1300_ می تواند با هر یک از حالتهای زیر تطابق داشته باشد. ^1300$ ^1300space space1300 {1300, ,1300, {1300} ,1300,

دومین قسمت عبارت را Piece می‌نامند. Piece که پس از Atom می آید، احتمالا یکی از کاراکترهای زیر خواهد بود:

کاراکتر	شرح	مثال
*	در صورت تطابق با 0 یا بیشتر از کاراکترهای Atom به عبارت دیگر منظور از * یعنی "هر چیزی"	*5 با هر رشته ای که حاوی عدد 5 باشد تطابق دارد. البته اگر شامل 5 هم نباشد، تطابق خواهد داشت.
+	در صورت تطابق حداقل با 1 یا تعداد بیشتری از کاراکترهای Atom	+8 در صورتی تطابق پیدا می‌کند که حداقل یک عدد8 در عبارت موجود باشد.
?	0 یا بیشتر از کاراکترهایی که بعد از ? می آید، باید وجود داشته باشد تا تطابق پیدا نماید.	**ab?a** با aa و یا aba تطابق پیدا می کند.

- **BGP Community Filtering**

یکی دیگر از روش‌های فیلتر کردن پیام‌های بروز رسانی، استفاده از Community Attribute می‌باشد.

ویژگیCommunity Attribute، انتقال دهنده Attributeهای مورد نظر می‌باشد. مقدار اختصاص داده شده به community-number می‌تواند در رنج 0 تا 4,294,967,200 قرار داشته باشد. توسط این ویژگی می توان اقدام به گروه بندی مقصدهای مختلف با Community معین نمود، تا بتوان تصمیمات مورد نظر درباره نحوه انتشار مسیرها را به صورت گروهی به اطلاع آنها رساند.

برای استفاده از ویژگی فوق می توان از دستورات زیر به همراه Route Map استفاده نمود.

set community *community-number* **[additive]** [*well-known-community*]

چند پارامتر که معمولا به جای [*well-known-community*] در دستور فوق مورد استفاده قرار می گیرند، به شرح زیر می باشد:

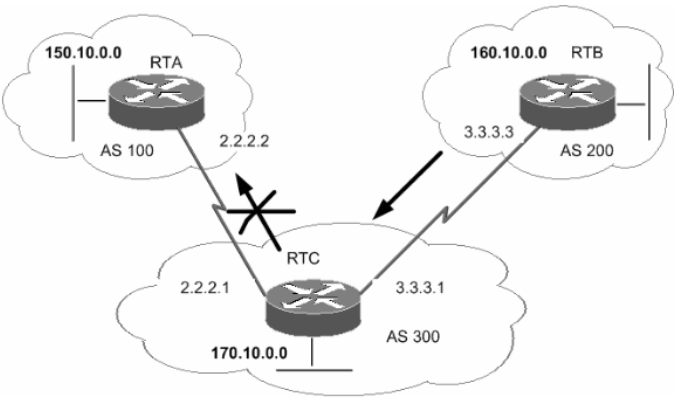
پارامتر	شرح
no-export	به همسایه هایEBGP تبلیغ نمی‌گردد. این مسیر داخل خودAS نگهداری می گردد.
no-advertise	این مسیر برای هیچ همسایه ای تبلیغ نمی‌گردد. فرقی ندارد که داخلی باشد یا خارجی.
internet	این مسیر به تمام روترهایی که در این Community قرار دارند، تبلیغ می‌شود.
local-as	باعث جلوگیری از انتقال بسته ها به خارج از AS محلی می‌شود.

پس از مشخص نمودن Community، باید توسط دستور زیر مشخص نماییم که قصد ارسال آنرا به همسایه مورد نظر داریم:

neighbor *neighbor_IP_Address* **send-community**

به عنوان مثال می توانید به سناریوی زیر توجه نمایید:

در این سناریو ما می خواهیم با پیکربندی روتر RTB و ارسال تنظیمات به روتر RTC، مشخص نماییم که روتر RTC باید مسیرهای AS 200 را در AS خود نگه داشته و از تبلیغ آنها به دیگر ASها خودداری نماید.



خروجی دستور show running-config روتر RTB به صورت زیر خواهد بود:

```
RTB# show running-config
router bgp 200
network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 send-community
neighbor 3.3.3.1 route-map setcommunity out

route-map setcommunity
match ip address 1
set community no-export

access-list 1 permit 0.0.0.0 255.255.255.255
```

همانطور که در سناریو فوق مشاهده می نمایید، روش های متفاوتی برای استفاده از ویژگی community وجود دارد که البته نیازی به تشریح آنها در این مبحث نمی‌باشد.

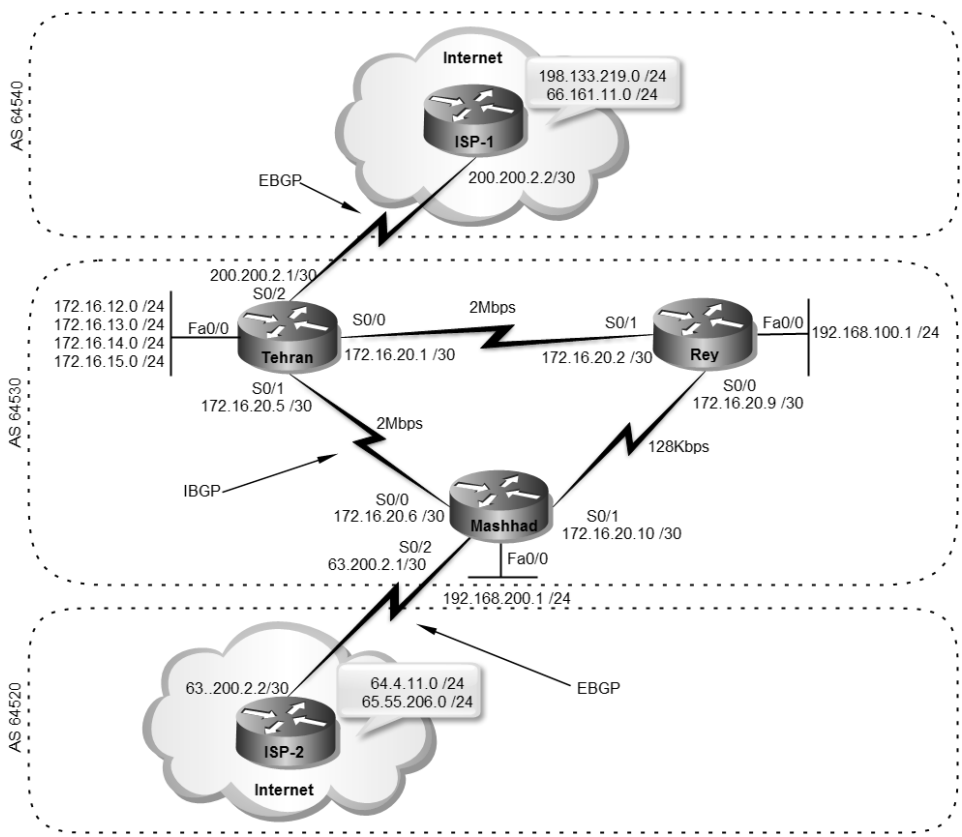
سناریو شماره(۱۴)؛ راه اندازی BGP

طرح مسئله:

شرکت MTR Electronic برای شعبه مشهد نیز اقدام به راه اندازی اتصال اینترنت نموده است. شرکت در حال حاضر دارای دو اتصال به اینترنت توسط دوISP مختلف می‌باشد. از شما خواسته شده برای استفاده بهینه از هر دو اتصال اینترنت، اقدام به راه اندازی پروتکلBGP نمایید.

نیاز سنجی:

برای برقراری اتصال روتر مشهد با ISP-2، باید یک کارت WIC به روتر اضافه نموده و پیکربندی نماییم.



با توجه به داشتن دوISP مختلف و داشتن یک لینک به ازاء هریک از آنها، می‌خواهیم بر اساس مدل Single Multihomed شبکه را پیکربندی نماییم. همچنین شبکه‌هایی که هر ISP مالک آنها است در تصویر نشان داده شده و ما در این سناریو می‌خواهیم نحوه دسترسی به شبکه‌های موجود در هر ISP را بررسی کنیم.

راه حل:

همانطور که در جریان هستید، در آخرین سناریو برای شرکت MTR Electronic پروتکل OSPF را جهت مسیریابی داخلی (IGP) راه اندازی نمودیم.

با توجه به اینکه پروتکلBGP یک پروتکل خارجی(EGP) محسوب می‌شود، نیازی به حذف پروتکل مسیریابیOSPF نداریم. این پروتکل‌ها در کنار هم کار کرده و هر یک وظیفه خود را انجام خواهند داد. اجرای همزمان پروتکل‌های IGP و EGP در شبکه، تداخلی با یکدیگر ندارند.

در گام اول اقدام به حذف Default Route ارسالی توسط پروتکل OSPF از روتر تهران می‌نماییم:

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router ospf 110
Tehran(config-router)#no default-information originate
Tehran(config-router)#exit
Tehran(config)#no ip route 0.0.0.0 0.0.0.0 200.200.2.2
```

پیکربندی روتر مشهد برای لینک جدید را بصورت زیر انجام می‌دهیم:

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#interface serial 0/2
Mashhad(config-if)#no shutdown
Mashhad(config-if)#ip address 63.200.2.1 255.255.255.252
Mashhad(config-if)#^Z
Mashhad#
```

برای دسترسی به اینترنت باید برای روتر مشهد NAT را نیز پیکربندی کنیم:

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ip access-list extended 100
Mashhad(config-ext-nacl)#permit ip  172.16.12.0 0.0.3.255 any
Mashhad(config-ext-nacl)#permit ip  192.168.100.0 0.0.0.255 any
Mashhad(config-ext-nacl)#permit ip  192.168. 200.0 0.0.0.255 any
```

```
Mashhad(config-ext-nacl)#exit
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#ip nat inside
Mashhad(config-if)#interface serial 0/0
Mashhad(config-if)#ip nat inside
Mashhad(config-if)#interface serial 0/1
Mashhad(config-if)#ip nat inside
Mashhad(config-if)#interface serial 0/2
Mashhad(config-if)#ip nat outside
Mashhad(config-if)#exit
Mashhad(config)#ip nat inside source list 100 interface serial 0/2 overload
Mashhad(config)#exit
Mashhad#
```

حالا نوبتی هم که باشه، نوبت پیکربندی پروتکل BGP بر روی روترها است:

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#router bgp 64530
Tehran(config-router)#neighbor 200.200.2.2 remote-as 64540
Tehran(config-router)#neighbor 172.16.20.6 remote-as 64530
```

ابتدا با دستور router bgp 64530 اقدام به فعال ساختن پروتکلBGP بر روی روتر می‌نماییم.

سپس توسط دستور Neighbor همسایه‌های مورد نظر را به روتر معرفی می‌کنیم.

اگر شماره AS موجود در دستورNeighbor با شماره AS روتر متفاوت باشد، روتر در حالت EBGP و اگر شماره ASها یکسان باشند روتر در حالت IBGP با روتر همسایه رابطه مجاورت برقرار می‌نماید.

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#router bgp 64530
Mashhad(config-router)#neighbor 63.200.2.2 remote-as 64520
Mashhad(config-router)#neighbor 172.16.20.5 remote-as 64530
Mashhad(config-router)#^Z
Mashhad#
```

پس از انجام مراحل فوق جداول مسیریابی روترهای تهران و مشهد بصورت زیر خواهد بود:

```
Tehran#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
     o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set

    66.0.0.0/24 is subnetted, 1 subnets
B      66.161.11.0 [20/0] via 200.200.2.2, 00:04:11
    200.200.2.0/30 is subnetted, 1 subnets
C      200.200.2.0 is directly connected, Serial0/2
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.20.8/30 [110/114] via 172.16.20.6, 00:05:28, Serial0/1
C      172.16.20.0/30 is directly connected, Serial0/0
C      172.16.20.4/30 is directly connected, Serial0/1
C      172.16.12.0/24 is directly connected, FastEthernet0/0.1
C      172.16.13.0/24 is directly connected, FastEthernet0/0.2
C      172.16.14.0/24 is directly connected, FastEthernet0/0.3
C      172.16.15.0/24 is directly connected, FastEthernet0/0.4
O   192.168.200.0/24 [110/60] via 172.16.20.6, 00:05:30, Serial0/1
B   198.133.219.0/24 [20/0] via 200.200.2.2, 00:04:15
O   192.168.100.0/24 [110/60] via 172.16.20.2, 00:05:32, Serial0/0
Tehran#
```

```
Mashhad#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    64.0.0.0/24 is subnetted, 1 subnets
B      64.4.11.0 [20/0] via 63.200.2.2, 00:02:32
    65.0.0.0/24 is subnetted, 1 subnets
B      65.55.206.0 [20/0] via 63.200.2.2, 00:02:32
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C      172.16.20.8/30 is directly connected, Serial0/1
O      172.16.20.0/30 [110/114] via 172.16.20.5, 00:07:23, Serial0/0
C      172.16.20.4/30 is directly connected, Serial0/0
O      172.16.12.0/24 [110/74] via 172.16.20.5, 00:07:23, Serial0/0
O      172.16.13.0/24 [110/74] via 172.16.20.5, 00:07:25, Serial0/0
O      172.16.14.0/24 [110/74] via 172.16.20.5, 00:07:25, Serial0/0
O      172.16.15.0/24 [110/74] via 172.16.20.5, 00:07:25, Serial0/0
C   192.168.200.0/24 is directly connected, FastEthernet0/0
    63.0.0.0/30 is subnetted, 1 subnets
C      63.200.2.0 is directly connected, Serial0/2
O   192.168.100.0/24 [110/74] via 172.16.20.9, 00:07:36, Serial0/1
Mashhad#
```

همانطور که در خروجی‌های فوق ملاحظه می‌کنید روتر تهران شبکه‌های ISP-1 و روتر مشهد شبکه‌های ISP-2 را از طریق BGP یاد گرفته‌اند. اما یک سوال! چرا علیرغم اینکه روتر تهران و مشهد با هم رابطه IBGP دارند، نتوانسته‌اند آدرس‌های بدست آمده توسط روتر مقابل را یاد بگیرند؟ با توجه به خروجی زیر جواب را به‌دست خواهید آورد:

```
Tehran#show ip bgp
```

```
BGP table version is 3, local router ID is 200.200.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i64.4.11.0/24     63.200.2.2             0    100      0 64520 i
* i65.55.206.0/24   63.200.2.2             0    100      0 64520 i
*> 66.161.11.0/24   200.200.2.2           0             0 64540 i
*> 198.133.219.0    200.200.2.2           0             0 64540 i
Tehran#
```

```
Mashhad#show ip bgp
BGP table version is 3, local router ID is 63.200.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 64.4.11.0/24     63.200.2.2             0             0 64520 i
*> 65.55.206.0/24   63.200.2.2             0             0 64520 i
* i66.161.11.0/24   200.200.2.2           0    100      0 64540 i
* i198.133.219.0    200.200.2.2           0    100      0 64540 i
Mashhad#
```

درست حدس زدید! آدرس‌ها توسط روترهای مقابل دریافت شده‌اند اما به دلیل فقدان آدرس Next Hop مربوطه در جداول مسیریابی، روترها از درج مسیرهای به دست آمده در جدول مسیریابی خودداری نموده‌اند. برای رفع مشکل فوق دستورات زیر را بر روی روترها اجرا می‌کنیم:

```
Tehran#configure terminal
Tehran(config)#router ospf 110
Tehran(config-router)#network 200.200.2.0 0.0.0.3 area 0
```

```
Mashhad#configure terminal
Mashhad(config)#router ospf 110
Mashhad(config-router)#network 63.200.2.0 0.0.0.3 area 0
```

پس از دستورات فوق، جدول مسیریابی به شکل زیر تغییر می‌کند:

```
Tehran#show ip route
<... Output Omitted...>
   64.0.0.0/24 is subnetted, 1 subnets
B     64.4.11.0 [200/0] via 63.200.2.2, 00:01:06
   65.0.0.0/24 is subnetted, 1 subnets
B     65.55.206.0 [200/0] via 63.200.2.2, 00:01:06
   66.0.0.0/24 is subnetted, 1 subnets
B     66.161.11.0 [20/0] via 200.200.2.2, 00:27:54
   200.200.2.0/30 is subnetted, 1 subnets
C     200.200.2.0 is directly connected, Serial0/2
```

```
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.20.8/30 [110/114] via 172.16.20.6, 00:29:11, Serial0/1
C      172.16.20.0/30 is directly connected, Serial0/0
C      172.16.20.4/30 is directly connected, Serial0/1
C      172.16.12.0/24 is directly connected, FastEthernet0/0.1
C      172.16.13.0/24 is directly connected, FastEthernet0/0.2
C      172.16.14.0/24 is directly connected, FastEthernet0/0.3
C      172.16.15.0/24 is directly connected, FastEthernet0/0.4
O   192.168.200.0/24 [110/60] via 172.16.20.6, 00:29:14, Serial0/1
B   198.133.219.0/24 [20/0] via 200.200.2.2, 00:27:57
    63.0.0.0/30 is subnetted, 1 subnets
O      63.200.2.0 [110/114] via 172.16.20.6, 00:01:14, Serial0/1
O   192.168.100.0/24 [110/60] via 172.16.20.2, 00:29:14, Serial0/0
Tehran#
```

```
Mashhad#show ip route
<… Output Omitted…>

    64.0.0.0/24 is subnetted, 1 subnets
B      64.4.11.0 [20/0] via 63.200.2.2, 00:23:48
    65.0.0.0/24 is subnetted, 1 subnets
B      65.55.206.0 [20/0] via 63.200.2.2, 00:23:48
    66.0.0.0/24 is subnetted, 1 subnets
B      66.161.11.0 [200/0] via 200.200.2.2, 00:02:21
    200.200.2.0/30 is subnetted, 1 subnets
O      200.200.2.0 [110/69] via 172.16.20.5, 00:02:26, Serial0/0
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C      172.16.20.8/30 is directly connected, Serial0/1
O      172.16.20.0/30 [110/114] via 172.16.20.5, 00:28:40, Serial0/0
C      172.16.20.4/30 is directly connected, Serial0/0
O      172.16.12.0/24 [110/74] via 172.16.20.5, 00:28:40, Serial0/0
O      172.16.13.0/24 [110/74] via 172.16.20.5, 00:28:42, Serial0/0
O      172.16.14.0/24 [110/74] via 172.16.20.5, 00:28:42, Serial0/0
O      172.16.15.0/24 [110/74] via 172.16.20.5, 00:28:42, Serial0/0
C   192.168.200.0/24 is directly connected, FastEthernet0/0
B   198.133.219.0/24 [200/0] via 200.200.2.2, 00:02:24
    63.0.0.0/30 is subnetted, 1 subnets
C      63.200.2.0 is directly connected, Serial0/2
O   192.168.100.0/24 [110/74] via 172.16.20.9, 00:28:52, Serial0/1
Mashhad#
```

حالا اگر شبکه‌های ISP-1 وISP-2 را توسط روترهای تهران و مشهد ping کنیم (البته به صورت حرفه‌ای) خروجی زیر را خواهیم داشت:

```
Tehran#ping
Protocol [ip]:
Target IP address: 66.161.11.90
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.12.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
```

```
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 66.161.11.90, timeout is 2 seconds:
Packet sent with a source address of 172.16.12.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/26/52 ms
Tehran#
```

مطمئن هستم به یاد دارید که چرا از دستور ping بصورت پیشرفته استفاده می‌کنیم. بدلیل اینکه فقط شبکه‌هایی امکان NAT شدن را دارند که در ACL معرفی شده باشند. اما به هر حال شما می‌توانید به جای ping توسط روتر، از طریق کلاینت‌ها اقدام به استفاده از این دستور نموده و خود را از شر ping پیشرفته نجات دهید، هر چند که این کار برای حرفه‌ای های شبکه صورت خوشی ندارد!!!

```
Mashhad#ping
Protocol [ip]:
Target IP address: 198.133.219.25
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.200.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/19/48 ms
Mashhad#
```

علیرغم دسترسی شبکه‌های تهران و مشهد همانطور که از دستور زیر پیداست، کلاینت‌های شهرری همچنان از نعمت اینترنت بی بهره هستند:

```
Rey#ping
Protocol [ip]:
Target IP address: 198.133.219.25
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
```

```
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
.....
Success rate is 0 percent (0/5)
Rey#
```

خوب، روتر شهرری در جدول مسیریابی خود نه دارای Default Route است و نه مسیری برای شبکه‌های ISP-1 و ISP-2 دارد، پس چه انتظاری داریم که امکان دسترسی به اینترنت فراهم باشد؟!

برای مشکل فوق چند راه حل داریم:

۱- چون در شبکه ما کلا ۳ روتر وجود دارد، و روترهای تهران و مشهد نیز درگیر BGP هستند، پس می‌توان روتر شهرری را نیز وارد پروسه IBGP نمود.

۲- می‌توان برای روترهایی که در پروسه IBGP شرکت ندارند اقدام به تعریف Default Route به سمت یکی از روترهای IBGP کرد.

۳- می‌توان از ویژگی Redistribute بهره برد.

از بین گزینه‌های فوق بهترین و البته فنی ترین کار Redistribute آدرس‌های BGP از طریق OSPF می‌باشد. من این ویژگی را بصورت مبسوط در "مبحث سوم فصل هفتم" شرح داده‌ام. لذا فقط اینجا به اجرای دستورات بسنده می‌کنم:

```
Tehran#configure terminal
Tehran(config)#router ospf 110
Tehran(config-router)#redistribute bgp 64530 subnets
```

```
Mashhad#configure terminal
Mashhad(config)#router ospf 110
Mashhad(config-router)#redistribute bgp 64530 subnets
```

توسط دستورات فوق ما از OSPF می‌خواهیم که مسیرهای BGP را در قالب پیام‌های خود تبلیغ نماید. پس از انجام مراحل فوق، جدول مسیریابی روتر شهرری به صورت زیر خواهد بود:

```
Rey#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     64.0.0.0/24 is subnetted, 1 subnets
O E2    64.4.11.0 [110/1] via 172.16.20.1, 00:03:25, Serial0/1
     65.0.0.0/24 is subnetted, 1 subnets
O E2    65.55.206.0 [110/1] via 172.16.20.1, 00:03:25, Serial0/1
     66.0.0.0/24 is subnetted, 1 subnets
O E2    66.161.11.0 [110/1] via 172.16.20.1, 00:06:34, Serial0/1
     200.200.2.0/30 is subnetted, 1 subnets
O       200.200.2.0 [110/69] via 172.16.20.1, 01:22:38, Serial0/1
     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C       172.16.20.8/30 is directly connected, Serial0/0
C       172.16.20.0/30 is directly connected, Serial0/1
O       172.16.20.4/30 [110/114] via 172.16.20.1, 01:48:51, Serial0/1
O       172.16.12.0/24 [110/74] via 172.16.20.1, 01:48:51, Serial0/1
O       172.16.13.0/24 [110/74] via 172.16.20.1, 01:48:53, Serial0/1
O       172.16.14.0/24 [110/74] via 172.16.20.1, 01:48:53, Serial0/1
O       172.16.15.0/24 [110/74] via 172.16.20.1, 01:48:53, Serial0/1
O    192.168.200.0/24 [110/124] via 172.16.20.1, 01:48:53, Serial0/1
O E2 198.133.219.0/24 [110/1] via 172.16.20.1, 00:06:38, Serial0/1
     63.0.0.0/30 is subnetted, 1 subnets
O       63.200.2.0 [110/178] via 172.16.20.1, 01:20:51, Serial0/1
C    192.168.100.0/24 is directly connected, FastEthernet0/0
Rey#
```

همانطور که ملاحظه می‌نمائید، روتر شهرری تمام شبکه‌های BGP را نیز از طریق OSPF شناخته است. اما به دلیل پهنای باند بهتر لینک تهران– شهرری نسبت به لینک شهرری– مشهد، مسیر اول برای تمام شبکه‌های BGP به عنوان بهترین مسیر انتخاب و در جدول مسیریابی ثبت گردیده است. به دلیل داشتن مسیرهای فوق، حالا خروجی ping سرور سیسکو و مایکروسافت بر روی اینترنت به صورت زیر خواهد بود:

```
Rey#ping
Protocol [ip]:
Target IP address: 198.133.219.25
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/14/32 ms

Rey#ping
Protocol [ip]:
```

```
Target IP address: 64.4.11.42
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.4.11.42, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/16/32 ms
```

طریقه عملکرد:

با توجه به اینکه دو روتر مختلف شبکه ما هر کدام با یک لینک به دو ISP مختلف متصل هستند، نوع توپولوژی BGP این شبکه، Single Multihomed می‌باشد.

پس از آنکه پروتکل BGP را بر روی روتر فعال کردیم، با دستور Neighbor اقدام به معرفی همسایه‌ها می‌نمائیم. همانطور که قبلا گفته شد به دلیل اینکه پروتکل BGP از TCP استفاده می‌کند امکان بهره برداری از پیام‌های Broadcast برای شناسایی پویای همسایه ها را ندارد، لذا معرفی دستی همسایه‌ها به روتر امری لازم می‌باشد.

اگر شماره AS که در دستور Neighbor وارد می‌شود مطابق با AS خود روتر باشد، رابطه مجاورت بصورت داخلی یاIBGP و اگر شماره AS متفاوت باشد رابطه مجاورت بصورت خارجی یا EBGP بر قرار می‌گردد.

برقراری رابطه مجاورت نیز با طی مراحل Idle، Connect، Active، Opensent، Openconfirm و Established انجام می‌گیرد و در صورتی که مجاورت امکانپذیر باشد در نهایت هر دو روتر در حالت Established قرار خواهند گرفت.

توسط دستور زیر می‌توانید وضعیت روترها در زمان برقراری رابطه مجاورت را مشاهده نمائید:

```
Tehran#show ip bgp neighbors
BGP neighbor is 172.16.20.6,  remote AS 64530, internal link
  BGP version 4, remote router ID 63.200.2.1
  BGP state = Established, up for 02:13:34
  Last read 00:00:34, last write 00:00:34, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
```

```
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                    Sent       Rcvd
    Opens:             1          1
    Notifications:     0          0
    Updates:           1          1
    Keepalives:      135        135
    Route Refresh:     0          0
    Total:           137        137
  Default minimum time between advertisement runs is 0 seconds

<... Output Omitted...>

BGP neighbor is 200.200.2.2,  remote AS 64540, external link
  BGP version 4, remote router ID 198.133.219.25
  BGP state = Established, up for 02:13:50
  Last read 00:00:50, last write 00:00:50, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                    Sent       Rcvd
    Opens:             1          1
    Notifications:     0          0
    Updates:           1          1
    Keepalives:      135        135
    Route Refresh:     0          0
    Total:           137        137
  Default minimum time between advertisement runs is 30 seconds
<... Output Omitted...>


Tehran#
```

در خروجی دستور فوق نحوه برقراری رابطه مجاورت، Router ID، وضعیت روتر، تعداد پیام‌های ارسال و دریافت شده و بسیاری اطلاعات دیگر نمایش داده می‌شود.

از خروجی فوق متوجه می‌شویم که روتر تهران توانسته به درستی با روتر مشهد ارتباط IBGP و با روتر ISP-1 ارتباط EBGP برقرار نماید.

اگر دستور فوق را بر روی روتر مشهد نیز اجرا نمائیم، خروجی زیر را مشاهده خواهیم کرد:

```
Mashhad#show ip bgp neighbors
BGP neighbor is 63.200.2.2,  remote AS 64520, external link
  BGP version 4, remote router ID 65.55.206.228
  BGP state = Established, up for 02:14:58
  Last read 00:00:08, last write 00:00:58, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

```
                    Sent      Rcvd
  Opens:              2         1
  Notifications:      1         0
  Updates:            1         1
  Keepalives:       137       138
  Route Refresh:      0         0
  Total:            141       140
 Default minimum time between advertisement runs is 30 seconds

 <... Output Omitted...>

BGP neighbor is 172.16.20.5,  remote AS 64530, internal link
 BGP version 4, remote router ID 200.200.2.1
 BGP state = Established, up for 02:19:08
 Last read 00:00:08, last write 00:00:08, hold time is 180, keepalive interval is 60 seconds
 Neighbor capabilities:
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
 Message statistics:
  InQ depth is 0
  OutQ depth is 0
                    Sent      Rcvd
  Opens:              1         1
  Notifications:      0         0
  Updates:            1         1
  Keepalives:       141       141
  Route Refresh:      0         0
  Total:            143       143
 Default minimum time between advertisement runs is 0 seconds

 <... Output Omitted...>
Mashhad#
```

پس از برقراری رابطه مجاورت، روترها اقدام به تبادل جداول مسیریابی با یکدیگر می‌نمایند. البته شما می‌توانید با استفاده از ACL و Route Map نوع ارسال و دریافت پیام‌های Update خود را مشخص نمائید.

جهت تعیین نحوه ارسال و دریافت Update می‌توان بر اساس BGP Filtering که در همین مبحث بصورت کامل تشریح شده، اقدام نمود. اما ما برای آنکه این سناریو را زیاد پیچیده نکنیم به تبلیغ شبکه‌هایی که هرISP مالک آنها بود، بسنده کردیم.

روترها پس از دریافت جداول مسیریابی روترهای همسایه، با توجه به Path Attributes مربوطه و با طی مراحل ذکر شده در همین مبحث (الگوریتم انتخاب بهترین مسیر در BGP) اقدام به انتخاب بهترین مسیر به مقصد مورد نظر و تصمیم گیری درباره نحوه تبلیغ آن می‌نمایند.

همانطور که در زمان پیکربندی ملاحظه کردید علیرغم اینکه مسیرهای خارجی به دست آمده توسط روتر تهران به روتر مشهد و بالعکس رسیده بود اما روترها از درج آن مسیرها در جداول مسیریابی خودداری کرده بودند. این اتفاق به دلیل همان گام 0 ذکر شده در جدول فوق می‌باشد

که اگر مسیری برای رسیدن به آدرس Next hop وجود نداشته باشد، مسیر به دست آمده توسط BGP، مورد استفاده قرار نخواهد گرفت.

```
Tehran#show ip bgp
BGP table version is 3, local router ID is 200.200.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i64.4.11.0/24     63.200.2.2             0    100      0 64520 i
* i65.55.206.0/24   63.200.2.2             0    100      0 64520 i
*> 66.161.11.0/24   200.200.2.2           0             0 64540 i
*> 198.133.219.0    200.200.2.2           0             0 64540 i
Tehran#
```

```
Mashhad#show ip bgp
BGP table version is 3, local router ID is 63.200.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 64.4.11.0/24     63.200.2.2             0             0 64520 i
*> 65.55.206.0/24   63.200.2.2             0             0 64520 i
* i66.161.11.0/24   200.200.2.2           0    100      0 64540 i
* i198.133.219.0    200.200.2.2           0    100      0 64540 i
Mashhad#
```

مشکل فوق با تبلیغ آدرس‌های Next hop توسط پروتکل OSPF حل شده و مسیرهای رد و بدل شده بین دو روتر تهران و مشهد در جداول مسیریابی یکدیگر درج شدند.

برای بررسی جدول مسیریابی پروتکل BGP که به RIB معروف است، می‌توان از دستور زیر استفاده نمود:

```
Tehran#show ip bgp
BGP table version is 8, local router ID is 200.200.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r>i64.4.11.0/24     63.200.2.2             0    100      0 64520 i
r>i65.55.206.0/24   63.200.2.2             0    100      0 64520 i
*> 66.161.11.0/24   200.200.2.2           0             0 64540 i
*> 198.133.219.0    200.200.2.2           0             0 64540 i
Tehran#
```

پس از آنکه روترهای IBGP اطلاعات مسیرهای خارجی را به درستی با یکدیگر تبادل کنند، کلاینت‌های هر دو شبکه می‌توانند به راحتی با شبکه‌های هر دو ISP ارتباط برقرار نمایند. اما سایر روترهای شبکه که در پروسه IBGP شرکت نمی‌کنند هم باید از آن مسیرها اطلاع داشته باشند. اینجاست که تبلیغ مسیرهای به دست آمده توسط یک پروتکل مسیریابی خارجی را باید بر عهده یک پروتکل مسیریابی داخلی نهاد که به این عمل، Redistribution گفته می‌شود. با توجه به اینکه شبکه ما برای مسیریابی داخلی از پروتکل OSPF استفاده می‌نماید، عملیات Redistribution را توسط این پروتکل بر روی روترهای تهران و مشهد اجرا نمودیم. پس از اجرای این عملیات روتر شهرری بدون آنکه در پروسه BGP شرکت نموده باشد از طریق OSPF مسیرهای خارجی را یاد گرفته و از آنها استفاده می‌نماید. البته لازم به ذکر است که هر تعداد روتر دیگری هم در شبکه داشتیم، همانند روتر شهرری و از طریق OSPF می‌توانستند به این مسیرها دسترسی داشته باشند.

در نهایت می توانید برای بررسی خلاصه وار پروتکل BGP از دستور زیر استفاده نمائید:

```
Mashhad#show ip bgp summary
BGP router identifier 63.200.2.1, local AS number 64530
BGP table version is 15, main routing table version 15
4 network entries using 480 bytes of memory
4 path entries using 208 bytes of memory
3/2 BGP path/bestpath attribute entries using 372 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 2 (at peak 2) using 64 bytes of memory
BGP using 1172 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
63.200.2.2      4 64520    139    141       15    0    0 02:14:23        2
172.16.20.5     4 64530    142    142       15    0    0 02:18:23        2
Mashhad#
```

```
Tehran#show ip bgp summary
BGP router identifier 200.200.2.1, local AS number 64530
BGP table version is 9, main routing table version 9
4 network entries using 480 bytes of memory
4 path entries using 208 bytes of memory
3/2 BGP path/bestpath attribute entries using 372 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 2 (at peak 2) using 64 bytes of memory
BGP using 1172 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.20.6     4 64530    137    137        9    0    0 02:13:18        2
200.200.2.2     4 64540    137    137        9    0    0 02:13:23        2
```

مرجع دستور Command Reference:

Enabling BGP Routing		
	Command	**Purpose**
Step 1	Router(config)# **router bgp** *as-number*	Enables a BGP routing process, which places the router in router configuration mode.
Step 2	Router(config-router)# **network** *network-number* [**mask** *network-mask*] [**route-map***route-map-name*]	Flags a network as local to this autonomous system and enters it to the BGP table.

Configuring BGP Neighbors	
Command	**Purpose**
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*	Specifies a BGP neighbor.

Configuring BGP Interactions with IGPs	
Command	**Purpose**
Router(config-router)# **no synchronization**	Disables synchronization between BGP and an IGP.

Disabling Next Hop Processing Using a Specific Address	
Command	**Purpose**
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	Disables next hop processing on BGP updates to a neighbor.

Using Route Maps to Modify Updates	
Command	**Purpose**
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}	Applies a route map to incoming or outgoing routes.

Displaying System and Network Statistics	
Command	**Purpose**
Router# **show ip bgp** *prefix*	Displays peer groups and peers not in peer groups to which the prefix has been advertised. Also displays prefix attributes such as the next hop and the local prefix.
Router# **show ip bgp cidr-only**	Displays all BGP routes that contain subnet and supernet network masks.
Router# **show ip bgp community** *community-*	Displays routes that belong to the specified

Displaying System and Network Statistics	
number [**exact**]	communities.
Router# **show ip bgp community-list** *community-list-number* [**exact**]	Displays routes that are permitted by the community list.
Router# **show ip bgp filter-list** *access-list-number*	Displays routes that are matched by the specified autonomous system path access list.
Router# **show ip bgp inconsistent-as**	Displays the routes with inconsistent originating autonomous systems.
Router# **show ip bgp regexp** *regexp*	Displays the routes that have an autonomous system path that matches the specified regular expression entered on the command line.
Router# **show ip bgp**	Displays the contents of the BGP routing table.
Router# **show ip bgp neighbors** [*neighbor-address*]	Displays detailed information on the BGP and TCP connections to individual neighbors.
Router# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes**]	Displays routes learned from a particular BGP neighbor.
Router# **show ip bgp paths**	Displays all BGP paths in the database.
Router# **show ip bgp peer-group** [*tag*] [**summary**]	Displays information about BGP peer groups.
Router# **show ip bgp summary**	Displays the status of all BGP connections.

فصل ششم

شبکه‌های گسترده؛ مسیریابی با IPv6

- ☑ مبحث اول: مفاهیم مسیریابی در IPv6
- ☑ مبحث دوم: پروتکل RIPng
- ☑ مبحث سوم: پروتکل EIGRP for IPv6
- ☑ مبحث چهارم: پروتکل OSPFv3

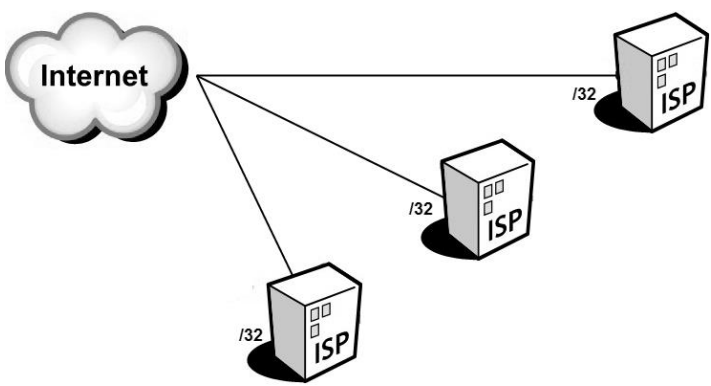
☑ مبحث اول

مفاهیم مسیریابی در IPv6

نحوه تخصیص آدرس Global

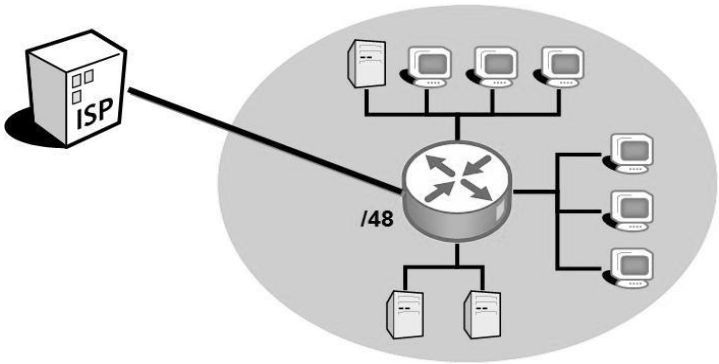
با توجه به اینکه رنج Global Unicast آدرس‌هایIPv6 باید بصورت منحصر بفرد در سراسر اینترنت وجود داشته باشند، تخصیص این رنج بر عهده سازمان IANA گذارده شده است. این سازمان نیز کشورهای جهان را به پنج گروه تقسیم کرده و تخصیص آدرس به هر گروه را بر عهده سازمان ذیربط قرار داده است.

هر یک از پنج سازمان فوق وظیفه اختصاص آدرس به ISPهای زیر مجموعه خود را داشته و بالطبع ISPها نیز اختصاص آدرس به شرکت‌ها و سازمان‌ها را بر عهده خواهند داشت.

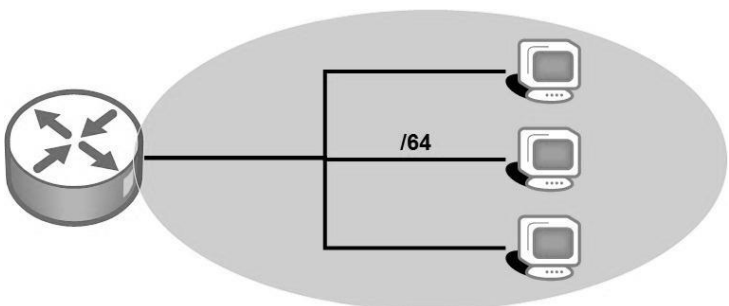


بطور معمول سازمان های منطقه‌ای IANA آدرس‌های با Prefix برابر با 32/ را به ISPها اختصاص می‌دهند. هر ISP نیز می تواند از 16 بیت برای زیر شبکه سازی خود استفاده نموده و آدرس های با Prefix برابر با 48/ را در اختیار سازمان‌های درخواست کننده قرار دهد.

شرکت ISP می تواند با 16 بیتی که در اختیار دارد $2^{16} = 65,536$ عدد زیر شبکه ایجاد نماید.



در نهایت شرکت دریافت کننده آدرس‌های IP نیز می‌تواند از حداقل 16 بیت برای زیر شبکه سازی در سازمان خود بهره برده و از Prefix برابر با 64/ برای میزبان ها استفاده نماید.



نکته: مراحل فوق بیانگر نحوه تخصیص آدرس‌های Global توسط IANA می‌باشد و ممکن است روش زیر شبکه سازی در انواع دیگر آدرس ها متفاوت باشد.

مهاجرت[1] و همزیستی[2] IPv4 با IPv6

مهاجرت از IPv4 به IPv6 برای بسیاری از شرکت‌ها و کارشناسان شبکه مطلوب نیست. مدیران و کارشناسان خیلی از شرکت‌ها تمایلی به شخم زدن شبکه خود ندارند. اما از طرف دیگر مهاجرت به IPv6 نیز اجتناب ناپذیر بوده و بالاخره باید به این سمت حرکت کرد. به همین دلیل نیاز است تا راهکارهایی جهت همزیستی مسالمت آمیز بین این دو پروتکل ایجاد گردد تا مهاجرت به IPv6 به آهستگی و بدون هیچ زد و خوردی انجام پذیرد. با توجه به سرعت کم استفاده از

[1] Migration
[2] Coexistence

IPv6، ممکن است این همزیستی مسالمت آمیز سالها به طول بیانجامد. پس یادگیری و راه اندازی این راهکارها از اهمیت خاصی برخوردار خواهد بود.

همزیستی یا Coexistence دارای سه راهکار کلی به شرح زیر می‌باشد:

۱- **Dual Stack**

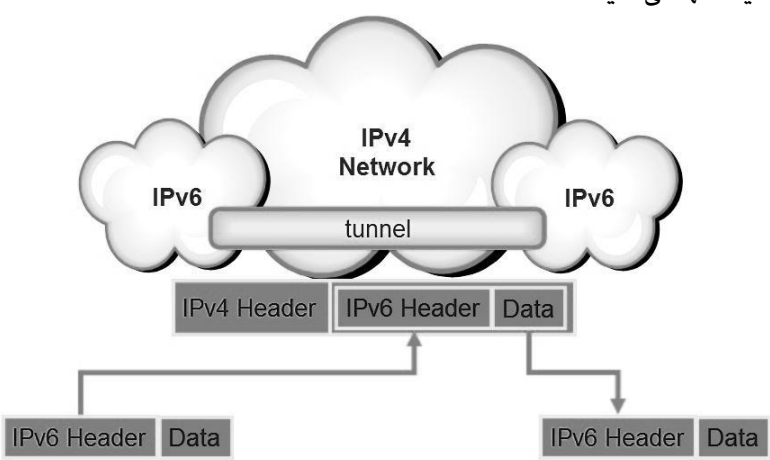
منظور از Dual Stack، استفاده هم زمان از هر دو پروتکل IPv4 و IPv6 بر روی رابط (اینترفیس)های شبکه میزبان(Host) و روتر می‌باشد.

اصطلاح Dual Stack برای میزبان به این معناست که کارت شبکه (NIC) میزبان دارای هر دو آدرس IPv4 و IPv6 بوده و می‌تواند بسته‌های IPv6 را به میزبان دیگر دارای IPv6 و بسته‌های IPv4 را برای میزبان دارای IPv4 ارسال نماید.

اما اصطلاح Dual Stack برای روتر به این معناست که روتر علاوه بر آدرس‌ها و پروتکل‌های مسیریابی IPv4، باید مسیرها و پروتکل‌های مسیریابی IPv6 را نیز پشتیبانی نماید.

۲- **Tunneling**

اصطلاح Tunneling اشاره به فرآیندی دارد که طی آن یک روتر یا میزبان اقدام به کپسوله کردن دیتای IPv6 خود در قالب بسته‌های IPv4 می‌نماید. در اینصورت تجهیزات واقع در مسیر که بر پایه IPv4 عمل می نمایند بدون اطلاع از محتویات بسته ها، اقدام به هدایت آنها می‌نمایند.



۳- **NAT-PT**

اصطلاح NAT-PT مخفف عبارت Network Address Translation-Protocol Translation به معنی "ترجمه آدرس شبکه-ترجمه پروتکل" می باشد.

از مکانیسم NAT-PT می توان برای ارتباط بین شبکه های مبتنی بر IPv4 با شبکه‌های مبتنی بر IPv6 استفاده نمود. در زمانی که مجبور به برقراری ارتباط بین یک شبکه مبتنی بر IPv6 با شبکه‌ای باشید که فقط امکان کار بر اساس IPv4 را دارد، می توانید از مکانیسم ترجمه پروتکل بهره ببرید.

بر خلاف مکانیسم NAT در IPv4 که فقط اقدام به تغییر آدرس مبدا بسته‌های ارسالی به بیرون از شبکه می‌نمود، مکانیسمNAT-PT اقدام به تغییر هر دو آدرس مبدا و مقصد بسته های ارسالی می‌نماید.

پروتکل NDP

پروتکل کشف همسایه NDP(Neighbor Discovery Protocol)، که توسطRFC 4861 منتشر گردیده، عملکردی شبیه پروتکل ARP در IPv4 را برای پروتکل IPv6 فراهم می‌آورد.

هنگامی که یک روتر یا میزبان IPv6 قصد دارد بسته‌ای را به یک میزبان یا روتر دیگر در همان شبکه ارسال نماید، در مرحله اول به Neighbor Database خود رجوع می‌نماید. پایگاه داده همسایه (Neighbor Database) حاوی لیستی از آدرس هایIPv6 همسایه‌ها به همراه آدرس MAC آنها می‌باشد.

اگر روتر یا میزبان آدرس مورد نظر را در Neighbor Database پیدا نکند، با استفاده از پروتکل NDP اقدام به تشخیص آدرس MAC همسایه مورد نظر به صورت پویا می‌نماید.

پروتکل NDP برای انجام عملیات کشف همسایه اقدام به ارسال پیام "درخواست همسایه" یا NS(Neighbor Solicitation) می‌نماید. این پیام که جزء پیام‌های پروتکل ICMPv6 می‌باشد در قالب Multicast در شبکه ارسال می‌گردد.

آدرس مورد استفاده پیام Multicast پروتکلNDP، یک آدرس خاص بوده که Solicited Node Multicast Address نامیده می‌شود. این آدرس با FF02::1:FF:0/104 شروع شده و برای ۲۴ بیت آخر آن نیز دقیقا ۲۴ بیت آخر آدرس IPv6 مورد نظر درج می گردد.

به مثال زیر توجه کنید:

آدرس IPv6 مورد نظر برای دریافت MAC : 2340:1111:AAAA:1:213:19FF:FE7B:5004

آدرس Multicast پیام ارسالی : FF02::1:FF:7B:5004

پیام Multicast ایجاد شده به روش فوق، تحویل تمام Hostهایی می‌شود که ۲۴ بیت آخر آدرس IPv6 آنها مطابق با ۲۴ بیت آخر آدرس Multicast باشد. با توجه به این موضوع، معمولا پیام فقط به دست مقصد مورد نظر می‌رسد.

پیام NS شامل سوالی درباره آدرس MAC مقصد مورد نظر می‌باشد. دریافت کننده پیام، آدرس IPv6 موجود در پیام NS را با آدرس خود مقایسه می‌نمایند. اگر این آدرس‌ها با یکدیگر مطابقت نداشته باشد، پیام دریافتی را دور انداخته و در غیر اینصورت با ارسال پیام NA(Neighbor Advertisement) در قالب Unicast به آدرس درخواست کننده، آدرس MAC خود را به همراه آدرس IPv6 به اطلاع آن می‌رساند.

در نهایت درخواست کننده پس از دریافت پیامNA که جزء پیام‌های پروتکلICMPv6 می‌باشد، آدرس MAC و IPv6 موجود در پیام را در جدول Neighbor Database خود ذخیره کرده و در ارجاعات بعدی از آن استفاده می‌نماید.

تشخیص آدرس تکراری (DAD)

مکانیسم تشخیص آدرس تکراری DAD(Duplicate Address Detection)، برای جلوگیری از ایرادات حاصل شده از انتخاب آدرس تکراری مورد استفاده قرار می‌گیرد.

زمانی که یک اینترفیس اقدام به یادگیری یک آدرس IPv6 می‌نماید و یا اینکه اینترفیس پس از راه اندازی مجدد می خواهد شروع به کار کند، از مکانیسم DAD استفاده می‌کند. این مکانیسم به میزبان کمک می‌کند تا به بررسی منحصر بفرد بودن آدرس خود در شبکه بپردازد.

مکانیسم DAD شبیه پروتکل NDP، برای بررسی آدرس مورد نظر خود از پیامNS (البته با اندکی تغییر) استفاده می‌نماید. این پیام در قالب Multicast به آدرس ایجاد شده بر اساس Solicited Node Multicast Address ارسال می‌شود. با این تفاوت که در مکانیسم DAD آدرس Solicited Node Multicast Address بر اساس آدرس خود میزبان ایجاد می‌گردد.

روش‌های تخصیص آدرس در IPv6

پروتکل IPv6 جهت تخصیص آدرس به میزبان‌های شبکه از روش‌های مختلفی پشتیبانی می‌نماید. بعضی از این روش‌ها شبیه روش‌های IPv4 و بعضی دیگر متفاوت با آن می‌باشد.

فرآیند تخصیص آدرس در IPv6 ممکن است به دو بخش تقسیم شود: تخصیص Prefix و تخصیص Interface ID.

در ادامه به شرح مختصری درباره انواع روش‌های تخصیص آدرس در IPv6 می‌پردازیم.

- **Stateful DHCP**

میزبانIPv6 می‌تواند همانند میزبانIPv4 از حالتStateful DHCP برای دریافت آدرس بهره ببرد. در این حالت میزبان با ارسال یک پیام Multicast درخواست خود را جهت دریافت آدرسIP اعلام می‌دارد. سپس سرور DHCP اقدام به تخصیص آدرس IP به میزبان درخواست کننده می‌نماید. همچنین معرفی Default Gateway و DNS نیز بر عهده سرور DHCP می‌باشد.

آدرس پیام Multicast ارسالی برای سرور DHCP برابر FF00::/8 می‌باشد.

- **Stateless autoconfiguration**

دومین روش تخصیص آدرس بصورت پویا، با استفاده از خصوصیت توکار موجود درIPv6 با نام Stateless autoconfiguration می‌باشد که توسط RFC 2462 منتشر گردیده است. این روش به میزبان اجازه می‌دهد تا بصورت خودکار اقدام به یادگیری قسمت‌های اصلی آدرس شامل اطلاعات Prefix، آدرس Default Gateway و آدرس سرور DNS نماید.

در روش Stateless autoconfig، میزبان برای یادگیری موارد فوق اقدام به طی سه گام زیر می‌نماید: در گام اول با استفاده از پروتکل NDP و پیام های Router Solicitation و Router Advertisement، اقدام به یادگیری Prefix و Default Route می‌نماید. در گام دوم، اقدام به محاسبه آدرس Interface ID خود بر اساس مکانیسم EUI-64 نموده و نهایتا در گام سوم اقدام به یادگیری آدرس سرور DNS از طریق سرور Stateless DHCP می‌نماید.

لازم به ذکر است که سرورStateless DHCP بر خلاف Stateful DHCP از اختصاص آدرس به میزبان‌ها و نگهداری اطلاعات مربوط آنها خودداری نموده و فقط اطلاعات مفیدی مثل آدرس سرورDNS را به اطلاع میزبان درخواست کننده می‌رساند.

- **Static configuration**

در روش Static configuration مدیر شبکه اقدام به اختصاص آدرس بصورت دستی برای میزبان می‌نماید. در این روش اختصاص هر ۱۲۸ بیت آدرس IPv6 بر عهده مدیر شبکه خواهد بود. اما در صورتیکه مدیر شبکه اطلاعات مورد نیاز دیگر را بصورت دستی بر روی میزبان پیکربندی ننماید، می توان از پروتکل NDP برای مشخص کردن Default Route و ازStateless DHCP برای دریافت آدرس DNS استفاده نمود.

- **Static configuration with EUI-64**

در روش Static configuration with EUI-64، نحوه اختصاص آدرس شبیه حالت قبلی بوده با این تفاوت که در این روش مدیر شبکه فقط اقدام به تخصیص ۶۴ بیت آدرس Prefix به صورت دستی نموده و تخصیص ۶۴ بیت مربوط به Interface ID را بر عهده مکانیزم EUI-64 می‌گذارد.

در این روش نیز می‌توان در صورت نیاز از پروتکلNDP برای مشخص کردن Default Route و از سرورStateless DHCP برای یادگیری آدرس سرور DNS استفاده نمود.

Static Route

پروتکلIPv6 امکان استفاده از هر دو نوع پروتکل‌های مسیریابی Static و Dynamic را دارد. اما همانند IPv4 استفاده از مسیریابی Static باعث کاهش استفاده از منابع روتر و شبکه گردیده ولی در عین حال باعث افزایش سربار مدیریتی و از دست دادن برخی ویژگی‌های پیشرفته نیز خواهد شد.

نوشتن Static Route در پروتکل IPv6 با اندکی تغییر شبیه IPv4 می‌باشد. دستور Static Route در پروتکل IPv6 برای تجهیزات سیسکو در زیر نمایش داده شده است.

ipv6 route *ipv6-prefix* **/** *prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* |**unicast**| **multicast**] [**tag** *tag*]

Static Default Route

همانطور که به یاد دارید درIPv4 برای نوشتن Static Default Route از بیت های 0 متوالی استفاده می‌کردیم. به اینصورت که با نوشتن 0.0.0.0 0.0.0.0 برای آدرس و NET Mask، مشخص می کردیم هر آدرسی که متناظری در جدول مسیریابی ندارد به سمت Default Route هدایت شود.

در IPv6 نیز از صفرهای متوالی برای هر ۱۲۸ بیت آدرس استفاده کرده ولی به جای نوشتن NET Mask از Prefix با مقدار 0 استفاده می نماییم.

IPv6 Default Route==> ::/0

استاندارد NPTv6

سازمان IETF اقدام به معرفی استاندارد RFC 6296 جهت ترجمه آدرس های IPv6 به IPv6، نموده است. این استاندارد که NPTv6(Network Prefix Translation) نامیده می‌شود[۱] بر خلاف مکانیسم NAT در IPv4 که آدرس را بصورت کامل ترجمه می‌کرد، فقط اقدام به ترجمه Prefix آدرس های IPv6 می‌نماید.

البته IETF به دلایل گفته شده در بخش پنجم RFC 2993، استفاده از NPTv6 را توصیه نمی‌کند. ولی در عین حال برای مواردی که نیاز به ترجمه آدرس شبکه می‌باشد، مکانیسم NPTv6 در دسترس قرار داده شده است.

مکانیسم NAT در IPv4 بصورت Stateful عمل می‌نماید ولی عملکرد مکانیزم NPTv6 به صورت Stateless است.

در زمان استفاده از NPTv6 به نکات زیر توجه داشته باشید:

- فواید امنیتی که ممکن است در NAT برای IPv4 وجود داشته باشد، در پروتکل NPTv6 در دسترس نمی‌باشد. به همین دلیل در صورتی که بخواهید همان فواید امنیتی را در NPTv6 نیز در اختیار داشته باشید نیاز به وجود یک Firewall خواهید داشت.
- علیرغم اینکه مکانیسم NPTv6 دارای آدرس‌های Inside و Outside می‌باشد، امکان برقراری ارتباط End-to-end در این پروتکل همچنان مُهیا می‌باشد.
- از آنجائیکه درNPTv6 ترجمه آدرس بصورت یک به یک انجام می‌شود، نیازی به تغییر شماره پورت و یا سایر پارامترهای Transport نمی‌باشد.
- در ارتباطات مبتنی برTCP که در آن شناسایی همسایه با استفاده از ویژگی TCP Authentication انجام می‌پذیرد، به علت کاربرد آدرس در محاسبه کد پیام تایید، استفاده از NPTv6 امکان پذیر نیست.

---

[۱] البته در برخی مستندات فنی از این مکانیسم با نام NAT66 نیز نام برده می شود.

سناریو شماره(۱۵): IPv6 Static Route

طرح مسئله:

سناریو شماره ۹ را که هنوز به یاد دارید!

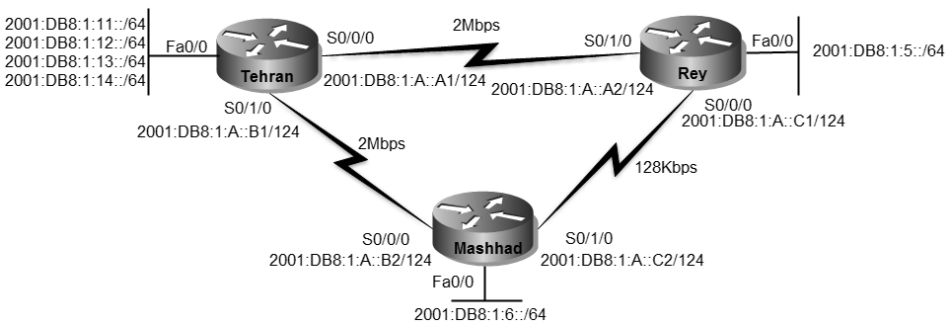
کمپانی MTR Electronics یک شرکت بزرگ است که ساختمان مرکزی آن در تهران بوده و دارای ۲ ساختمان دیگر در شهرری و مشهد مقدس می‌باشد. این شرکت برای برقراری ارتباط بین ساختمان‌های مختلف، از شما کمک خواسته است.

ساختمان تهران دارای ۴ زیر شبکه و ساختمان‌های ری و مشهد هر کدام دارای یک شبکه می‌باشند. لینک های مخابراتی بین تهران با شهرری و مشهد دارای 2Mb پهنای باند می‌باشند. همچنین یک لینک مخابراتی پشتیبان نیز بین شهرری و مشهد برقرار می باشد که دارای 128Kb پهنای باند است.

دقیقا همان سناریو را این بار می خواهیم بر اساس IPv6 انجام دهیم.

نیاز سنجی:

برای برقراری ارتباط بین ساختمان‌ها در شهرهای مختلف، شرکت نیاز به اجاره خطوط مخابراتی و خرید ۳ روتر با کارت های مربوطه دارد.



قبل از اجرای سناریو، اقدام به تخصیص آدرسIP به شبکه‌ها می‌نماییم. پس از مشخص شدن آدرس‌ها، شبکه به صورت فوق خواهد بود. البته در واقعیت زیر شبکه سازی برای قسمت های مختلف سازمان باید بر اساس رنج آدرس اختصاص یافته توسط ISP به شرکت شما انجام پذیرد تا مشکلی در ارتباط با اینترنت نداشته باشید.

راه حل:

پس از پیکربندی اولیه روترها، اقدام به پیکربندی روتر تهران می‌نماییم. به دلیل اینکه از یک اینترفیس روتر برای Inter-VLAN Routing استفاده می‌کنیم، باید اینترفیس روتر را به صورت Subinterface پیکربندی نماییم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface fastEthernet 0/0
Tehran(config-if)#no shutdown
Tehran(config-if)#interface fastethernet 0/0.2
Tehran(config-subif)#encapsulation dot1Q 2
Tehran(config-subif)#ipv6 address 2001:DB8:1:11::1/64
Tehran(config-subif)#interface fastethernet 0/0.3
Tehran(config-subif)#encapsulation dot1Q 3
Tehran(config-subif)#ipv6 address 2001:DB8:1:12::1/64
Tehran(config-subif)#interface fastethernet 0/0.4
Tehran(config-subif)#encapsulation dot1Q 4
Tehran(config-subif)#ipv6 address 2001:DB8:1:13::1/64
Tehran(config-subif)#interface fastethernet 0/0.5
Tehran(config-subif)#encapsulation dot1Q 5
Tehran(config-subif)#ipv6 address 2001:DB8:1:14::1/64
Tehran(config-subif)#^Z
Tehran#write
```

همانطور که ملاحظه می کنید تفاوت خاصی بین پیکربندی IPv6 با IPv4 نمی‌باشد. فقط اینکه به جای دستور ip address باید از دستور ipv6 address استفاده نمایید.

پس از پیکربندی Subinterfaceهای روتر تهران، اقدام به پیکربندی پورت‌های سریال روتر تهران می‌کنیم.

```
Tehran(config)#interface serial 0/0/0
Tehran(config-if)#no shutdown
Tehran(config-if)#clock rate 2000000
Tehran(config-if)#bandwidth 2000
Tehran(config-if)#ipv6 address 2001:DB8:1:A::A1/124
Tehran(config-if)#interface serial 0/1/0
Tehran(config-if)#no shutdown
Tehran(config-if)#clock rate 2000000
Tehran(config-if)#bandwidth 2000
Tehran(config-if)#ipv6 address 2001:DB8:1:A::B1/124
Tehran(config-if)#
```

به دلیل استفاده بهینه از رنج آدرس‌های IP، برای لینک‌های سریال از Prefix با طول 124 استفاده می‌نماییم.

حالا نوبتی هم که باشه نوبت به روترهای شهرری و مشهد می رسد:

```
Rey>enable
Rey#configure terminal
Rey(config)#interface fastEthernet 0/0
Rey(config-if)#no shutdown
Rey(config-if)#ipv6 address 2001:DB8:1:5::1/64
Rey(config-if)#interface serial 0/0/0
Rey(config-if)#no shutdown
Rey(config-if)#bandwidth 128
Rey(config-if)#clock rate 128000
Rey(config-if)#ipv6 address 2001:DB8:1:A::C1/124
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#no shutdown
Rey(config-if)#bandwidth 2000
Rey(config-if)#ipv6 address 2001:DB8:1:A::A2/124
Rey(config-if)#^Z
Rey#write
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#ipv6 address 2001:DB8:1:6::1/64
Mashhad(config-if)#interface serial 0/0/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#bandwidth 2000
Mashhad(config-if)#ipv6 address 2001:DB8:1:A::B2/124
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#no shutdown
Mashhad(config-if)#bandwidth 128
Mashhad(config-if)#ipv6 address 2001:DB8:1:A::C2/124
Mashhad(config-if)#^Z
Mashhad#write
```

هر چند که پیکربندی روترها تمام شد ولی نمی‌توان هیچ یک از شبکه‌های متصل به دیگر روترها را ping نمود. به همین دلیل باید اقدام به راه اندازی یک پروتکل مسیریابی نماییم. در این سناریو نیت کردیم تا از مسیریابی بصورت Static استفاده نماییم.

```
Tehran(config)#ipv6 unicast-routing
Tehran(config)#ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::A2
```

```
Tehran(config)#ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::B2 5
Tehran(config)#ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::B2
Tehran(config)#ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::A2 5
```

توسط دستور ipv6 unicast-routing، امکان مسیریابیIPv6 را در روتر فعال می‌کنیم. همانطور که مشاهده می‌فرمایید در نوشتن Static Route نیز تفاوت اندکی بین IPv4 با IPv6 می‌باشد. در این سناریو هم می‌توانیم با نوشتن مسیرهایی با AD متفاوت به صورت دستی، اقدام به ایجاد لینک پشتیبان برای مسیرهای مختلف نماییم.

```
Rey(config)#ipv6 unicast-routing
Rey(config)#ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::A1
Rey(config)#ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::C2 5
Rey(config)#ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::C2
Rey(config)#ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::A1 5
```

در نوشتن مسیرهای مربوط به روتر تهران اقدام به خلاصه نویسی کرده و به جای نوشتن چهار خط مسیر، تنها با یک خط Route شبکه های متصل به روتر تهران را مشخص نمودیم.

```
Mashhad(config)#ipv6 unicast-routing
Mashhad(config)#ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::B1
Mashhad(config)#ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::C1 5
Mashhad(config)#ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::C1
Mashhad(config)#ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::B1 5
```

پس از انجام مراحل فوق، در صورتی که توسط هر کدام از روترها اقدام به ping شبکه‌های دیگر نماییم، خروجی خوشحال کننده زیر را خواهیم دید:

```
Mashhad#ping 2001:db8:1:11::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:11::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/9/29 ms

Mashhad#
Mashhad#ping 2001:db8:1:14::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:14::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/11/34 ms

Mashhad#ping 2001:db8:1:5::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:5::1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/19 ms

Mashhad#
```

طریقه عملکرد:

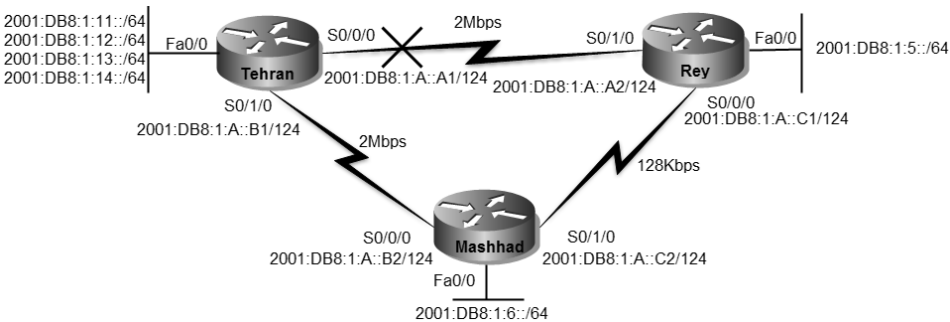
برای بررسی جداول مسیریابی روترها از دستور show ipv6 route استفاده می‌نماییم:

```
Tehran#show ipv6 route
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2001:DB8:1:5::/64 [1/0]
    via 2001:DB8:1:A::A2
S   2001:DB8:1:6::/64 [1/0]
    via 2001:DB8:1:A::B2
C   2001:DB8:1:A::A0/124 [0/0]
    via ::, Serial0/0/0
L   2001:DB8:1:A::A1/128 [0/0]
    via ::, Serial0/0/0
C   2001:DB8:1:A::B0/124 [0/0]
    via ::, Serial0/1/0
L   2001:DB8:1:A::B1/128 [0/0]
    via ::, Serial0/1/0
C   2001:DB8:1:11::/64 [0/0]
    via ::, FastEthernet0/0.2
L   2001:DB8:1:11::1/128 [0/0]
    via ::, FastEthernet0/0.2
C   2001:DB8:1:12::/64 [0/0]
    via ::, FastEthernet0/0.3
L   2001:DB8:1:12::1/128 [0/0]
    via ::, FastEthernet0/0.3
C   2001:DB8:1:13::/64 [0/0]
    via ::, FastEthernet0/0.4
L   2001:DB8:1:13::1/128 [0/0]
    via ::, FastEthernet0/0.4
C   2001:DB8:1:14::/64 [0/0]
    via ::, FastEthernet0/0.5
L   2001:DB8:1:14::1/128 [0/0]
    via ::, FastEthernet0/0.5
L   FF00::/8 [0/0]
    via ::, Null0
Tehran#
```

شبکه‌هایی که بصورت مستقیم به روتر متصل هستند با حرف "C" نمایش داده می‌شوند. همچنین مسیرهایی که به صورت Static به جدول مسیریابی روتر افزوده شده با حرف "S" نشان داده می‌شود. حرف "L" نیز نمایش دهنده آدرس‌هایی می‌باشد که بر روی خود روتر پیکربندی گردیده است.

همانطور که ملاحظه می کنید در جدول مسیریابی خبری از مسیرهای با AD بالاتر نیست، به دلیل اینکه جدول مسیریابی همواره شامل بهترین مسیرهای موجود می‌باشد.

فرض کنید لینک مستقیم شهرری با تهران قطع شود، آنوقت چه تغییری در جدول مسیریابی روتر تهران پیش خواهد آمد؟



واضح است که پس از قطع لینک مستقیم تهران با شهرری، روتر اقدام به درج مسیری که دارای AD بالاتری نسبت به مسیر قبلی بوده در جدول مسیریابی خود می‌نماید. خروجی دستور show ipv6 route بر روی تهران مبین این امر خواهد بود:

```
Tehran#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2001:DB8:1:5::/64 [5/0]
    via 2001:DB8:1:A::B2
S   2001:DB8:1:6::/64 [1/0]
    via 2001:DB8:1:A::B2
C   2001:DB8:1:A::B0/124 [0/0]
    via ::, Serial0/1/0
L   2001:DB8:1:A::B1/128 [0/0]
    via ::, Serial0/1/0
C   2001:DB8:1:11::/64 [0/0]
    via ::, FastEthernet0/0.2
L   2001:DB8:1:11::1/128 [0/0]
    via ::, FastEthernet0/0.2
C   2001:DB8:1:12::/64 [0/0]
    via ::, FastEthernet0/0.3
L   2001:DB8:1:12::1/128 [0/0]
    via ::, FastEthernet0/0.3
C   2001:DB8:1:13::/64 [0/0]
    via ::, FastEthernet0/0.4
L   2001:DB8:1:13::1/128 [0/0]
    via ::, FastEthernet0/0.4
```

```
C   2001:DB8:1:14::/64 [0/0]
    via ::, FastEthernet0/0.5
L   2001:DB8:1:14::1/128 [0/0]
    via ::, FastEthernet0/0.5
L   FF00::/8 [0/0]
    via ::, Null0
Tehran#
```

مرجع دستور Command Reference:

Configure IPv6		
	Command or Action	**Purpose**
Step 1	enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	interface *type number* Example: Router(config)# interface ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 address** *ipv6-prefix/prefix-length* eui-64 **or** **ipv6 address** *ipv6-address/prefix-length* link-local **or** **ipv6 address** *ipv6-prefix/prefix-length* anycast **or** ipv6 enable Example: Router(config-if)# ipv6 address 2001:DB8:0:1::/64 eui-64 or Example: Router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local or Example: Router(config-if) ipv6 address 2001:DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast or Example: Router(config-if)# ipv6 enable	Specifies an IPv6 network assigned to the interface and enables IPv6 processing on the interface. or Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface. or Automatically configures an IPv6 link-local address on the interface while also enabling the interface for IPv6 processing. The link-local address can be used only to communicate with nodes on the same link. • Specifying the ipv6 address eui-64command configures global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. Only the 64-bit network prefix for the address needs to be specified; the last 64 bits are automatically computed from the interface ID. • Specifying the ipv6 address link-localcommand configures a link-local address on the interface that is used instead of the link-local address that is

Configure IPv6		
		automatically configured when IPv6 is enabled on the interface. • Specifying the ipv6 address anycastcommand adds an IPv6 anycast address.
Step 5	exit Example: Router(config-if)# exit	Exits interface configuration mode, and returns the router to global configuration mode.
Step 6	ipv6 unicast-routing Example: Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

Configuring a Static IPv6 Route		
	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**ipv6 route** *ipv6-prefix* **/** *prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*] **Example:** Device(config)# ipv6 route ::/0 serial 2/0	Configures a static IPv6 route. A static default IPv6 route is being configured on a serial interface. See the syntax examples that immediately follow this table for specific uses of the **ipv6 route**command for configuring static routes.

Verifying Static IPv6 Route Configuration and Operation		
	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Do one of the following: **show ipv6 static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*][**interface** *interface-typeinterface-number*] [**recursive**] [**detail**] **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-typeinterface-number*	Displays the current contents of the IPv6 routing table. These examples show two different ways of displaying IPv6 static routes. Refer to the **show ipv6 static** and **show ipv6 route** command entries in the Cisco IOS IPv6 Command Reference for more details on the arguments and keywords used in this command.

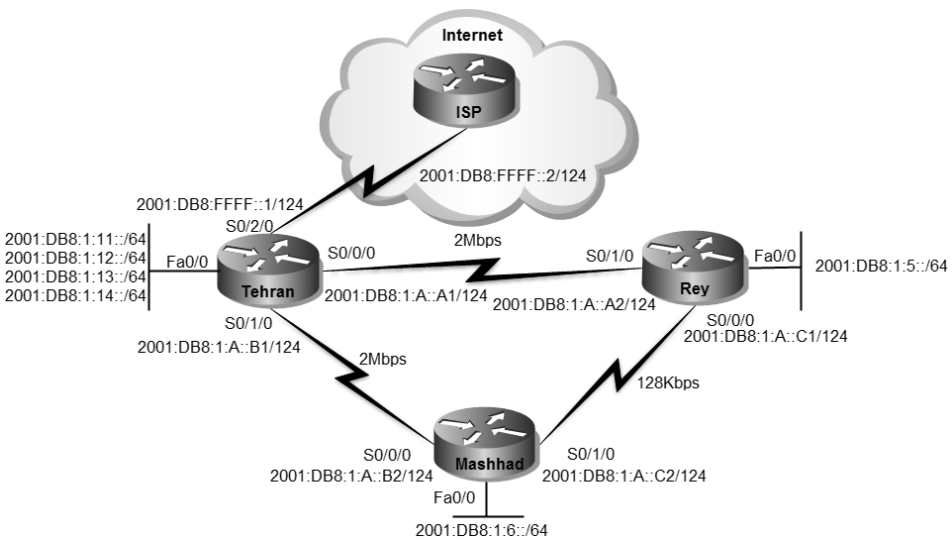
سناریو شماره(۱۶): IPv6 Static Default Route

طرح مسئله:

شرکت MTR اقدام به دریافت یک لینک اینترنت برای شعبه تهران نموده و می‌خواهد تمام کلاینت های تهران، مشهد و شهرری بتوانند به اینترنت دسترسی داشته باشند.

نیاز سنجی:

در قدم اول نیاز به یک کارت WIC برای اتصال روتر تهران به اینترنت داریم. همچنین برای دسترسی به اینترنت نیاز به داشتن Default Route به سمت لینک متصل به اینترنت داریم.



نکته: همانطور که در مبحث سوم فصل دو گفته شد، رنج آدرس 2001:DB8::/32 توسط IANA برای مستندات فنی رزرو گردیده و قابل مسیریابی در اینترنت نمی باشد. این رنج صرفا برای سناریوها استفاده شده و در دنیای واقعی باید زیر شبکه سازی سازمان خود را بر اساس رنج دریافتی از ISP انجام دهید.

راه حل:

در اولین گام باید به پیکربندی اینترفیس متصل به ISP بپردازیم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#interface serial 0/2/0
Tehran(config-if)#no shutdown
Tehran(config-if)#ipv6 address 2001:DB8:FFFF::1/124
Tehran(config-if)#^Z
Tehran#
```

پس از پیکربندی اینترفیس متصل به ISP، باید اقدام مشخص نمودن Default Route برای روترها نماییم:

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#ipv6 route ::/0 2001:DB8:FFFF::2
Tehran(config)#^Z
Tehran#
```

نحوه نوشتن Default Route در IPv6 نیز شبیه IPv4 می‌باشد. در این حالت برای آدرس و Prefix از عدد "0" استفاده می‌نماییم.

دستور Default Route را در روترهای شهرری و مشهد نیز باید اعمال نماییم:

```
Rey>enable
Rey#configure terminal
Rey(config)#ipv6 route ::/0 2001:DB8:1:A::A1
Rey(config)#ipv6 route ::/0 2001:DB8:1:A::C2 5
Rey(config)#^Z
Rey#
```

برای در اختیار داشتن Redundancy البته به صورت دستی! اقدام به نوشتن دو Static Default Route با ADهای مختلف نمودیم.

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ipv6 route ::/0 2001:DB8:1:A::B1
Mashhad(config)#ipv6 route ::/0 2001:DB8:1:A::C1 5
Mashhad(config)#^Z
Mashhad#
```

پس از انجام مراحل فوق در صورتیکه اقدام به ping یک میزبان را بر روی اینترنت نماییم، به آن دسترسی خواهیم داشت. به عنوان مثال اقدام به ping وب سایت سیسکو با آدرس 2001:420:1101:1::A بر روی اینترنت می‌نماییم:

```
Mashhad#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/15/27 ms
```

```
Rey#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/10/13 ms
```

طریقه عملکرد:

عملکرد Static Default Route در IPv6 تفاوت خاصی با IPv4 ندارد. در صورتیکه روتر متناظری برای آدرس مقصد بسته دریافتی در جدول مسیریابی خود پیدا نکند، اقدام به تحویل آن به آدرس Default Route می‌نماید. در غیر اینصورت بسته توسط روتر دور انداخته می‌شود.

برای دیدن آدرس Default Static Route می‌توانید از دستور show ipv6 route استفاده نمایید:

```
Mashhad#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
    via 2001:DB8:1:A::B1
S   2001:DB8:1:5::/64 [1/0]
    via 2001:DB8:1:A::C1
C   2001:DB8:1:6::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:DB8:1:6::1/128 [0/0]
    via ::, FastEthernet0/0
C   2001:DB8:1:A::B0/124 [0/0]
```

```
   via ::, Serial0/0/0
L  2001:DB8:1:A::B2/128 [0/0]
   via ::, Serial0/0/0
C  2001:DB8:1:A::C0/124 [0/0]
   via ::, Serial0/1/0
L  2001:DB8:1:A::C2/128 [0/0]
   via ::, Serial0/1/0
S  2001:DB8:1:10::/60 [1/0]
   via 2001:DB8:1:A::B1
L  FF00::/8 [0/0]
   via ::, Null0
Mashhad#
```

همانطور که در خروجی فوق مشاهده می نمایید، مسیر Static Default Route با AD بهتر در جدول مسیریابی قرار داده شده است. حال اگر لینک مستقیم بین مشهد و تهران قطع گردد، جدول مسیریابی به صورت زیر تغییر خواهد نمود:

```
Mashhad#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
     U - Per-user Static route, M - MIPv6
     I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
     O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
     ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
     D - EIGRP, EX - EIGRP external
S  ::/0 [5/0]
   via 2001:DB8:1:A::C1
S  2001:DB8:1:5::/64 [1/0]
   via 2001:DB8:1:A::C1
C  2001:DB8:1:6::/64 [0/0]
   via ::, FastEthernet0/0
L  2001:DB8:1:6::1/128 [0/0]
   via ::, FastEthernet0/0
C  2001:DB8:1:A::C0/124 [0/0]
   via ::, Serial0/1/0
L  2001:DB8:1:A::C2/128 [0/0]
   via ::, Serial0/1/0
S  2001:DB8:1:10::/60 [5/0]
   via 2001:DB8:1:A::C1
L  FF00::/8 [0/0]
   via ::, Null0
Mashhad#
```

به‌دلیل قطع شدن لینک مستقیم مشهد و تهران، لینک مشهد و شهرری جایگزین مسیر قبلی گردیده است. در این حالت ضمن در دسترس بودن شبکه‌های تهران، دسترسی به اینترنت نیز برای روتر مشهد برقرار می‌باشد.

```
Mashhad#ping ipv6 2001:db8:1:11::1 source fastEthernet 0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:11::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Mashhad#ping ipv6 2001:420:1101:1::a source fastEthernet 0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 20 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/20/4 ms
```

البته همانطور که از سناریوهای IPv4 به یاد دارید، باید از ping در حالت Extended برای بررسی لینک پشتیبان استفاده نماییم. این اتفاق به دلیل آن است که آدرس مربوط به لینک‌های WAN بین هر زوج روتر در جدول مسیریابی روتر دیگر وجود ندارد.

نحوه استفاده از ping در حالت Extended در پروتکل های IPv4 با IPv6 متفاوت می باشد. برای دریافت راهنمایی استفاده بهتر از این دستور در تجهیزات سیسکو می توانید از "?" استفاده نمایید.

مرجع دستور Command Reference :

Configuring a Static IPv6 Route		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ipv6 route** *ipv6-prefix***/***prefix-length*{*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* |**unicast** | **multicast**] [**tag** *tag*] **Example:** Router(config)# ipv6 route ::/0 serial 2/0	Configures a static IPv6 route. • A static default IPv6 route is being configured on a serial interface. • See the syntax examples that immediately follow this table for specific uses of the **ipv6 route** command for configuring static routes.

Verifying Static IPv6 Route Configuration and Operation		
	Command or Action	**Purpose**
Step 1	**enable**	Enables privileged EXEC mode.
Step 2	**show ipv6 static** [*ipv6-address* |*ipv6-prefix*/*prefix-length*][**interface***interface-type interface-number*] [**recursive**] [**detail**] or **show ipv6 route** [*ipv6-address* |*ipv6-prefix*/*prefix-length* | *protocol*| *interface-type interface-number*] **Example:** Router# show ipv6 static or **Example:** Router# show ipv6 route static	Displays the current contents of the IPv6 routing table. • These examples show two different ways of displaying IPv6 static routes.
Step 3	**debug ipv6 routing** **Example:** Router# debug ipv6 routing	Displays debugging messages for IPv6 routing table updates.

☑ مبحث دوم

پروتکل RIPng

پروتکل RIPng(RIP next generation)، نسل جدید پروتکل مسیریابیRIP می‌باشد که سازمان IETF آن را اواسط دهه ۱۹۹۰ میلادی طی استاندارد RFC 2080 برای کار در شبکه‌های مبتنی بر IPv6 ارائه نموده است.

پروتکل RIPng بر پایه RIPv2 ایجاد گردیده و عملکردی شبیه به همان پروتکل را در محیط IPv6 فراهم نموده است. در جدول زیر به مقایسه بین این دو نسخه پرداخته ایم.

ویژگی	پروتکل RIPv2	پروتکل RIPng
پروتکل مورد استفاده در لایه ۳	IPv4	IPv6
پروتکل و پورت مورد استفاده در لایه ۴	UDP 520	UDP 521
زیر مجموعه Distance Vector	بلی	بلی
مقدار پیش فرض Administrative Distance	120	120
پشتیبانی از VLSM	بلی	بلی
خلاصه سازی اتوماتیک	بلی	خیر
استفاده از Split Horizon / Poison Revers	بلی	بلی
ارسال پیام های متناوب Full Update	هر ۳۰ ثانیه	هر ۳۰ ثانیه
ارسال Trigged Update	بلی	بلی
استفاده Metric از Hop Count	بلی	بلی
حداکثر تعداد گام (Hop) یا روتر در شبکه	۱۵ گام	۱۵ گام
آدرس Multicast مورد استفاده	224.0.0.9	FF02::9
نوع Authentication	MD5	IPv6 AH/ESP

پروتکل RIPng نیز همانند نسخه RIPv2 دارای محدودیت در تعداد روترهای مورد استفاده در شبکه می‌باشد. از این پروتکل در شبکه‌های کوچکی می توان استفاده نمود که حداکثر دارای تعداد ۱۵ روتر باشد.

زمان سنج‌ها

در این بخش قصد داریم به توصیف زمان سنج(Timer)های مورد استفاده در پروتکل RIPng بپردازیم:

- **Periodic Timer**

پروتکل RIPng هر ۳۰ ثانیه یک بار به صورت متناوب اقدام به ارسال پیام های Full Update به روترهای همسایه خود می‌نماید.

- **Time out**

زمان سنج Time out دارای مقدار ۱۸۰ ثانیه می‌باشد. هر مسیر ثبت شده در جدول مسیریابی دارای فیلد Time out بوده و در صورتیکه تا اتمام این زمان سنج یعنی پس از ۱۸۰ ثانیه هیچ پیام بروز رسانی حاوی این مسیر دریافت نشود، مسیر مورد نظر از درجه اعتبار ساقط شده و دیگر توسط روتر مورد استفاده قرار نمی‌گیرد.

- **Garbage-Collection Timer**

همانطور که گفته شده پس از پایان مدت زمان Time out روتر دیگر از مسیر مورد نظر استفاده نمی‌نماید ولی تا پایان مدت زمان Garbage-Collection Timer مسیر را بصورت غیر فعال در جدول مسیریابی نگه می‌دارد تا روترهای همسایه نیز از خرابی مسیر فوق اطلاع حاصل نمایند. پس از اتمام این مدت زمان که ۱۲۰ ثانیه می‌باشد، روتر مسیر مورد نظر را به طور کامل از جدول مسیریابی خود حذف می‌نماید.

نحوه پیکربندی RIPng

در روترهای سیسکو نحوه پیکربندی پروتکل RIPng با RIP متفاوت می‌باشد. برای فعال سازی این پروتکل باید گام‌های زیر برداشته شود:

۱- ابتدا باید اقدام به فعال سازی مسیریابی بر مبنای IPv6 بر روی روتر نماییم:

Router(config)# ipv6 unicast-routing

۲- دستور زیر نیز باعث فعال سازی RIPng بر روی روتر می‌گردد:

Router(config)# **ipv6 router rip** *name*

باید در زمان راه اندازی پروتکل RIPng برای آن یک نام هم انتخاب نمایید.

توجه داشته باشید در صورتی که مرحله ۱ را انجام نداده باشید، روتر در جواب دستور فوق پیام خطا صادر می‌نماید.

۳- برای فعال سازی IPv6 بر روی اینترفیس‌ها، می توان به دو صورت اقدام نمود. اول اینکه از دستور زیر برای آدرس دهی IPv6 به ازاء هر اینترفیس استفاده نماییم:

Router(config-if)# **ipv6 address** *address/prefix- length*

دومین روش، استفاده از دستور زیر می باشد:

Router(config-if)# ipv6 enable

۴- اگر به یاد داشته باشید، در پروتکلRIP برای تبلیغ شبکه‌های مورد نظر، پس از فعال سازی پروتکل و در همان محیط اقدام به معرفی شبکه‌ها می‌کردیم. اما در RIPng برای معرفی شبکه‌ها باید از طریق اینترفیس‌های مورد نظر اقدام نماییم. برای فعال سازی پروتکل RIPng بر روی اینترفیس می‌توان از دستور زیر استفاده نمود:

Route(config-if)# **ipv6 rip** *name* **enable**

جدول دیتابیس RIPng

روترهایی که پروتکل RIPng بر روی آنها فعال گردیده است، دارای یک جدول دیتابیس جهت انجام فعالیت خود می‌باشند. این جدول برای تمام مقاصدی که برای روتر قابل دسترس می باشند دارای یک Entry بوده که در تصمیم گیری نهایی روتر برای ثبت یک مسیر در جدول مسیریابی موثر می‌باشد. هر Entry حداقل شامل موارد زیر خواهد بود:

- IPv6 Prefix مقصد.
- مقدار Metric که نشان دهنده هزینه کامل دسترسی به مقصد مورد نظر از طریق این روتر می‌باشد. این مقدار مجموع تمام Metricهای مسیر از مبدا تا مقصد می‌باشد. همانطور که می‌دانید پروتکلRIP برای تعیینMetric از تعداد گام یا hop count استفاده می‌نماید.
- آدرسIPv6 روتر بعدی (next hop) برای رسیدن به مقصد مورد نظر. البته اگر مقصد مورد نظر یکی از شبکه‌های متصل شده به خود روتر باشد(Directly Connected)، به این فیلد نیازی نخواهد بود.
- پرچم یا Flag. این Flag مشخص می کند که اطلاعات مربوط به این مسیر، اخیرا تغییر یافته است یا خیر.
- زمان سنج‌های مختلف که همراه هر مسیر خواهد بود. این زمان سنج‌ها در همین مبحث توضیح داده شده است.

برای مشاهده جدول فوق می توانید از دستور show ipv6 rip database استفاده نمایید.

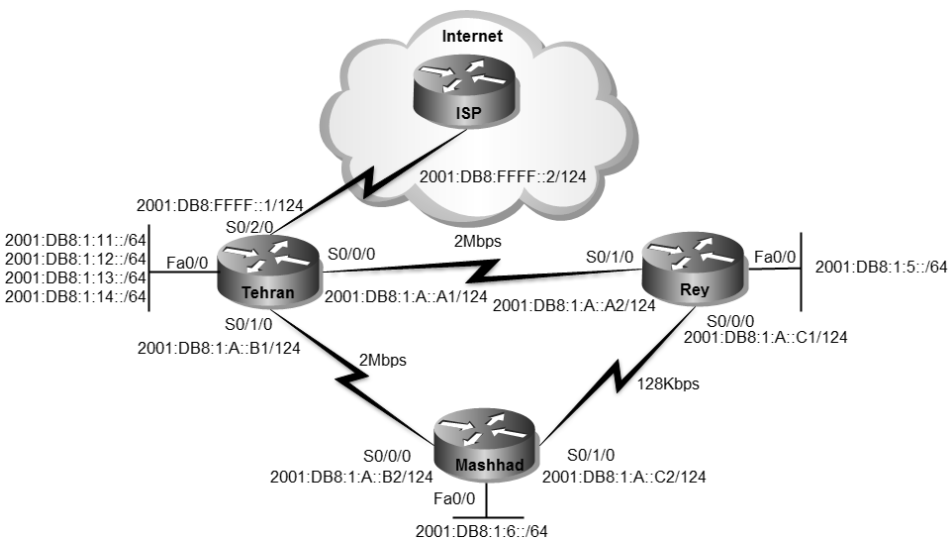
سناریو شماره(۱۷)؛ راه اندازی RIPng

طرح مسئله:

شرکتMTR از شما خواسته تا همانطور که زمان استفاده ازIPv4 برایشان پروتکل مسیریابی پویا راه اندازی کرده بودید، اینبار نیز با توجه به مهاجرت به IPv6 اقدام به راه اندازی یک پروتکل مسیریابی پویا و سازگار با IPv6 نمایید. شما هم با توجه به آموزش این مبحث، می‌خواهید RIPng را در شبکه پیکربندی کنید.

نیاز سنجی:

نیازی نیست جز یک شبکه برای راه اندازی پروتکل، که شکر خدا به راحتی در اختیارمان قرار گرفته است.



راه حل:

در اولین گام باید اقدام به حذف مسیرهای Static اضافه شده در سناریوهای ۱۵ و ۱۶ از روترها نموده تا بتوانیم به خوبی نتیجه راه اندازی پروتکل مسیریابی پویا را بررسی کنیم.

```
Mashhad(config)#no ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::B1
Mashhad(config)#no ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::C1 5
Mashhad(config)#no ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::C1
```

```
Mashhad(config)#no ipv6 route 2001:DB8:1:5::/64 2001:DB8:1:A::B1 5
Mashhad(config)#no ipv6 route ::/0 2001:DB8:1:A::B1
Mashhad(config)#no ipv6 route ::/0 2001:DB8:1:A::C1 5
```

```
Tehran(config)#no ipv6 route ::/0 2001:DB8:FFFF::2
Tehran(config)#no ipv6 route 2001:DB8:1:5::/60 2001:DB8:1:A::A2
Tehran(config)#no ipv6 route 2001:DB8:1:5::/60 2001:DB8:1:A::B2 5
Tehran(config)#no ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::B2
Tehran(config)#no ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::A2 5
```

```
Rey(config)#no ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::A1
Rey(config)#no ipv6 route 2001:DB8:1:10::/60 2001:DB8:1:A::C2 5
Rey(config)#no ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::C2
Rey(config)#no ipv6 route 2001:DB8:1:6::/64 2001:DB8:1:A::A1 5
Rey(config)#no ipv6 route ::/0 2001:DB8:1:A::A1
Rey(config)#no ipv6 route ::/0 2001:DB8:1:A::C2 5
```

حالا نوبت به کار اصلی این پروژه، یعنی راه اندازی پروتکل RIPng رسیده است. همانطور که در این مبحث آموزش داده شد، قبل از هر کاری باید مسیریابی IPv6 را بر روی روتر فعال کنیم.

```
Rey>enable
Rey#configure terminal
Rey(config)#ipv6 unicast-routing
```

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#ipv6 unicast-routing
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ipv6 unicast-routing
```

پس از فعال سازی مسیریابی IPv6، باید اقدام به پیکربندی پروتکل RIPng نمایید. همچنین شبکه‌های مورد نظر جهت تبلیغ توسط RIPng نیز باید مشخص شوند.

```
Tehran(config)#ipv6 router rip MTR
Tehran(config-rtr)#exit
Tehran(config)#interface serial 0/0/0
Tehran(config-if)#ipv6 rip MTR enable
Tehran(config-if)#interface serial 0/1/0
Tehran(config-if)#ipv6 rip MTR enable
Tehran(config-if)#exit
Tehran(config)#interface fastEthernet 0/0.2
```

```
Tehran(config-subif)#ipv6 rip MTR enable
Tehran(config-subif)#interface fastEthernet 0/0.3
Tehran(config-subif)#ipv6 rip MTR enable
Tehran(config-subif)#interface fastEthernet 0/0.4
Tehran(config-subif)#ipv6 rip MTR enable
Tehran(config-subif)#interface fastEthernet 0/0.5
Tehran(config-subif)#ipv6 rip MTR enable
Tehran(config-subif)#^Z
Tehran(config-subif)#write
```

با دستور ipv6 router rip MTR اقدام به راه اندازی پروتکل RIPng بر روی روتر نمودیم. در این نسخه باید برای پروتکل RIPng یک نام نیز تعیین نمایید که ما از نام MTR استفاده کردیم.

برای مشخص کردن شبکه‌هایی که می‌خواهید توسط پروتکل مسیریابی تبلیغ شوند باید از محیط پیکربندی اینترفیس استفاده نموده و با دستور ipv6 rip MTR enable، ضمن فعال سازی، نام پروتکل مورد نظر را نیز برای اینترفیس مشخص نمایید.

```
Rey(config)#ipv6 router rip MTR
Rey(config-rtr)#exit
Rey(config)#interface fastEthernet 0/0
Rey(config-if)#ipv6 rip MTR enable
Rey(config-if)#interface serial 0/0/0
Rey(config-if)#ipv6 rip MTR enable
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#ipv6 rip MTR enable
Rey(config-if)#^Z
Rey#write
```

```
Mashhad(config)#ipv6 router rip MTR
Mashhad(config-rtr)#exit
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#ipv6 rip MTR enable
Mashhad(config)#interface serial 0/0/0
Mashhad(config-if)#ipv6 rip MTR enable
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#ipv6 rip MTR enable
Mashhad(config-if)#^Z
Mashhad#write
```

خروجی دستور ping شبکه های متصل به روترها به صورت زیر خواهد بود:

```
Mashhad#ping 2001:db8:1:11::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:11::1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms

Mashhad#ping 2001:db8:1:12::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:12::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms

Mashhad#ping 2001:db8:1:13::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:13::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/28 ms

Mashhad#
```

در این حالت تمام شبکه‌های متصل به روترها از طریق روتر دیگر قابل دسترس هستند ولی هنوز شبکه های اینترنت در دسترس نیستند. به عنوان مثال اگر سرور سیسکو را ping نمایید، خروجی زیر را خواهید دید:

```
Mashhad#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

برای تبلیغ مسیرDefault Route توسط پروتکلRIPng باید از دستورات زیر استفاده نمایید:

```
Tehran(config)#interface serial 0/1/0
Tehran(config-if)#ipv6 rip MTR default-information originate
Tehran(config-if)#interface serial 0/0/0
Tehran(config-if)#ipv6 rip MTR default-information originate
Tehran(config-if)#exit
Tehran(config)#ipv6 route ::/0 2001:db8:ffff::2
Tehran(config)#^Z
Tehran#write
```

توسط دستور ipv6 rip MTR default-information originate، اینترفیس‌هایی که باید اقدام به تبلیغ Default Route نمایند را مشخص می‌کنیم. همانطور که ملاحظه می‌کنید علیرغم اینکه RIPng جدیدترین نسخه RIP است، ولی نحوه پیکربندی آن در تجهیزات سیسکو روال غیر معمولی نسبت به نسخه‌های پیشین دارد. همچنین توسط دستور ipv6 route ::/0 2001:db8:ffff::2 اقدام به مشخص نمودن Default Route در روتر تهران می‌نماییم.

حالا اگر اقدام به ping سرور سیسکو بر روی اینترنت نمایید، خروجی زیر را مشاهده خواهید نمود:

```
Mashhad#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/31/43 ms
```

```
Rey#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/13/18 ms
```

طریقه عملکرد:

نحوه عملکرد RIPng شبیه به نسخه قبلی خود می‌باشد. پروتکل مسیریابی پویا مسیرهایی را در جدول مسیریابی روتر قرار می‌دهد که بهترین Metric را نسبت به مسیرهای مشابه خود داشته باشند. برای بررسی عملکرد روترها نگاهی به خروجی دستور show ipv6 route می‌اندازیم.

```
Rey#show ipv6 route
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   ::/0 [120/1]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
C   2001:DB8:1:5::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:DB8:1:5::1/128 [0/0]
    via ::, FastEthernet0/0
R   2001:DB8:1:6::/64 [120/2]
    via FE80::2D0:97FF:FE58:ED01, FastEthernet0/0
    via FE80::202:17FF:FEA9:85A, Serial0/0/0
C   2001:DB8:1:A::A0/124 [0/0]
    via ::, Serial0/1/0
L   2001:DB8:1:A::A2/128 [0/0]
    via ::, Serial0/1/0
R   2001:DB8:1:A::B0/124 [120/2]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
```

```
    via FE80::202:17FF:FEA9:85A, Serial0/0/0
    via FE80::2D0:97FF:FE58:ED01, FastEthernet0/0
C   2001:DB8:1:A::C0/124 [0/0]
    via ::, Serial0/0/0
L   2001:DB8:1:A::C1/128 [0/0]
    via ::, Serial0/0/0
R   2001:DB8:1:11::/64 [120/2]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
R   2001:DB8:1:12::/64 [120/2]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
R   2001:DB8:1:13::/64 [120/2]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
R   2001:DB8:1:14::/64 [120/2]
    via FE80::20D:BDFF:FE76:EBEE, Serial0/1/0
L   FF00::/8 [0/0]
    via ::, Null0
Rey#
```

مسیرهای به دست آمده توسط پروتکل مسیریابی RIPng در جدول مسیریابی با حرف R نشان داده شده است. روتر شهرری شبکه‌های متصل به روتر تهران و روتر مشهد که توسط پروتکلRIP تبلیغ شده‌اند را یاد گرفته است.

نکته قابل توجه در خروجی فوق، آدرس Default Route می‌باشد. با نوشتن حرفR در ابتدای این مسیر، مشخص می شود که از طریق پروتکل RIPng به دست آمده است. اما اگر توجه کنید آدرسIPv6 که Default Route به آن مسیردهی شده FE80::20D:BDFF:FE76:EBEE, Serial0/1/0 می‌باشد. اگر به یاد داشته باشید آدرس رنج FE80::/64 به عنوان آدرس‌های Link-Local تعیین شده است. جدول مسیریابی نیز برای مشخص کردن مسیر Default Route از آدرس Link-Local مربوط به اینترفیس مورد نظر استفاده می‌نماید.

در گام بعدی برای بررسی پویا بودن مسیریابی، اقدام به قطع اتصال مستقیم بین تهران و شهرری می‌نماییم. در این صورت خروجی show ipv6 route روتر شهرری به صورت زیر تغییر خواهد کرد:

```
Rey#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
     U - Per-user Static route, M - MIPv6
     I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
     O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
     ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
     D - EIGRP, EX - EIGRP external
R   ::/0 [120/2]
       via FE80::202:17FF:FEA9:85A, Serial0/0/0
C   2001:DB8:1:5::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:DB8:1:5::1/128 [0/0]
```

```
   via ::, FastEthernet0/0
R  2001:DB8:1:6::/64 [120/2]
      via FE80::202:17FF:FEA9:85A, Serial0/0/0
R  2001:DB8:1:A::A0/124 [120/3]
   via FE80::2D0:97FF:FE58:ED01, FastEthernet0/0
R  2001:DB8:1:A::B0/124 [120/2]
   via FE80::2D0:97FF:FE58:ED01, FastEthernet0/0
   via FE80::202:17FF:FEA9:85A, Serial0/0/0
C  2001:DB8:1:A::C0/124 [0/0]
   via ::, Serial0/0/0
L  2001:DB8:1:A::C1/128 [0/0]
   via ::, Serial0/0/0
R  2001:DB8:1:11::/64 [120/3]
      via FE80::202:17FF:FEA9:85A, Serial0/0/0
R  2001:DB8:1:12::/64 [120/3]
      via FE80::202:17FF:FEA9:85A, Serial0/0/0
R  2001:DB8:1:13::/64 [120/3]
      via FE80::202:17FF:FEA9:85A, Serial0/0/0
R  2001:DB8:1:14::/64 [120/3]
      via FE80::202:17FF:FEA9:85A, Serial0/0/0
L  FF00::/8 [0/0]
   via ::, Null0
Rey#
```

همانطور که در خروجی فوق ملاحظه می‌نمایید به دلیل خرابی لینک مستقیم تهران و شهرری، مسیر جدید Default Route و شبکه‌های متصل به روتر تهران با Metric بالاتری جایگزین مسیرهای اصلی گردیده است. با استفاده از دستور Traceroute می‌توان مسیر دستیابی به شبکه‌های متصل به روتر تهران از طریق روتر شهرری را مورد بررسی قرار داد.

```
Rey#traceroute 2001:db8:1:14::1
Type escape sequence to abort.
Tracing the route to 2001:db8:1:14::1

 1  2001:DB8:1:A::C2  13 msec   6 msec   10 msec
 2  2001:DB8:1:A::B1  11 msec   14 msec   15 msec
```

مرجع دستور Command Reference:

Enabling the IPv6 RIP Process		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

Enabling the IPv6 RIP Process		
Step 3	**ipv6 unicast-routing** **Example:** Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**interface** *type number* **Example:** Router(config)# interface Ethernet 0/0	Specifies the interface type and number, and enters interface configuration mode.
Step 5	**ipv6 rip** *name* **enable** **Example:** Router(config-if)# ipv6 rip process1 enable	Enables the specified IPv6 RIP routing process on an interface.

Customizing IPv6 RIP		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ipv6 router rip** *word* **Example:** Router(config)# ipv6 router rip process1	Configures an IPv6 RIP routing process and enters router configuration mode for the IPv6 RIP routing process. • Use the *word* argument to identify a specific IPv6 RIP routing process.
Step 4	**maximum-paths** *number-paths* **Example:** Router(config-router)# maximum-paths 1	(Optional) Defines the maximum number of equal-cost routes that IPv6 RIP can support. • The *number-paths* argument is an integer from 1 to 64. The default for RIP is four paths.
Step 5	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** Router(config)# interface Ethernet 0/0	Specifies the interface type and number, and enters interface configuration mode.

☑ مبحث سوم

پروتکل EIGRP for IPv6

همگام با بروز رسانی پروتکل‌های مسیریابی استاندارد، سیسکو نیز اقدام به ارائه نسخه جدیدی از پروتکل مسیریابی خود برای شبکه‌های مبتنی بر IPv6 نموده است. این پروتکل که بر پایهEIGRP منتشر گردیده است با عبارات EIGRPv6 ، EIGRP for IPv6 و EIGRPng یاد می‌شود. البته منظور از v6 در EIGRPv6 نسخه ششم از این پروتکل نیست، بلکه منظور نسخه مربوط به IPv6 می‌باشد. همچنین نام EIGRPng نیز برگرفته از RIPng و به معنی next generation است. هر چند که از هر سه نام فوق در مستندات فنی استفاده شده است ولی سیسکو در مستندات جدید خود، از این پروتکل تنها با نام EIGRP for IPv6 یاد می‌نماید.

همانطور که می‌دانید سیسکو پروتکلEIGRP را با قابلیت پشتیبانی از پروتکل‌های IPv4، IPX و AppleTalk ارائه نموده است. به همین دلیل EIGRP قابلیت اضافه شدن یک پروتکل لایه سوم دیگر که همان IPv6 باشد را نیز داشته است. لذا سیسکو به راحتی پروتکل EIGRP را ارتقاء داده تا قابلیت کار در شبکه‌های مبتنی برIPv6 را نیز به دست آورد. به همین دلیل تفاوت خاصی بین ویژگی‌ها و عملکرد EIGRP با EIGRP for IPv6 وجود ندارد.

پروتکل EIGRP for IPv6 همانند نسخه قبلی خود از پروتکل‌های TCP یا UPD استفاده نکرده و اقدام به بسته بندی مجدد پیام‌های خود در قالب Protocol Type 88 می‌نماید.

جدول زیر شامل مقایسه بین پروتکل EIGRP for IPv6 با نسخه قبلی خود که مربوط به IPv4 بود، می‌باشد:

ویژگی	EIGRP for IPv4	EIGRP for IPv6
پروتکل لایه سوم مورد استفاده	IPv4	IPv6
شماره پروتکل (Protocol Type)	88	88
استفاده از پروتکل و پورت UDP	خیر	خیر
استفاده از منطق Successor & Feasible Successor	بلی	بلی
الگوریتم مورد استفاده برای مسیریابی	Dual	Dual
پشتیبانی از VLSM	بلی	بلی

ویژگی	EIGRP for IPv4	EIGRP for IPv6
خلاصه سازی اتوماتیک	بلی	خیر
ارسال پیام های Triggered Updates	بلی	بلی
آدرس Multicast مورد استفاده	224.0.0.10	FF02::10
نحوه Authentication	EIGRP-specific	IPv6 AH/ESP

نحوه پیکربندی EIGRP for IPv6

پیکربندی EIGRP for IPv6 نیز مثل پروتکل RIPng، نسبت به نسخه قبلی خود دچار تغییرات گردیده است. نحوه پیکربندی این پروتکل از طریق مراحل زیر شرح داده شده است:

۱- در اولین گام باید اقدام به فعال سازی مسیریابی IPv6 بر روی روتر نمایید:

Router(config)#ipv6 unicast-routing

۲- در گام دوم پروتکل مسیریابیEIGRP for IPv6 را بر روی روتر راه اندازی می‌نماییم:

Router(config)#**ipv6 router eigrp** *as-number*

در دستور فوق AS-Number می تواند عددی در رنج 65535 – 1 قرار داشته باشد.

۳- سپس باید IPv6 بر روی اینترفیس‌های مورد نظر نیز فعال گردد. این کار را می‌توان به دو شیوه انجام داد:

اول اینکه اقدام به آدرس دهی IPv6 به اینترفیس مورد نماییم:

Router(config-if)#**ipv6 address** *address/prefix-length*

دومین روش نیز استفاده از دستور زیر می باشد:

Router(config-if)#ipv6 enable

در صورت استفاده از دستور فوق، روتر از آدرس‌های رنج Link-Local برای IPv6 استفاده می‌نماید.

۴- پروتکل EIGRP for IPv6 را بر روی اینترفیس‌هایی که قرار است آدرس آنها توسط مسیریابی پویا تبلیغ گردد، فعال می‌نماییم:

Router(config-if)#**ipv6 eigrp** *as-number*

عدد as-number در دستور فوق باید متناظر با عدد مورد استفاده در گام دوم باشد.

۵- با دستور زیر EIGRP را فعال می سازیم:

Router(config)#**ipv6 router eigrp** *as-number*
Router(config-rtr)#no shutdown

توجه داشته باشید که صرف ایجاد پروتکلEIGRP توسط دستور **ipv6 router eigrp** *as-number*، این پروتکل بر روی روتر فعال نمی‌شود. بلکه برای فعال کردن پروتکل EIGRP for IPv6 باید همانند فعال کردن اینترفیس از دستور no shutdown استفاده نمایید.

۶- اگر نمی خواهید مقدارEIGRP Router ID به صورت خودکار و بر اساس آدرس IPv4 اینترفیس‌های روتر انتخاب گردد، و یا اصلا هیچ آدرس IPv4ای روی روتر موجود نباشد، باید توسط دستور زیر به صورت دستی اقدام به تعیین Router ID نمایید:

Router(config-rtr)#**eigrp router-id** *rid*

البته در اینصورت نیز باید یک آدرس IPv4 به‌عنوان rid در دستور فوق وارد نمایید!

فرآیند محاسبه Router ID

نحوه محاسبه Router ID در EIGRP for IPv6 دقیقا شبیه به نسخه قبلی این پروتکل و به صورت زیر می‌باشد:

۱- اولویت اول با RID مشخص شده توسط دستور **eigrp router-id** *rid* می‌باشد. در صورتیکه این عدد به صورت دستی مشخص نشده باشد، روتر برای انتخاب اتوماتیک RID، سراغ مراحل بعدی می‌رود.

۲- استفاده از بالاترین آدرسIP اختصاص داده شده به اینترفیس‌های Loopback که در حالت up/up قرار داشته باشد.

۳- استفاده از بالاترین آدرسIP اختصاص داده شده به اینترفیس‌های غیر Loopback که در حالت up/up قرار داشته باشد.

در صورتیکه بر روی روتر هیچ آدرس IPv4 ای تنظیم نشده و شما هم بصورت دستی RID را مشخص نکرده باشید، اجرای پروتکل EIGRP for IPv6 به مشکل بر خواهد خورد. با توجه به حساسیت موضوع بد نیست تنظیم دستیRID را به عنوان یک عادت خوب به مجموعه عادات خوبتان اضافه فرمایید!

سناریو شماره(۱۸)؛ راه اندازی EIGRP for IPv6

طرح مسئله:

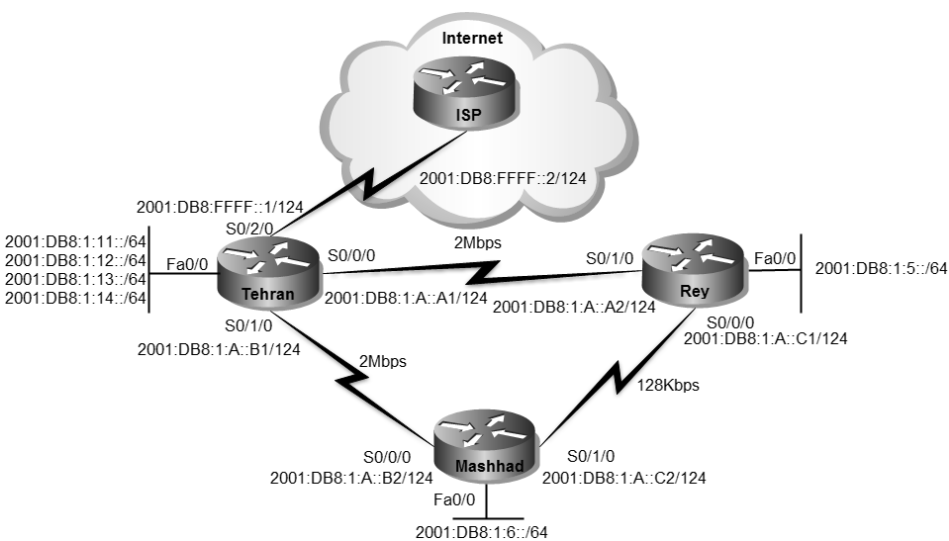
اشتباه حدس زدید! اینبار شرکت هیچ چیز جدیدی از شما نخواسته است. این شما هستید که می‌خواهید دانش خود را بر روی شبکه مردم! تست نمایید. به همین دلیل اقدام به راه اندازی پروتکل EIGRP for IPv6 بر روی شبکه شرکت MTR می‌نماییم.

البته دلیل استفاده از شبکه شرکت MTR برای اجرای دانسته‌های شما، رفاقت دیرینه بنده حقیر با مدیریت معظم شرکت است. همین جا اعلام می‌کنم مدیون هستید اگر دانش خودتون را بدون اجازه بر روی شبکه مردم آزمایش کنید!!!

نیاز سنجی:

نیازی نیست جز یک شبکه برای راه اندازی پروتکل، که شکر خدا به راحتی در اختیارمان قرار گرفته است.

در صورتیکه بر روی روترهای سناریوی قبل می خواهید سناریوی جدید را اجرا نمایید، باید پروتکل RIPng را از روی روترها حذف نمایید.



راه حل:

قبل از هر کاری باید پروتکل RIPng را بر روی روترها غیر فعال نماییم تا بتوانیم به درستی عملکرد پروتکل EIGRP for IPv6 را مورد بررسی قرار دهیم:

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#no ipv6 router rip MTR
```

```
Rey>enable
Rey#configure terminal
Rey(config)#no ipv6 router rip MTR
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#no ipv6 router rip MTR
```

با توجه به اینکه در سناریوی قبل ما مسیریابی IPv6 را بر روی روترها فعال کرده بودیم دیگر نیازی به فعال سازی مجدد نیست. اما به هر حال برای خالی نبودن عریضه، مجددا دستور مربوطه را بر روی روترها اعمال می‌کنیم.

در گام اول پیکربندی EIGRP for IPv6، ضمن فعال سازی مسیریابی IPv6، باید اقدام به راه اندازی و فعال سازی پروتکل مسیریابی مورد نظر بر روی روترها نماییم:

```
Mashhad(config)#ipv6 unicast-routing
Mashhad(config)#ipv6 router eigrp 110
Mashhad(config-rtr)#no shutdown
Mashhad(config-rtr)#router-id 192.168.1.1
```

```
Rey(config)#ipv6 unicast-routing
Rey(config)#ipv6 router eigrp 110
Rey(config-rtr)#no shutdown
Rey(config-rtr)#router-id 192.168.1.2
```

```
Tehran(config)#ipv6 unicast-routing
Tehran(config)#ipv6 router eigrp 110
Tehran(config-rtr)#no shutdown
Tehran(config-rtr)#router-id 192.168.1.3
```

دستور ipv6 unicast-routing جهت دوباره کاری! و فعال سازی مسیریابی IPv6 بر روی روتر مورد استفاده قرار گرفته است. توسط دستور ipv6 router eigrp 110 اقدام به راه

اندازی پروتکل EIGRP for IPv6 نمودیم. عدد110 نیز جهت AS-number به‌دستور تعلق گرفته است.

همانطور که قبلا گفته شد، پروتکل EIGRP for IPv6 صرف ایجاد، فعال نمی‌گردد و باید توسط دستور no shutdown، شبیه اینترفیس روتر، اقدام به فعال سازی آن نماییم.

به دلیل اینکه شبکه ما کاملا مبتنی بر IPv6 بوده و هیچ آدرس IPv4 بر روی اینترفیس‌های Loopback و فیزیکی تنظیم نشده است، باید برای انجام فرآیند محاسبه RID اقدام به تعیین مقدار بصورت دستی و توسط دستور router-id 192.168.1.3 نماییم.

پس از انجام مراحل فوق باید اینترفیس‌هایی که می خواهیم در پروسه مسیریابی فعال شوند را مشخص نماییم.

```
Tehran(config)#interface fastEthernet 0/0.2
Tehran(config-subif)#ipv6 eigrp 110
Tehran(config-subif)#interface fastEthernet 0/0.3
Tehran(config-subif)#ipv6 eigrp 110
Tehran(config-subif)#interface fastEthernet 0/0.4
Tehran(config-subif)#ipv6 eigrp 110
Tehran(config-subif)#interface fastEthernet 0/0.5
Tehran(config-subif)#ipv6 eigrp 110
Tehran(config-subif)#interface serial 0/0/0
Tehran(config-if)#ipv6 eigrp 110
Tehran(config-if)#interface serial 0/1/0
Tehran(config-if)#ipv6 eigrp 110
```

برای مشخص کردن شبکه های مورد نظر جهت تبلیغ توسط پروتکل مسیریابی پویا، باید دستور ipv6 eigrp 110 را در محیط اینترفیس روتر اعمال نماییم.

```
Rey(config)#interface fastEthernet 0/0
Rey(config-if)#ipv6 eigrp 110
Rey(config-if)#interface serial 0/0/0
Rey(config-if)#ipv6 eigrp 110
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#ipv6 eigrp 110
```

```
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#ipv6 eigrp 110
Mashhad(config-if)#interface serial 0/0/0
Mashhad(config-if)#ipv6 eigrp 110
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#ipv6 eigrp 110
```

پس از انجام مراحل فوق شبکه‌های متصل به روترها قابل دسترسی از طریق سایر روترهای شبکه می باشد:

```
Mashhad#ping 2001:db8:1:11::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:11::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/10 ms
```

همانطور که به یاد دارید در سناریوی قبل اقدام به مشخص کردن Default Route در روتر تهران کرده بودیم. ولی اگر بخواهید دوباره کاری کنید باید دستور زیر را به روتر تهران اعمال کنید.

```
Tehran(config)#ipv6 route ::/0 2001:DB8:FFFF::2
```

نکته قابل توجه در این پروتکل این است که با کمال تعجب! سیسکو در زمینه تبلیغ Default Route در پروتکل EIGRP for IPv6 از دیگر رقبای خود عقب مانده و باید Default Route را بصورت دستی در تمام روترهای شبکه پیکربندی نماییم.

```
Rey#configure terminal
Rey(config)#ipv6 route ::/0 2001:db8:1:a::a1
Rey(config)#ipv6 route ::/0 2001:db8:1:a::c2 5
```

```
Mashhad#configure terminal
Mashhad(config)#ipv6 route ::/0 2001:db8:1:a::b1
Mashhad(config)#ipv6 route ::/0 2001:db8:1:a::c1 5
```

همانطور که می‌بینید، برای اینکه خاصیت Redundancy را در اختیار داشته باشیم مجبور به نوشتن دو مسیر با Metric های متفاوت شده‌ایم.

برای آزمایش در دسترس بودن اینترنت اقدام به ping سرور سیسکو بر روی اینترنت می‌نماییم:

```
Rey#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::a, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/19/36 ms
```

طریقه عملکرد:

عملکردEIGRP for IPv6 شبیه بهEIGRP بوده و تفاوت خاصی در نحوه انجام وظایف ندارند. برای بررسی وضعیت پیکربندی پروتکل مسیریابی اولین کار مشاهده جدول مسیریابی روترها می‌باشد:

```
Mashhad#show ipv6 route
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
     U - Per-user Static route, M - MIPv6
     I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
     O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
     ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
     D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
    via 2001:DB8:1:A::B1
D   2001:DB8:1:5::/64 [90/2329600]
    via FE80::C200:DFF:FEA0:0, Serial0/0
C   2001:DB8:1:6::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:DB8:1:6::1/128 [0/0]
    via ::, FastEthernet0/0
D   2001:DB8:1:A::A0/124 [90/2304000]
    via FE80::C200:DFF:FEA0:0, Serial0/0
C   2001:DB8:1:A::B0/124 [0/0]
    via ::, Serial0/0
L   2001:DB8:1:A::B2/128 [0/0]
    via ::, Serial0/0
C   2001:DB8:1:A::C0/124 [0/0]
    via ::, Serial0/1
L   2001:DB8:1:A::C2/128 [0/0]
    via ::, Serial0/1
D   2001:DB8:1:C::B0/124 [90/2304000]
    via FE80::C200:DFF:FEA0:0, Serial0/0
D   2001:DB8:1:11::/64 [90/1817600]
    via FE80::C200:DFF:FEA0:0, Serial0/0
D   2001:DB8:1:12::/64 [90/1817600]
    via FE80::C200:DFF:FEA0:0, Serial0/0
D   2001:DB8:1:13::/64 [90/1817600]
    via FE80::C200:DFF:FEA0:0, Serial0/0
D   2001:DB8:1:14::/64 [90/1817600]
    via FE80::C200:DFF:FEA0:0, Serial0/0
L   FF00::/8 [0/0]
    via ::, Null0
```

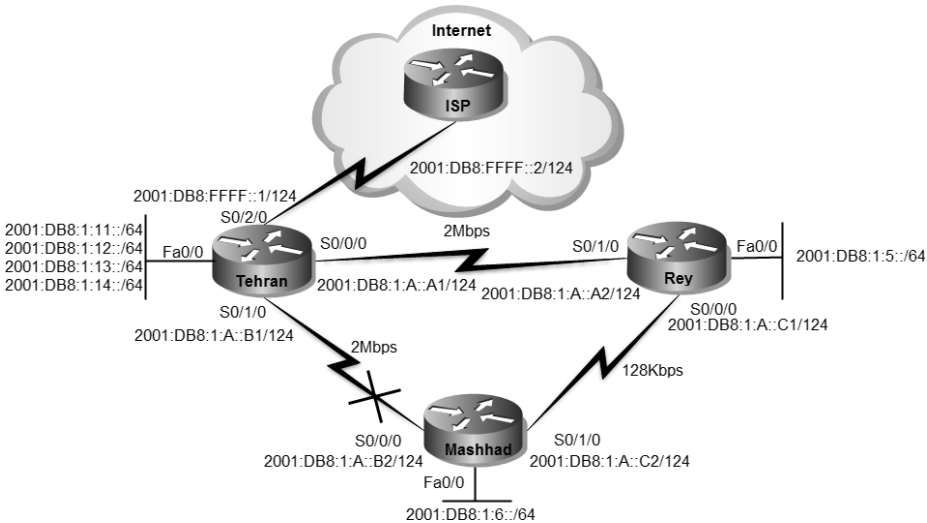
مسیرهای به دست آمده از طریق پروتکل EIGRP با درج حرف "D" در ابتدای آنها، مشخص شده‌اند. بر خلاف پروتکل‌های مسیریابی دیگر، پروتکل EIGRP for IPv6 امکان تبلیغ Default Route را به سایر روترهای شبکه ندارد. به همین دلیل در خروجی فوق Default Route را به صورت Static مشاهده می‌نمایید.

یکی دیگر از راه‌هایی که در بررسی عملکرد پروتکل مسیریابی مفید است، بررسی جداول مختص به خود پروتکل می‌باشد:

```
Mashhad#show ipv6 eigrp topology
IPv6-EIGRP Topology Table for AS(110)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
     r - reply Status, s - sia Status

P 2001:DB8:1:A::B0/124, 1 successors, FD is 1792000
      via Connected, Serial0/0
P 2001:DB8:1:C::B0/124, 1 successors, FD is 2304000
      via FE80::C200:DFF:FEA0:0 (2304000/1792000), Serial0/0
P 2001:DB8:1:A::A0/124, 1 successors, FD is 2304000
      via FE80::C200:DFF:FEA0:0 (2304000/1792000), Serial0/0
      via FE80::C201:DFF:FEA0:0 (21024000/2169856), Serial0/1
P 2001:DB8:1:A::C0/124, 1 successors, FD is 20512000
      via Connected, Serial0/1
      via FE80::C200:DFF:FEA0:0 (3193856/2681856), Serial0/0
      via FE80::C201:DFF:FEA0:0 (21024000/2169856), Serial0/1
P 2001:DB8:1:11::/64, 1 successors, FD is 1817600
      via FE80::C200:DFF:FEA0:0 (1817600/281600), Serial0/0
P 2001:DB8:1:12::/64, 1 successors, FD is 1817600
      via FE80::C200:DFF:FEA0:0 (1817600/281600), Serial0/0
P 2001:DB8:1:13::/64, 1 successors, FD is 1817600
      via FE80::C200:DFF:FEA0:0 (1817600/281600), Serial0/0
P 2001:DB8:1:14::/64, 1 successors, FD is 1817600

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
     r - reply Status, s - sia Status

      via FE80::C200:DFF:FEA0:0 (1817600/281600), Serial0/0
P 2001:DB8:1:5::/64, 1 successors, FD is 2329600
      via FE80::C200:DFF:FEA0:0 (2329600/1817600), Serial0/0
      via FE80::C201:DFF:FEA0:0 (20537600/281600), Serial0/1
P 2001:DB8:1:6::/64, 1 successors, FD is 281600
      via Connected, FastEthernet0/0
```

در خروجی فوق تمام مسیرهای موجود برای دسترسی به یک شبکه مشخص نمایش داده می‌شود. مسیری که دارای Metric بهتری نسبت به بقیه مسیرها می‌باشد به عنوان مسیر successor مشخص شده و در جدول توپولوژی ثبت گردیده است. مسیرهای با Metric بالاتر نیز به عنوان feasible successor جهت جایگزینی مسیرهای اصلی در نظر گرفته می‌شود.

برای بررسی پویا بودن مسیریابی می‌توانیم لینک مستقیم بین مشهد و تهران را غیرفعال نماییم. در این صورت خروجی دو دستور فوق به صورت زیر تغییر خواهد کرد:




```
Mashhad#show ipv6 route
<…Output Omitted…>
S   ::/0 [1/0]
    via 2001:DB8:1:A::B1
D   2001:DB8:1:5::/64 [90/20537600]
    via FE80::C201:DFF:FEA0:0, Serial0/1
C   2001:DB8:1:6::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:DB8:1:6::1/128 [0/0]
    via ::, FastEthernet0/0
D   2001:DB8:1:A::A0/124 [90/21024000]
    via FE80::C201:DFF:FEA0:0, Serial0/1
C   2001:DB8:1:A::C0/124 [0/0]
    via ::, Serial0/1
L   2001:DB8:1:A::C2/128 [0/0]
    via ::, Serial0/1
D   2001:DB8:1:11::/64 [90/21049600]
    via FE80::C201:DFF:FEA0:0, Serial0/1
D   2001:DB8:1:12::/64 [90/21049600]
    via FE80::C201:DFF:FEA0:0, Serial0/1
D   2001:DB8:1:13::/64 [90/21049600]
    via FE80::C201:DFF:FEA0:0, Serial0/1
D   2001:DB8:1:14::/64 [90/21049600]
    via FE80::C201:DFF:FEA0:0, Serial0/1
L   FF00::/8 [0/0]
    via ::, Null0
```

```
Mashhad#show ipv6 eigrp topology
<…Output Omitted…>
P 2001:DB8:1:A::A0/124, 1 successors, FD is 2304000
      via FE80::C201:DFF:FEA0:0 (21024000/2169856), Serial0/1
P 2001:DB8:1:A::C0/124, 1 successors, FD is 20512000
      via Connected, Serial0/1
```

```
    via FE80::C201:DFF:FEA0:0 (21024000/2169856), Serial0/1
P 2001:DB8:1:11::/64, 1 successors, FD is 21049600
    via FE80::C201:DFF:FEA0:0 (21049600/2195456), Serial0/1
P 2001:DB8:1:12::/64, 1 successors, FD is 21049600
    via FE80::C201:DFF:FEA0:0 (21049600/2195456), Serial0/1
P 2001:DB8:1:13::/64, 1 successors, FD is 21049600
    via FE80::C201:DFF:FEA0:0 (21049600/2195456), Serial0/1
P 2001:DB8:1:14::/64, 1 successors, FD is 21049600
    via FE80::C201:DFF:FEA0:0 (21049600/2195456), Serial0/1
P 2001:DB8:1:5::/64, 1 successors, FD is 2329600
    via FE80::C201:DFF:FEA0:0 (20537600/281600), Serial0/1
P 2001:DB8:1:6::/64, 1 successors, FD is 281600
    via Connected, FastEthernet0/0
```

پس از قطع شدن لینک مستقیم بین مشهد و تهران، مسیر مشهد، ری، تهران با Metric بالاتر جایگزین مسیرهای قبلی شده است.

می توان توسط دستور traceroute تغییر مسیر دسترسی را مشاهده نمود:

```
Mashhad#traceroute 2001:db8:1:12::1
Type escape sequence to abort.
Tracing the route to 2001:db8:1:12::1

  1  2001:DB8:1:5::1 38 msec   7 msec   14 msec
  2  2001:DB8:1:A::A1 15 msec   20 msec   18 msec
```

اما در صورتیکه مجددا لینک بین تهران و مشهد برقرار گردد، خروجی فوق به صورت زیر خواهد بود:

```
Mashhad#traceroute 2001:db8:1:12::1
Type escape sequence to abort.
Tracing the route to 2001:db8:1:12::1

  1  2001:DB8:1:A::B18 msec   5 msec   6 msec
```

مرجع دستورات Command Reference:

Enabling EIGRP for IPv6 on an Interface		
	Command or Action	**Purpose**
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`configure terminal`** **Example:** `Router# configure terminal`	Enters global configuration mode.

Enabling EIGRP for IPv6 on an Interface		
Step 3	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Specifies the interface on which EIGRP is to be configured.
Step 5	**no shut** **Example:** `Router(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 6	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 7	**ipv6 eigrp** *as-number* **Example:** `Router(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on a specified interface.
Step 8	**ipv6 router eigrp** *as-number* **Example:** `Router(config-if)# ipv6 router eigrp 1`	Enters router configuration mode and creates an EIGRP IPv6 routing process.
Step 9	**eigrp router-id** *ip-address* **Example:** `Router(config-router)# eigrp router-id 10.1.1.1`	Enables the use of a fixed router ID. Use this command only if an IPv4 address is not defined on the router eligible for router ID.
Step 10	**no shut** **Example:** `Router(config-rtr)# no shutdown`	Enable EIGRP.
Step 11	**show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [**detail**] **Example:** `Router# show ipv6 eigrp interfaces`	Displays information about interfaces configured for EIGRP for IPv6.

☑ مبحث چهارم

پروتکل OSPFv3

پروتکلOSPF برای شبکه‌های مبتنی برIPv4 اقدام به انتشار دو نسخه از این پروتکل نمود. نسخه اول OSPFv1 عمومیت نیافته و خیلی سریع جای خود را به نسخه بعدی، یعنی OSPFv2 داد. این نسخه از پروتکل بصورت عمومی مورد استفاده قرار گرفت و مورد اقبال هم واقع شد. پس از ارائه نسخه جدید پروتکل IP با نام IPv6، سازمان IETF برای پشتیبانیOSPF از شبکه‌های مبتنی بر IPv6 اقدام به انتشار نسخه جدید این پروتکل با نام OSPFv3 نمود.

پروتکلOSPFv3 که طی استاندارد RFC 5340 منتشر گردیده است، عملکردی شبیه OSPFv2 داشته و بر اساس همان نسخه قبلی خود گسترش داده شده است.

در جدول زیر شباهت‌ها و تفاوت‌های بین دو نسخه اصلی OSPF نشان داده شده است.

ویژگی	OSPFv2	OSPFv3
پروتکل لایه سوم مورد استفاده	IPv4	IPv6
شماره پروتکل مورد استفاده (Protocol Type)	89	89
استفاده از پروتکل های TCP / UDP	خیر	خیر
استفاده از منطق Link State	بلی	بلی
پشتیبانی از VLSM	بلی	بلی
نحوه محاسبه Metric	Cost	Cost
نحوه انتخاب روتر DR	شبیه به هم	شبیه به هم
الگوریتم مسیریابی مورد استفاده	SPF	SPF
آدرس Multicast مورد استفاده برای پیام های SPF	224.0.0.5	FF02::5
آدرس Multicast مورد استفاده توسط روترهای DR	224.0.0.6	FF02::6
نحوه Authentication	MD5	IPv6 AH/ESP

همانطور که در جدول فوق مشاهده می‌کنید، این دو نسخه از بسیاری جهات شبیه به یکدیگر بوده و عملکردی یکسان دارند.

نکات مربوط به OSPFv3

پروتکلOSPF دارای نکات خاصی در نحوه عملکرد می‌باشد که در زیر به آنها پرداخته شده است:

- پروتکل OSPFv3 همانند نسخه قبلی خود، برای انتقال اطلاعات مربوط به مسیریابی از پروتکل‌هایTCP وUDP استفاده نمی‌نماید. این پروتکل اطلاعات مربوطه را مجددا بسته بندی کرده[1] و در قالب IP Protocol Type 89 ارسال می‌نماید.
- مثل پروتکل‌هایRIPng وEIGRP for IPv6، پروتکل OSPFv3 نیز برای عملیات مربوط به Authentication نیازی به پروتکل‌های دیگر نداشته و از خصوصیت AH/ESP موجود در IPv6 استفاده می‌نماید.
- همانطور که در سناریوهای مربوط به RIPng و EIGRP for IPv6 نیز مشاهده نمودید، پروتکل های مسیریابی در IPv6 آدرس دهی مربوط به Next hop را بر اساس آدرس های رنج Link-Local انجام می‌دهند.
- به علت استفاده از آدرس‌های Link-Local برای آدرس‌های Next hop، نیازی به شباهت Prefix آدرس‌ها جهت برقراری رابطه مجاورت نبوده و امکان برقراری رابطه مجاورت بین آدرس‌های IPv6 با Prefixهای متفاوت وجود دارد.
- با کمال تعجب! همانند پروتکلEIGRP for IPv6 در پروتکل OSPFv3 نیز همچنان محاسبه مقدار RID بر اساس آدرس‌های IPv4 انجام می پذیرد.

  توجه داشته باشید آدرس 0.0.0.0 رزرو شده و امکان استفاده به عنوانRID را ندارد.
- پروتکل OSPFv3 امکان پشتیبانی از چند Instance را بر روی یک اینترفیس دارد. این امکان در نسخه قبلی این پروتکل موجود نبوده است.

  پروتکل OSPFv3 برای فراهم آوردن امکان پشتیبانی چند Instance بر روی یک اینترفیس، از ویژگیInstance ID موجود در سرآیند[2] بسته‌ها و ساختار رابط OSPF [3] استفاده می‌نماید.

  از موارد کاربرد پشتیبانی از Instanceهای مختلف بر روی یک اینترفیس، می توان به قرار گرفتن یک اینترفیس در Area ها و یا حوزه‌های[4] مختلف اشاره کرد.

---

[1] Encapsulation
[2] Header
[3] OSPF interface structures
[4] Domain

نحوه پیکربندی OSPFv3

جهت پیکربندی OSPFv3 بر روی روترها باید مراحل زیر انجام پذیرد:

۱- همانند دیگر پروتکل‌های مسیریابی، اولین گام، فعال سازی مسیریابی IPv6 بر روی روترها می‌باشد:

Router(config)#ipv6 unicast-routing

۲- در گام دوم، اقدام به راه اندازی پروتکل OSPFv3 بر روی روترها می نماییم:

Router(config)#**ipv6 router ospf** *process-id*

نیازی به یکسان بودن process-id بر روی تمام روترهایی که می خواهند توسط پروتکل OSPFv3 با یکدیگر ارتباط داشته باشند، نیست. پارامتر process-id فقط بصورت محلی بر روی روتر مورد استفاده قرار می‌گیرد.

توجه داشته باشید پروتکل OSPF پس از ایجاد به صورت پیش فرض فعال می گردد. ولی به هر حال می توانید از دستورات shutdown و no shutdown برای فعال یا غیر فعال سازی پروتکل استفاده نمایید.

۳- قبل از انجام مرحله چهارم، حتما باید IPv6 توسط یکی از دو روش زیر بر روی اینترفیس فعال گردیده باشد:

در روش اول می توان اقدام به تنظیم آدرس مورد نظر بر روی اینترفیس نمود:

Router(config-if)#**ipv6 address** *address/prefix-length*

روش دیگر نیز فعال سازی آدرس بر روی اینترفیس توسط دستور زیر می باشد:

Router(config-if)#ipv6 enable

در صورت استفاده از دستور فوق، روتر به صورت خودکار یک آدرس از رنج Link-Local را به اینترفیس مورد نظر اختصاص خواهد داد.

۴- در این مرحله باید اینترفیس های مورد نظر جهت شرکت در عملیات مسیریابی را مشخص نماییم:

Router(config-if)#**ipv6 ospf** *process-id* **area** *area-number*

۵- اگر هیچ آدرس IPv4 فعالی بر روی روتر وجود ندارد و یا اینکه نمی خواهید محاسبه RID بصورت اتوماتیک صورت بگیرد؛ می توانید توسط دستور زیر RID را مشخص نمایید. این دستور در حالت پیکربندی پروتکل مسیریابی اعمال می شود:

Router(config-rtr)#**router-id** *RID*

برای مقدار RID در دستور فوق، باید یک آدرس IPv4 در نظر بگیرید.

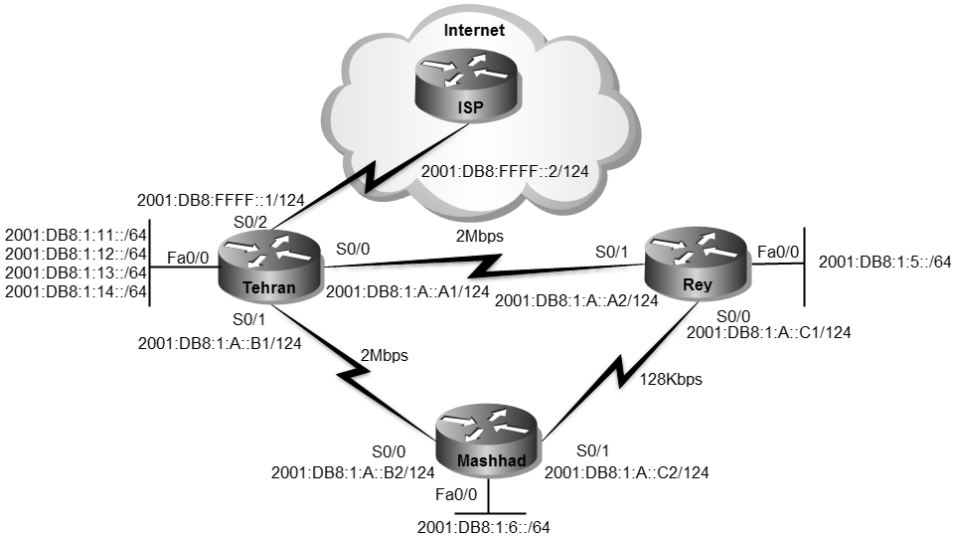
سناریو شماره(۱۹): راه اندازی OSPFv3

طرح مسئله:

قصد دارید یک پروتکل مسیریابی پویای استاندارد بر روی شبکه شرکت MTR راه اندازی نمایید تا در صورت اضافه شدن تجهیزات جدید شبکه‌ای غیر سیسکو، بتوان به راحتی پروتکل مسیریابی پویا را گسترش داد.

نیاز سنجی:

به دلیل کوچک بودن شبکه، راه اندازی OSPFv3 بر اساس یک Area راه حل قابل قبولی خواهد بود.



راه حل:

به دلیل آنکه قبلا پروتکل مسیریابی EIGRP for IPv6 بر روی شبکه راه اندازی شده است، قبل از هر کاری باید اقدام به غیر فعال سازی این پروتکل بر روی روترها نموده تا بتوان به درستی عملکرد پروتکل OSPFv3 را مورد بررسی قرار داد.

```
Tehran(config)#no ipv6 router eigrp 110
```

```
Rey(config)#no ipv6 router eigrp 110
```

```
Rey(config)#no ipv6 route ::/0 2001:DB8:1:A::A1
Rey(config)#no ipv6 route ::/0 2001:DB8:1:A::C2 5
```

```
Mashhad(config)#no ipv6 router eigrp 110
Mashhad(config)#no ipv6 route ::/0 2001:DB8:1:A::B1
Mashhad(config)#no ipv6 route ::/0 2001:DB8:1:A::C1 5
```

همانطور که ملاحظه می‌کنید، Static Default Route هایی را که در روتر شهرری و مشهد بصورت دستی ایجاد کرده بودیم، نیز غیر فعال کردیم.

حالا روترها آماده راه اندازی پروتکل مسیریابی جدید هستند. اولین گام برای راه اندازی پروتکل مسیریابی، فعال کردن مسیریابی IPv6 بر روی روترها است. این کار در سناریوی قبل انجام شده ولی در دستورات زیر نیز مجددا تکرار گردیده است. پس از فعال سازی مسیریابی IPv6 باید اقدام به پیکربندی پروتکل مورد نظر بر روی روترها نماییم.

به دلیل کوچک بودن شبکه، همه روترها را در یک Area که همان Area 0 یا Backbone می‌باشد، قرار می‌دهیم.

```
Tehran>enable
Tehran#configure terminal
Tehran(config)#ipv6 unicast-routing
Tehran(config)#ipv6 router ospf 110
Tehran(config-rtr)#router-id 3.3.3.3
```

توسط دستور ipv6 router ospf 110 اقدام به فعال سازی پروتکل OSPFv3 بر روی روتر نمودیم. عدد 110 در این دستور مشخص کننده process-id می‌باشد. الزامی به یکسان بودن process-id بر روی تمام روترهای شبکه وجود ندارد.

```
Rey>enable
Rey#configure terminal
Rey(config)#ipv6 unicast-routing
Rey(config)#ipv6 router ospf 110
Rey(config-rtr)#router-id 2.2.2.2
```

```
Mashhad>enable
Mashhad#configure terminal
Mashhad(config)#ipv6 router ospf 110
Mashhad(config-rtr)#router-id 1.1.1.1
```

حالا نوبت مشخص نمودن اینترفیس‌های مورد نظر جهت شرکت در پروسه مسیریابی می‌باشد که توسط دستورات زیر انجام می‌پذیرد:

```
Tehran(config)#interface fastEthernet 0/0.2
Tehran(config-subif)#ipv6 ospf 110 area 0
Tehran(config-subif)#interface fastEthernet 0/0.3
Tehran(config-subif)#ipv6 ospf 110 area 0
Tehran(config-subif)#interface fastEthernet 0/0.4
Tehran(config-subif)#ipv6 ospf 110 area 0
Tehran(config-subif)#interface fastEthernet 0/0.5
Tehran(config-subif)#ipv6 ospf 110 area 0
Tehran(config-subif)#interface serial 0/0/0
Tehran(config-if)#ipv6 ospf 110 area 0
Tehran(config-if)#interface serial 0/1/0
Tehran(config-if)#ipv6 ospf 110 area 0
```

```
Rey(config)#interface fastEthernet 0/0
Rey(config-if)#ipv6 ospf 110 area 0
Rey(config-if)#interface serial 0/0/0
Rey(config-if)#ipv6 ospf 110 area 0
Rey(config-if)#interface serial 0/1/0
Rey(config-if)#ipv6 ospf 110 area 0
```

```
Mashhad(config)#interface fastEthernet 0/0
Mashhad(config-if)#ipv6 ospf 110 area 0
Mashhad(config-if)#interface serial 0/0/0
Mashhad(config-if)#ipv6 ospf 110 area 0
Mashhad(config-if)#interface serial 0/1/0
Mashhad(config-if)#ipv6 ospf 110 area 0
```

با اعمال دستور ipv6 ospf 110 area 0 بر روی اینترفیس، ضمن مشخص نمودن پروتکل مورد استفاده، Area قرار گیری اینترفیس را نیز مشخص می‌نماییم.

پس از انجام مراحل فوق، در صورتیکه اقدام بهping شبکه‌های متصل به دیگر روترها نمایید، خروجی زیر را مشاهده خواهید کرد:

```
Mashhad#ping 2001:db8:1:11::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:11::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/20/36 ms

Mashhad#ping 2001:db8:1:14::1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:1:14::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
```

علیرغم اینکه، شبکه‌های دیگر در دسترس هستند اما همچنان دسترسی به اینترنت از طریق روترها شهرری و مشهد امکان پذیر نیست.

جهت تبلیغ Default Route توسط پروتکلOSPFv3 باید به صورت زیر عمل نمایید. در ضمن یادآوری می کنم که Default Route روتر تهران، در سناریوی قبلی نوشته شده است.

```
Tehran#configure terminal
Tehran(config)#ipv6 router ospf 110
Tehran(config-rtr)#default-information originate
```

پس از اعمال دستور فوق در صورتی که اقدام به ping سرور سیسکو در اینترنت نمایید، خروجی زیر را مشاهده خواهید نمود:

```
Rey#ping 2001:420:1101:1::a

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1101:1::A, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/200/548 ms
```

طریقه عملکرد:

نحوه عملکرد پروتکل OSPFv3 کاملا شبیه پروتکل OSPFv2 می‌باشد. فقط این دو پروتکل در نحوه پیکربندی با یکدیگر تفاوت دارند که در این سناریو به آن پرداخته شد.

طبق روال سناریوهای قبل، در اولین گام اقدام به بررسی جداول مسیریابی و دیتابیس روترها می‌نماییم.

```
Rey#show ipv6 ospf database

        OSPFv3 Router with ID (2.2.2.2) (Process ID 110)

            Router Link States (Area 0)

ADV Router     Age       Seq#       Fragment ID  Link count  Bits
1.1.1.1        621       0x80000006  0           2           None
2.2.2.2        776       0x80000007  0           2           None
3.3.3.3        1049      0x8000000E  0           2           E

            Link (Type-8) Link States (Area 0)

ADV Router     Age       Seq#       Link ID    Interface
```

```
2.2.2.2      1021      0x80000002  7       Se0/1
3.3.3.3      1209      0x80000003  6       Se0/1
1.1.1.1      621       0x80000002  7       Se0/0
2.2.2.2      776       0x80000003  6       Se0/0
2.2.2.2      1021      0x80000002  4       Fa0/0

            Intra Area Prefix Link States (Area 0)

ADV Router     Age        Seq#       Link ID    Ref-lstype  Ref-LSID
1.1.1.1        621        0x80000004  0         0x2001      0
2.2.2.2        776        0x80000004  0         0x2001      0
3.3.3.3        217        0x80000005  0         0x2001      0

            Type-5 AS External Link States

ADV Router     Age        Seq#       Prefix
3.3.3.3        1059       0x80000001  ::/0
```

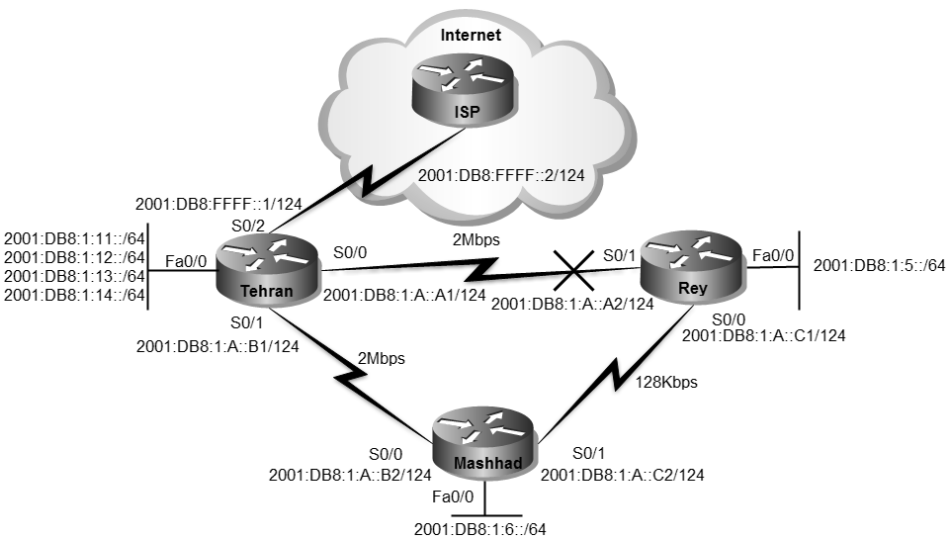
```
Rey#show ipv6 route
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
OE2  ::/0 [110/1], tag 110
     via FE80::C204:8FF:FEE8:0, Serial0/1
C   2001:DB8:1:5::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8:1:5::1/128 [0/0]
     via ::, FastEthernet0/0
O   2001:DB8:1:6::/64 [110/74]
     via FE80::C206:8FF:FEE8:0, Serial0/0
C   2001:DB8:1:A::A0/124 [0/0]
     via ::, Serial0/1
L   2001:DB8:1:A::A2/128 [0/0]
     via ::, Serial0/1
O   2001:DB8:1:A::B0/124 [110/128]
     via FE80::C206:8FF:FEE8:0, Serial0/0
C   2001:DB8:1:A::C0/124 [0/0]
     via ::, Serial0/0
L   2001:DB8:1:A::C1/128 [0/0]
     via ::, Serial0/0
O   2001:DB8:1:C::B0/124 [110/128]
     via FE80::C204:8FF:FEE8:0, Serial0/1
O   2001:DB8:1:11::/64 [110/74]
     via FE80::C204:8FF:FEE8:0, Serial0/1
O   2001:DB8:1:12::/64 [110/74]
     via FE80::C204:8FF:FEE8:0, Serial0/1
O   2001:DB8:1:13::/64 [110/74]
     via FE80::C204:8FF:FEE8:0, Serial0/1
O   2001:DB8:FFFF::/124 [110/128]
     via FE80::C204:8FF:FEE8:0, Serial0/1
L   FF00::/8 [0/0]
     via ::, Null0
Rey#
```

در خروجی فوق مسیرهایی که از طریق پروتکل مسیریابی OSPF به دست آمده است با حرف "O" در ابتدای آنها، مشخص شده است.

همچنین مسیر Default Route به دست آمده از طریق پروتکل مسیریابیOSPF نیز در خروجی فوق با حرف "OE2" مشخص گردیده است.

در این پروتکل نیز همانند پروتکل‌های مسیریابی قبلی، روتر برای آدرس Next hop جدول مسیریابی خود، از آدرس‌های Link-Local اینترفیس‌ها استفاده می‌نماید.

برای بررسی عملکرد پروتکل مسیریابی OSPFv3 می‌توانیم اقدام به قطع لینک مستقیم بین شهرری و تهران نماییم.



پس از قطع ارتباط مستقیم بین تهران و شهرری، خروجی show ipv6 route روتر شهرری به صورت زیر تغییر خواهد نمود:

```
Rey#sh ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
     U - Per-user Static route, M - MIPv6
     I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
     O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
     ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
     D - EIGRP, EX - EIGRP external
OE2  ::/0 [110/1], tag 110
    via FE80::C206:8FF:FEE8:0, Serial0/0
C   2001:DB8:1:5::/64 [0/0]
    via ::, FastEthernet0/0
```

```
L   2001:DB8:1:5::1/128 [0/0]
    via ::, FastEthernet0/0
O   2001:DB8:1:6::/64 [110/791]
    via FE80::C206:8FF:FEE8:0, Serial0/0
O   2001:DB8:1:A::B0/124 [110/831]
    via FE80::C206:8FF:FEE8:0, Serial0/0
C   2001:DB8:1:A::C0/124 [0/0]
    via ::, Serial0/0
L   2001:DB8:1:A::C1/128 [0/0]
    via ::, Serial0/0
O   2001:DB8:1:C::B0/124 [110/881]
    via FE80::C206:8FF:FEE8:0, Serial0/0
O   2001:DB8:1:11::/64 [110/841]
    via FE80::C206:8FF:FEE8:0, Serial0/0
O   2001:DB8:1:12::/64 [110/841]
    via FE80::C206:8FF:FEE8:0, Serial0/0
O   2001:DB8:1:13::/64 [110/841]
    via FE80::C206:8FF:FEE8:0, Serial0/0
O   2001:DB8:FFFF::/124 [110/895]
    via FE80::C206:8FF:FEE8:0, Serial0/0
L   FF00::/8 [0/0]
    via ::, Null0
```

همانطور که در خروجی فوق مشهود است، مسیرهای با Metric بالاتر جایگزین مسیرهای قبلی ارتباط شهرری با تهران گردیده است.

توسط دستور show ipv6 ospf neighbor می‌توان همسایه‌های فعال روتر شهرری را مشاهده نمود:

```
Rey#show ipv6 ospf neighbor

Neighbor ID     Pri   State        Dead Time   Interface ID    Interface
1.1.1.1         1   FULL/  -      00:00:31    7             Serial0/0
```

خروجی فوق نیز نشان دهنده این است که فقط روتر مشهد در ارتباط مستقیم با روتر شهرری بوده و بین این دو روتر ارتباط مجاورت برقرار گردیده است.

پس از قطع ارتباط مستقیم بین شهرری و تهران، برای بررسی تغییر مسیر می‌توانیم از دستور Traceroute بهره ببریم.

```
Rey#traceroute 2001:db8:1:11::1

Type escape sequence to abort.
Tracing the route to 2001:DB8:1:11::1

  1 2001:DB8:1:A::C2 328 msec 292 msec 60 msec
  2 2001:DB8:1:11::1 124 msec 552 msec 580 msec
```

خروجی دستور traceroute در صورتیکه لینک مستقیم تهران و شهرری برقرار باشد، به صورت زیر خواهد بود.

```
Rey#traceroute 2001:db8:1:11::1

Type escape sequence to abort.
Tracing the route to 2001:DB8:1:11::1

 1 2001:DB8:1:11::1 56 msec 84 msec 168 msec
```

با مقایسه دو خروجی فوق با یکدیگر می‌توان تفاوت مسیرهای برقراری ارتباط بین شهرری و تهران را در صورت قطعی لینک‌ها مورد بررسی قرار داد.

مرجع دستور Command Reference:

Configuring the OSPFv3 Router Process		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**Ipv6 router ospf** [*process-id*] **Example:** Router(config)# ipv6 router ospf 1	Enables OSPFv3 router configuration mode for the IPv6 address family.
Step 5	**area** *area-ID* [**default-cost** | **nssa** |**stub**] **Example:** Router(config-rtr)# area 1	Configures the OSPFv3 area.
Step 6	**default** {**area** *area-ID* [**range** *ipv6-prefix*| **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** |**metric-type** | **route-map**] | **distance** |**distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* |**summary-prefix** *ipv6-prefix*] **Example:** Router(config-rtr)# default area 1	Returns an OSPFv3 parameter to its default value.

Configuring the OSPFv3 Router Process		
Step 7	**log-adjacency-changes** [**detail**] **Example:** Router(config-rtr)# log-adjacency-changes	Configures the router to send a syslog message when an OSPFv3 neighbor goes up or down.
Step 8	**passive-interface** [**default** | *interface-type interface-number*] **Example:** Router(config-rtr)# passive-interface default	Suppresses sending routing updates on an interface when using an IPv4 OSPFv3 process.
Step 9	**queue-depth** {**hello** | **update**} {*queue-size*| **unlimited**} **Example:** Router(config-rtr)# queue-depth update 1500	Configures the number of incoming packets that the IPv4 OSPFv3 process can keep in its queue.
Step 10	**router-id** {*router-id*} **Example:** Router(config-rtr)# router-id 10.1.1.1	Use a fixed router ID.

Enabling OSPFv3 on an Interface		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface ethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 ospf** *process-id* **area** *area-id*[**instance** *instance-id*] **Example:** Router(config-if)# ipv6 ospf 1 area 0	Enables OSPFv3 on an interface.

فصل هفتم

مباحث ویـــژه

- ☑ مبحث اول: مدل سلسله مراتبی سیسکو
- ☑ مبحث دوم: High Availability
- ☑ مبحث سوم: Redistribution
- ☑ مبحث چهارم: سایر پروتکل‌ها

☑ مبحث اول

مدل سلسله مراتبی سیسکو

سیسکو به عنوان یکی از معتبرترین ارائه کنندگان محصولات شبکه، اقدام به معرفی یک مدل برای برپایی شبکه‌های Campus نموده است. این مدل که با نام مدل سلسله مراتبی[1] یا مدل سه لایه خوانده می‌شود، شبکه را به سه لایه بخش بندی کرده و انجام عملیات مختلف را بین این سه لایه تقسیم نموده است.[2]

خاطره:

تازه در یک شبکه بزرگ و گسترده در سراسر ایران شروع به کار کرده بودم. به واسطه قبولی در مصاحبه سخت فنی بدو ورود به سازمان، از معلومات فنی! خودم نیز مطمئن بودم.

روزهای اول کاری می دیدم بچه‌های بخش مانیتورینگ وقتی درباره روترها صحبت می‌کنند می‌گویند: "روتر فلان شهرستان که در لایه دو کار می کرده، قطع شده!" و یا "روتر فلان استان که تو لایه یک! بوده به مشکل برخورده!"

من بعد از شنیدن این حرفها خون در مغزم منجمد می‌شد! نمی‌دونستم اینا بی سواد هستند یا کتابها و اساتید بنده کم اطلاع! یا شاید خودم خیلی خنگ بودم و نتوانسته‌ام خوب آموزش ببینم؟!!!

خلاصه پس از چند روز دیگه طاقت نیاورده و دل به دریا زدم. با اقتدار به مدیر فنی گفتم: **"مهندس جان! شما از روترها تو لایه‌های یک و دو استفاده می کنید؟! فکر نمی کنید بهتر باشه از همان هاب و سوئیچ در این لایه‌ها استفاده نمایید؟!!!"**

مدیر فنی مربوطه پس از شنیدن سخن حکیمانه من چند ثانیه هنگ فرموده و بعد از سر دادن چند قهقهه فرمودند: "ما به دلیل بزرگی شبکه و تقسیم کار بین گروه‌های مختلف، اقدام به تقسیم بندی روترها در لایه های مختلف کاری و مدیریتی نموده ایم! و این لایه ها هیچ ربطی به لایه های مدل OSI یا TCP/IP ندارند!!!"

من: |:

:)

---

[1] Hierarchical Model

[2] روم به دیوار! یه وقت این سه لایه را با لایه های مدل OSI یا TCP/IP اشتباه نگیرید!!!

تعریف Campus

منظور از شبکه Campus یک شبکه سازمانی بزرگ است که از تعدادی شبکه‌های کوچک و بزرگ واقع در یک یا چند ساختمان که معمولا در یک منطقه جغرافیایی قرار گرفته، تشکیل گردیده است. در این حالت سازمان صاحب تمام شبکه، از سیم‌ها و زیرساخت‌ها تا تجهیزات اکتیو شبکه می‌باشد.

درک درست از ترافیک شبکه، بخش مهمی از طراحی یک شبکه Campus می‌باشد. ترافیک شبکه می‌تواند به طور موثر مدیریت و منتقل شده تا شما بتوانید یک معیار درست جهت رفع نیازهای آینده داشته باشید.

طراحی سلسله مراتبی شبکه

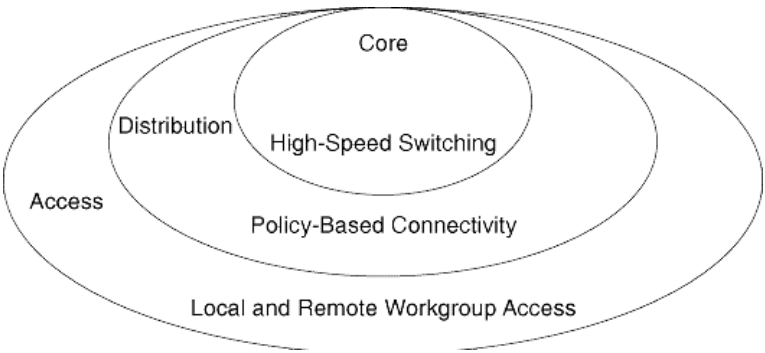
مدل سلسله مراتبی طراح را قادر می‌سازد تا شبکه‌ای بر اساس لایه‌های مختلف ایجاد نموده و با تقسیم وظایف مختلف برای هر لایه، کمک قابل توجهی در انتخاب تجهیزات و پیکربندی آنها به طراح شبکه می‌شود. مدل سلسله مراتبی قابل استفاده در طراحی هر دو نوع شبکه LAN و WAN می‌باشد.

این نوع طراحی، شبکه را به سه لایه زیر تقسیم می‌نماید:

۱- لایه هسته (Core Layer)

۲- لایه توزیع (Distribution Layer)

۳- لایه دسترسی (Access Layer)



با توجه به گستردگی و نیازهای شبکه، می توان بعضی از لایه‌های فوق را ادغام نمود ولی توجه داشته باشید که در این صورت باید همچنان وضعیت سلسله مراتبی شبکه حفظ گردد.

لایه هسته (Core Layer)

لایهCore، ستون فقرات[1] سوئیچینگ سرعت بالای شبکه می‌باشد که در فعال سازی ارتباطات سازمانی نقش حیاتی بر عهده دارد. این لایه محل اتصال تمام تجهیزات واقع در لایه توزیع می‌باشد. لایه Core باید دارای مشخصات زیر باشد:

- ارائه قابلیت اطمینان بالا (High Reliability)
- فراهم نمودن افزونگی (Redundancy)
- فراهم کردن تحمل خطا (Fault Tolerance)
- انطباق سریع با تغییرات
- ارائه تاخیر کم (Low Latency) و قابلیت مدیریت خوب
- جلوگیری از کاهش سرعت ناشی از اعمال فیلتر یا پردازش‌های دیگر

تجهیزات واقع در لایه هسته باید برای سوئیچینگ با کارآیی بالا[2] بهینه سازی شده باشند. همچنین به دلیل اینکه لایه هسته باید حجم بالایی از داده‌های شبکه را اداره نماید، طراحی این لایه باید بصورت ساده و با بهره‌وری بالا انجام پذیرد.

تجهیزات مورد استفاده در این لایه باید دارای خصوصیات زیر باشند:

- توان عملیاتی بسیار بالا در لایه سه
- خودداری از انجام کارهای با هزینه بالا و غیر ضروری بر روی داده‌ها مثل اعمال Access List یا فیلترینگ بسته‌ها.
- فراهم آوردن افزونگی[3] و انعطاف پذیری[4] برای در دسترس بودن بالا[5]
- پشتیبانی از ویژگی‌های پیشرفته QoS [6]

لایه توزیع (Distribution Layer)

لایه توزیع شبکه، نقطه تمایز میان لایه دسترسی و لایه هسته می‌باشد. لایه توزیع می‌تواند نقش‌های بسیاری از جمله موارد زیر را بر عهده داشته باشد:

---

[1] Backbone
[2] High-Performance
[3] Redundancy
[4] Resilience
[5] High Availability
[6] Quality of Service

- سیاست[1] ؛ به عنوان مثال می‌توان اطمینان حاصل نمود که ترافیک ارسال شده از بخش خاصی در شبکه، توسط یک اینترفیس و بقیه ترافیک از اینترفیس دیگری ارسال گردد.
- امنیت
- تجمیع[2] یا خلاصه سازی آدرس یا ناحیه
- دسترسی کار گروه[3] یا دپارتمان
- تعریف حوزه‌های Broadcast / Multicast
- مسیریابی بین شبکه‌های مجازی[4]
- عملیات ترجمه رسانه[5]، به عنوان مثال بین ایترنت و Token Ring
- توزیع مجدد[6] بین حوزه‌های مسیریابی، به عنوان مثال بین دو پروتکل مسیریابی مختلف
- علامت گذاری بین پروتکل‌های مسیریابی Static و Dynamic

همچنین برخی از ویژگی‌هایی که می‌توان توسط OSهای سیسکو در لایه توزیع مورد استفاده قرار داد، به شرح زیر است:

- فیلتر اطلاعات بر اساس آدرس مبدا یا مقصد
- اعمال فیلتر بر روی پورت‌های ورودی یا خروجی
- مخفی سازی آدرس‌های شبکه داخلی با فیلتر کردن تبلیغ مسیرها
- مسیریابی Static
- اعمال مکانیسم QoS

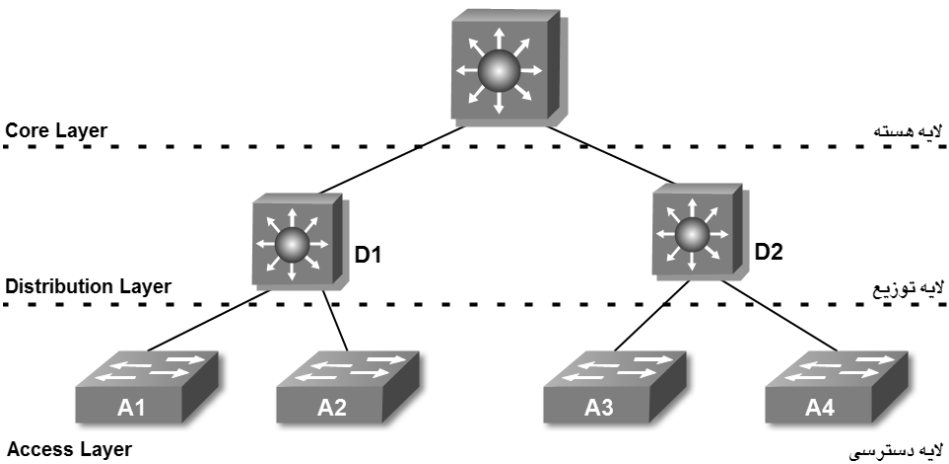
تمام پورت های Uplink تجهیزات موجود در لایه دسترسی در این لایه جمع آوری می‌شوند. سوئیچ‌های لایه توزیع باید ظرفیت پردازش حجم کل ترافیک دستگاه‌های متصل به خود را داشته باشند. این سوئیچ‌ها باید دارای تراکم بالایی از پورت‌های پر سرعت برای امکان پشتیبانی از مجموع سوئیچ‌های لایه دسترسی را داشته باشند.

سوئیچ‌های مورد استفاده در این لایه بهتر است دارای قابلیت های زیر باشند:

---

[1] Policy
[2] Aggregation
[3] Workgroup
[4] Inter VLAN Routing
[5] Media Translation
[6] Redistribution

- تجمیع چندین سوئیچ لایه Access
- توان خروجی بالا در جهت اداره بسته‌های لایه سه
- امنیت و سیاست‌های مبتنی بر عملکرد اتصال از طریق Access List یا فیلتر بسته‌ها
- ویژگی‌های QoS
- لینک‌های سرعت بالا جهت اتصال به لایه‌های هسته و دسترسی
- قابلیت سوئیچینگ چند لایه[1] با توان عملیاتی بالا



لایه دسترسی (Access Layer)

لایه دسترسی فراهم آورنده دسترسی کاربر به بخش‌های محلی یک شبکه می‌باشد. لایه دسترسی معمولا شامل سوئیچ‌ها و پهنای باند به اشتراک گذاشته شده بین کاربران نهایی می‌باشد. سوئیچ‌های مورد استفاده در این لایه بهتر است ویژگی‌های زیر را فراهم آوردند:

- هزینه کم به ازاء هر پورت سوئیچ
- سوئیچ با تراکم پورت بالا (تعداد زیاد پورت)
- دارای پورت Uplink برای اتصال به لایه‌های بالاتر
- اعمال مربوط به دسترسی کاربر، مثل امکان عضویت در VLAN، فیلتر ترافیک، پروتکل و QoS

[1] Multilayer Switching

البته در لایه Access صرفا از سوئیچ‌های لایه دو استفاده نمی‌شود، بلکه ممکن است در برخی مواقع مثل شبکه‌های SOHO [1]، لایه دسترسی فراهم آورنده امکان دسترسی سایتهای راه دور[2] به شبکه سازمانی توسط فناوری‌های مورد استفاده در WAN از قبیل ISDN، Frame Relay یا خطوط اجاره‌ای[3] نیز باشد.

به هر حال این لایه محل اتصال کاربر نهایی به شبکه خواهد بود.

مزایای استفاده از مدل سلسله مراتبی

استفاده از مدل سلسله مراتبی در طراحی شبکه می‌تواند دارای مزایای زیادی باشد که برخی از آنها به شرح زیر است:

- **صرفه جویی در هزینه**

بسیاری سازمان‌ها پس از اتخاذ سیاست استفاده از مدل سلسله مراتبی، گزارش‌هایی مبنی بر صرفه اقتصادی صادر کرده‌اند. این صرفه‌جویی به دلیل آن است که سازمان‌ها دیگر نیازی به تلاش برای انجام تمام کارها بر روی یک پلتفرم Switching/Routing ندارند. همچنین ماهیت مدولار[4] بودن، این مدل را قادر می سازد تا با استفاده بهینه از پهنای باند در هر لایه از سلسله مراتب شبکه، باعث کاهش پهنای باند به هدر رفته گردد.

- **سهولت در درک بهتر**

نگهداری عناصر طراحی به صورت ساده و کوچک، باعث سهولت در درک آنها شده و متعاقباً کمک به کنترل هزینه‌های آموزش و پرسنل می‌نماید. پاسخگویی و سیستم‌های مدیریت شبکه می‌توانند بین لایه‌های مختلف تقسیم شده تا باعث کنترل هزینه‌های مربوط به مدیریت شوند.

- **رشد آسان شبکه**

طراحی سلسله مراتبی باعث تسهیل اعمال تغییرات می‌گردد. در زمان طراحی، خاصیت مدولار بودن اجازه می‌دهد عناصری در طراحی ساخته شوند که بتوان برای رشد شبکه اقدام به تکرار آنها نمود و باعث تسهیل در رشد شبکه شد. در اینصورت چنانچه هر عنصری در طراحی شبکه نیاز به تغییر داشته باشد، هزینه و پیچیدگی ارتقاء آن

---

[1] Small Office/Home Office
[2] Remote Sites
[3] Leased Line
[4] Modular

محدود به بخش کوچکی از شبکه خواهد شد. در صورتیکه هر تغییر جزئی در معماری های دیگر مثل Large، Flat و Meshed، ممکن است تعداد زیادی از سیستم های دیگر را نیز تحت تاثیر قرار دهد.

- **بهبود ایزوله کردن خطاها**

نوع ساختار مدل سلسله مراتبی که شبکه را به عناصر کوچک و با درک آسان تقسیم بندی نموده، باعث بهبود ایزوله نمودن خطاها در این مدل گردیده است. در این مدل مدیران شبکه می‌توانند به راحتی نقاط انتقال در شبکه را تشخیص دهند که این امر می‌تواند در شناسایی نقاط بروز خطا کمک قابل توجهی به آنها باشد.

نکته: برای کسب اطلاعات بیشتر راجع به نحوه طراحی شبکه و همچنین تشریح کاملتر مدل سلسله مراتبی سیسکو، می توانید به کتاب CCDA (Cisco Certified Design Associate) منتشر شده توسط Cisco Press مراجعه نمایید.

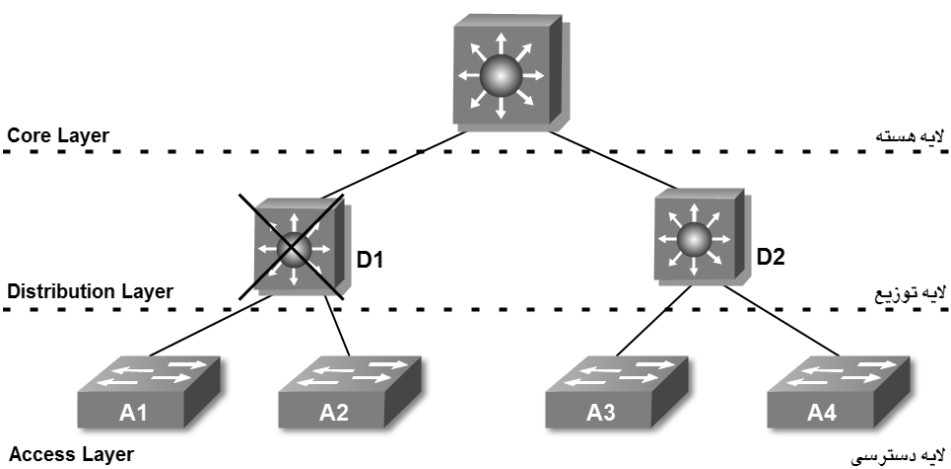
☑ مبحث دوم

High Availability

امروزه شاید به سختی بتوان کسب و کاری در سطح بزرگ و یا حتی متوسط را پیدا کرد که وابستگی حیاتی به فناوری اطلاعات نداشته باشد. در این صورت تداوم کسب و کار نیز بالطبع وابسته به تداوم دسترس‌پذیری سرویس‌های فناوری اطلاعات خواهد بود. مهم ترین بخش تداوم سرویس‌دهی فناوری اطلاعات که با بحث‌های این کتاب نیز در ارتباط است، بخش شبکه سازمان می‌باشد.

در این مبحث می خواهیم دسترس پذیری بالا (High Availability) را بر اساس مدل سه لایه سیسکو و با استفاده از ویژگی‌های Redundancy یا افزونگی تشریح نماییم.

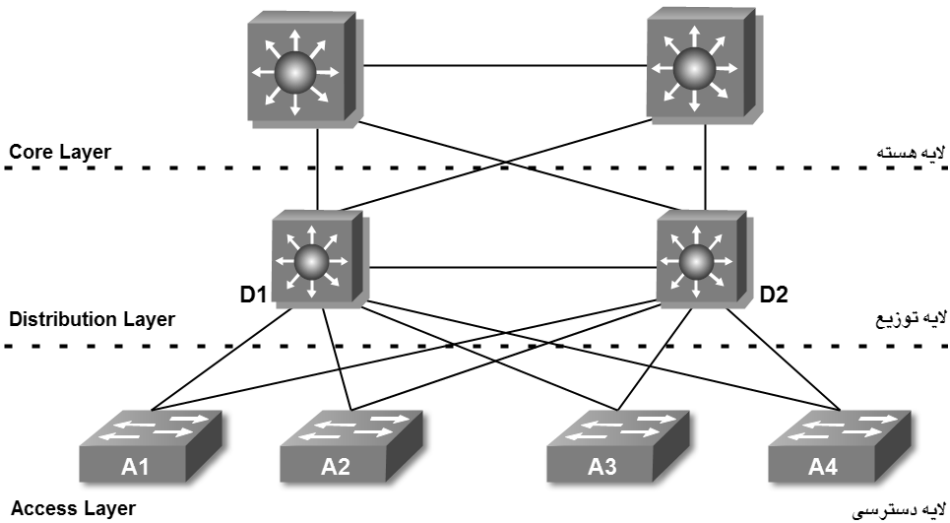
به عنوان مثال به تصویر زیر توجه نمایید. به نظر شما در صورت از دسترس خارج شدن یکی از سوئیچ های لایه توزیع چه اتفاقی خواهد افتاد؟



واضح است که در صورت خرابی سوئیچ D1 دسترسی تمام کاربران متصل به سوئیچ‌های A1 و A2 در شبکه نیز قطع خواهد شد. این اتفاق بد علیرغم سالم بودن سوئیچ‌های A1 ، A2 و لینک‌های متصل به آنها رخ می‌دهد.

در صورت نداشتن افزونگی (Redundancy) در شبکه، خراب شدن حتی یک پورت سوئیچ نیز می تواند باعث از دسترس خارج شدن قسمت بزرگی از کاربران شبکه گردد.

حال فرض کنید در صورتیکه شبکه بالا توسط ویژگی Redundancy به شکل زیر درآید، قطع شدن یک لینک یا سوئیچ چه تاثیری در شبکه خواهد گذاشت؟



در حالت فوق با اعمال ویژگی افزونگی در تجهیزات و لینک‌ها، شبکه‌ای حاصل می‌شود که می‌تواند در بالاترین حالت دسترس پذیری قرار داشته باشد. در این صورت اگر همان مشکل قبلی، یعنی از دسترس خارج شدن سوئیچ D1 اتفاق بیافتد، هیچ خللی در دسترسی کاربران متصل به سوئیچ های A1 و A2 روی نخواهد داد.

همانطور که از مقایسه دو تصویر فوق مشخص است، اعمال Redundancy برای شبکه، شرکت را متحمل هزینه خواهد کرد. تشخیص اینکه آیا نیازی به صرف هزینه بیشتر برای راه اندازی HA با توجه به نحوه کسب و کار شرکت وجود دارد یا خیر، بر عهده مدیر فناوری اطلاعات و مدیران ارشد سازمان می‌باشد.

اما در صورت گذر از هفت خوان رستم! برای متقاعد کردن مدیران ارشد سازمان و ان‌شاءاله کسب رضایت آنها و خرید تجهیزات، نیاز به راه اندازی پروتکل‌هایی برای استفاده از افزونگی لینک‌ها و تجهیزات برای برقراری ویژگی HA خواهید داشت.

اگر صرفا افزونگی شامل سوئیچ‌های لایه دو شود، می‌توان توسط پروتکلSTP و یا Port Channel، از لینک‌ها و مسیرهای جایگزین استفاده نمود. اما در صورتی که بخواهیم از ویژگی

افزونگی در تجهیزات لایه سه بهره ببریم، باید از پروتکل‌های HA در پیکربندی روترها و یا سوئیچ‌های Multilayer استفاده نماییم.

در صورت استفاده از سوئیچ‌های Multilayer باید به این نکته توجه داشته باشید که از اینترفیس SVI این سوئیچ‌ها می‌توان همانند اینترفیس روتر به عنوان Gateway لایه سه کلاینت‌های متصل به شبکه استفاده نمود. البته این سوئیچ‌ها امکان کار با پروتکل‌های مسیریابی را نیز دارند ولی کارآیی آنها در مسیریابی در حد فعالیت‌های پایه‌ای مسیریابی بوده و تمام انتظارات یک روتر را نمی توانند برآورده نمایند.

برای برقراری High Availability، سوئیچ‌های Multilayer باید در صورت خرابی یک لینک یا سوئیچ، باعث جلوگیری از دسترس خارج شدن Gateway کلاینت‌های شبکه گردند.

پروتکل‌های HA که برای افزونگی روترها یا سوئیچ‌هایMultilayer در این مبحث به صورت مشروح به آنها خواهیم پرداخت، عبارتند از: پروتکل‌های HSRP، VRRP و GLBP .

پروتکل HSRP

سیسکو برای راه اندازی HA بر روی محصولات خود اقدام به انتشار یک پروتکل مخصوص به خود با نام HSRP(Hot Standby Router Protocol) نموده است. نکته جالب این است که علیرغم آنکه این پروتکل مخصوص سیسکو بوده و فقط قابلیت کار بر روی تجهیزات این شرکت را دارد ولی توسط سازمان IETF و تحت RFC 2281 نیز منتشر گردیده است.

پروتکل HSRP باعث می‌گردد چندین روتر یا سوئیچ Multilayer از دید کلاینت‌های شبکه به صورت یک Gateway واحد به نظر رسیده و در صورت ایجاد مشکل برای روتر اصلی، روترهای دیگر به نحوی جایگزین روتر معیوب می گردند که از نظر کلاینت‌ها هیچ اتفاقی در شبکه رخ نداده است.

روترهایی که وظیفه برقراری افزونگی برای یک Gateway مشخص را دارند باید در یک گروه HSRP مشترک عضو باشند. در فرآیند راه اندازی پروتکل HSRP، از بین روترهای موجود در گروه، یک روتر با عنوان Primary HSRP Router یا Active HSRP Router انتخاب گردیده و یک روتر نیز به عنوان Standby HSRP Router انتخاب می‌گردد. بقیه روترهای موجود در آن گروه نیز در حالت Listen [۱] قرار می‌گیرند.

---

[۱] منظور از حالت Listen، همان حالت گوش به فرمان است.

روترهای گروه با ارسال متناوب پیام‌های HSRP Hello به یکدیگر، اقدام به بررسی وضعیت روتر Active و دیگر روترهای موجود در گروه خود می‌نمایند. پیام Hello بصورت Multicast به آدرس 224.0.0.2 (تمام روترها) و توسط پورت 1985 پروتکل UDP ارسال می‌گردد. مقدار زمان پیش فرض ارسال پیام Hello نیز هر ۳ ثانیه یکبار می‌باشد.

به گروه‌های HSRP می‌توان یک عدد دلخواه در رنج 0 تا 255 اختصاص داد. به عنوان مثال می توانید عددی شبیه به شماره VLANهای مربوطه به گروه HSRP اختصاص دهید. البته به یاد داشته باشید که اکثر سوئیچ‌های Catalyst سیسکو فقط می‌توانند تا ۱۶ گروه HSRP با ID منحصر بفرد را بر روی یک اینترفیس خود پشتیبانی نمایند. البته منحصر بفرد بودن ID گروه HSRP فقط روی اینترفیس محلی الزامی است. به عنوان مثال شما می توانید یک HSRP Group 10 روی اینترفیس interface VLAN 10 و همزمان یک HSRP Group 10 نیز بر روی اینترفیس interface VLAN 20 داشته باشید. در اینصورت هیچ مشکلی بوجود نیامده و هر گروهHSRP برای اینترفیس مربوطه به صورت منحصر بفرد محسوب می‌گردد.

نحوه انتخاب روتر در HSRP

اساس انتخاب درHSRP مقدار تخصیص داده شده به Priority روترها می‌باشد. این مقدار که می‌تواند در رنج 1 تا 255 باشد، بصورت پیش فرض بر روی مقدار 100 تنظیم گردیده است.

روتری که دارای بالاترین مقدار Priority در گروه باشد به عنوان روتر Active انتخاب می‌گردد. اما در صورتی که Priority روی تمام روترها برابر مقدار پیش فرض(۱۰۰) باشد، انتخاب روتر Active بر اساس اینترفیس دارای بزرگترین آدرسIP در گروه انجام می‌پذیرد. البته در صورتیکه بخواهید اعمال پارتی بازی نمائید می‌توانید توسط دستور زیر اقدام به تخصیص Priority مورد نظر به اینترفیس‌ها نمایید:

Switch(config-if)# **standby** *group* **priority** *priority*

به‌عنوان مثال می‌توان با اختصاص مقدار200 به یک اینترفیس، روتر را به عنوان روتر Active برای گروه مورد نظر معرفی نمود:

Switch(config-if)# standby 1 priority 200

وقتی که پروتکل HSRP بر روی اینترفیس پیکربندی می‌گردد، روتر قبل از وارد شدن به وضعیت Active اقدام به طی یک سری از وضعیت‌ها می‌نماید. در حین طی این مراحل، روتر باید وضعیت بقیه روترهای گروه را مورد بررسی قرار داده تا بتواند وضعیت متناسب با خود را

شناسایی نماید. تجهیزات شرکت کننده در پروسهHSRP باید وضعیت‌های زیر را به ترتیب توسط اینترفیس خود طی نمایند:

۱. Disabled
۲. Init
۳. Listen
۴. Speak
۵. Standby
۶. Active

زمان سنج‌هایHSRP

پروتکل HSRP برای انجام وظایف خود دارای زمان سنج‌های زیر می‌باشد:

۱- **زمان سنج پیام Hello**

پیام Hello در قالب Multicast هر ۳ ثانیه یکبار جهت اعلام وضعیت، توسط هر روتر به دیگر روترهای هم گروه خود ارسال می‌گردد.

۲- **زمان سنج Hold down**

روتری که دارای بالاترین مقدار Priority باشد به عنوان روتر Active و روتر دارای دومین مقدار Priority نیز به عنوان روتر Standby انتخاب می‌شود. فقط روتر Standby است که وظیفه چک کردن وضعیت روتر Active را توسط بررسی پیام‌های Hello بر عهده دارد. در صورتیکه پس از ۱۰ ثانیه یا سپری شدن حداقل سه برابر مدت زمان ارسال پیام Hello، هیچ پیام دیگری از روتر Active توسط روتر Standby دریافت نگردد، فرض را بر خراب شدن روتر Active گذاشته و روتر Standby جایگزین روتر Active می‌گردد.

پس از جایگزین شدن روتر Standby به جای روتر Active، در صورتیکه روترهای دیگری در همان گروه HSRP و در حالت Listen موجود باشند، روتر دارای بالاترین مقدار Priority، به عنوان روتر Standby انتخاب می‌گردد.

جهت تغییر مقدار پیش فرض زمان سنج های فوق، می توان از دستور زیر بهره برد:

Switch(config-if)# **standby** *group* **timers** [**msec**] *hello* [**msec**] *holdtime*

نحوه آدرس دهی Gateway در HSRP

هر روتر موجود در یک گروهHSRP دارای آدرسIP منحصر بفرد بر روی اینترفیس خود می‌باشد. این آدرس برای پروتکل‌های مسیریابی و همچنین مدیریت ترافیک ارسال و دریافت شده توسط روتر مورد استفاده قرار می‌گیرد.

علاوه بر آدرس فوق، روترهای گروه دارای یک آدرسIP مشترک نیز می‌باشند که از آن به عنوان Gateway برای لایه پائین‌تر استفاده می‌شود. این آدرس که آدرس روتر مجازی (Virtual Router Address) نامیده می‌شود، باید توسط پروتکلHSRP همواره در دسترس نگه داشته شود. از این آدرس با نام HSRP Address نیز یاد می‌شود.

آدرس Virtual Router یا HSRP Address به عنوان آدرس Default Gateway، توسط لایه پائین‌تر مورد استفاده قرار می‌گیرد. این آدرس به دلیل خصوصیت HA همواره در دسترس خواهد بود.

به یاد داشته باشید که آدرس IP اینترفیس‌های روتر Active و Standby که می‌خواهند به عنوان Virtual Router ایفای نقش کنند، باید در یک Subnet قرار داشته باشند.

برای تخصیص آدرس HSRP به اینترفیس، می توان از دستور زیر استفاده نمود:

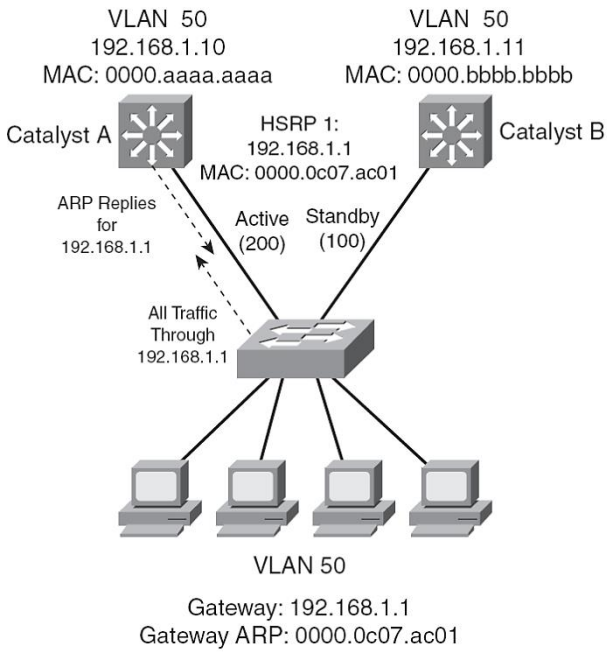
Switch(config-if)# **standby** *group* **ip** *ip-address* [**secondary**]

همانطور که می‌دانید بطور طبیعی روترها برای هر اینترفیس خود یک آدرسMAC منحصر بفرد دارند تا متناظر با آدرسIP پیکربندی شده بر روی اینترفیس مورد استفاده قرار گیرد. پروتکل HSRP نیز برای تخصیص آدرسMAC به اینترفیس‌های پیکربندی شده در این پروتکل، از آدرس اختصاصی خود در رنج 0000.0c07.acXX استفاده می‌نماید که در آن XX یک عدد Hexadecimal و نشان دهنده شماره گروه HSRP می‌باشد. به عنوان مثال آدرس MAC گروه HSRP Group 1 به صورت 0000.0c07.ac01 نمایش داده خواهد شد.

در تصویر زیر یک شبکه ساده نمایش داده شده که در آن یک گروهHSRP وظیفه برقراری Redundancy جهت Gateway شبکه را بر عهده دارد. Catalyst A با Priority=200 به عنوان روترActive انتخاب شده و مسئولیت پاسخگویی به درخواست‌های ARP مربوط به آدرس Gateway را بر عهده دارد. اما Catalyst B در وضعیت Standby قرار گرفته و تا زمانیکه روتر Active در دسترس باشد، از این روتر برای انتقال ترافیک استفاده نمی‌شود.

پیکربندی Catalyst A بصورت زیر انجام گرفته است. البته Catalyst B نیز به همین صورت پیکربندی گردیده و تنها تفاوت در مقدار Priority می‌باشد که در Catalyst B بصورت پیش فرض باقی مانده است.

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# standby 1 priority 200
CatalystA(config-if)# standby 1 preempt
CatalystA(config-if)# standby 1 ip 192.168.1.1
```



پروتکلHSRP دستگاه Catalyst A را به دلیل Priority بالاتر، به عنوان روتر Active و Catalyst B را با توجه به Priority پایین‌تر، به عنوان روتر Standby انتخاب می‌نماید. سپس شماره HSRP Group را در آدرس MAC اختصاصی خود گنجانده و در نهایت آدرس 0000.0c07.ac01 را به عنوان MAC Address برای Virtual Router Address که همان آدرس 192.168.1.1 می‌باشد، در نظر می‌گیرد.

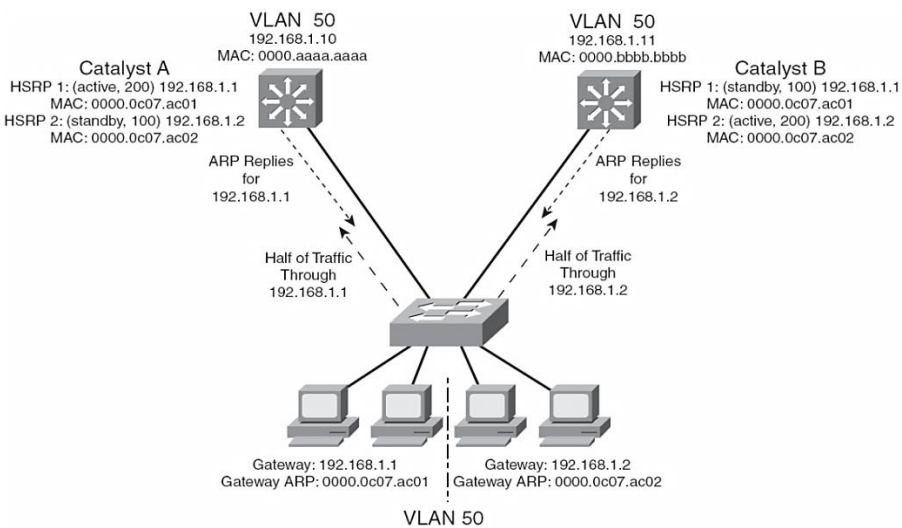
همانطور که در تصویر فوق مشاهده می‌نمایید، آدرسDefault Gateway کلاینت‌ها بصورت 192.168.1.1 پیکربندی گردیده است. کلاینت‌ها برای پیدا کردن آدرس MAC متناظر با آدرسIP مربوط به Default Gateway، اقدام به ارسال پیامARP می‌نمایند. پروتکل HSRP روتر Active را مسئول جواب‌گویی این درخواست‌ها قرار می‌دهد. روتر Active نیز آدرس0000.0c07.ac01 را به عنوان آدرس MAC مربوط به 192.168.1.1 به کلاینت‌ها معرفی می‌نماید.

با توجه به اینکه آدرس MAC مربوط به Default Gateway به صورت مجازی بوده و در روی هر دو روتر Active و Standby موجود می‌باشد، در صورت از دسترس خارج شدن روتر Active، این آدرس همچنان توسط روتر Standby برای کلاینت‌ها قابل دسترس خواهد بود، بدون آنکه کلاینت ها متوجه روی دادن اتفاقی در شبکه گردند.

Load Balancing با HSRP

اگر در طریقه عملکرد پروتکل HSRP دقت کرده باشید، متوجه شده‌اید که این پروتکل ماهیتاً ویژگی Load Balancing را پشتیبانی نمی‌نماید. زمانی که روتر Active در دسترس است، تمام بار شبکه را به تنهایی بر دوش کشیده و روتر محترمStandby در طول این مدت در خواب زمستانی به سر می‌برد. استفاده از یک روتر باعث می‌شود که کل ترافیک از روی یک لینک تبادل گردد که در صورت زیاد بودن حجم ترافیک می‌تواند باعث کندی سرعت تبادل اطلاعات گردد.

برای حل مشکل فوق و برقراری امکان Load Balancing در پروتکل HSRP می‌توان از یک کلک مهندسی! استفاده نمود. در این کلک می‌توان کلاینت‌های شبکه را به دو گروه مختلف با دو آدرس Default Gateway متفاوت تقسیم نمود. سپس به ازاء هر Default Gateway یک گروه HSRP ایجاد کرده و به هر یک از روترها هر دو نقش Active و Standby را اعمال می‌نماییم. به این صورت که روتر اول در گروه یک دارای نقشActive جهت Gateway اول و نقش Standby برای Gateway دوم خواهد بود. روتر دوم نیز بر عکس روتر اول، نقش‌ها را برای هر گروه بر عهده خواهد گرفت. به عنوان مثال، شبکه قبلی با اعمال کلک فوق، به صورت زیر خواهد بود:



پروتکل VRRP

پروتکل VRRP(Virtual Router Redundancy Protocol) توسط سازمان IETF طی RFC 2338 به عنوان جایگزین استاندارد پروتکل HSRP معرفی گردید.

این پروتکل از نظر عملکرد بسیار شبیه پروتکل HSRP بوده و برای یادگیری فقط نیاز به آشنایی با اصطلاحات[1] مورد استفاده در این پروتکل خواهید داشت. به عبارت دیگر اگر نحوه عملکرد و پیکربندی پروتکل HSRP را درک نموده باشید، می‌توان گفت که پروتکل VRRP را نیز یاد گرفته‌اید.

پروتکلVRRP برای ایجاد Redundancy جهت Default Gateway مورد استفاده قرار می‌گیرد. روتر Active در پروتکل VRRP با نام Master Router شناخته می‌شود. روتری به عنوان Master انتخاب می‌شود که دارای بالاترین مقدار Priority در بین روترهای موجود در گروه باشد. بقیه روترهای موجود در گروه VRRP در وضعیت Backup قرار می‌گیرند.

عدد اختصاص داده شده به VRRP Group می‌تواند در رنج 1 تا 255 قرار داشته باشد. همچنین مقدار تخصیص داده شده به Priority روترها نیز می‌تواند در رنج 1 تا 254 قرار داشته باشد. مقدار پیش فرض Priority در پروتکل VRRP برابر با 100 می‌باشد.

آدرس MAC اختصاص داده شده به Virtual Router باید در رنج 0000.5e00.01XX باشد که در آن XX نشان دهنده عدد مربوط به VRRP Group می‌باشد که به صورت Hexadecimal نمایش داده می‌شود.

مدت زمان ارسال پیام VRRP Hello هر یک ثانیه می‌باشد. این پیام‌ها در قالب Multicast به آدرس 224.0.0.18 و توسط IP Protocol Type 112 ارسال می‌شوند.

پروتکلVRRP بر خلاف پروتکل HSRP امکان پشتیبانی از مکانیسم Tracking برای انتخاب روترهایی با ظرفیت بهتر به عنوان روتر Master را ندارد.

همانطور که ملاحظه می نمایید، هر چند پروتکل VRRP بر اساس پروتکل HSRP شکل گرفته، و بصورت استاندارد توسط سازمان IETF منتشر گردیده، اما امکانات پروتکل HSRP را بصورت کامل پشتیبانی نمی‌نماید.

البته لازم به ذکر است که برای برقراری Load Balancing در این پروتکل نیز باید همانند HSRP از کلک مهندسی گفته شده بهره برد.

[1] Terminology

پروتکل GLBP

سیسکو برای غلبه بر مشکلات موجود در پروتکل‌های HSRP و VRRP مخصوصا در زمینه Load Balancing، اقدام به معرفی پروتکل GLBP(Gateway Load Balancing Protocol) نموده است. این پروتکل مختص سیسکو بوده و فقط تجهیزات سیسکو از آن پشتیبانی می‌کنند.

پروتکلGLBP برای برپایی HA، عملکردی شبیه پروتکل‌های HSRP و VRRP داشته و فقط در استفاده از اصلاحات دارای تفاوت‌هایی با آنها می‌باشد. پروتکل GLBP برای برقراری امکان Load Balancing، همان کلک مهندسی مورد استفاده در پروتکل‌های قبلی را با کمی تغییر و به صورت پویا انجام می‌دهد.

در پروتکلGLBP نیز همانند دو پروتکل قبلی، باید روترهای مورد نظر برای برقراری Virtual Router را در یک گروه قرار داد. این گروه می تواند دارای شناسه عددی در رنج 0 تا 1024 باشد.

در پروتکلGLBP به جای داشتن یک روتر Active در گروه، همه روترها در وضعیت Active قرار گرفته و اقدام به ارائه Virtual Router به صورت گروهی می‌نمایند. با توجه به فعال بودن تمام روترهای گروه، امکان توزیع بار (Load Balancing) نیز فراهم می‌گردد.

در این صورت کلاینت‌های شبکه فقط دارای یک آدرسIP جهت Default Gateway خواهند بود. روترهای گروه GLBP نیز همگی در حالت فعال قرار داشته و علیرغم پشتیبانی از یک آدرس IP خاص جهت Virtual Router، آدرس MAC اختصاص داده شده هر یک از روترها به آدرس Gateway متفاوت خواهد بود. کلاینت‌های شبکه با ارسال پیام‌هایARP اقدام به یادگیری آدرس MAC مربوط به آدرسGateway خود می‌نمایند. پروتکلGLBP نیز در جواب درخواست ARP هر کلاینت، اقدام به ارسال آدرسMAC مربوط به یکی از روترهای Active موجود در گروه می‌نماید.

روتر Active Virtual Gateway

ترفند پروتکلGLBP برای برقراریLoad Balancing، استفاده از ویژگی AVG جهت انجام کلک مهندسی مورد نظر می‌باشد. به این صورت که روتر دارای بالاترین مقدار Priority یا بزرگترین آدرس IP در گروه، به عنوان روتر Active Virtual Gateway انتخاب می‌گردد. این روتر که به اختصار AVG نامیده می‌شود، مسئول پاسخگویی به تمام درخواست‌های ARP مربوط به Virtual Router خواهد بود.

روترAVG بر اساس نوع الگوریتم Load Balancing پیکربندی شده بر روی خود، اقدام به بازگرداندن آدرس‌های MAC مجازی مربوط به روترهای گروه می‌نماید.

این روتر همچنین وظیفه اختصاص آدرس‌های MAC مجازی به روترهای شرکت کننده در گروهGLBP را بر عهده دارد. تعداد آدرس‌های MAC مجازی در هر گروه نهایتا می‌تواند به چهار عدد برسد. معنی این محدودیت آن است که عملیات Load Balancing در پروتکل GLBP نهایتا می‌تواند توسط چهار عدد روتر انجام پذیرد.

هر یک از چهار روتر فوق به عنوان روتر AVF (Active Virtual Forwarder)، وظیفه تبادل دیتای مربوط به یک Virtual MAC Address را بر عهده می‌گیرند.

روترهای دیگر موجود در گروه GLBP، می‌توانند به عنوان Backup یا Secondary Virtual Forwarder برای پشتیبانی روترهایAVF مورد استفاده قرار گیرند. البته توجه داشته باشید که ویژگی AVG نیز می‌تواند به عنوان نقش دوم به یک روتر اعمال گردد.

برای تنظیم Priority در پروتکل GLBP می توان از دستور زیر بهره برد. این مقدار می تواند در رنج 0 تا 255 تنظیم گردد.

Switch(config-if)# **glbp** *group* **priority** *level*

پروتکل GLBP برای بررسی وضعیت روترهای موجود در گروه از پیام‌های GLBP Hello استفاده می‌نماید. زمان سنج‌های مورد استفاده در GLBP نیز شبیه پروتکل HSRP بوده و برای تغییر مقدار پیش فرض آنها می‌توانید از دستور زیر استفاده نمایید:

Switch(config-if)# **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*

روتر Active Virtual Forwarder

از بین روترهای شرکت کننده در گروهGLBP، چهار روتر می‌توانند نقشAVF را بر عهده بگیرند. زمانی که روترAVG اقدام به انتخاب یک روتر به عنوان AVF می‌نماید، یک آدرسMAC مجازی نیز به آن اختصاص می‌دهد.

آدرسMAC مجازی مورد استفاده توسط پروتکلGLBP، در رنج0007.b4xx.xxyy قرار دارد. که در آن xx.xx یک عدد شانزده بیتی می‌باشد که 6 بیت آن صفر متوالی و 10 بیت دیگر معادل عدد مربوط به GLBP Group است. همچنین yy نیز یک مقدار 8 بیتی است که نشان دهنده عدد Virtual Forwarder می‌باشد.

پروتکلGLBP برای بررسی وضعیت روترهایAVF از ارسال متناوب پیام‌های Hello استفاده می‌نماید. بدین صورت که اگر روترAVG پس از اتمام مدت زمانHold Time، هیچ پیامی از

روترAVF دریافت ننماید، فرض را بر خرابی روتر مذکور گذاشته و نقش آن را بر عهده روتر دیگر موجود در گروه قرار خواهد داد.

همچنین پروتکلGLBP برای تخصیص نقش AVF به یک روتر، می‌تواند از خصوصیت Weight استفاده نماید. مقدار Weight که باید عددی بین 1 تا 254 باشد، بصورت پیش فرض بر روی مقدار 100 قرار داده شده است. البته مقدارWeight به ازاء Down شدن اینترفیس‌های روتر، بصورت خودکار کاهش می‌یابد.

پروتکلGLBP برای تعیین زمانی که یک روتر دیگر نمی‌تواند با توجه به مقدار Weight دارای نقشAVF باشد، از ویژگی آستانه تحمل[1] استفاده می‌نماید. زمانی که مقدار Weight کمتر از مقدار آستانه تحمل گردد، روتر باید نقش AVF خود را تحویل داده و تا هنگامیکه مقدار Weight مجددا بالاتر از مقدار Threshold قرار گیرد و روتر بتواند نقش خود را باز پس گیرد، صبر کند.

GLBP Load Balancing

پروتکلGLBP برای برقراری Load Balancing از روترAVG بهره می‌برد. روترAVG نیز Load Balancing را با توزیع آدرس‌های MAC مجازی در بین کلاینت‌ها انجام می‌دهد. توزیع آدرسMAC را می‌توان توسط یکی از روش‌های زیر انجام داد:

۱- **Round Robin**

در این حالت آدرس‌های MAC مجازی قابل دسترس بصورت نوبتی در جواب هر پیام جدید درخواستARP ارسال می‌گردد. این کار باعث می‌شود بار ترافیک بصورت مساوی بین تمام روترهای AVF موجود در گروه تقسیم گردد.

این روش بصورت پیش فرض در GLBP فعال می‌باشد.

۲- **Weighted**

در این حالت مقدار Weight مشخص کننده سهم ترافیکی است که باید از طریق یک روتر AVF ارسال گردد. هر چه مقدار Weight یک روترAVF بالاتر باشد، آدرسMAC مجازی آن روتر، بیشتر در جواب درخواست‌هایARP ارسال خواهد شد.

در صورتیکه ویژگی ردیابی[2] اینترفیس‌ها بر روی روتر AVF تنظیم نشده باشد، مقدار Maximum Weight به عنوان مقدار Weight روتر در نظر گرفته می شود.

---

[1] Threshold
[2] Tracking

۳- **Host dependent**

در این روش که Host Dependent یا وابسته به میزبان نامیده می‌شود، در جواب درخواست‌های ARP یک میزبان همواره یک آدرس MAC مجازی پاسخ داده می‌شود.
این روش وقتی مورد استفاده قرار می‌گیرد که کلاینت‌ها به یک آدرس MAC ثابت نیاز داشته باشند.

از دستور زیر می‌توان برای پیکربندی روش Load Balancing مورد نظر بر روی روتر AVF استفاده نمود:

Switch(config-if)# **glbp** *group* **load-balancing** [**round-robin** | **weighted** | **hostdependent**]

فعال سازی GLBP

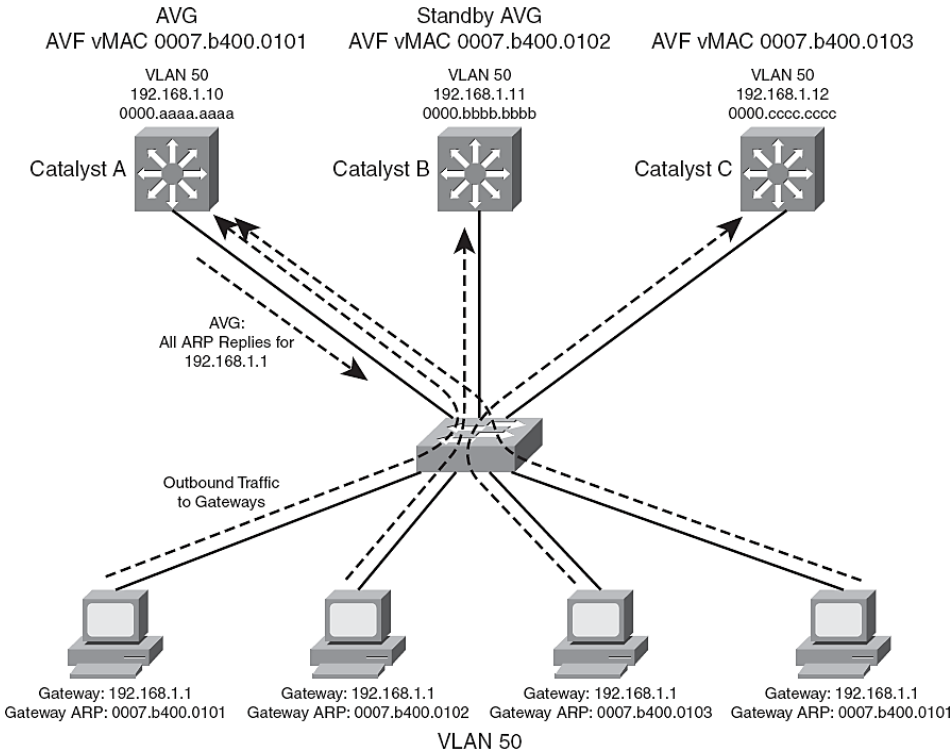
برای فعال سازی پروتکلGLBP، باید توسط دستور زیر اقدام به اختصاص آدرس Virtual IP Address به گروه مورد نظر نمایید:

Switch(config-if)# **glbp** *group* **ip** [*ip-address* [**secondary**]]

اگر از دستور فوق برای تنظیم آدرس Virtual IP استفاده نکنید، روتر به صورت خودکار می‌تواند این آدرس را از روترهای هم گروهی خود یاد بگیرد. البته این یادگیری خودکار در صورتی امکان پذیر خواهد بود که آدرسVirtual IP را حداقل بر روی روتر AVG پیکربندی کرده باشید.

به عنوان مثال به تصویر زیر دقت نمایید. در این شبکه سه سوئیچ Multilayer وجود دارند که همگی عضو یک گروهGLBP هستند. با توجه به اینکه، Catalyst A به عنوان روتر AVG انتخاب گردیده، بنابراین وظیفه انجام عملیات مربوط به GLBP بر عهده Catalyst A خواهد بود. این سوئیچ به تمام درخواست‌های ARP صادر شده از کلاینت‌ها پاسخ خواهد داد.

سوئیچ‌های Catalyst A ,B ,C، نقش AVF را بر عهده دارند. همچنین Catalyst B به عنوان پشتیبان AVG در نظر گرفته شده تا در صورت از دسترس خارج شدن Catalyst A، نقش AVG را سریعا بر عهده گیرد.



روش Load Balancing در این شبکه نیز به صورت پیش فرض و بر اساس Round Robin انجام می‌گیرد. به همین دلیل روتر AVG در جواب درخواست‌های ARP کلاینت‌ها، به ترتیب اقدام به معرفی آدرس‌های MAC مجازی سوئیچ‌های AVF می‌نماید. با توجه به اینکه در این شبکه سه سوئیچ دارای نقش AVF می‌باشند، در جواب سه درخواست اول به ترتیب آدرس‌های MAC مربوط به Catalyst A ، B و C را ارسال نموده و در جواب درخواست چهارم، چرخه مجدد به اول برگشته و آدرس MAC مجازی مربوط به Catalyst A داده می‌شود. علیرغم اینکه بر روی تمام کلاینت‌ها یک آدرسGateway مشترک تنظیم گردیده شده است، پروتکلGLBP با کمک روترAVG و آدرس‌های MAC مجازی، عمل Load Balancing را بر روی تمام روترهای AVF موجود در گروه (نهایتا چهار روتر AVF) انجام می‌دهد.

جدول مقایسه پروتکل‌های HA

برای درک بهتر، پروتکل‌های HSRP، VRRP و GLBP در جدول زیر مقایسه گردیده است:

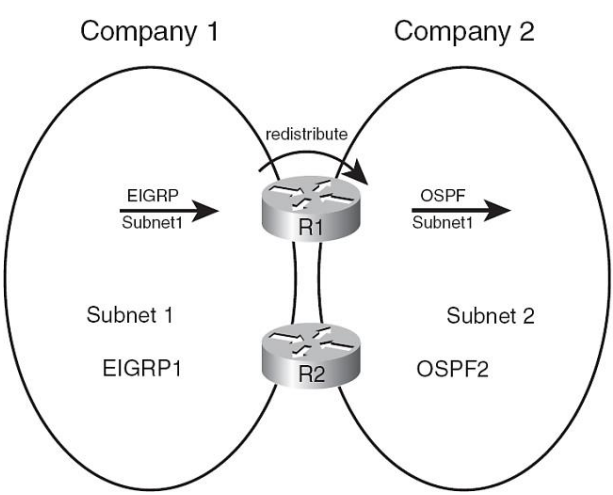
Protocol Features		HSRP	VRRP	GLBP
Router role		1 active router. 1 standby router. 1 or more listening routers.	1 master router. 1 or more backup routers.	1 AVG up to 4 AVF routers passing traffic.- up to 1024 virtual routers
		Use virtual ip address.	Can use real router ip address, if not, the one with highest priority become master.	Use virtual ip address.
Scope		Cisco proprietary	IEEE standard	Cisco proprietary
Election		Active Router: 1-Highest Priority 2-Highest IP	Master Router: 1-Highest Priority 2-Highest IP	Active Virtual Gateway (AVG): 1-Highest Priority 2-Highest IP
Optimization features	**Tracking**	yes	no	yes
	Preempt	yes	yes	yes
	Timer adjustments	yes	yes	yes
Traffic type		224.0.0.2 – UDP 1985 (version1) 224.0.0.102-UDP 1985 (version2)	224.0.0.18 – IP 112	224.0.0.102 UDP 3222
Timers		Hello – 3 seconds	Advertisement 1 second	Hello – 3 seconds
		(Hold) 10 seconds	(Master Down Interval)3 * Advertisement + skew time (Skew time)(256-priority) / 256	(Hold) 10 seconds
Load-balancing functionality		Multiple HSRP group per interface/SVI/routed int.	Multiple VRRP group per interface/SVI/routed int.	Load-balancing : 1.Weighted 2.Host-dependent 3. Round-Robin
		Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP)	Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP)	Clients are transparently updated with virtual MAC according to load-balancing algorithm through ARP requesting a unique virtual gateway.

☑ مبحث سوم

Redistribution

در فصل‌های گذشته پروتکل‌های مسیریابی بطور کامل تشریح شده است. همانطور که می‌دانید در بحث پروتکل‌های مسیریابی داخلی(IGP) ما دارای سه پروتکل اصلی با نام‌های RIP، EIGRP و OSPF هستیم. هر یک از سه پروتکل مذکور ممکن است با توجه به شرایط و نیازهای شبکه، توسط طراحان مورد استفاده قرار گیرند. استفاده دلخواه هر یک از این پروتکل‌ها در شبکه‌های مختلف هیچ اشکالی ندارد، اما مشکل وقتی پیش می‌آید که بنا به دلایلی بخواهیم دو شبکه مستقل که هر کدام دارای پروتکل مسیریابی مختص به خود می‌باشد را با یکدیگر ادغام نماییم. همچنین در برخی موارد روترها مسیرهای یاد گرفته شده توسط پروتکل هایIGP را باید توسط پروتکلBGP تبلیغ نموده و یا بالعکس مسیرهای یاد گرفته شده توسطBGP را باید از طریق پروتکل‌های IGP تبلیغ نمایند.

برای حل مشکل اتصال شبکه‌های دارای پروتکل‌های مسیریابی متفاوت با یکدیگر، از ویژگی Redistribution استفاده می‌نماییم. به عنوان مثال اگر بخواهیم دو شبکه را به یکدیگر متصل نماییم که یکی از آنها بر اساسEIGRP و دیگری بر اساسOSPF مسیریابی می‌شوند، می‌توان از خصوصیت Redistribution جهت توزیع مجدد مسیرها استفاده نمود.



دلایل استفاده از Redistribution

دلایل گسترده و متفاوتی می‌تواند برای استفاده از Redistribution وجود داشته باشد. از جمله این دلایل می توان به موارد زیر اشاره نمود:

- ادغام شبکه‌هایی که از پروتکل‌های IGP متفاوتی استفاده می‌نمایند.
- ادغام شبکه‌هایی که از پروتکل IGP شبیه به هم استفاده نموده ولی ممکن است پارامترهای پیکربندی شده پروتکل‌ها در هر شبکه با یکدیگر متفاوت باشد.
- شبکه گسترده‌ای که برای مدت زمان طولانی از چندین پروتکل مسیریابی استفاده نموده است.
- شرکتی که به بخش‌های مختلف کاری یا تجاری تقسیم بندی گردیده و هر بخش دارای مدیریت مستقل شبکه می‌باشد.
- برقراری ارتباط بین همکاران.
- برای قابلیت همکاری بین تجهیزات شبکه‌ای با برندهای متفاوت. (به عنوان مثال اجرای OSPF بر روی تجهیزات غیر سیسکو و راه اندازی EIGRP بر روی تجهیزات سیسکو)
- استفاده بین پروتکل‌هایIGP با پروتکلBGP. مخصوصا زمانی که برای برقراری ارتباط بین بخشهای زیاد یک شرکت چند ملیتی از پروتکل BGP استفاده می‌شود.
- ارتباطات WAN لایه سه (MPLS).

مفاهیم Redistribution و فرآیندها

برای Redistribution حداقل یک روتر برای انجام موارد زیر مورد نیاز می‌باشد:

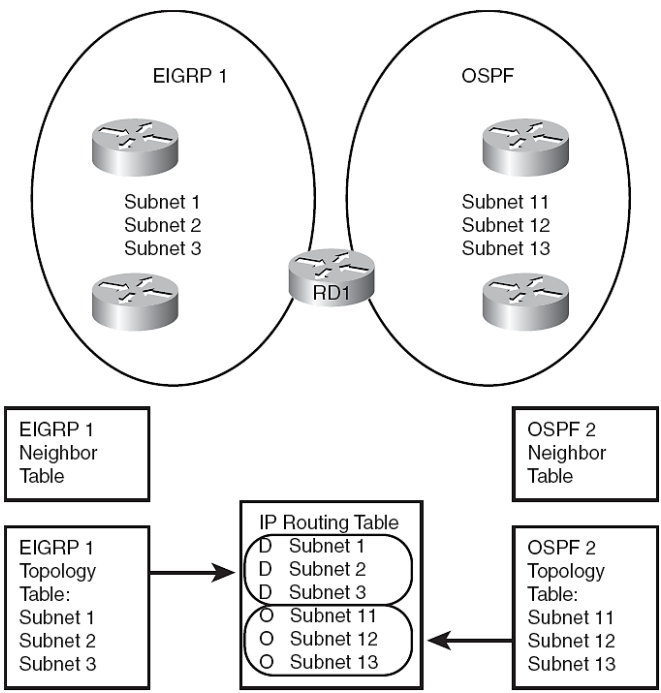
۱- حداقل دارای یک لینک فیزیکی متصل به هر حوزه مسیریابی باشد.

۲- روتر برای کار در حوزه‌های مسیریابی مورد نظر، پیکربندی شده باشد.

۳- به طور خاص برای هر پروتکل مسیریابی باید پیکربندی Distribution مربوطه نیز انجام پذیرد.

به عنوان مثال در تصویر زیر مراحل اول و دوم بر روی روتر RD1 انجام گردیده است. روترRD1 در شبکه سمت چپ برای پروتکلEIGRP و در شبکه سمت راست برای پروتکل OSPF پیکربندی گردیده و از هر دو پروتکل شبکه‌های تبلیغ شده را فرا می‌گیرد. ولی این روتر هنوز جهت عملیات Redistribution پیکربندی نشده و بین دو شبکه مسیریابی نمی‌نماید.

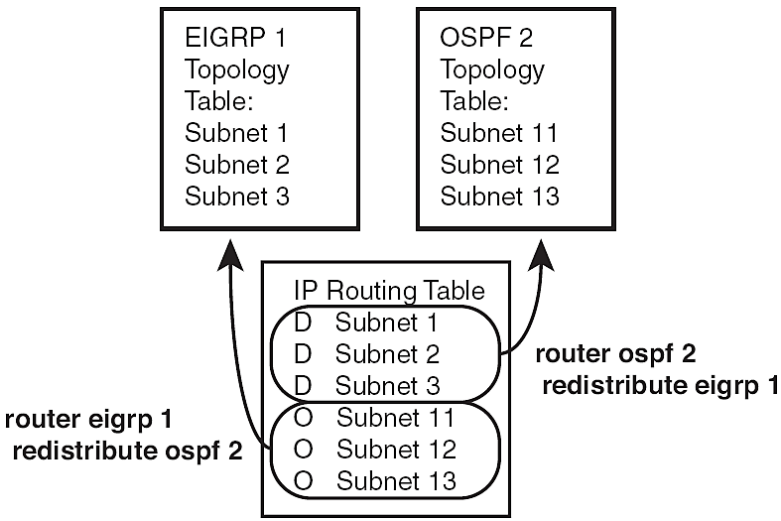
هدف نهایی در این شبکه آن است که آدرس‌های تبلیغ شده توسط پروتکل EIGRP (زیر شبکه های 1، 2 و3) در محدوده OSPF منتشر شده و همچنین شبکه‌های تبلیغ شده توسط پروتکل OSPF (زیر شبکه های 11، 12 و 13) نیز در محدوده EIGRP منتشر گردند. برای این منظور باید اطلاعات هر یک از شبکه‌ها در جدول Topology پروتکل مسیریابی شبکه مقابل ثبت گردد. اما با توجه به اینکه هر پروتکل مسیریابی اطلاعات متفاوتی درباره مسیرها را در جدول Topology خود ذخیره می نماید، این اطلاعات با یکدیگر متفاوت خواهند بود.



از آنجا که جزئیات بین جداول توپولوژی پروتکل‌های مختلف، متفاوت است؛ مکانیسم Redistribution نمی‌تواند از جدول Topology برای توزیع مجدد مسیرها استفاده نماید. لذا عملیات توزیع مجدد مسیرها بر اساس جدول IP Routing که یک جدول حاوی مسیرهای هر دو پروتکل می‌باشد، انجام می‌پذیرد.

روتر RD1 پس از تکمیل جدول IP Routing، اقدام به کامل کردن جداول Topology هر یک از پروتکل‌های مسیریابی موجود بر روی خود می‌نماید. به این صورت که مسیرهای به دست آمده از طریق OSPF را در جدول توپولوژی EIGRP موجود بر روی خود و مسیرهای به دست

آمده توسط EIGRP را در جدول توپولوژی OSPF بر روی خود ثبت می‌نماید. اما همانطور که گفتیم فیلدهای موجود در جداول توپولوژی پروتکل‌های مسیریابی مختلف با یکدیگر متفاوت هستند لذا نحوه پیکربندی Redistribution است که مشخص می‌نماید مسیرهای به دست آمده توسط پروتکل‌های مسیریابی با چه پارامترهایی باید در جدول Topology یکدیگر ثبت گردند.



در ادامه به بررسی نحوه پیکربندی پارامترهای Redistribution پروتکل‌های مسیریابی مختلف می‌پردازیم.

Redistribution در EIGRP

دستور زیر برای پیکربندی Redistribution در محیط EIGRP مورد استفاده قرار می‌گیرد:

redistribute *protocol* [*process-id* | *as-number*] [**metric** *bw delay reliability load mtu*] [**match** {**internal** | **nssa-external** | **external 1** | **external 2**}] [**tag** *tagvalue*] [**route-map** *name*]

جدول زیر شامل تشریح پارامترهای مورد استفاده در دستور فوق می‌باشد:

پارامتر	توضیح
Protocol	مشخص کننده پروتکل مورد نظر برای عملیات توزیع مجدد می‌باشد. (مثل پروتکل های RIP، EIGRP، OSPF، BGP، مسیرهای Static و اتصالات مستقیم)

پارامتر	توضیح
Process-id as-number	اگر یک پروتکل مسیریابی دارای Process-id یا AS-number جهت Redistribution مد نظر باشد، از این پارامتر می‌توان استفاده نمود.
Metric	جهت مشخص نمودن چهار مؤلفه bandwidth، delay، reliability و link load به همراه MTU استفاده می‌گردد.
Match	اگر توزیع مجددOSPF مد نظر باشد، این گزینه برای تطبیق مسیرهای داخلی و خارجی مورد استفاده قرار می‌گیرد.
Tag	اختصاص مقدار صحیح به مسیرهای توزیع شده. مقدار تخصیص داده شده به Tag می‌تواند بعدا جهت تطبیق با Route map مسیرها مورد استفاده قرار گیرد.
Rout-map	برای فیلتر نمودن مسیرها، تنظیم Metric و Rout-tag مورد استفاده قرار می‌گیرد.

Redistribution در OSPF

دستور مورد استفاده برای Redistribution در محیط‌های OSPF بسیار شبیه دستور مورد استفاده در EIGRP می‌باشد:

redistribute *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2** | **nssa-external**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]

به دلیل شباهت دستور فوق با دستور مورد استفاده در EIGRP، فقط به تشریح پارامترهای متفاوت این دو دستور می‌پردازیم:

پارامتر	توضیح
Metric	برای تخصیص Cost به مسیرهای مورد نظر جهت توزیع مجدد مورد استفاده قرار می‌گیرد.
Metric-type {1 | 2}	جهت تعیین نوع Metric خارجی مورد استفاده برای مسیرهای توزیع مجدد شده توسط این دستور: (E1 Routes) 1 یا (E2 Routes) 2
Subnet	این دستور منحصراً برای پروتکل OSPF بوده و جهت توزیع مجدد زیر شبکه‌های مشتق شده از Classful مورد استفاده قرار می‌گیرد. بدون این پارامتر فقط می‌توان شبکه‌های Classful را در Redistribution مورد استفاده قرار داد.

Redistribution در RIP

همان دستور مورد استفاده در پروتکل‌های قبلی با اندکی تغییر برای RIP نیز مورد استفاده قرار می‌گیرد:

redistribute *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2** | **nssa-external**}] [**route-map** *map-tag*]

توجه داشته باشید Metric مورد استفاده در پروتکلRIP، تعداد گام (hop-count) می‌باشد. حداکثر گام (روتر)های موجود در شبکه‌های مبتنی بر RIP می تواند ۱۵ عدد باشد.

Redistribution در BGP

همانطور که قبلا گفته شد یک راه جهت تبلیغ شبکه‌ها توسط پروتکلBGP استفاده از دستور Network می‌باشد. اما راه دیگر، توزیع مجدد (Redistribute) مسیرهای به دست آمده از طریق پروتکل‌هایIGP درBGP می‌باشد. این پروتکل IGP می‌تواند هر یک از پروتکل‌های RIP، EIGRP، OSPF و یا هر پروتکل دیگری باشد.

انجام Redistribution شبکه‌های داخلی درBGP می‌تواند ترسناک به نظر برسد؛ چرا که شما با دستان خود! آدرس شبکه داخلی را فاش می‌کنید!! همچنین قبل از انجام این کار در نظر داشته باشید که یادگیری برخی از مسیرها توسط پروتکلBGP امکان پذیر می‌باشد بدون آنکه نیازی به Redistribution آنها داشته باشید.

اما اگر در نهایت تصمیم به توزیع مجدد مسیرهای داخلی درBGP گرفتید، اعمال دقیق فیلترینگ می‌تواند کمک موثری باشد تا فقط مسیرهای مورد نظر شما درBGP توزیع مجدد یابند.

دستور اجرای Redistribution در BGP نیز شبیه به دستورات قبلی در پروتکل‌های مسیریابی دیگر و به صورت زیر می‌باشد:

redistribute *protocol* [***process-id***] {**level-1** | **level-1-2** | **level-2**} [***autonomous-system-number***] [**metric**{***metric-value*** | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

☑ مبحث چهارم

سایر پروتکل‌ها

در این مبحث به تشریح پروتکل‌ها و سرویس‌هایی می‌پردازیم که ممکن است در بخش‌های مختلف سوئیچینگ یا مسیریابی مورد استفاده قرار گیرند، اما به قدری گسترده نیستند که بتوان یک فصل یا مبحث خاص را برای آنها در نظر گرفت.

پروتکل CDP

پروتکل CDP(Cisco Discovery Protocol) در درجه اول جهت کشف آدرس تجهیزات همسایه و همچنین کشف نوع و مدل سخت افزاری آنها مورد استفاده قرار می‌گیرد.

این پروتکل همچنین می‌تواند برای نمایش اطلاعات مربوط به اینترفیس‌های روتر محلی نیز به کار گرفته شود.

پروتکل CDP یک پروتکل مستقل است که فقط امکان اجرا بر روی تجهیزات تولیدی سیسکو از قبیل روترها، Bridgeها، سوئیچ‌ها و Access Serverهای این شرکت را دارد. سیسکو تا کنون دو نسخه از این پروتکل را منتشر نموده است.

استفاده ازCDP MIB[1] در کنار پروتکلSNMP، نرم افزارهای مدیریت شبکه را قادر می‌سازد تا با تشخیص نوع تجهیزات همسایه و یادگیری آدرس SNMP Agent آنها، اقدام به ارسال پیام‌های SNMP query به آن تجهیزات نمایند.

پروتکل CDP امکان اجرا بر روی رسانه‌های مختلف از جمله شبکه‌های محلی (LAN)، Frame Relay و ATM[2] را دارد. به دلیل اینکه پروتکلCDP بر روی لایه دوم (Data Link) اجرا می‌گردد هیچ وابستگی به پروتکل مورد استفاده در لایه سوم (Network) نداشته و بنابراین می‌تواند بین تجهیزات دارای پروتکل‌های مختلف لایه سوم نیز اجرا گردد.

پس از راه اندازی CDP، تجهیزات اقدام به ارسال پیام‌های Advertisement بصورت متناوب و در قالب Multicast در شبکه می‌نمایند.

---

[1] CDP Management Information Base
[2] Asynchronous Transfer Mode

پیام‌های Advertisement حداقل اقدام به معرفی یک آدرس جهت دریافت پیام‌های SNMP می‌نمایند. این پیام‌ها همچنین حاوی زمان سنج‌های مورد نیاز پروتکل CDP از قبیل Holdtime و Information می‌باشند. دستگاه‌ها ضمن ارسال پیام‌های Advertisement، پیام‌های رسیده از تجهیزات همسایه خود را نیز مورد بررسی قرار داده تا مشخص نمایند چه زمانی نیاز است که اینترفیس‌های خود را برای رسانه‌های مورد نظر Up و یا Down نمایند.

برای راه اندازی پروتکل CDP می‌توان از دستورات زیر استفاده نمود:

Setting the CDP Transmission Timer and Hold Time		
	Command	**Purpose**
Step 1	**cdp timer** seconds	Specifies frequency of transmission of CDP updates.
Step 2	**cdp holdtime** seconds	Specifies the amount of time a receiving device should hold the information sent by your device before discarding it.

Enabling CDP on a Local Router	
Command	**Purpose**
cdp run	Enable CDP.
cdp advertise-v2	Enables CDP Version-2 advertising functionality on a device.

Enabling CDP on an Interface	
Command	**Purpose**
cdp enable	Enables CDP on an interface.

Monitoring and Maintaining CDP	
Command	**Purpose**
clear cdp counters	Resets the traffic counters to zero.
clear cdp table	Deletes the CDP table of information about neighbors.
show cdp	Displays the interval between transmissions of CDP advertisements, the number of seconds the CDP advertisement is valid for a given port, and the version of the advertisement.
show cdp entryentry-name [**protocol**| **version**]	Displays information about a specific neighbor. Display can be limited to protocol or version information.
show cdp interface[**type number**]	Displays information about interfaces on which CDP is enabled.
show cdp	Displays the type of device that has been discovered, the name of the

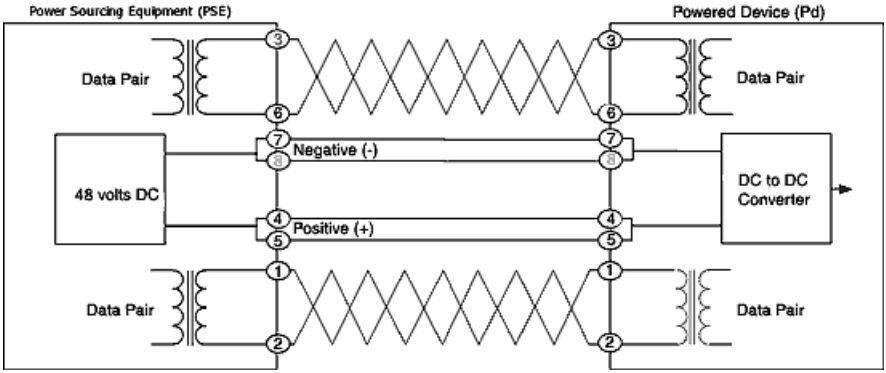
Monitoring and Maintaining CDP	
neighbors[*type number*] [**detail**]	device, the number and type of the local interface (port), the number of seconds the CDP advertisement is valid for the port, the device type, the device product number, and the port ID. Issuing the **detail** keyword displays information on the native VLAN ID, the duplex mode, and the VTP domain name associated with neighbor devices.
show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.
show debugging	Displays information about the types of debugging that are enabled for your router. See the *Cisco IOS Debug Command Reference* for more information about CDP **debug** commands.

استاندارد PoE

سازمان IEEE برای حمل جریان انرژی (جریان برق) مورد نیاز برخی تجهیزات بر روی کابل دیتای شبکه‌های کامپیوتری، اقدام به معرفی استاندارد PoE(Power over Ethernet) در قالب سری استانداردهای IEEE 802.1aX نموده که X بیانگر نسخه‌های مختلف این استاندارد می‌باشد.

استانداردPoE برق مورد نیاز برخی تجهیزات شبکه را توسط سوئیچ شبکه تامین نموده و از طریق کابل شبکه تا تجهیزات مورد نظر انتقال می‌دهد. در اینصورت تجهیزات با قابلیت PoE از اتصال به برق بی نیاز شده و انرژی مورد نیاز خود را از طریق سوئیچ تامین می‌نمایند. از جمله تجهیزاتPoE می توان تلفن‌هایIP، ایستگاه‌های Wirelessو دوربین‌های تحت شبکه را نام برد.

در این ارتباط دو جانبه تجهیزات تامین کننده انرژی مثل سوئیچ‌ها را (Power Sourcing Equipment)PSE و تجهیزاتی که قابلیت دریافت انرژی مورد نیاز خود را از طریق PSE دارند را (Powered Device)PD می‌نامند.



استاندارد PoE بر اساس مقدار توان خروجی به گروه‌های زیر تقسیم می‌شود:

- **Inline Power**

Inline Power مختص سیسکو بوده و در ردیف استانداردهای IEEE قرار نمی‌گیرد. سیسکو در سال2000 میلادی و قبل از استاندارد شدنPoE از این ویژگی در تجهیزات خود پشتیبانی می‌نموده است. در این حالت توان خروجی به صورت زیر می‌باشد:

10 W at the PSE

- **استاندارد IEEE 802.3af**

سازمان IEEE در سال2003 میلادی اقدام به معرفی استاندارد IEEE 802.3af نمود. در این استاندارد با بررسی وضعیت دستگاه مورد نظر مقدار توان خروجی مورد نیاز در یکی از چهار کلاس زیر تعیین می گردد:

Class 0: Up to 15.4 W[1] (0.44-12.95 W at the PD; default classification)
Class 1: Up to 4 W (0.44-3.84 W at the PD)
Class 2: Up to 7 W (3.84-6.49 W at the PD)
Class 3: Up to 15.4 W (6.49-12.95 W at the PD)

- **استاندارد IEEE 802.3at**

سازمان IEEE برای پشتیبانی از تجهیزاتی که نیاز به قدرت[2] بالاتری دارند اقدام به معرفی استاندارد IEEE 802.3at در سال2009 میلادی نموده است. از این استاندارد در تجهیزات سیسکو با اصطلاح POE+ و یا POEP نیز نام برده می‌شود. استاندارد IEEE 802.3at دارای یک کلاس توان به صورت زیر می‌باشد:

Class 4: 30.00 W at the PSE (12.95 W to 25.50 W at the PD)

استاندارد 802.3at برای اجرا نیاز به کابل Cat5 به بالا دارد. ولتاژ مورد استفاده در این استاندارد بین ۴۴ تا ۵۷ ولت می‌باشد.

- **UPOE**

UPOE نیز مختص سیسکو بوده و برای پشتیبانی از تجهیزاتی با قدرت بالاتر طراحی گردیده است. با توجه به نیاز تجهیزات جدید به توان بالاتر، در سال2001 میلادی سیسکو مجددا به صورت مستقل اقدام به معرفی نسخه جدیدی برای PoE با نام UPOE (Universal PoE) نموده که توان خروجی آن به صورت زیر می باشد:

---

[1] حرف W مخفف Watt و بیانگر مقدار توان خروجی می باشد. (فرمول محاسبه وات W=V*A می باشد که در آن V به معنی ولتاژ و A به معنی آمپر می باشد)

[2] Power

60.00 W PoE per switch port (PSE Port)

با توجه به گسترش روز افزون تجهیزات با توان مورد نیاز بالاتر، اصلا دور از انتظار نیست که IEEE بزودی این نسخه سیسکو را نیز به صورت استاندارد گسترش دهد.

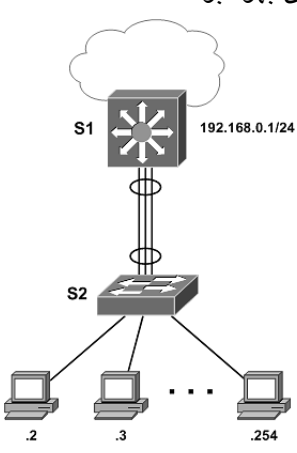
سوئیچ‌های سیسکو با کمک پروتکل CDP می‌توانند تشخیص دهند که آیا تجهیزات متصل به سوئیچ از استانداردPOE پشتیبانی می‌کنند یا خیر. همچنین در صورت پشتیبانی، می توانند مقدار توان مورد نیاز تجهیزات را نیز مشخص کرده و انرژی مورد نیاز آنها را تامین نمایند.

هنگام راه اندازی تجهیزات مبتنی برPOE باید توجه داشته باشید که سوئیچ مورد استفاده قابلیت پشتیبانی از استانداردهای POE مورد نیاز تجهیزات را داشته باشد. در سوئیچ‌های سیسکو معمولا نهایت توان خروجی برای استاندارد POE مشخص شده است و شما می توانید نسبت به توان مورد نیاز تجهیزاتPD مورد استفاده، تعدادی از پورت‌های سوئیچ را در حالت POE پیکربندی نمایید.

برخی برندهای دیگر تولید کننده سوئیچ‌های POE نیز تعداد پورت‌های قابل استفاده جهت این استاندارد را تعیین نموده و معمولا با رنگ متفاوتی روی شاسی سوئیچ مشخص می‌نمایند.

تکنولوژی EtherChannel

تکنولوژی EtherChannel امکان تبدیل چند لینک فیزیکی را به یک لینک منطقی فراهم می‌آورد. در اینصورت می‌توان از لینک‌ها جهت Load Balancing ترافیک و همچنین افزونگی استفاده نمود. از ویژگی EtherChannel می‌توان در بین سوئیچ‌ها، روترها، سرورها و کلاینت‌ها از طریق کابل مسی و یا فیبر نوری بهره برد.



می‌توان از دو تا هشت لینک FastEthernet، Giagabit Ethernet یا 10Gigabit Ethernet برای برقراری یک لینک منطقی EtherChannel استفاده نمود. در این صورت با توجه به اینکه لینک‌های تشکیل دهنده دارای چه سرعتی باشند با یکی از اصطلاحات Fast EtherChannel، Gigabit EtherChannel یا 10Gigabit EtherChannel نامیده می‌شود.

پس از برقراری EtherChannel تمام لینک‌ها به صورت یک لینک منطقی در نظر گرفته شده که دارای مجموع ظرفیت لینک‌های تشکیل دهنده EtherChannel می‌باشد. این لینک‌ها از نظر پروتکلSTP نیز به عنوان یک لینک در نظر گرفته شده و چون باعث ایجاد حلقه (Loop) در شبکه نمی‌گردند هیچ یک از آنها توسط STP غیرفعال نمی‌گردد.

پورت‌های فیزیکی تشکیل دهنده EtherChannel باید از نظر نوع، سرعت، حالت duplex، تنظیمات مربوط به STP و VLAN شبیه به یکدیگر باشند. البته می‌توان برای پورت‌های Trunk نیز از تکنولوژی EtherChannel بهره برد که در اینصورت علاوه بر موارد فوق تنظیمات Native VLAN و شماره VLANهایی که می‌توانند برای تبادل دیتا از این لینک استفاده نمایند، باید بر روی پورت‌های Trunk شبیه به یکدیگر پیکربندی گردیده باشند.

نحوه Load Balancing بر روی پورت‌های فیزیکی حتما نباید به صورت برابر انجام پذیرد و ممکن است نحوه توزیع ترافیک با توجه به تعداد پورت‌های تشکیل دهنده متفاوت باشد. جدول زیر نمایش دهنده نحوه Load Balancing با توجه به تعداد پورت‌های تشکیل دهنده می‌باشد:

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

پیکربندی EtherChannel معمولا به صورت دستی توسط مدیر شبکه انجام می‌پذیرد. ولی تکنولوژی EtherChannel می‌تواند علاوه بر حالت فوق، توسط پروتکل‌های زیر بصورت اتوماتیک اقدام به ایجاد لینک منطقی بر اساس پورتهای فیزیکی نماید:

- **PAgP**

پروتکل PAgP(Port Aggregation Protocol) مختص سیسکو بوده و فقط قابلیت استفاده بر روی تجهیزات این برند را دارد. این پروتکل با تبادل بسته‌های PAgP اقدام به تشخیص پورت‌هایی که قابلیت تشکیل EtherChannel را دارند، نموده و بصورت اتوماتیک اقدام به ایجاد لینک‌های مجازی می‌نماید. بسته‌های PAgP فقط بین پورت‌هایی تبادل می‌شوند که در یکی از دو حالت auto یا desirable قرار داشته باشند.

- **LACP**

پروتکل LACP(Link Aggregation Control Protocol) توسط سازمان IEEE و تحت استاندارد IEEE 802.3ad توسعه یافته است. این پروتکل با تبادل بسته‌های LACP بین پورت‌هایی که در یکی از دو حالت active یا passive قرار دارند، اقدام به شناسایی پورت‌های دارای قابلیت تشکیل EtherChannel نموده و توسط آنها لینک منطقی مورد نظر را به وجود می‌آورد.

برای پیکربندی EtherChannel بر روی تجهیزات سیسکو می توانید از دستورات زیر بهره ببرید:

Configuring Layer 2 EtherChannels		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**Interface** *interface-id*	Specify a physical interface to configure, and enter interface configuration mode. Valid interfaces include physical interfaces. Up to eight interfaces of the same type and speed can be configured for the same group.
Step 3	**channel-group** *channel-group-number* **mode** {{**auto**[**non-silent**] | **desirable**[**non-silent**] | **on**} | {**active** |**passive**}}	Assign the interface to a channel group, and specify the PAgP or LACP mode. For *channel-group-number*, the range is 1 to 6. Each EtherChannel can have up to eight compatibly configured Ethernet interfaces. For **mode**, select one of these keywords: • **active**—Enables LACP only if an LACP device is detected. It places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending LACP packets. • **auto**—Enables PAgP only if a PAgP device is detected. It places an interface into a passive

Configuring Layer 2 EtherChannels		
		negotiating state, in which the interface responds to PAgP packets it receives but does not start PAgP packet negotiation. • **desirable**—Unconditionally enables PAgP. It places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets. • **on**—Forces the interface to channel without PAgP. With the **on** mode, a usable EtherChannel exists only when an interface group in the **on** mode is connected to another interface group in the **on** mode. • **non-silent**—If your switch is connected to a partner that is PAgP-capable, you can configure the switch interface for nonsilent operation. You can configure an interface with the **non-silent** keyword for use with the**auto** or **desirable** mode. If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the interface to a channel group, and to use the interface for transmission. • passive—Enables LACP on an interface and places it into a passive negotiating state, in which the interface responds to LACP packets that it receives, but does not start LACP packet negotiation.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Displaying EtherChannel, PAgP, and LACP Status	
Command	Description
show etherchannel [channel-group-number] **{detail | load-balance | port | port-channel |summary}**	Displays EtherChannel information in a detailed and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, and port-channel information.
show pagp [channel-group-number]	Displays PAgP information such as traffic

Displaying EtherChannel, PAgP, and LACP Status	
{counters | internal |neighbor}	information, the internal PAgP configuration, and neighbor information.
show lacp [channel-group-number] **{counters | internal | neighbor}**	Displays LACP information such as traffic information, the internal PAgP configuration, and neighbor information.

ویژگی IP Helper

همانطور که می‌دانید کلاینت‌ها برای دریافت آدرسIP از DHCP، درخواست‌های خود را به صورت پیام‌های Broadcast در شبکه پخش نموده تا به سرور مورد نظر برسد و سرور در جواب درخواست آنها یک آدرس به کلاینت اختصاص دهد.

اما اگر سرورDHCP در VLAN متفاوتی نسبت به کلاینت درخواست کننده قرار داشته باشد چه اتفاقی می‌افتد؟ واضح است کهVLAN اجازه خروج پیام‌های Broadcast را از داخل خود نمی‌دهد و هیچ پیام درخواستی از آنVLAN به سرورDHCP نرسیده و کلاینت‌ها بدون آدرس می‌مانند.

برای رفع مشکل فوق، سیسکو از ویژگی IP Helper برای رساندن درخواست‌ها به سرور DHCP استفاده می‌نماید. ویژگیIP Helper با دانستن آدرس سرورDHCP، پیام‌های درخواست کلاینت‌ها را به صورت Broadcast دریافت نموده و با تبدیل درخواست‌ها به Unicast، آن ها را به سمت سرور DHCP ارسال می‌نماید. در اینصورت آدرس مبدا[1] پیام درخواست همان آدرس کلاینت و آدرس مقصد[2] درخواست آدرس سرور DHCP خواهد بود.

توسط دستور زیر می توانید ویژگی IP Helper را بر روی سوئیچ‌های سیسکو پیکربندی نمایید:

Switch(config-if)#**ip helper-address** *dhcp-server-address*

[1] Source
[2] Destination

بخش سوم

امنیت

فصل هشتم

امنیت؛ مفاهیم کلی

- ☑ مبحث اول: استاندارد سیستم مدیریت امنیت اطلاعات (ISMS)
- ☑ مبحث دوم: مدل امنیتی سیسکو
- ☑ مبحث سوم: تجهیزات و نرم افزارهای امنیتی

☑ مبحث اول

استاندارد سیستم مدیریت امنیت اطلاعات(ISMS)

سازمان‌ها در هر اندازه و هر نوع فعالیت علمی، سیاسی و اقتصادی که قرار داشته باشند، باید مقداری اطلاعات را جمع‌آوری، پردازش، نگهداری و ارسال نمایند. سازمان‌ها دارای مخاطبانی نیز هستند که ممکن است در صورت اعمال نکردن سیاست‌ها و کنترل‌های امنیتی مناسب، خواسته یا ناخواسته تاثیر نامطلوب یا مخرب بر روی سیستم بگذارند. همچنین اطلاعات سازمان می‌تواند همواره برای اشخاص دیگر جالب و مورد توجه باشد و بخواهند با استفاده از ضعف‌های امنیتی موجود در سیستم، به اطلاعات حساس و حیاتی سازمان دسترسی پیدا کنند. اما تهدیدات سازمان تنها به کاربران ناشی، ضعف سیستم و اشخاص خرابکار ختم نمی‌شود؛ بلکه بلایای طبیعی مثل سیل و زلزله یا اتفاقات پیش بینی نشده مثل آتش سوزی و حتی مخاطرات نوظهور نیز تهدید به حساب می‌آیند.

مدیران سازمان‌ها در صورتی که بخواهند سطح امنیت خود را افزایش داده و از اطلاعات خود محافظت کنند باید استانداردهای امنیتی جامعی را مورد استفاده قرار دهند که تمام ابعاد امنیت اطلاعات را مورد توجه قرار داده باشد. سپس استاندارد مورد نظر را توسط افراد متخصص و با تجربه در سازمان خود پیاده سازی نموده و همواره برای تداوم عملکرد مناسب، بر آن نظارت داشته باشند.

سازمان استاندارد جهانی (ISO) با همکاری کمیسیون بین المللی الکتروتکنیک (IEC) جهت امنیت اطلاعات، اقدام به معرفی استانداردهای سری ISO/IEC 27000 نموده است. در این استانداردها که سیستم مدیریت امنیت اطلاعات (Information Security Management System) یا به اختصار ISMS، نامیده می شوند؛ سعی شده تا تمام مؤلفه‌های مورد نیاز امنیت اطلاعات، از امنیت فیزیکی تا نحوه مدیریت مد نظر قرار داده شود.

در سال ۱۳۸۷ سازمان استاندارد ملی ایران نیز بر اساس استانداردهای 27001 و 27002 اقدام به معرفی استاندارد ملی امنیت نموده است. شما می‌توانید استاندارد ملی ایران را از طریق وب سایت این سازمان به آدرس www.isiri.org دانلود نمایید.

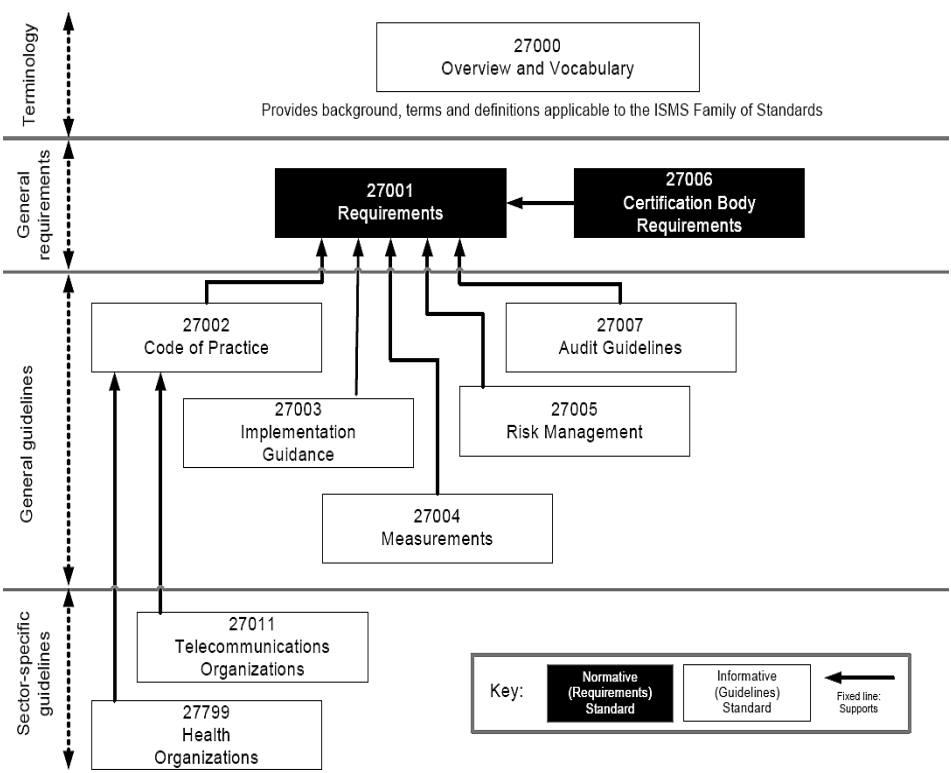
ما هم در این مبحث به شرح مختصری از ISO/IEC 27000 که در برگیرنده اصطلاحات و مرور کلی استانداردهای خانواده ISMS می باشد، بسنده می‌کنیم.

استانداردهای خانواده ISMS

خانواده ISMS متشکل از استانداردهای مرتبط با هم می‌باشد که بعضی از آنها در حال تدوین بوده و هنوز منتشر نشده و بعضی دیگر نیز منتشر گردیده است. این استانداردها دارای تعدادی مؤلفه مهم ساختاری می‌باشند که بر استانداردهای اصلی تمرکز دارند. استانداردهای اصلی شامل توصیف کننده الزامات ISMS (استاندارد ISO/IEC 27001) و الزامات مرکز صدور گواهینامه[1] (ISO/IEC 27006) جهت صادر کردن گواهی انطباق با ISO/IEC 27001 می‌باشند.

استانداردهای دیگر نیز فراهم کننده راهنما[2] برای جنبه‌های اجرایی مختلف ISMS، فرآیند عمومی، دستورالعمل‌های مربوط به کنترل و همچنین راهنمای یک بخش خاص می‌باشند.

تصویر زیر نشان دهنده ارتباطات درون خانواده استاندارد ISMS می‌باشد.



[1] Certification
[2] Guidance

مروری بر استانداردهای خانواده ISMS

برای آشنایی با محتویات استانداردهای خانوادهISMS که در تصویر فوق نیز به آنها اشاره گردیده است، به شرح مختصری از آنها می‌پردازیم:

۱- **استاندارد ISO/IEC 27000 (همین استاندارد)**

طبقه بندی: فناوری اطلاعات- فنون امنیتی[1]- سیستم مدیریت امنیت اطلاعات- مرور کلی و واژگان

حوزه کاربرد: این استاندارد بین المللی به افراد و سازمانها در زمینه های زیر کمک می کند:

i. بررسی اجمالی استانداردهای خانواده ISMS
ii. مقدمه ای بر سیستم مدیریت امنیت اطلاعات (ISMS)
iii. شرح مختصری بر فرآیند PDCA
iv. آشنایی با اصطلاحات و تعاریف استفاده شده در استانداردهای خانواده ISMS

هدف: استاندارد ISO/IEC 27000 به توصیف مبانی ISMS و اصطلاحات به کار رفته در این سری استاندارد می‌پردازد.

۲- **استاندارد ISO/IEC 27001**

طبقه بندی: فناوری اطلاعات- فنون امنیتی- سیستم مدیریت امنیت اطلاعات- الزامات[2]

حوزه کاربرد: این استاندارد بین المللی الزامات ایجاد، پیاده سازی، راه اندازی، نظارت، بررسی، نگهداری و بهبود رسمی سیستم مدیریت امنیت اطلاعات (ISMS) را در زمینه مخاطرات کلی کسب و کار سازمان تنظیم می‌نماید. همچنین این استاندارد مشخص کننده الزامات پیاده سازی کنترل‌های امنیتی سفارشی شده مورد نیاز سازمانهای مختلف و یا بخش‌های وابسته به آنها می‌باشد. این استاندارد بین المللی تمام انواع سازمانها (به عنوان مثال شرکت‌های تجاری، سازمان‌های دولتی و سازمان‌های غیرانتفاعی) را در بر می‌گیرد.

هدف: استاندارد ISO/IEC 27001 الزامات اصلی توسعه و راه اندازی ISMS را ارائه می‌نماید. این الزامات شامل مجموعه‌ای از کنترل‌ها برای مهار و کاهش خطرات مربوط به دارایی های اطلاعاتی بوده که سازمان می‌خواهد از طریق عملیاتی کردن ISMS از آنها محافظت نماید.

---

[1] Security Techniques
[2] Requirements

۳- استاندارد ISO/IEC 27006

طبقه بندی: فناوری اطلاعات- فنون امنیتی- الزامات نهادهای ارائه دهنده خدمات ممیزی[1] و صدور گواهینامه ISMS

حوزه کاربرد: این استاندارد بین المللی علاوه بر الزامات موجود در ISO/IEC 17021، الزامات دیگری نیز مشخص نموده و راهنمایی‌هایی را برای نهادهای ارائه کننده ممیزی و صدور گواهینامه ISMS طبق استاندارد 27001 فراهم می‌نماید. در واقع این استاندارد برای پشتیبانی از تائید صلاحیت نهادهایی می‌باشد که بر اساس استاندارد 27001 اقدام به صدور گواهینامه ISMS می‌نمایند.

هدف: استاندارد ISO/IEC 27006 مکمل[2] استاندارد 17021 در جهت مشخص نمودن الزاماتی است که باید توسط نهادهایی که قصد ارائه خدمات ممیزی یا صدور گواهی نامه دارند، رعایت گردد تا امکان ممیزی یا صدور گواهی انطباق با استاندارد 27001 توسط آنها فراهم گردد.

۴- استاندارد ISO/IEC 27002

طبقه بندی: فناوری اطلاعات- فنون امنیتی- دستورالعمل[3] مدیریت امنیت اطلاعات

حوزه کاربرد: این استاندارد بین المللی لیستی از اهداف کنترلی پذیرفته شده و بهترین شیوه‌های[4] کنترلی فراهم آورده تا جهت راهنمایی در زمان انتخاب و پیاده سازی کنترل‌ها برای دست یابی به امنیت اطلاعات، مورد استفاده قرار گیرند.

هدف: استاندارد ISO/IEC 27002 فراهم کننده راهنما جهت پیاده سازی کنترل‌های امنیت اطلاعات می‌باشد. بندهای ۵ تا ۱۵ این استاندارد به طور خاص به مشاوره و راهنمایی پیاده سازی بر اساس بهترین شیوه‌ها در خصوص کنترل‌های موجود در بندهای A.5 تا A.15 استاندارد ISO/IEC 27001 می‌باشد.

۵- استاندارد ISO/IEC 27003

طبقه بندی: فناوری اطلاعات- فنون امنیتی- راهنمای پیاده سازی ISMS

حوزه کاربرد: این استاندارد بین المللی ضمن فراهم سازی راهنمای پیاده سازی عملی، اطلاعات بیشتری را نیز برای برقراری، پیاده‌سازی، راه اندازی، نظارت، بررسی، نگهداری و بهبود ISMS طبق استاندارد 27001 ارائه می‌نماید.

---

[1] Audit
[2] Supplement
[3] Code of practice
[4] Best practice

هدف: استاندارد ISO/IEC 27003 رویکردی فرآیندگرا[1] جهت اجرای موفقیت آمیز ISMS مطابق با استاندارد 27001 فراهم می‌آورد.

۶- استاندارد ISO/IEC 27004

طبقه بندی: فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- سنجش[2]

حوزه کاربرد: این استاندارد بین المللی راهنمایی و مشاوره برای توسعه و نحوه سنجش را بمنظور ارزیابی اثربخشی ISMS، اهداف کنترلی و کنترل‌های استفاده شده برای پیاده سازی و مدیریت امنیت اطلاعات طبق استاندارد 27001، فراهم می‌نماید.

هدف: استاندارد ISO/IEC 27004 با ارائه چارچوب مشخصی برای سنجش، امکان ارزیابی تاثیر گذاری ISMS را مطابق با استاندارد 27001 فراهم می‌آورد.

۷- استاندارد ISO/IEC 27005

طبقه بندی: فناوری اطلاعات- فنون امنیتی- مدیریت مخاطره امنیت اطلاعات

حوزه کاربرد: استاندارد بین المللی 27005 راهنمایی‌هایی را جهت مدیریت مخاطرات امنیت اطلاعات ارائه می‌نماید.

نحوه تشریح در این استاندارد با توجه به مفاهیم کلی مشخص شده در استاندارد 27001 انجام پذیرفته است.

هدف: استاندارد ISO/IEC 27005 ارائه دهنده راهنمایی‌هایی جهت پیاده سازی رضایت بخش یک مدیریت مخاطره فرآیندگرا و همچنین تحقق الزامات مدیریت مخاطره امنیت اطلاعات بر اساس استاندارد 27001 می‌باشد.

۸- استاندارد ISO/IEC 27007

طبقه بندی: فناوری اطلاعات- فنون امنیتی- راهنمای ممیزی ISMS

حوزه کاربرد: این استاندارد بین المللی علاوه بر شرایط موجود در استاندارد ISO 19011 شامل راهنمای طریقه انجام ممیزی ISMS و همچنین نحوه احراز صلاحیت بازرسان سیستم مدیریت امنیت اطلاعات، می‌باشد.

هدف: استاندارد ISO/IEC 27007 به ارائه راهنمایی برای سازمان‌هایی می پردازد که نیاز به انجام بازرسی داخلی یا خارجی ISMS داشته و یا برنامه ممیزی ISMS را جهت اجرای الزامات مشخص شده در استاندارد 27001 مدیریت می‌کنند.

---

[1] Process oriented
[2] Measurement

۹- استاندارد ISO/IEC 27011

طبقه بندی: فناوری اطلاعات- فنون امنیتی- راهنمای مدیریت امنیت اطلاعات بر اساس استاندارد ISO/IEC 27002 برای سازمان‌های مخابراتی[1]

حوزه کاربرد: این استاندارد بین المللی شامل دستورالعمل نحوه پیاده سازی مدیریت امنیت اطلاعات (ISM) در سازمان های مخابراتی می‌باشد.

هدف: استاندارد ISO/IEC 27011 علاوه بر الزامات موجود در ضمیمه A استاندارد 27001، دستورالعمل خاصی را با اقتباس از استاندارد 27002 برای سازمان‌های مخابراتی فراهم نموده است.

۱۰-استاندارد ISO/IEC 27799

طبقه بندی: انفورماتیک بهداشت[2]- مدیریت امنیت اطلاعات در بهداشت بر اساس استاندارد 27002

حوزه عملکرد: این استاندارد بین المللی دستورالعمل پیاده سازی مدیریت امنیت اطلاعات (ISM) را در سازمان های بهداشت و درمان ارائه می‌نماید.

هدف: استاندارد ISO/IEC 27799 علاوه بر الزامات موجود در ضمیمه A استاندارد 27001، دستورالعمل خاصی را با اقتباس از استاندارد 27002 برای سازمان‌های بهداشت و درمان ارائه نموده است.

اصطلاحات و تعاریف[3]

- **کنترل دسترسی (Access Control)**

اطمینان از دسترسی به دارایی‌ها به صورت مجاز و محدود شده بر اساس الزامات امنیتی و کسب و کار.

- **مسئولیت پذیری و پاسخ گویی (Accountability)**

مسئولیت پذیری یک نهاد در ازاء تصمیمات و اقدامات خود.

- **دارایی (Asset)**

هر چیزی که برای سازمان ارزشمند باشد دارایی محسوب می‌گردد. دارایی می‌تواند شامل طیف گسترده‌ای از قبیل: اطلاعات، برنامه های کاربردی، تجهیزات سخت افزاری، افراد و غیره باشد.

---

[1] Telecommunication
[2] Health
[3] Terms and Definitions

- **حمله (Attack)**

تلاش برای تخریب[1]، افشا[2]، تغییر[3]، غیرفعال کردن، سرقت[4] و دسترسی یا استفاده غیر مجاز[5] از یک دارایی را حمله می‌نامند.

- **احراز هویت (Authentication)**

ارائه تضمینی جهت درست بودن مشخصات ادعا شده.

- **اصالت (Authenticity)**

بررسی اینکه ارائه دهنده مشخصات، همان است که ادعا می‌کند.

- **دسترس پذیری (Availability)**

دارایی‌ها باید برای تقاضاهای مجاز همواره در دسترس و قابل استفاده باشد.

- **تداوم کسب و کار (Business Continuity)**

حصول اطمینان تداوم عملیات کسب و کار از طریق فرآیندها و رویه‌ها.

- **محرمانگی (Confidentiality)**

غیر قابل دسترس بودن یا آشکار نبودن اطلاعات برای افراد و فرآیندهای غیرمجاز را محرمانگی می‌گویند.

- **دارایی اطلاعاتی (Information Asset)**

دانش یا دیتای دارای ارزش برای سازمان را دارایی های اطلاعاتی گویند.

- **امنیت اطلاعات (Information Security)**

منظور از امنیت اطلاعات حفظ محرمانگی، درستی و دسترس پذیری اطلاعات می‌باشد. البته امنیت اطلاعات علاوه بر موارد فوق می‌تواند شامل مواردی نظیر صحت، پاسخگویی[6]، انکار ناپذیری و قابلیت اطمینان بودن اطلاعات نیز باشد.

- **رویداد امنیت اطلاعات (Information Security Event)**

یک رویداد امنیت اطلاعات می‌تواند شامل وقوع حالت شناخته شده‌ای در سیستم، شبکه یا سرویس باشد که نشان دهنده نقص احتمالی در امنیت اطلاعات، خط مشی یا مشکل در کنترل ها است. همچنین ممکن است رویداد شامل وضعیت نا شناخته‌ای باشد که به امنیت اطلاعات مربوط است.

---

[1] Destroy
[2] Expose
[3] Alter
[4] Steal
[5] Unauthorized
[6] Accountability

- **حادثه امنیت اطلاعات (Information Security Incident)**

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا غیر منتظره که به احتمال زیاد عملیات کسب و کار را به خطر انداخته و تهدیدی برای امنیت اطلاعات محسوب می گردد.

- **مدیریت حوادث امنیت اطلاعات (Information Security Incident Management)**

به مجموع فرآیندهایی که برای آشکار سازی[1]، گزارش دهی[2]، ارزیابی[3]، پاسخ دهی به[4]، به[4]، رسیدگی به[5] و یادگیری حوادث امنیت اطلاعات مورد استفاده قرار می‌گیرد، مدیریت حوادث امنیت اطلاعات می‌گویند.

- **سیستم مدیریت امنیت اطلاعات (Information Security Management System)**

سیستم مدیریت امنیت اطلاعات یا ISMS، بخشی از سیستم کلان مدیریتی است که اساس آن بر رویکرد مخاطره کسب و کار بوده و شامل برقراری[6]، پیاده سازی، عملیات، نظارت، بررسی، نگهداری و بهبود امنیت اطلاعات می‌باشد.

- **مخاطره امنیت اطلاعات (Information Security Risk)**

توانایی بالقوه یک تهدید در بهره برداری از آسیب پذیری یک یا گروهی از دارایی ها که در نهایت منجر به آسیب رسیدن به سازمان می گردد.

- **درستی[7] (Integrity)**

خاصیت حفاظت از صحت[8] و تمامیت[9] دارایی‌ها.

- **خط مشی (Policy)**

خط مشی عبارت است از قصد و جهت دهی کلی سازمان که به صورت رسمی توسط مدیریت تبیین شده است.

- **فرآیند (Process)**

مجموعه فعالیت های مرتبط با هم که باعث تبدیل ورودی به خروجی می گردد.

---

[1] Detecting
[2] Reporting
[3] Assessing
[4] Responding to
[5] Dealing with
[6] Establish
[7] عبارت Integrity دارای معانی بسیاری از جمله درستی، صحت، یکپارچگی و تمامیت می‌باشد. اما به نظر بنده معنی معنی قابل قبول در جملات این بخش، درستی می باشد.
[8] Accuracy
[9] Completeness

- **رویه (Procedure)**

راه و روش مشخص شده برای انجام یک فعالیت یا فرآیند را رویه می‌گویند.

- **تهدید (Threat)**

عامل بالقوه حادثه ای ناخواسته که ممکن است منجر به آسیب یک سازمان یا سیستم گردد.

- **آسیب پذیری (Vulnerability)**

ضعف موجود در یک دارایی یا کنترل که می‌تواند توسط یک تهدید مورد سوء استفاده قرار گیرد را آسیب پذیری می‌گویند.

مروری بر ISMS

سیستم مدیریت امنیت اطلاعات یا ISMS، مدلی را برای برقراری، پیاده سازی، راه اندازی[1]، نظارت[2]، بررسی[3]، حفظ و نگهداری[4] و بهبود حفاظت از دارایی‌های اطلاعاتی بمنظور تحقق اهداف اهداف کسب و کار فراهم می‌نماید. طراحی این مدل بر اساس ارزیابی مخاطره و سطح پذیرش آن توسط سازمان انجام گرفته تا مدیریت و رفع مخاطره به صورت موثر انجام پذیرد.

تجزیه و تحلیل الزامات حفاظت از دارایی‌های اطلاعاتی و اعمال کنترل‌های مناسب جهت حصول اطمینان از حفاظت آنها به پیاده سازی موفق ISMS کمک می‌نماید.

اصول اساسی زیر می‌تواند کمک شایانی در جهت اجرای موفقیت آمیز ISMS باشد:

- آگاهی از ضرورت نیاز به امنیت اطلاعات.
- تخصیص مسئولیت برای امنیت اطلاعات.
- ترکیب تعهد مدیریتی و منافع ذینفعان.
- افزایش ارزش‌های اجتماعی.
- ارزیابی مخاطره جهت تعیین کنترل‌های مناسب برای دستیابی به سطح قابل قبول ریسک.
- گنجاندن امنیت به عنوان یک عنصر ضروری در سیستم‌ها و شبکه‌های اطلاعاتی.
- پیشگیری و تشخیص فعال حوادث امنیت اطلاعات.

---

[1] Operating
[2] Monitoring
[3] Reviewing
[4] Maintaining

- حصول اطمینان از یک رویکرد جامع برای مدیریت امنیت اطلاعات.
- ارزیابی مستمر امنیت اطلاعات و ایجاد تغییرات مناسب.

دستیابی به امنیت اطلاعات نیازمند مدیریت مخاطرات ناشی از تهدیدات فیزیکی، انسانی و فناوری‌های مربوط به اطلاعات در تمام اشکال مورد استفاده سازمان می‌باشد. لذا همواره بخشی از ISMS هر سازمان را مخاطرات مرتبط با دارایی‌های اطلاعاتی تشکیل می‌دهد.

انتظار می‌رود پیاده سازی ISMS در سازمان به عنوان یک تصمیم استراتژیک مورد پذیرش قرار گیرد. این تصمیم لازم است مطابق با نیازهای سازمان کاملا یکپارچه، متناسب و بروز باشد.

طراحی و پیاده سازی ISMS تحت تاثیر نیازها، اهداف سازمانی، الزامات امنیتی، فرآیندهای کسب و کار، وسعت و ساختار آن سازمان خواهد بود. توجه داشته باشید که منافع و امنیت اطلاعات مورد نیاز همه ذینفعان از جمله مشتریان، تامین کنندگان[1]، شرکای تجاری، سهامداران[2] و سایر اشخاص ثالث[3] باید در طراحی و راه اندازی ISMS منعکس گردد.

سیستم مدیریت امنیت اطلاعات(ISMS) برای کسب و کار هر دو بخش خصوصی و عمومی مهم می‌باشد. این سیستم که برای فعالیت‌های مدیریت مخاطره نیز ضروری است، هر صنعتی را قادر می‌سازد تا از کسب و کار الکترونیکی پشتیبانی نماید. زمانیکه یک سازمان اقدام به اتخاذ استانداردهای خانواده ISMS می‌نماید، توانایی خود را در اعمال اصول امنیت اطلاعات متقابل و پایدار در برابر شرکای تجاری و سایر طرف های ذینفع نشان می‌دهد.

با همه این اوصاف در برخی موارد هنگام طراحی و توسعه سیستم های اطلاعات، ممکن است امنیت اطلاعات مورد توجه قرار نگیرد. علاوه بر این امنیت اطلاعات اغلب به عنوان یک راه حل فنی در نظر گرفته می‌شود ولی امنیتی که از راه های فنی به دست می‌آید محدود بوده و حتی ممکن است بدون پشتیبانی توسط مدیریت و فقدان روش‌های اجرایی مناسب، بی‌تاثیر باشد. همچنین گنجاندن امنیت داخل یک سیستم اطلاعاتی پس از پیاده سازی آن می‌تواند پرهزینه و پر زحمت باشد. در مقابل سیستم ISMS شامل تمام کنترل‌ها بوده و نیازمند برنامه‌ریزی دقیق و توجه به تمام جزئیات می‌باشد. به عنوان مثال کنترل‌های دسترسی که ممکن است فنی[4](منطقی)، فیزیکی، اداری (مدیریتی) و یا ترکیبی از اینها باشد؛ ابزارهایی فراهم می‌آورد تا از دسترسی مجاز و محدود شده به دارایی‌های اطلاعاتی اطمینان حاصل شود.

---

[1] Suppliers
[2] Shareholders
[3] Third parties
[4] Technical

امنیت اطلاعات با اجرای مجموعه‌ای از کنترل‌هایی به دست می‌آید که از طریق فرآیند مدیریت مخاطره انتخاب و توسط ISMS مدیریت می‌شوند. این کنترل‌ها شامل سیاستها (خط مشی‌ها)، فرآیندها، روش‌های اجرایی، ساختار سازمانی، نرم افزار و سخت افزارهایی می‌باشد که در جهت حفاظت از دارایی‌های اطلاعاتی شناسایی شده، می‌باشند. برای حصول اطمینان از دستیابی به اهداف مورد نظر امنیتی و کسب و کار سازمان، نیاز است که این کنترل‌ها مشخص، پیاده سازی، نظارت و بررسی گردیده و در صورت لزوم بهبود یابند. این انتظار وجود دارد که همواره کنترل‌های امنیت اطلاعات با فرآیندهای کسب و کار سازمان یکپارچه شده باشند.

اصول PDCA

استانداردهای سیستم مدیریتیISO دارای اصول بهره برداری مصوب با نامPDCA می باشند که این اصول در استانداردهای خانواده ISMS نیز مورد استفاده قرار می‌گیرد. منظور از PDCA، فرآیندهای Plan، Do، Check و Act می‌باشد که در ادامه به تشریح آنها می‌پردازیم:

۱- **برنامه (Plan)**

تعیین اهداف و ایجاد برنامه‌ها (تجزیه و تحلیل وضعیت سازمان، تعیین اهداف کلی و زیر مجموعه‌ها و در نهایت توسعه برنامه جهت دستیابی به آنها).

۲- **اجرا (Do)**

اجرای برنامه‌ها (انجام کارهایی که در برنامه مشخص شده‌اند).

۳- **بررسی (Check)**

سنجش نتایج به دست آمده (سنجش و نظارت بر دست آوردها، تا مشخص شود چه حد به اهداف مورد نظر نزدیک شده‌ایم).

۴- **اقدام (Act)**

اصلاح و بهبود فعالیت‌ها (به قول خودمون شکست پلی است برای پیروزی! درس گرفتن از اشتباهات گذشته به منظور بهبود فعالیت‌ها در دستیابی به نتایج بهتر).

برقراری، نظارت، نگهداری و بهبود عملکرد ISMS

یک سازمان جهت برقراری، نظارت، نگهداری و بهبود عملکرد ISMS، نیازمند تعهد به انجام مراحل زیر می‌باشد:

۱- شناسایی دارایی‌های اطلاعاتی و الزامات امنیتی مربوط به آنها.

۲- ارزیابی مخاطرات امنیت اطلاعات.

۳- انتخاب و پیاده سازی کنترل‌های مربوطه برای مدیریت مخاطرات غیرقابل قبول.
۴- نظارت، نگهداری و بهبود اثربخشی کنترل‌های امنیتی مرتبط با دارایی‌های اطلاعاتی سازمان.

برای اطمینان از عملکرد موثرISMS در محافظت از دارایی‌های اطلاعاتی سازمان، لازم است تا موارد فوق به صورت مداوم جهت شناسایی تغییرات ایجاد شده در مخاطرات، راهبردهای سازمان و یا اهداف کسب و کار تکرار شوند.

☑ مبحث دوم

مدل امنیتی سیسکو

در مبحث اول استاندارد ISMS را مورد بررسی قرار دادیم. همانطور که گفته شد، این استاندارد امنیت را به صورت جامع و در تمام ابعاد آن بررسی می‌نماید. از طرف دیگر شرکت سیسکو نیز به عنوان پیشتاز فناوری شبکه و با توجه به تنوع و گستردگی محصولات خود، اقدام به معرفی یک مدل امنیتی با نامSCF نموده است. توجه داشته باشید که مدل سیسکو بر خلاف دید جامع ISMS، بیشتر امنیت شبکه را مورد توجه قرار داده و به بیان بهترین شیوه‌های امنیتی در این مورد می‌پردازد.

در طراحی و پیاده سازی معماری زیرساختIT باید امنیت به صورتی در نظر گرفته شود که بتوان ضمن فعال نگه داشتن عملیات کلیدی کسب و کار، از محرمانگی، درستی و دسترس پذیری زیرساخت های فناوری اطلاعات و دیتای حساس کسب و کار و مشتری اطمینان حاصل نمود.

نیازمندی‌های امنیتی یک سازمان شامل منابع مختلفی از جمله اهداف خرد و کلان، استانداردهای بین المللی و خاص همان صنعت و مقررات دولتی و صنفی می‌باشد. از مزایای در نظر داشتن این الزامات امنیتی و تجاری در فرآیندهای طراحی، پیاده‌سازی و راه‌اندازی یک زیرساخت، امکان استفاده از یک مدل منسجم برای نظارت و سازماندهی تعداد بیشماری الزامات کنترل امنیتی می‌باشد.

مدل SCF(Security Control Framework) سیسکو، به تعریف یک ساختار متشکل از اهداف امنیتی و پشتیبانی از اقدامات امنیتی مربوطه در جهت سازماندهی کنترل‌های امنیتی، می‌پردازد. مدلSCF سیسکو بر اساس بهترین شیوه‌ها، اصول معماری امنیتی و مجموعه‌ای گسترده از تجربیات عملی مهندسین سیسکو در طراحی، پیاده سازی، ارزیابی و مدیریت ارائه خدمات به شرکت‌های تجاری بزرگ، متوسط و کوچک، ایجاد گردیده است. با استفاده از مدل SCF سیسکو، سازمان‌ها می‌توانند به منظور سهولت درک و ارتباط کنترل‌های معماری برای زیرساخت IT، الزامات و کنترل‌های امنیتی خود را به گروه‌های منطقی تقسیم نمایند.

مدل SCF سیسکو برای افزایش تمرکز بر سه هدف اصلی مربوط به امنیت زیرساخت IT و دارایی‌های سازمان طراحی شده است. این اهداف اصلی عبارتند از:

۱- حفاظت از زیرساخت‌های IT

۲- حفاظت از دارایی‌های IT با استفاده از کنترل‌های مبتنی بر شبکه
۳- کاهش حوادث امنیتی و پاسخ به آنها با استفاده از کنترل‌های مبتنی بر شبکه

اصطلاحات و تعاریف

مدل SCF نیز همانند سایر استانداردها و مدل‌ها دارای اصطلاحات و تعاریف مربوط به خود می‌باشد. در این بخش به تشریح برخی از اصطلاحات و تعاریف این مدل می‌پردازیم.

- **چارچوب کنترل امنیتی سیسکو (Security Control Framework)**

ترکیبی از مدل، روش شناسی[1]، ساختار کنترل و مجموعه‌های کنترل می‌باشد که بر اساس دانش امنیتی سیسکو تدوین گردیده و برای ارزیابی پیاده سازی و معماری امنیت زیرساخت IT مورد استفاده قرار می‌گیرد.

- **مدل SCF سیسکو(Security Control Framework Model)**

اهداف و اقدامات امنیتی استفاده شده برای سازماندهی کنترل‌های امنیتی در قالب یک مدل برای کمک به ارزیابی معماری امنیت و پیاده سازی جنبه‌های متعدد زیرساخت سازمان، ارائه می‌نماید.

مدلSCF از دو بخش اصلی : اهداف امنیتی و اقدامات امنیتی تشکیل گردیده است.

- **کنترل (Control)**

یک استاندارد سنجش یا مکانیسمی که به تعریف یک ویژگی، توانایی و یا تابع[2] مورد نیاز در یک زیرساخت که یک یا چند عملیات امنیتی را جهت دستیابی به یک هدف خاص امنیتی پشتیبانی می‌کند، می پردازد.

کنترل‌ها از طریق پیاده سازی تکنیک‌هایی در زیرساخت تحقق می‌یابند. برای تحقق کامل یک کنترل ممکن است یک یا چند تکنیک مورد نیاز باشد.

- **مجموعه کنترل (Control Set)**

یک گروه منطقی شامل کنترل‌های موجود در سرتاسر اقدامات امنیتی مورد استفاده برای پشتیبانی از یک یا چند جنبه زیرساخت، را مجموعه کنترل می‌نامند.

- **نوع کنترل (Control Type)**

یک مفهوم سازمانی است که برای توصیف گونه کنترل و ماهیت تکنیک‌های مرتبط با اجرای آن، مورد استفاده قرار می‌گیرد.

---

[1] Methodology
[2] Function

انواع کنترل‌های معمول عبارتند از: فنی، خط مشی[1] و رویه‌ای[2].

- **بلوک کاربردی (Functional Block)**

تقسیم زیرساخت اصلی به بخش‌های عمومی کوچک‌تر و بر اساس مرزهای عملکردی را بلوک کاربردی می‌گویند. نمونه‌هایی از بلوک کاربردی شامل موارد زیر است:

i. مرکز داده (Data Center)
ii. داخلی (Interior)
iii. پیرامونی (Perimeter)
iv. امنیت فیزیکی (Physical Security)

- **جنبه‌های زیرساخت(Infrastructure Aspects)**

جنبه‌های زیرساخت یک بخش منطقی، فیزیکی، عملکردی، یا سازمانی، قسمت[3]، منطقه[4]، موقعیت تجهیزات شبکه، برنامه‌های کاربردی[5]، سرورها یا هر دستگاه انتهایی[6] دیگر متصل به زیرساخت شبکه است که می‌تواند تسهیل کننده مباحث، تحلیل‌ها، یا هدف گذاری درباره مجموعه کنترل، ارزیابی، معماری یا طراحی باشد.

جنبه‌های مشترک زیرساخت استفاده شده در اسناد مرتبط عبارتند از: PINها، بلوک‌های تابع(Function Blocks) و نوع کنترل(Control Type).

- **زیرساخت فناوری اطلاعات (IT Infrastructure)**

مجموعه‌ای از تجهیزات شبکه، سرویس‌های شبکه، تجهیزات متصل به شبکه، و زیرساخت‌های مربوط به حفاظت شبکه و تجهیزات را زیرساختIT می‌گویند.

نمونه‌هایی از عناصر زیرساخت شبکه عبارتند از:

i. تجهیزات سوئیچینگ(Switching) و مسیریابی(Routing)
ii. امنیت (مثل فایروال، IPS، IDS و فایروال برنامه‌های وب)
iii. مرکز داده (مثل Server farm، تجهیزات ذخیره سازی SAN، توزیع باز)
iv. تجهیزات ارتباطی یکپارچه (Unified Communication Devices)
v. کنترل کننده‌های بی سیم و Access Point ها
vi. تجهیزات امنیت فیزیکی

---

[1] Policy
[2] Procedural
[3] Section
[4] Area
[5] Application
[6] Endpoint

- **سرویس های شبکه (Network Services)**

یک برنامه کاربردی یا قابلیت که توسط زیرساخت، سرورهای برنامه کاربردی یا دیگر تجهیزات متصل به شبکه ایجاد و در دسترس قرار داده شده را سرویس شبکه گویند.

- **موقعیت در شبکه (Place In the Network)**

شامل جنبه‌های عمومی زیرساخت است که از آنها برای نمایش زیرساخت در گروه‌های فیزیکی، منطقی و کاربردی استفاده شده و با اصطلاحات مشترک ترسیم می‌گردند.

از نمونه‌های زیر می‌توان به عنوان مثال برای PIN(Place In The Network) نام برد:

i. شعبه (Branch)
ii. Campus
iii. هسته (Core)
iv. مرکز داده (Data Center)
v. تجارت الکترونیک (E-Commerce)
vi. مرز اینترنت (Internet Edge)
vii. مرز WAN

چارچوب کنترل امنیتی سیسکو (Cisco Security Control Framework)

چارچوب کنترل امنیتی سیسکو(SCF) متشکل از مدل، روش شناسی، ساختار کنترلی و مجموعه کنترل‌هایی است که برای پشتیبانی از ارزیابی مخاطرات فنی در یک معماری زیرساخت، طراحی شده است. سیسکوSCF به عنوان یک فرآیند مداوم در جهت بهبود وضعیت امنیتی زیرساخت‌ها تا رسیدن به استقرار امنیت برای رسیدگی به تهدیدات کلیدی جاری و همچنین شناسایی، ردیابی[1] و دفاع[2] در برابر تهدیدات جدید و نوظهور می‌باشد. دلیل توانایی SCF سیسکو در این موارد، عملکردSCF بر مبنای اصول معماری دقیق به جای تمرکز بر تهدیدات، فناوری ها، محصول برند خاص یا اجرای پیکربندی می‌باشد.

[1] Tracking
[2] Defense

اجزای SCF

SCF سیسکو از سه بخش زیر تشکیل گردیده است:

۱- **مدل (Model)** (همین مبحث)

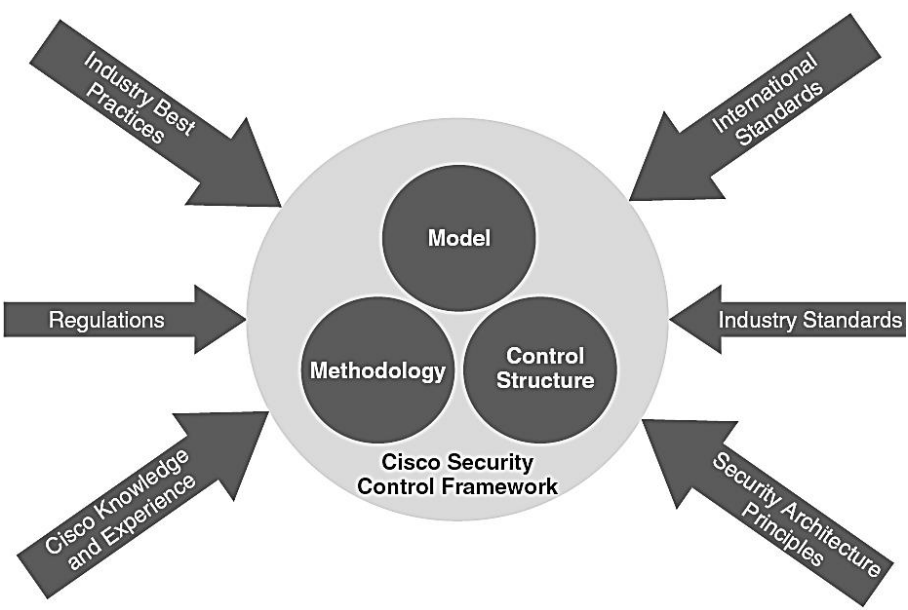
مدل به تعریف اهداف امنیتی و پشتیبانی از اقدامات امنیتی مربوط به آن اهداف، به عنوان مکانیزمی جهت سازماندهی کنترل‌های اختصاصی و اصول مربوط به معماری زیر مجموعه می‌پردازد.

۲- **ساختار کنترل (Control Structure)**

ساختار کنترل به ارائه سازماندهی کنترل‌های اختصاصی و مجموعه کنترل‌ها (Control Set) و چگونگی ارتباط آنها با مدل و متدولوژی می‌پردازد.

۳- **روش شناسی (Methodology)**

روش شناسی یا متدولوژی تعریف کننده مراحل اصلی مورد نیاز جهت ارزیابی معماری امنیتی با استفاده از SCF سیسکو می‌باشد. همچنین تعریف ساختار کنترل‌ها، فرآیند امتیازات و مکانیسم گردآوری این امتیازات در قالب نتایج قابل فهم نیز، بر عهده متدولوژی می‌باشد.



مدل SCF سیسکو

مدلSCF سیسکو با استفاده از اصول بنیادی امنیت، اقدام به تعریف دستورالعمل‌ها و قوانین مورد نیاز برای دستیابی به یک زیر ساخت امن، می‌نماید. معماری امنیت به چگونگی ایجاد یا اجرای زیرساخت امن نمی‌پردازد؛ بلکه اقدام به تعریف ویژگی‌ها، قابلیت‌ها، فرآیندها و کنترل‌هایی می‌نماید که توسط یک زیر ساخت امن باید رعایت شود تا در برابر طیف وسیعی از تهدیدات محافظت گردد. مدلSCF سیسکو فراهم آورنده یک ساختار سازمانی مفید برای دستیابی به یک معماری بر اساس الزامات اصول بنیادی می‌باشد.

تعریف مدلSCF سیسکو با اصول بنیادی امنیت شروع می‌شود. این اصول فاکتورهای اصلی رسیدن به اهداف و اقدامات امنیتی تعریف شده در مدلSCF می‌باشند. در ادامه به توضیح اصول بنیادی مدلSCF می‌پردازیم.

- **دفاع در عمق (Defense-in-Depth)**

هرگز تصور نکنید که یک کنترل به تنهایی می‌تواند باعث کاهش خطرات ناشی از یک تهدید خاص شود.

استفاده از لایه‌های چندگانه کنترل برای جلوگیری، شناسایی و به تاخیر انداختن حملات به منظور محدودیت و به حداقل رساندن خسارت، امری لازم می‌باشد.

- **دسترسی و ارتجاع سرویس (Service Availability and Resilience)**

حصول اطمینان از در دسترس بودن سرویس از طریق Hardening [۱] تجهیزات و تقویت حالت ارتجاع تنظیمات شبکه و بازگشت از شرایط غیرطبیعی پیش آمده به شرایط عادی.

- **تفکیک و ماژولار نمودن (Segregation and Modularity)**

زیرساخت بر اساس بلوک‌های کاربردی با نقش متمایز تسهیل مدیریت، استقرار و تامین امنیت تجهیزات و دارایی‌های کسب و کار در داخل هر بلوک، سازماندهی می‌گردد.

- **پذیرش مقررات و استانداردهای صنعتی (Regulatory Compliance and Industry Standards)**

پیروی از استانداردهای صنعتی و بهترین شیوه‌ها(Best Practices) ، در جهت تسهیل دست یابی به مقررات و استانداردها.

---

[۱] به معنی سخت کردن، مقاوم کردن یا محکم کردن می باشد. (نحوه Hardening در فصل بعد تشریح داده می شود.)

- **کارآیی عملیاتی (Operational Efficiency)**

پیکربندی ساده و کارآمد، استقرار، و مدیریت زیرساخت منجر به افزایش کنترل و دید گردیده و باعث می‌شود ممیزی، عیب یابی، ایزوله مشکل، و پاسخ به حادثه با سرعت بیشتری انجام پذیرد.

- **محرمانگی، درستی و دسترس پذیری (Confidentiality, Integrity, Availability)**

کنترل های امنیتی برای فراهم کردن سطح قابل قبولی از محرمانگی، درستی و دسترس پذیر بودن دیتا کاربرد دارند.

- **کنترل های ممیزی و سنجش (Auditable and Measurable Controls)**

کنترل های امنیتی برای موثر بودن باید همواره مورد ممیزی و سنجش واقع شوند.

- **سیستم گسترده همکاری و ارتباط (System-wide Collaboration and Correlation)**

امنیت زیرساخت را نمی‌توان مجموعه‌ای از راه حل‌های مستقل از یکدیگر دانست. برای دستیابی به یک امنیت موثر نیاز به اشتراک گذاری، تحلیل، و ارتباط اطلاعات تمام منابع سیستم گسترده می‌باشد.

مدلSCF سیسکو به ارائه دو هدف امنیتی اصلی: دید کلی[1] و کنترل کامل[2] می‌پردازد. در نهایت میزان موفقیت یک معماری امنیتی و پیاده سازی زیرساخت، به مقدار تاثیر گذاری آن در افزایش ایجاد شده در دید و کنترل بستگی دارد. بدون دید، کنترلی وجود نخواهد داشت؛ و بدون کنترل، امنیتی به دست نخواهد آمد. به همین دلیلSCF تمرکز اصلی خود را بر روی فعالیت‌های امنیتی و کنترل‌های زیر مجموعه آن معطوف نموده تا موجب افزایش اصول اساسی دید و کنترل گردد. در عمل ازSCF برای انتخاب و بکارگیری پلتفرم هاو قابلیت‌ها برای دستیابی به درجه قابل قبولی از دید و کنترل استفاده می‌شود.

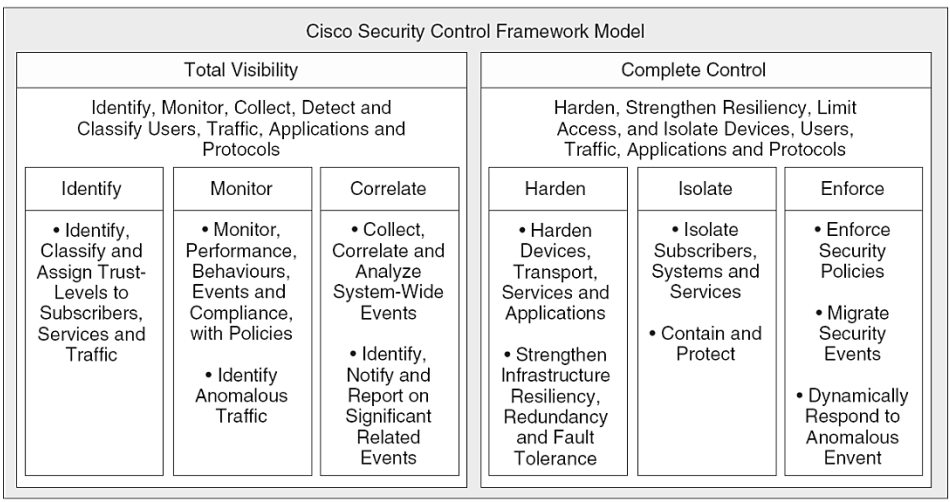
اهداف امنیتی

برای پشتیبانی از اهداف امنیتی، SCF با بهبود دید و کنترل، اقدام به تعریف شش اقدام امنیتی نموده است. سه عدد از این اقدام ها برای دید کلی و سه عدد دیگر مربوط به کنترل کامل بوده که

[1] Total visibility
[2] Complete control

برای سازماندهی دقیق تر، به ازاء هر کنترل امنیتی، یک گروه منطقی با زیر مجموعه‌های مربوطه ایجاد گردیده است.

در تصویر زیر شش اقدام امنیتی و زیر مجموعه‌هایشان به همراه ارتباط آنها با دید کلی و کنترل کامل، نمایش داده شده است.



در ادامه به تشریح رئوس ملاحظات کلیدی دید کلی و کنترل کامل می‌پردازیم:

- **دید کلی (Total Visibility)**

دید کل متشکل از عناصر: شناسایی(Identity)، اعتماد(Trust)، انطباق(Compliance)، نظارت بر رویداد(Event Monitoring) و نظارت بر کارآیی (Performance Monitoring) می‌باشد.

ملاحظات کلیدی برای دید کلی شامل موارد زیر است:

i. شناسایی و طبقه‌بندی[1] کاربران، ترافیک، برنامه‌های کاربردی، پروتکل‌ها و رفتار طریقه استفاده.

ii. نظارت و ثبت فعالیت‌ها و الگوها

iii. جمع‌آوری و ارتباط دیتا از منابع متعدد برای شناسایی روندها و رویدادهای سیستم گسترده

iv. تشخیص و شناسایی ترافیک غیر عادی[2] و تهدیدات

[1] Classification
[2] Anomalous traffic

- **کنترل کامل (Complete Control)**

کنترل کامل شامل: Hardening تجهیزات، افزایش حالت ارتجاعی شبکه، جداسازی کاربران، سیستم‌ها و تجهیزات، اجرای سیاست‌های امنیتی و کاهش رویداد می‌باشد.

ملاحظات کلیدی برای کنترل کامل شامل موارد زیر است:

i. Hardening زیرساختIT و افزایش حالت ارتجاعی شبکه
ii. محدودسازی دسترسی و استفاده به ازاء کاربر، پروتکل، سرویس و برنامه کاربردی
iii. جداسازی کاربران، سرویس‌ها و برنامه‌های کاربردی
iv. حفاظت در مقابل تهدیدات شناخته شده و سوء استفاده
v. عکس العمل پویا در واکنش به رویدادهای غیرعادی

اقدامات امنیتی

اقدامات امنیتی ارائه دهنده گروه‌های سازمان یافته از ویژگی‌های مرتبط، قابلیت‌ها و عملکردهای مورد نیاز در معماری امنیت برای پشتیبانی از یک هدف امنیتی، می‌باشد.

این اقدامات امنیتی در ادامه توضیح داده شده است:

- **دید کلی (Total Visibility)**

هدف امنیتی دید کلی از طریق شناسایی، نظارت و اقدامات امنیتی مرتبط پشتیبانی می‌شود، که در ادامه به تشریح آنها می پردازیم:

i. **شناسایی (Identify)**

کنترل‌های شناسایی ارائه دهنده قابلیت‌هایی برای یک سیستم جهت شناسایی و طبقه‌بندی اشخاص در دسترسی به منابع، و سپس تعیین سطح اعتماد برای آن شخص می‌باشد. توجه داشته باشید در این حالت معمولا برقراری اعتماد از طریق مکانیسم‌های دیگری غیر از بازرسی آدرسIP، انجام می‌شود؛ که از جمله می‌توان به بازرسی اطلاعات کاربری اشاره نمود. این کنترل جهت شناسایی موجودیت، به ترافیک داخلی یا ترافیک خارجی که وارد شبکه می‌شود، اعمال می‌گردد.

ii. **نظارت (Monitor)**

کنترل‌های نظارتی ارائه دهنده قابلیت‌ها و ابزار اصلی بمنظور تسهیل دید امنیتی همراه با توانایی نظارت بر رفتار و استفاده از اجزای زیرساخت از جمله: منابع، سیستم‌های متصل شده، کاربران، برنامه‌های کاربردی و ترافیک IP می‌باشد.

iii. **رابطه متقابل[1] (Correlate)**

تمرکز کنترل‌های Correlate بر روی توانایی سیستم برای استخراج و ارائه اطلاعات مربوط به وضعیت زیرساخت مبتنی بر برقراری رابطه و مدیریت دیتای قابل رویت می‌باشد.

منظور از برقراری رابطه یا Correlation، تفسیر، انتشار، تحلیل و گروه‌بندی دیتای قابل رویت به صورت اطلاعات اجرایی معناداری است که از طریق بررسی رویدادها یا تغییرات به ظاهر غیر مرتبط به دست می‌آید. این کار، اصولی را برای اعمال سیاست‌های اجرایی و کنترل‌های جداسازی از منظر عملیات‌های امنیتی فراهم می‌آورد.

در این صورت مدیریت قادر به نمایش بلادرنگ بصری اطلاعات به‌دست آمده از عناصر مختلف شبکه از جمله گزارش‌های ممیزی، نظارت بر رویداد، علم خطا[2] و اطلاعات سلامت/وضعیت می‌باشد.

- **کنترل کامل (Complete Control)**

هدف امنیتی کنترل کامل توسطHarden کردن، جداسازی و اجرای اقدامات امنیتی پشتیبانی میشود؛ که در ادامه به توضیح آنها می‌پردازیم.

i. **مقاوم سازی (Harden)**

کنترل‌های Harden جهت توانمند سازی یک زیرساخت در مقاوم کردن، تنظیم و یا بازگشت از شرایط نامطلوب کنترل نشده، مورد استفاده قرار می‌گیرند. عملیات Hardening شامل هر دو حالت: تجهیزات تامین کننده امنیت و زیرساخت به عنوان یک کل (که دربر گیرنده افزایش انعطاف پذیری، تحمل خطا[3]، تکرار مسیر و دیگر مفاهیم است)، می‌باشد.

ii. **جداسازی (Isolate)**

تمرکز کنترل‌های جداسازی بر قادر ساختن یک سیستم برای محدود سازی دامنه و به حداقل رساندن تاثیر اختلال‌های شناخته و ناشناخته، بر روی کاربران، سرویس ها و سیستم‌ها می‌باشد.

---

[1] در دیکشنری آکسفورد لغت Correlate به این صورت تعریف گردیده است: داشتن ارتباط یا اتصال متقابل، که در آن یک چیز تاثیر گذار یا وابسته به چیز دیگری باشد.

[2] Fault knowledge

[3] Fault tolerance

با پیاده سازی کنترل‌های جداسازی، می توان بلوک‌های عملکردی فیزیکی و منطقی یک زیر ساخت را در قالب مناطق امنیتی از یکدیگر جدا نمود تا امکان کنترل یا محافظت دسترسی بین بلوک‌های عملکردی زیرساخت و مشخص کردن محدوده امنیتی، فراهم گردد.

iii. **اجبار نمودن (Enforce)**

کنترل‌های اجباری، ارائه دهنده قابلیت‌های مورد نیاز برای اجبار سیستم‌های متصل شده، کاربران، برنامه های کاربردی و ترافیک IP، به رفتار مجاز می‌باشد. سیاست اجبار سازی ممکن است ایستا[1] (کنترلی که بصورت دائمی اعمال شده است)، یا پویا (کنترلی که به صورت خاص برای کاهش برخی رویدادها یا حوادث امنیتی اعمال شده است)، باشد.

سازماندهی کنترل‌ها با SCF سیسکو

در این بخش به ذکر نمونه‌هایی از انواع تکنیک‌ها و فناوری‌های مربوط به کنترل‌ها می‌پردازیم که در هر یک از اقدامات امنیتی مورد استفاده قرار می‌گیرند. مثال‌های ذکر شده در این جدول جهت کمک به توصیف دامنه و هدف هر یک از اقدامات امنیتی و تعریف کنترل‌های متفاوت، می‌باشند.

Total Visibility	**Identify**	Identity-based network solutions (802.1x, NAC, and so on)
		Authentication, Authorization, and Accounting (AAA)—Authentication
		Biometric recognition
		Routing authentication (MD5)
		Secure messaging (encrypted E-mail)
		VPN authentication: – Digital certificates – Pre-shared keys – User authentication
	Monitor	AAA—Accounting
		Anomaly Detection System
		Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
		Network flow data collection
		Simple Network Management Protocol (SNMP) / Remote Monitoring (RMON) /Management Information Base (MIB) – CPU, memory threshold

[1] Static

Total Visibility	**Monitor**	Syslog – Topologies: Cisco Discovery Protocol (CDP); routing protocols; multiprotocol label switching (MPLS) Label Distribution Protocol (LDP)
		Sinkholes
	Correlate	Analysis of network flow data (Arbor, Cisco Security Monitoring, Analysis, and Response System (CS-MARS), and so on)
		Host intrusion protection event correlation
		Security incident management system
		Event analysis and correlation – Syslog – SNMP – AAA – Antivirus
		Network Time Protocol (NTP) synchronization
Complete Control	**Harden**	Control plane policing
		Device hardening – Disable unused services – Latest patch level – Restrict device accessibility
		Component redundancy – Power supply – Link and interface
		Device redundancy
		Topology redundancy
	Isolate	Firewall access control policies
		Network and segment isolation
		Out of band management
		VPN encryption
		Management traffic encryption—Secure Shell (SSH), SNMP, and so on
		Virtual LAN (VLAN)
	Enforce	Content filtering
		Distributed-denial-of-service (DDoS) protection
		Host intrusion prevention
		Port security
		Quality-of-Service (QoS) enforcement
		Network access control – Access control lists (ACL), filters – Unicast reverse path forwarding (uRFP) – Anti-spoofing
		Policy-based routing
		AAA authorization

☑ مبحث سوم

تجهیزات و نرم افزارهای امنیتی

در این مبحث به تعریف سخت افزارها و نرم افزارهایی می‌پردازیم که برای برقراری امنیت مورد استفاده قرار می‌گیرند. این توضیحات صرفا جهت آشنایی با برخی محصولات بوده و برای مطالعه دقیق تر و یادگیری نحوه پیکربندی هر یک از آنها، باید به مستندات فنی مخصوص همان موضوع مراجعه نمایید.

فایروال[۱] (Firewall)

یکی از متداول‌ترین محصولات مربوط به امنیت شبکه، فایروال می‌باشد. ظهور تکنولوژی فایروال در اواخر دهه 1980 میلادی و در زمانی که اینترنت کودکی نوپا بود شکل گرفت. از فایروال برای کنترل ترافیک ورودی و خروجی شبکه استفاده می‌شود. فایروال با تجزیه و تحلیل بسته‌های[۲] دیتا بر اساس قوانین موجود بر روی خود، تشخیص می‌دهد که آیا این بسته اجازه ورود یا خروج را دارد یا خیر؟ در صورتیکه قوانین تنظیم شده بر روی فایروال بسته را مجاز بداند، امکان عبور آن بسته وجود دارد، در غیر اینصورت فایروال اقدام به حذف بسته می‌نماید.

یک فایروال ممکن است به صورت نرم افزاری یا سخت افزاری وجود داشته باشد. مرسوم‌ترین محل قرار گیری فایروال‌های سخت افزاری در مرز[۳] شبکه داخلی با اینترنت یا یک شبکه خود مختار دیگر می‌باشد. اما می‌توان با نصب فایروال‌های نرم افزاری بر روی کلاینت‌ها، به ازاء هر کلاینت یک فایروال مخصوص به خود نیز داشت. امروزه علاوه بر فایروال‌های نرم افزاری که به همراه سیستم عامل ارائه می‌گردد، بسیاری از نرم افزارهای آنتی ویروس نیز از تکنولوژی فایروال پشتیبانی می‌کنند.

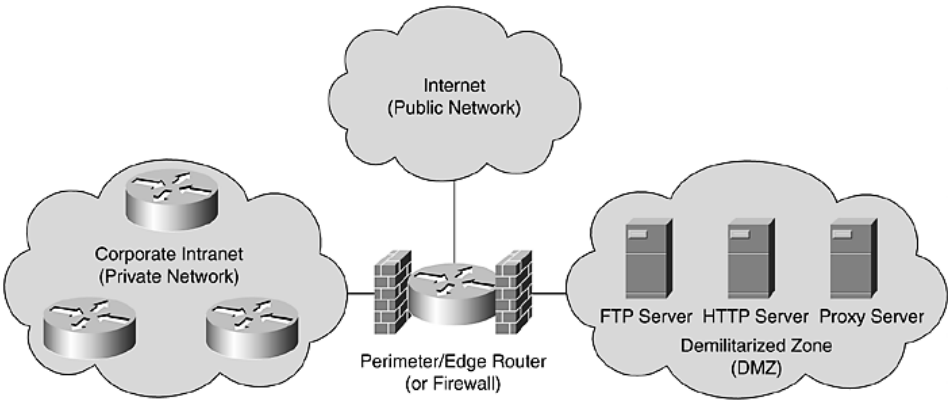
فایروال به عنوان دروازه بین شبکه‌های مختلف با یکدیگر و یا با اینترنت مورد استفاده قرار می‌گیرد. توسط فایروال می‌توان شبکه را از نظر قابلیت اعتماد به بخش‌های مختلف تقسیم کرد.

---

[۱] فایروال به معنی دیوار آتش می باشد.

[2] Packet

[3] Edge



همانطور که در تصویر فوق ملاحظه می نمائید، مدیران شبکه با استفاده از فایروال معمولا شبکه را به سه منطقه زیر تقسیم می‌نمایند:

- **Private Network**

قسمتی از شبکه که به صورت کامل تحت سیاست‌های امنیتی مدیر شبکه اداره شده و از قابلیت اطمینان بالاتری نسبت به سایر شبکه‌ها برخوردار است را شبکه قابل اطمینان می‌نامند. این بخش در فایروال‌های مختلف ممکن است با نام‌های Trust، LAN، Private Network یا Local نیز خوانده شود.

- **DMZ**

در صورتیکه سازمان بخواهد سرویس هایی را به مشتریان خود در بستر اینترنت ارائه نماید از منطقه کمتر حفاظت شده (Demilitarized Zone) استفاده می‌نماید. هر چند این سرورها تحت سیاست‌های مدیر شبکه اداره می‌شوند، ولی به منظور ارائه سرویس‌های مورد نظر، باید برخی از دسترسی‌ها برای کاربران موجود بر روی اینترنت فراهم آورده شود. به همین دلیل این منطقه را کمتر حفاظت شده یا DMZ می‌نامند.

- **Internet**

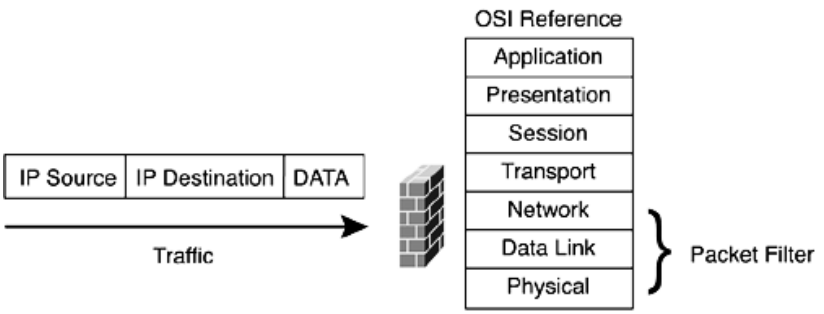
همانطور که از اسم این منطقه مشخص است، فراهم آورنده دسترسی به اینترنت می‌باشد. منطقه اینترنت از نظر مدیر شبکه یک منطقه خطرناک و غیر قابل اعتماد است، به همین دلیل است که در بعضی از فایروال‌ها این منطقه Untrust نامیده می‌شود. معمولا سخت‌ترین سیاست‌های امنیتی بر روی این ناحیه جهت دسترسی به شبکه قابل اعتماد (Trust) و شبکه DMZ اعمال می‌شود.

انواع فایروال

با افزایش کاربران، برنامه‌های کاربردی و نیازهای امنیتی، فایروال‌ها نیز با تغییراتی جهت پشتیبانی از نیازهای روز شبکه‌های کامپیوتری، در سه نسل عرضه گردیده است:

۱- فیلترینگ بسته (Packet Filtering)

فیلترینگ بسته که با نام Stateless Firewall نیز شناخته می‌شود، نسل اول فایروال را تشکیل می‌دهد. در این حالت فایروال دیدی کاملا یکطرفه به تبادل جریان اطلاعات داشته و با بررسی بسته‌ها در هنگام ورود یا خروج شبکه، بدون توجه به اینکه آیا این بسته بخشی از جریان موجود است یا نه! اقدام به اعمال قوانین خود می‌نماید. مواردی که اغلب توسط فیلترینگ بسته مورد بازرسی قرار می‌گیرد عبارتند از: آدرس مبدا، آدرس مقصد، پروتکل و شماره پورت ترافیک مربوط به پروتکل‌های TCP و UDP.



هر چند که اساس کار این نسل از فایروال‌ها بر سه لایه اول مدل OSI می‌باشد، ولی توجه کمی هم به لایه چهارم جهت بررسی پورت های TCP وUDP دارد.

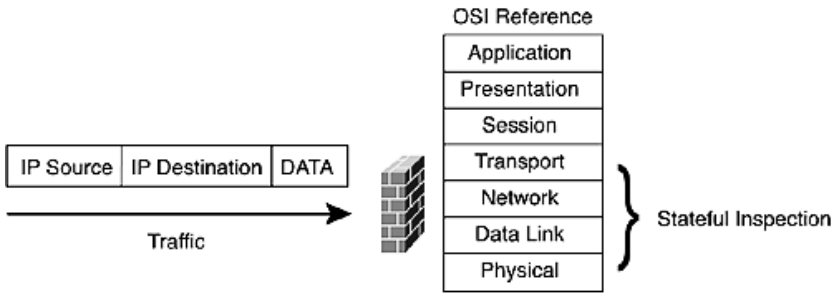
یکی از رایج‌ترین Stateless Firewallها که هنوز هم به طور وسیع مورد استفاده قرار می گیرد، Access Listهای مورد استفاده در روترهای سیسکو می‌باشد.

۲- Stateful Firewall

این نسل از فایروال در سال 1990 میلادی متولد شد. اساس کار Stateful Firewall شبیه نسل قبلی خود بوده، با این تفاوت که سطح عملیات آن تا لایه چهارم مدل OSI (Transport Layer) ارتقاء یافته است. این ارتقاء سطح با نگهداری اطلاعات مربوط به بسته‌ها، به دست آمده است.

این فایروال‌ها با ثبت و ضبط تمام اتصالات عبوری، توانایی تشخیص اینکه آیا این بسته آغاز کننده یک رابطه جدید است یا بخشی از یک اتصال موجود را دارند، به همین دلیل این نسل فایروال‌ها را Stateful Firewall می‌نامند. اگرچه در این فایروال‌ها

همچنان قوانین به صورت ایستا تعریف می‌شوند، ولی این قوانین می‌توانند وضعیت ارتباط(Connection State) را به عنوان یکی از معیارهای تصمیم‌گیری خود، مورد توجه قرار دهند.

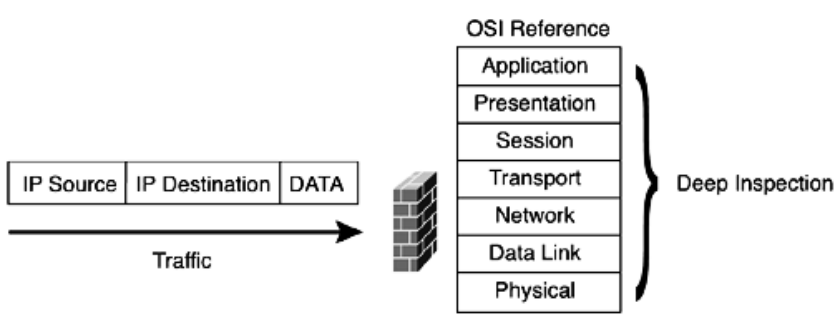


۳- فایروال لایه برنامه کاربردی (Application Layer Firewall)

پس از عمری تلاش بالاخره نسل سوم فایروال‌ها با نام Application Layer Firewall در سال 1998، معرفی گردیدند. در مستندات سیسکو از این نسل با نام Deep Packet Layer Inspection نیز یاد می‌شود. این نوع فایروال‌ها سطح عملیات خود را تا لایه هفتم مدل OSI ارتقاء داده‌اند.

مزیت کلیدی این نسل، توانایی درک فایروال در مورد برنامه‌های کاربردی خاص و پروتکل‌ها از جمله: FTP، DNS وHTTP می‌باشد. توانایی تشخیص پروتکل‌های ناخواسته که قصد دور زدن فایروال را با استفاده از پورتهای مجاز دارند و یا تشخیص پروتکلی که قصد سوء استفاده دارد، امری بسیار مفید در برقراری امنیت می‌باشد. همچنین اطمینان از درستی (Integrity) جریان داده بین دستگاه‌های TCP/IP، از جمله قابلیت های فایروال لایه برنامه کاربردی می‌باشد.

برای سرعت بخشیدن به عملیات در این نوع فایروال‌ها، معمولا انجام آن بر عهده سخت افزارها یا ASIC ها گذاشته می‌شود.



سیستم تشخیص نفوذ (IDS)

وقتی اهمیت منابع سازمان بالاتر می‌رود، پرسنل امنیت شبکه علاوه بر راه کارهایی مانند استفاده از فایروال، شبکه خصوصی مجازی[1] و تکنیک‌های رمزنگاری، به سراغ تجهیزات و ابزارهایی گرایش پیدا می‌کنند که توانایی مقابله فعال با افراد خرابکار را برایشان فراهم نماید. یکی از این ابزارها سیستم تشخیص نفوذ (Intrusion Detection System) یا IDS، می‌باشد.

به طور کلی منظور از نفوذ، تلاش برای ورود غیر مجاز، سوء استفاده و بهره برداری از یک سیستم می باشد؛ که ممکن است توسط دو گروه: مزاحم خارجی[2] یا مزاحم داخلی[3]، انجام پذیرد.

یکی از رایج‌ترین اقدامات امنیتی قرار دادن منابع مهم در محل امنی در داخل شبکه می‌باشد تا بتوان آن را دور از دسترس افراد خرابکار خارج از سازمان قرار داد، اما غافل از آنکه ممکن است بسیاری از نفوذها از داخل شبکه، توسط افراد مزاحم داخلی و یا کارکنان آموزش ندیده ای که ناآگاهانه سیستم خود را در اختیار مزاحمان خارجی قرار داده‌اند، صورت پذیرد.

پس واضح است که برای تشخیص هر دو نوع نفوذ نیاز به یک مکانیزم موثر و مداوم می‌باشد. راه حل موثر برای شناسایی هر دو نوع حملات، استفاده از IDSها می‌باشد. این سیستم‌ها بطور مداوم در سرتاسر شبکه اجرا شده و به محض تشخیص یک تلاش مشکوک، اقدام به آگاه سازی پرسنل امنیت شبکه می‌نمایند.

اجزای IDS

سیستم IDS از دو جزء اصلی تشکیل گردیده است:

- **سنسورهای IDS**

سنسور IDS می‌تواند نرم افزار یا سخت افزار مورد نیاز برای جمع آوری و تحلیل ترافیک شبکه باشد. این سنسورها در دو نوع: IDS میزبان (HIDS)[4] و IDS شبکه (NIDS) موجود می باشند. IDS میزبان معمولا برای نظارت بر یک سرور خاص و IDS شبکه برای نظارت بر تجهیزات و ترافیک شبکه مورد استفاده قرار می‌گیرند.

- **مدیریت IDS**

مدیریت IDS به عنوان نقطه جمع آوری هشدارها و انجام خدمات پیکربندی و استقرار سنسورهای IDS در شبکه مورد استفاده قرار می‌گیرد.

---

[1] Virtual Private Network
[2] Outside Intruder
[3] Inside Intruder
[4] Host IDS

تکنولوژی‌های مورد استفاده در IDS

سیستم IDS برای انجام عملیات خود دارای سه تکنولوژی می‌باشد که بسته به نوع IDS، ممکن است از یک یا چند نوع از این تکنولوژی‌ها بهره ببرد:

- **Anomaly-Based**

در این حالت IDS بنای تشخیص خود را بر اساس آمار رفتاری که بر خلاف حالت عادی در شبکه رخ داده، قرار می‌دهد و در صورت شناسایی ترافیک غیر طبیعی سریعا اقدام به ارسال پیام هشدار به مدیریت شبکه می‌نماید.

از جمله این رفتارها می توان از بررسی مقدار پهنای باند مورد استفاده، پروتکل مورد استفاده، تجهیزات و پورتهایی که به یکدیگر متصل شده اند، نام برد.

- **Signature-Based**

در این حالت الگوهایی از پیش تعیین شده برایIDS تعریف گشته تا نظارت بر بسته‌های انتقالی در شبکه بر اساس همان الگوها انجام پذیرد. در اصطلاح به این الگوها Signature یا امضاء گفته می‌شود.

سیستمIDS مبتنی بر Signature، جریان داده را با دیتابیس خود مقایسه نموده و در صورت تطابق دیتای خاص با یکی از Signature های موجود در دیتابیس، اقدام به تولید پیام هشدار برای مدیر شبکه می‌نماید.

انواع IDS مبتنی بر Signature به صورت زیر می باشد:

i. Simple and stateful pattern matching
ii. Protocol decode-based analysis
iii. Heuristic-base analysis

- **Policy-based**

IDSهای مبتنی برPolicy عمدتا به صورت HIDS وجود دارند. این نوع IDSها، در صورت بروز نقض سیاست‌های پیکربندی، اقدام به ارسال پیام هشدار می‌نمایند.

به عنوان مثال بخش بازاریابی شبکه فقط اجازه دارد به وب سایت‌هایی دسترسی داشته باشد که جزء سایت های فنی و مهندسی است ولی اجازه بازدید از دیگر سایت‌ها و یا استفاده از سرویسFTP را نداشته باشد.

اصطلاحات IDS

سیستم‌های تشخیص نفوذ دارای اصطلاحاتی است که در ادامه به تشریح آنها می‌پردازیم:

- **هشدار / خطر (Alert / Alarm)**

سیگنالی است جهت نشان دادن اینکه یک سیستم مورد حمله قرار گرفته یا می‌خواهد مورد حمله واقع شود.

- **مثبت حقیقی (True Positive)**

حمله‌ای واقعی صورت گرفته و باعث تولید پیام خطر توسط IDS می‌گردد.

- **مثبت کاذب (False Positive)**

تولید پیام خطر، زمانی که هیچ حمله‌ای صورت نگرفته است.

- **منفی کاذب (False Negative)**

خطای IDS در تشخیص حملات واقعی.

- **منفی حقیقی (True Negative)**

حمله‌ای واقع نشده و هیچ پیام خطری هم از طرف IDS صادر نگردیده است.

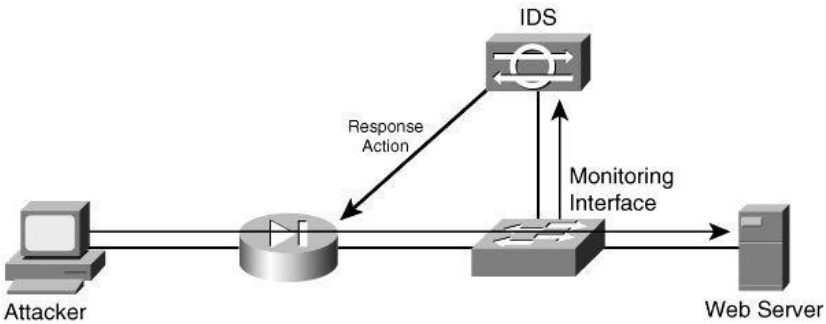
- **نرخ هشدار غلط (False Alarm Rate)**

به صورت: تقسیم تعداد False Positive اتفاق افتاده بر مجموع حملات پیش آمده، تعریف می‌گردد.

- **نرخ تشخیص (Detection Rate)**

به صورت: تقسیم تعداد True Positive تشخیص داده شده بر مجموع حملات پیش آمده، تعریف می‌گردد.

در تصویر زیر تفاوت نحوه قرارگیریIDS و فایروال در شبکه، نمایش داده شده است. فایروال بصورت In-Line و بر سر راه جریان داده قرار می‌گیرد ولی IDS از طریق دریافت یک کپی از اطلاعات، فقط اقدام به نظارت بر ترافیک عبوری می‌نماید :



سیستم پیشگیری از نفوذ (IPS)

سیستم پیشگیری از نفوذ (Intrusion Prevention System) یا IPS، بر اساس سیستم تشخیص نفوذ (IDS) شکل گرفته، با این تفاوت که IPS به دلیل قرار گیری بر خط[1] در شبکه، علاوه بر نظارت روی ترافیک، می‌تواند به صورت فعال اقدام به پیشگیری از نفوذهای تشخیص داده شده نماید.

عملکرد اصلی سیستم‌هایIPS، بر روی شناسایی فعالیت‌های مخرب، ثبت اطلاعات فعالیت‌های مذکور، تلاش برای جلوگیری/توقف یک فعالیت و گزارش فعالیت، متمرکز می‌باشد. همچنین IPS می‌تواند به طور خاص اقداماتی مانند: ارسال پیام هشدار، حذف بسته‌های مخرب، تنظیم مجدد اتصال و یا مسدود کردن ترافیک مربوط به آدرس‌های IP متخلف، را انجام دهد.

یکIPS همچنین قادر به تصحیح خطاهای CRC[2]، یکپارچه کردن قطعات جریان بسته‌ها، محافظت از توالی شماره‌هایTCP و پاک کردن گزینه‌های ناخواسته لایه‌های Network و Transport، می‌باشد.

به دلیل ادغام سرویس‌های IDS و IPS با یکدیگر، از این محصول با نام‌هایی مثل IDPS یا IDS/IPS نیز یاد می‌شود. محصولات IPS به صورت نرم افزاری یا سخت افزاری و در چهار نوع مختلف ارائه می گردند:

- NIPS(Network Intrusion Prevention System)
- HIPS(Host Intrusion Prevention System)
- WIPS(Wireless Intrusion Prevention System)
- NBA(Network Behavior Analysis)

سرویس پروکسی (Proxy)

استفاده از سرویس پروکسی در یک شبکه، می‌تواند چندین هدف داشته باشد. سرویس پروکسی می‌تواند آدرسIP واقعی کاربران را پنهان نماید. به این معنی که وقتی فرد حمله کننده سعی دارد آدرسIP را جعل[3] نماید، هیچ تصوری درباره آدرس های پنهان شده ندارد، لذا سرور پروکسی طوری طراحی شده تا در صورت بروز حمله، برای از بین بردن بسته و اعلام هشدار به مدیر شبکه درباره واقعه روی داده شده، اقدام نماید.

---

[1] In-line
[2] Cyclic Redundancy Check
[3] Spoof

همچنین سرورهای پروکسی می‌توانند اطلاعاتی را که به صورت متناوب توسط کاربران شبکه از اینترنت مورد درخواست واقع می‌شوند را در نهانگاه (Cache) خود نگهداری نمایند. در این صورت کاربران جواب درخواست‌های تکراری خود را می‌توانند سریع‌تر دریافت نمایند بدون آنکه از پهنای باند اینترنت استفاده کرده باشند.

کاربران باید در هنگام استفاده از سرورهای پروکسی عمومی، نهایت دقت را به خرج دهند. توجه داشته باشید که وقتی شما از یک سرور پروکسی استفاده می کنید، تمام جریان دیتای شما از جمله: Accountها و کلمات عبور، از طریق آن سرور پروکسی ارسال می‌شود. بنابراین ضروری است که پروکسی مورد استفاده، توسط یک نهاد کاملا مورد اعتماد اجرا شده باشد.

فیلترینگ محتوا (Content Filtering)

توسط فیلترینگ محتوا (شبیه فیلترینگ URL)، یک سازمان می‌تواند سیاستهای خود را مبنی بر محتوای سایت‌های مجاز، به کاربران خود اعمال نماید. فیلتر محتوا می‌تواند نظارت، مدیریت و محدود نمودن دسترسی به اینترنت را فراهم نماید. به عنوان مثال مدیر شبکه می‌تواند با مشخص نمودن محتوای مورد نیاز سازمان، از استفاده نادرست اینترنت توسط کاربران اتصالات گران قیمت و کم سرعت WAN، جلوگیری به عمل آورد.

آنتی ویروس (Anti-Virus)

یک ویروس کامپیوتری می‌تواند بصورت یک برنامه کوچک یا چند خط کد، به سیستم عامل نفوذ کرده و باعث یک رویداد غیر منتظره و معمولا منفی گردد. در اینجاست که نرم افزارهای آنتی ویروس به کمک شما آمده و با اسکن کردن حافظه موقت و دیسک سخت سیستم، اقدام به شناسایی این کدهای مخرب می‌نماید. در صورتیکه نرم افزار یک فایل مخرب مطابق با دیتابیس خود پیدا نماید، آنرا به اطلاع کاربر می‌رساند و این کاربر است که تصمیم می‌گیرد چه برخوردی با این فایل انجام پذیرد.

امروزه آنتی ویروس‌ها قادر به شناسایی طیف گسترده‌ای از کدهای مخرب[1] از جمله: ویروس‌ها، ربایندگان[2]، Keylogger ها، Backdoor ها، روت کیت‌ها، اسب‌های تروجان، کرم‌ها[3]، ابزار تبلیغاتی ناخواسته(مزاحم)[4] و جاسوس افزارها(Spy Ware)، می‌باشند.

---

[1] Malware
[2] Hijackers
[3] Worms
[4] Adware

اگرچه متداول‌ترین حالت استفاده از آنتی ویروس، نصب آن بر روی کلاینت‌ها می باشد، ولی چند سالی است که از آنتی ویروس‌ها برای نظارت بر ترافیک شبکه نیز استفاده می‌شود.

روش‌های شناسایی کدهای مخرب

نرم افزارهای آنتی ویروس برای شناسایی کدهای مخرب از چهار روش اصلی زیر استفاده می کنند. البته تعداد روش‌ها در آنتی ویروس‌های مختلف ممکن است متفاوت باشد.

- **Signature-Based**

تشخیص مبتنی بر امضاء(Signature) رایج‌ترین روش شناسایی کدهای مخرب توسط نرم افزارهای آنتی ویروس می‌باشد. در این حالت آنتی ویروس دارای یک دیتابیس از امضاهای مربوط به کدهای مخرب مختلف بوده و با مقایسه آنها با فایلهای موجود، اقدام به تشخیص کدهای مخرب می‌نماید. البته به دلیل اینکه کدهای مخرب می‌توانند خود را در داخل فایلهای دیگر جاسازی نمایند، آنتی ویروس اقدام به جستجوی کامل همه فایل‌ها می‌نماید.

دیتابیس مربوط به Signature نرم افزارهای آنتی ویروس باید همواره به روز رسانی شود.

- **Heuristic**

همانطور که می‌دانید هر لحظه به تعداد کدهای مخرب موجود بر روی اینترنت افزوده می‌شود. اگر در مدت زمان بین ایجاد کد مخرب تا بروز رسانی امضای آن در دیتابیس آنتی ویروس، کد مخرب به سیستم شما برسد قطعا کاری از دست آنتی ویروس بر نیامده و سیستم شما آلوده خواهد شد. برای رفع این ایراد، شرکت‌های تولید کننده آنتی ویروس از ویژگی کشف کننده یا Heuristic، برای کشف کدهای مخرب نوظهور و ناشناخته استفاده می‌نمایند.

ویژگی کشف کننده، با تجزیه و تحلیل فایلها و اثرات آنها، اقدام به کشف و شناسایی کدهای مخرب می‌نماید.

- **Rootkit Detection**

روت کیت، نوعی کد مخرب برای به دست آوردن کنترل سطح مدیر سیستم بوده و نحوه طراحی آن به گونه‌ای انجام می‌پذیرد که قابل شناسایی نباشد. روت کیت می‌تواند عملکرد سیستم عامل را تغییر داده و در بعضی مواقع با دستکاری[1] آنتی ویروس، آنرا تبدیل به یک برنامه بی اثر نماید.

[1] Tamper

به دلیل اینکه روت کیت‌ها اغلب در سطح سیستم عامل فعالیت می‌نمایند، نرم افزارهای آنتی ویروس برای شناسایی آنها باید تمهیدات خاصی را در نظر بگیرند.

- **Real-time Protection**

حفاظت بلادرنگ که از آن با نام‌هایی مثل Guard یا Autoprotect نیز یاد می‌شود، جهت حفاظت خودکار سیستم توسط نرم افزارهای آنتی ویروس ارائه می‌گردد. این ویژگی بصورت مداوم بر روی سیستم نظارت دارد تا به محض ورود یک کد مخرب، بصورت بلادرنگ آنرا شناسایی نماید.

مدیریت یکپارچه تهدیدات (UTM)

مدیریت یکپارچه تهدیدات (Unified Threat Management) که به اختصارUTM نامیده می‌شود، یک راهکار جدید در دنیای امنیت شبکه، برای محافظت از دروازه[1] اصلی شبکه سازمان، می‌باشد.

یکUTM شامل مجموعه‌ای کامل و جامع از راهکارهای امنیتی از جمله: فایروال، آنتی ویروس، ضد هرز نامه[2]، IDS/IPS، ضد جاسوس افزار، مدیریت پهنای باند، شبکه خصوصی مجازی(VPN)، فیلترینگ URL و فیلترینگ محتوا، می‌باشد.

هرچند که UTMها از زمان تولد (سال 2003) تا کنون توانسته‌اند سهم قابل ملاحظه‌ای از بازار امنیت شبکه را به تسخیر خود در آورند، ولی برخی کمپانی‌های بزرگ مثل سیسکو هنوز اقدام به تولید تجهیزات UTM ننموده و غالب UTM ها توسط شرکت های کمتر شناخته شده در زمینه شبکه، تولید و ارائه می‌گردند.

تجمیع تمام راهکارهای امنیتی در یک دستگاه، ضمن فراهم آوردن مزایای قابل توجه ممکن است ایرادات یا نواقصی را نیز به همراه داشته باشد. اغلب برندهای تولید کننده UTM نمی‌توانند سخت افزاری را فراهم نمایند که بتواند به خوبی تمام این امکانات را پشتیبانی نماید و در بعضی برندهای معتبر که سخت افزار قابل قبولی دارند، قیمت این تجهیزات ممکن است خارج از توان خرید سازمان باشد. از دیگر نواقص این تجهیزات یکپارچه نبودن تولیدکننده محصولات جاسازی شده در UTMها می‌باشد. به عنوان مثال تمام تولیدکنندگان UTM، آنتی ویروس و ضد هرزنامه مورد استفاده در تجهیزات خود را از سایر شرکت ها تهیه می‌نمایند.

---

[1] Gateway
[2] Anti-spam

فصل نهم

امنیت شبکه

- ☑ مبحث اول: Hardening تجهیزات شبکه
- ☑ مبحث دوم: امنیت سوئیچینگ
- ☑ مبحث سوم: امنیت مسیریابی

☑ مبحث اول

Hardening تجهیزات شبکه

اولین گام در امنیت شبکه، مقاوم سازی تجهیزات شبکه می‌باشد. در این مبحث به تشریح عملیاتی می‌پردازیم که جهت مقاوم سازی در بین سوئیچ‌ها و روترها مشترک می‌باشد.

Management Plane

Management Plane شامل عملیاتی می‌باشد که برای دستیابی به اهداف مدیریتی در شبکه مورد استفاده واقع می‌گردد. وقتی شما می‌خواهید امنیت تجهیزات شبکه را تامین نمایید، حفاظت از Management Plane بسیار مهم خواهد بود. اگر یک حادثه امنیتی قادر به تخریب عملکرد مربوط به Management Plane باشد، بازیابی یا ثبات در شبکه برای شما غیر ممکن می‌گردد. در این مبحث برای کمک به استحکام Management Plane به بررسی ویژگی‌های امنیتی و تنظیمات موجود بر روی IOS سیسکو می‌پردازیم.

مقاوم سازی عمومی Management Plane

از Management Plane برای دسترسی، پیکربندی، مدیریت و نظارت بر عملکرد تجهیزات و شبکه‌ای که توسط آنها گسترش پیدا نموده، استفاده می‌گردد.

برای مقاوم‌سازیManagement Plane، باید اقدام به امن سازی پروتکل‌های مورد استفاده توسط آن نمایید. این پروتکل‌ها در فهرست زیر آورده شده است:

- Simple Network Management Protocol (SNMP)
- Telnet
- Secure Shell Protocol
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Secure Copy Protocol
- TACACS+
- RADIUS

- Netflow
- Network Time Protocol (NTP)
- Syslog

این امن سازی برای حصول اطمینان از بقای مدیریت در صورت رخداد حوادث امنیتی، باید انجام شود. چراکه اگر یکی از این اجزاء مورد سوء استفاده قرار گیرد، ممکن است تمام اجزای دیگر نیز در معرض خطر واقع شوند.

کنترل خطوط tty و vty

نشست‌های تعاملی مدیر شبکه با تجهیزات از طریق خطوط tty یا vty انجام می‌گیرند. یک خط tty(Terminal Type)، خط ناهمگام محلی مربوط به یک پورت فیزیکی می‌باشد که بصورت محلی یا از طریق مودم Dialup، جهت دسترسی به تجهیزات کاربرد دارد.

یک خط vty(virtual tty) برای تمام اتصالات از راه دور دیگر شبکه (بدون در نظر گرفتن پروتکل مورد استفاده مثل SSH، SCP و Telnet) که توسط تجهیزات پشتیبانی می‌شود مورد استفاده قرار می‌گیرد. تجهیزات سیسکو از تعداد محدودی از خطوط vty پشتیبانی می‌کنند که می‌توان با استفاده از دستور show line از خطوط موجود مطلع شد. زمانی که تمام خطوط vty اشغال باشند، امکان ایجاد یک نشست جدید مدیریتی وجود نخواهد داشت؛ لذا ممکن است باعث ایجاد وضعیت DoS[1] برای دسترسی به دستگاه گردد.

برای کنترل این خطوط علاوه بر استفاده از کلمه عبور، تمهیدات دیگری نیز باید در نظر گرفته شود که در این مبحث به تشریح آنها خواهیم پرداخت.

مدیریت Password

با کلمه عبور(Password)، می‌توان دسترسی به تجهیزات و منابع را کنترل کرد. این عمل از طریق تعریف یک Password یا Secret که در درخواست‌های اعتبار سنجی مورد استفاده قرار می‌گیرند، انجام می‌پذیرد. زمانیکه یک درخواست دسترسی به منابع یا تجهیزات دریافت می‌شود، هویت(Identity) و کلمه عبور مورد بررسی قرار گرفته و در نهایت دسترسی در یکی از این حالات اتفاق می افتد: اعطای دسترسی[2]، رد دسترسی[3] یا اعطای دسترسی بصورت محدود شده[4].

---

[1] Denial of Service
[2] Granted
[3] Denied
[4] Limited Access

به عنوان بهترین شیوه امنیت، کلمات عبور باید توسط سرورهای TACACS+ یا RADIUS مدیریت شوند. البته توجه داشته باشید در اینصورت نیز تنظیم دسترسی روی تجهیزات به صورت محلی همچنان امکان پذیر است تا در صورت از دسترس خارج شدن سرورهای احراز هویت، امکان ورود به تجهیزات فراهم باشد.

اولین و مهمترین نکته درباره کلمه عبور، انتخاب یک عبارت قدرتمند می‌باشد. منظور از کلمه عبور قدرتمند، عبارتی است که حدس آن چه برای انسان و چه برای ماشین کاری سخت و طاقت فرسا باشد. برای ایجاد یکStrong Password توجه به نکات زیر ضروری است[۱]:

i. کلمه عبور حداقل شامل ۸ کاراکتر باشد. (توصیه می‌شود دارای ۱۵ کاراکتر باشد.)
ii. از حروف بزرگ و کوچک استفاده شود.
iii. از اعداد استفاده شود.
iv. از نماد(Symbol) ها استفاده شود. مثل @، !، #، % و غیره.
v. از اطلاعات شخصی مثل نام، فامیل، تاریخ تولد و یا شماره تلفن استفاده نگردد.
vi. از الگوی صفحه کلید استفاده نشود. مثل: asdfghjkl یا 123456789 و یا qwerty.
vii. این عبارت نباید عمومی بوده یا در فرهنگ لغت موجود باشد.
viii. در بازه‌های زمانی مشخص اقدام به تعویض کلمه عبور نمایید.
ix. کلمه عبور جدید، شبیه کلمه عبور قبلی نباشد.
x. برای اهداف مختلف از کلمه های عبور یکسان استفاده نکنید.

تجهیزات شبکه غیر از کلمه عبور، امکان دارد اطلاعات دیگر امنیتی از جمله: NTP key، رشته SNMP یا Routing Protocol key، را نیز در فایل پیکربندی خود داشته باشند.

کلمات عبور و دیگر اطلاعات امنیتی مانند موارد فوق، در حالت پیش فرض بصورت متن واضح در فایل پیکربندی تجهیزات ذخیره می‌گردند. در اینصورت با مشاهده فایل به راحتی می‌توان از تمام کلمات عبور موجود روی دستگاه با خبر شد.

یک راه رمزنگاری کلمات عبور استفاده از دستورenable password می‌باشد، ولی الگوریتم رمزنگاری مورد استفاده در آن ساده بوده و به راحتی قابل شکستن می‌باشد. اما در صورت استفاده از دستورenable secret به جایenable password، می‌توان از یک الگوریتم قوی‌تر برای رمزنگاری کلمات عبور بهره برد.

---

[۱] برای اینکه ببینید اجرای هر کدام از این مراحل، تا چه اندازه می‌تواند بر قدرت کلمه عبور شما تاثیر گذار باشد؛ می‌توانید به این وب سایت ها مراجعه نمائید:

http://howsecureismypassword.net / http://www.passwordmeter.com

توجه داشته باشید اگر بدون فعال کردن enable secret، برای پورت کنسول کلمه عبور تعیین کرده باشید، این کلمه عبور می‌تواند از طریق vty(Virtual tty) جهت دریافت سطح دسترسی ویژه(Privilege) مورد سوء استفاده قرار گیرد. این اتفاق که اغلب بصورت ناخواسته روی می‌دهد، می‌تواند دلیل دیگری بر الزام استفاده از enable secret باشد.

برای فراهم کردن شرایط استفاده از enable secret یا ویژگی بهبود امنیت کلمه عبور[1] (که در ادامه شرح داده می‌شود)، بهتر است اقدام به حذف کلمات عبور ایجاد شده توسط دستور enable password نمائید. به عبارت دیگر اگر هر دو حالت فوق بر روی تجهیزات فعال باشند، اولویت استفاده با کلمه عبور ایجاد شده توسط دستور enable secret خواهد بود.

دستورenable secret و ویژگی بهبود امنیت کلمه عبور، از الگوریتمMD5 برای پنهان سازی کلمه عبور استفاده می‌نمایند که باعث ایجاد امنیت بیشتری نسبت به حالت استفاده از enable password خواهد شد. هر چند این الگوریتم از امنیت قابل ملاحظه ای برخوردار است ولی ممکن است یک هکر از طریق روش دیکشنری و صرف مدت زمان زیاد بتواند به کلمات عبور دست پیدا نماید، لذا باز هم توصیه می‌شود ضمن انتخاب یک کلمه عبور قدرتمند، از فایل‌های پیکربندی به دقت محافظت گردد.

استفاده از روش‌های enable password و enable secret، فقط باعث رمزگذاری Password تجهیزات می شود. اما همانطور که قبلا نیز گفته شد اطلاعات حساس دیگری در فایل پیکربندی موجود است که در حالت پیش فرض بصورت متن واضح ذخیره می‌شوند. اجرای دستورservice password-encryption در محیط پیکربندی Global، بصورت مستقیم اقدام به رمزنگاری کلمات عبور، امنیت CHAP[2] و دیتای حساس مشابه ذخیره شده در فایل پیکربندی، می‌نماید. این قبیل رمزنگاری بمنظور جلوگیری از خوانده شدن کلمات عبور، مثل زمانیکه مدیر شبکه درحال بررسی فایل پیکربندی تجهیزات می‌باشد و یک شخص غیرقابل اعتماد امکان مشاهده مانیتور ایشان را دارد، نیز می تواند مفید واقع شود.

با این حال الگوریتم رمزنگاری استفاده شده توسط service password-encryption، الگوریتم قدرتمندی نمی‌باشد. از این الگوریتم نباید توقع زیادی برای محافظت کامل از فایل پیکربندی در مقابل حملات پیچیده هکرهای قدرتمند، را داشته باشید. لذا باید همان محافظتی که از فایل‌های دارای متن ساده انجام می‌دهید، برای این نوع فایلها نیز به کار برید.

در ادامه به ذکر دستورات مورد استفاده جهت اجرای موارد فوق می‌پردازیم:

---

[1] Enhanced password security feature
[2] Challenge Handshake Authentication Protocol

Setting or Changing a Line Password	
Command	**Purpose**
Router(config)#**password** *password*	Establishes a new password or change an existing password for the privileged command level.

Setting or Changing a Static Enable Password	
Command	**Purpose**
Router(config)# **enable password** *password*	Establishes a new password or change an existing password for the privileged command level.

Protecting Passwords with Enable Password and Enable Secret	
Command	**Purpose**
Router(config)# **enable password** [**level** *level*] {*password*| *encryption-typeencrypted-password*} or Router(config)# **enable secret** [**level** *level*] {*password* | *encryption-type encrypted-password*}	Establishes a password for a privilege command mode. Specifies a secret password, saved using a non-reversible encryption method. (If enable password and enable secret are both set, users must enter the enable secret password.)

Encrypting Passwords	
Command	**Purpose**
Router(config)# **service password-encryption**	Encrypts a password.

بهبود امنیت کلمه عبور

سیسکو از نسخه 12.2(8)T اقدام به معرفی ویژگی بهبود امنیت کلمه عبور، در IOSهای خود نموده است. این ویژگی مدیر شبکه را قادر می‌سازد تا علاوه بر Password اقدام به ایجاد نام کاربری نیز نموده و همچنین از MD5 برای پنهان نمودن کلمه عبور مربوط به نام کاربری، بهره ببرد. قبل از این ویژگی، دو نوع کلمه عبور وجود داشت: نوع 0 که یک کلمه عبور با متن ساده بود، و نوع 7 که از الگوریتم رمزنگاری قدیمی Vigenère استفاده می‌نمود.

توجه داشته باشید این ویژگی امکان استفاده با پروتکل‌هایی که نیاز به کلمه عبور بصورت متن واضح دارند(مثل CHAP)، را ندارد.

نحوه استفاده از ویژگی بهبود کلمه عبور بصورت زیر می باشد:

Device(config)#**username** <*user*> **secret** <*password*>

قفل کلمه عبور در صورت تکرار اشتباه

سیسکو ویژگی قفل کلمه عبور در صورت تکرار اشتباه، را از نسخه 12.3(14) به بعد در IOSهای خود گنجانیده است. این ویژگی در صورت تکرار اشتباه در وارد کردن کلمه عبور، حساب کاربری مورد نظر را قفل کرده و تنها مدیر شبکه(یا کاربر دارای سطح دسترسی15) است که می تواند حساب کاربری را از این حالت خارج نماید.

برای پیکربندی این ویژگی، از دستورات زیر استفاده می نماییم:

Device(config)#aaa new-model
Device(config)#**aaa local authentication attempts max-fail** *<max-attempts>*
Device(config)#aaa authentication login default local
Device(config)#**username** *<user>* **secret** *<password>*

در دستورات فوق، <max-attempts> مشخص کننده تعداد دفعاتی است که کاربر مجاز به وارد نمودن کلمه عبور میباشد.

از این ویژگی می‌توان در روش‌های تائید هویت CHAP و PAP[1] نیز بهره برد.

سرویس عدم بازیابی کلمه عبور

در IOSهای سیسکو می‌توان در هنگام Boot شدن دستگاه با استفاده از کلید Break، از اجرای فایل پیکربندی جلوگیری نموده و پس از قرار دادن دستگاه در حالت ROMMON با استفاده از پورت کنسول اقدام به تغییر یا حذف کلمه عبور نمود. این سرویس در مواقع فراموشی کلمه عبور می‌تواند کمک قابل توجهی به مدیر شبکه برای بازیابی کلمه عبور و امکان استفاده مجدد از تجهیزات (بدون از دست دادن فایل پیکربندی) باشد.

اما در برخی شرایط یا مکان‌ها، این سرویس حساس می‌تواند از طریق فرد مهاجم مورد سوء استفاده قرار گیرد. سیسکو برای جلوگیری از این اتفاق، سرویس عدم بازیابی کلمه عبور را از IOS نسخه 12.3(14)T به بعد در تجهیزات خود قرار داده است. در صورت فعال نمودن این ویژگی، دیگر کسی نمی‌تواند با استفاده از کلید Break و دسترسی به پورت کنسول، اقدام به بازیابی یا پاک کردن کلمه عبور نماید. همچنین این سرویس از تغییر مقدار رجیستر و دسترسی به NVRAM، توسط افراد خرابکار جلوگیری به عمل می‌آورد.

برای فعال سازی سرویس عدم بازیابی کلمه عبور، می توان از دستور زیر استفاده نمود:

Device(config)#no service password-recovery

[1] Password Authentication Protocol

توجه داشته باشید با فعال کردن این سرویس، حتی خودتان هم دیگر نمی‌توانید اقدام به Password Recovery نمایید! (چاه نکن بهر کسی/ اول خودت دوم کسی)، و هیچ راهی جز حذف کامل فایل پیکربندی برای شما باقی نخواهد ماند، لذا توصیه می‌شود حتما یک نسخه پشتیبان از فایل پیکربندی را بصورت آرشیو و در محل قابل اطمینان نگهداری نمایید.

غیرفعال کردن سرویس‌های بلا استفاده

به عنوان بهترین شیوه امنیتی، باید تمام سرویس‌های غیر ضروری و بلااستفاده را بصورت غیرفعال نگاه داشت. این سرویس‌های غیر ضروری به ویژه آنهایی که از پروتکلUDP استفاده می‌نمایند، می‌توانند توسط افراد مهاجم در حملات منع خدمت (DoS) و دیگر حملات مورد استفاده قرار گیرند.

سرویس‌هایTCP وUDP کوچکی که بستن آنها پیشنهاد می‌گردد، به صورت زیر می‌باشد:

- Echo (پورت شماره ۷)[1]
- Discard (پورت شماره ۹)[2]
- Daytime (پورت شماره ۱۳)[3]
- Chargen (پورت شماره ۱۹)[4]

اگر چه می‌توان با استفاده از لیست‌های دسترسی Anti-spoofing از خطرات و تهدیدات مربوط به این سرویس‌های کوچک کاست، ولی بهتر است که این سرویس‌ها بر روی تجهیزات قابل دسترس شبکه، غیرفعال گردیده باشند. سیسکو از نسخه 12.0 به بعد، بصورت پیش فرض این سرویس‌ها را غیرفعال نموده است. اما در نسخه‌های قبل از آن شما باید به صورت دستی اقدام به غیرفعال نمودن آنها نمائید.

علاوه بر موارد فوق، لیست زیر شامل دستوراتی است که برای غیر فعال نمودن سرویس‌های اضافی مورد استفاده قرار می‌گیرند:

- **No ip finger**

برای غیر فعال نمودن سرویس finger می‌توان از دستور زیر استفاده نمود. سیسکو در نسخه‌های 12.1(5) و 12.1(5)T، بصورت پیش فرض این سرویس را غیرفعال نموده است.

---

[1] RFC 862
[2] RFC 863
[3] RFC 867
[4] RFC 864

Device(config)#no ip finger

- **No ip bootp server**

از دستور زیر برای غیرفعال نمودن پروتکل خود راه انداز(BOOTP)[1]، استفاده می‌شود:

Device(config)#no ip bootp server

- **Ip dhcp bootp ignore**

در IOSهای نسخه 12.2(8)T به بعد، باید از دستور زیر برای غیرفعال نمودن BOOTP استفاده نمود. این دستور باعث غیرفعال شدن BOOTP و فعال شدن استفاده از سرویس DHCP می‌گردد.

Device(config)#ip dhcp bootp ignore

- **No service dhcp**

اگر نیازی به DHCP Relay در شبکه ندارید، می‌توانید توسط دستور زیر اقدام به غیرفعال نمودن سرویس DHCP نمایید:

Device(config)#no service dhcp

- **No mop enabled**

بمنظور غیرفعال سازی سرویس MOP(Maintenance Operation Protocol)، می‌توانید از دستور زیر استفاده نمایید:

Device(config)#no mop enabled

- **No ip domain-lookup**

برای غیرفعال کردن سرویس DNS می‌توان از این دستور استفاده نمود:

Device(config)#no ip domain-lookup

- **No service pad**

در شبکه‌های X.25 برای غیرفعال نمودن سرویس (Packet Assembler / Disassembler) PAD، از دستور زیر استفاده می‌شود:

Device(config)#no service pad

- **No ip http server**

برای غیر فعال کردن سرویس‌های Http و Https، از دستورات زیر استفاده می‌شود:

Device(confgi)#no ip http server
Device(confgi)#no ip http secure-server

منظور از سرویس‌های HTTP و HTTPS در این قسمت، سرویس‌هایی است که امکان مدیریت تجهیزات را بصورت Web Base فراهم می‌آورد.

---

[1] Bootstrap Protocol

- **No service config**

به‌جز مواردیکه مجبور هستید با استفاده از TFTP یک فایل را در زمان Startup به تجهیزات معرفی نمایید، باید این سرویس را توسط دستور زیر غیرفعال نگه دارید:

```
Device(config)#no service config
```

این دستور باعث حفاظت از تجهیزات در مقابل قرار دادن فایل پیکربندی جعلی از طریق TFTP می‌گردد.

- **No cdp**

همانطور که می‌دانید، سیسکو از پروتکلCDP برای کشف تجهیزات همسایه بهره می‌برد. این پروتکل می‌تواند توسط سیستم مدیریت شبکه (NMS)[1] یا در هنگام عیب‌یابی مورد بهره‌برداری قرار گیرد. اما توجه داشته باشید که این پروتکل باید بر روی اینترفیس‌هایی که به تجهیزات غیرقابل اطمینان متصل هستند، غیرفعال گردد. در غیر اینصورت فرد خرابکار می‌تواند با جمع آوری پیام‌های CDP اطلاعات مورد نیاز برای شناسایی شبکه شما را به دست آورد.

برای غیرفعال نمودنCDP بر روی یک اینترفیس خاص می‌توان از دستور زیر استفاده نمود:

```
Device(config-if)#no cdp enable
```

برای غیرفعال نمودنCDP بر روی تمام اینترفیس‌ها نیز می توان از این دستور استفاده نمود:

```
Device(config)#no cdp run
```

- **No lldp**

سرویس LLDP(Link Layer Discovery Protocol)، نسخه استاندارد شده CDP می‌باشد که توسط تجهیزات برندهای متفاوت پشتیبانی می‌شود. خطرات گفته شده در CDP ممکن است در LLDP نیز بوجود آید. به همین دلیل می‌توانید این پروتکل را بر روی یک اینترفیس خاص یا بطور عمومی، بر روی تجهیزات غیر فعال نمود:

```
Device(config-if)#no lldp transmit
Device(config-if)#no lldp receive
Device(config)#no lldp run global
```

[1] Network Management System

دستور EXEC Timeout

برای مشخص نمودن زمان انقضای یک نشست(Session) می‌توان از دستورexec timeout استفاده نمود. این دستور مشخص کننده مقدار زمانی است که دستگاه در صورت عدم فعالیت[1] کاربر در خط فرمان، بصورت خودکار به آن جلسه خاتمه می‌دهد. مدت زمان این ویژگی که در هر دو ارتباط vty و tty مورد استفاده قرار می‌گیرد، بصورت پیش فرض ۱۰ دقیقه می‌باشد.

برای تغییر مقدار پیش فرض exec timeout می‌توان از دستور زیر استفاده کرد:

Device(config-line)#**exec-timeout** *<minutes>* [second]

دستور Keepalive برای نشست TCP

دستورات Tcp-keepalives-in و Tcp-keepalives-out، تجهیزات را قادر به ارسال پیام keepalive برای نشست هایTCP، می‌سازد. پیکربندی این ویژگی می‌تواند هم بر روی ورودی (in) و هم بر روی خروجی (out) تجهیزات انجام پذیرد. ارسال این پیام باعث می‌شود تا طرف‌های نشست یک اتصال TCP، از در دسترس بودن دستگاه مقابل اطمینان حاصل نمایند. در این صورت تجهیزات قادر به شناسایی نشست‌های نیمه باز[2] یا بی سرپرست[3] بوده و قبل از آنکه توسط افراد خرابکار مورد سوء استفاده واقع شوند، اقدام به حذف آنها نمایند.

دستورات زیر جهت فعال سازی پیام Keepalive مورد استفاده قرار می گیرند:

Device(config)#service tcp-keepalives-in
Device(config)#service tcp-keepalives-out

استفاده از اینترفیس مدیریت

مدیریت تجهیزات از طریقin-band یاout-of-band یک اینترفیس مدیریتی فیزیکی یا منطقی، امکان پذیر می‌باشد. در حالت ایده‌آل، دسترسی در هر دو حالت in-band و out-of-band بر روی تجهیزات شبکه جهت انجام دستورات مدیریت در دسترس می‌باشد.

یکی از اینترفیس‌هایی که غالبا برای دسترسی in-band بر روی تجهیزات به کار برده می‌شوند، اینترفیس منطقیLoopback می‌باشد. این اینترفیس‌ها پس از ایجاد همواره up است، در حالی که اینترفیس‌های فیزیکی ممکن است به دلایل مختلف به حالت up یا down تغییر حالت

[1] Idle
[2] Half-open
[3] Orphan

دهند. پیشنهاد میشود برای مدیریت تجهیزات، یک اینترفیس Loopback در آنها ایجاد و از آن بطور انحصاری برای مدیریت آن دستگاه استفاده گردد. از این اینترفیس برای ارسال و دریافت ترافیک پروتکل‌های مدیریتی از قبیل: SNMP، SSH و Syslog نیز می‌توان بهره برد.

برای ایجاد اینترفیس منطقی Loopback می‌توان از دستورات زیر استفاده نمود:

Device(config)#**interface loopback** *<number>*
Device(config-if)#**ip address** *<ip_address> <subnet_mask>*

هشدار آستانه حافظه

ویژگی هشدار آستانه حافظه که از نسخه12.3(4)T درIOSهای سیسکو اضافه گردیده، به شما اجازه می‌دهد تا امکان قرارگیری تجهیزات در شرایط low-memory را کاهش دهید. این قابلیت با استفاده از دو روش زیر قابل استفاده می‌باشد:

- **هشدار آستانه حافظه (Memory Threshold Notification)**

در این حالت، در صورتی که حافظه آزاد یک دستگاه از مقدار مشخص شده توسط مدیر شبکه کمتر شود، یک پیام هشدار صادر می‌گردد.

تنظیم مقدار آستانه حافظه، از طریق دستورات زیر انجام می‌پذیرد. در صورت اجرای این دستورات، پیام‌ها در دو صورت ارسال می‌گردد. اول در صورتیکه مقدار حافظه آزاد کمتر از مقدار مشخص شده گردد. دوم در صورتیکه مقدار حافظه دوباره به حالت عادی (۵ درصد بیشتر از آستانه مشخص شده) باز گردد.

Device(config)#**memory free low-watermark processor** *<threshold>*
Device(config)#**memory free low-watermark io** *<threshold>*

- **رزرو حافظه (Memory Reservation)**

از این حالت برای رزرو حافظه کافی برای پیام‌های حیاتی استفاده می‌شود. این حالت تضمین کننده حافظه دستگاه برای ادامه فرآیندهای مدیریتی در هر شرایطی می‌باشد.

برای رزرو حافظه می‌توان از دستور زیر استفاده کرد:

Device(config)#**memory reserve critical** *<value>*

هشدار آستانه CPU

ویژگی هشدار آستانه CPU از نسخه 12.3(4)T به IOSهای سیسکو اضافه گردیده است. با استفاده از این ویژگی، در صورتی که مقدار بار CPU از آستانه مشخص شده فراتر رود، دستگاه

اقدام به ارسال پیام هشدار می‌نماید. این پیام‌های هشدار در قالب پیام SNMP Trap ایجاد و ارسال می‌گردند.

Enabling CPU Thresholding Notification		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enables global configuration mode.
Step 3	**snmp-server enable traps cpu threshold** **Example:** Router(config)# snmp-server enable traps cpu threshold	Enables CPU thresholding violation notification as traps and inform requests.
Step 4	**snmp-server host** *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] **cpu** [*notification-type*] [**vrf***vrf-name*] **Example:** Router(config)# snmp-server host 192.168.0.0 traps public cpu	Sends CPU traps to the specified address.

Defining CPU Thresholding Notification		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *percentage* **interval** *seconds*] **Example:** Router(config)# process cpu	Sets the CPU thresholding notifications types and values. • In this example, the CPU utilization threshold is set to 80 percent for a rising threshold notification and 20 percent for a falling threshold notification, with a 5-second polling interval.

Defining CPU Thresholding Notification		
	threshold type total rising 80 interval 5 falling 20 interval 5	

Setting the Entry Limit and Size of CPU Utilization Statistics		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**process cpu statistics limit entry-percentage***number* [**size** *seconds*] **Example:** Router(config)# process cpu statistics limit entry-percentage 40 size 300	Sets the process entry limit and the size of the history table for CPU utilization statistics. • In this example, to generate an entry in the history table, a process must exceed 40 percent CPU utilization. • In this example, the duration of time for which the most recent history is saved in the history table is 300 seconds.

رزرو حافظه جهت دسترسی کنسول

این ویژگی از نسخه 12.4(15)T به بعد توسط IOSهای سیسکو پشتیبانی شده و باعث رزرو حافظه مورد نیاز جهت دسترسی از طریق کنسول و عملیات عیب‌یابی می‌گردد. استفاده از این ویژگی بخصوص وقتی سودمند است که دستگاه مورد نظر با مقدار حافظه کمی راه اندازی می‌گردد. برای رزرو حافظه برای مقاصد دسترسی کنسول و عیب‌یابی می‌توانید از این دستورات بهره ببرید:

Configuring Reserve Memory for Console Access		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

Configuring Reserve Memory for Console Access		
Step 3	**memory reserved console** *number-of-kilobytes* **Example:** Router(config)# memory reserved console 512	Increases the amount of memory reserved for console access. • The *number-of-kilobytes* argument is the amount of memory to be reserved in kilobytes. Valid values are 1 to 4096 KB.
Step 4	**exit** **Example:** Router(config)# exit	Exits to privileged exit mode.
Step 5	**show memory console reserved** **Example:** Router# show memory console reserved	Displays the actual amount of memory that has been reserved.

آشکار ساز نشت[1] حافظه

سیسکو این ویژگی را از نسخه12.3(8)T1 در IOSهای خود گنجانیده است. آشکار ساز نشت حافظه قادر به تشخیص نشت‌های بوجود آمده در تمام منابع حافظه‌ها، بافر بسته‌ها و Chunkها[2] می‌باشد.

منظور از نشت حافظه، مقدار حافظه اختصاص داده شده ایستا یا پویایی می‌باشد که شامل هیچ خدمت مفیدی نیست. البته تمرکز این قابلیت بر روی حافظه های پویای اختصاص داده شده، می‌باشد.

توسط دستور زیر می توانید از این ویژگی استفاده نمائید:

Device#show memory overflow

تمهیدات پروتکل NTP

پروتکل NTP(Network Time Protocol)، یک سرویس خطرناک نیست، بلکه توجه به این نکته ضروری است که هر سرویسی که بطور صحیح مورد استفاده قرار نگیرد ممکن است ابزاری جهت کمک به افراد خرابکار محسوب گردد. اگر می‌خواهید از سرویسNTP استفاده نمائید، پیکربندی دقیق یک منبع قابل اعتماد و استفاده از سرویس احراز هویت مناسب، امری ضروری خواهد بود.

---

[1] Leak

[2] یک واحد با اندازه ثابت اختصاص داده شده از حافظه.(Chunk از نظر لغوی به معنای تکه یا قسمت می باشد)

Configuring NTP Authentication		
	Command	**Purpose**
Step 1	**config t** **Example:** switch# config t	Places you in global configuration mode.
Step 2	[**no**] **ntp authentication-key***number* **md5** *md5-string* switch(config)# ntp authentication-key 42 md5 aNiceKey	Defines the authentication keys. The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key** *number*command.
Step 3	**show ntp authentication-keys** **Example:** switch(config)# show ntp authentication-keys	(Optional) Displays the configured NTP authentication keys.
Step 4	[**no**] **ntp trusted-key** *number* **Example:** switch(config)# ntp trusted-key 42	Specifies one or more keys (defined in Step 2) that a time source must provide in its NTP packets in order for the device to synchronize to it. The range for trusted keys is from 1 to 65535. This command provides protection against accidentally synchronizing the device to a time source that is not trusted.
Step 5	**show ntp trusted-keys** **Example:** switch(config)# show ntp trusted-keys	(Optional) Displays the configured NTP trusted keys.
Step 6	[**no**] **ntp authenticate** **Example:** switch(config)# ntp authenticate	Enables or disables the NTP authentication feature. NTP authentication is disabled by default.
Step 7	**show ntp authentication-status** **Example:** switch(config)# show ntp authentication-status	(Optional) Displays the status of NTP authentication.
Step 8	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

محدود کردن دسترسی‌ها

یکی از رایج‌ترین روش‌های اعمال محدودیت در دسترسی افراد به منابع مختلف شبکه، استفاده از لیست های دسترسی (Access List) می‌باشد. کاربرد ACLها طیف وسیعی از عملیات تجهیزات شبکه را شامل می شود که از جمله می‌توان به اعمال محدودیت دسترسی از طریق tty و vty به تجهیزات شبکه و همچنین کنترل ارتباط کلاینت‌های موجود در شبکه‌های مختلف با یکدیگر، اشاره نمود.

تشریح کامل ACL در مبحث امنیت مسیریابی در همین فصل آمده است.

فیلتر بسته‌های ICMP

پروتکل ICMP، برای کنترل شبکه‌های مبتنی بر IP طراحی گردیده و نقش مهمی در مدیریت و عیب‌یابی شبکه ایفا می‌کند. به عنوان مثال دو دستور مهم ping و traceroute، که همواره از پر کاربردترین دستورات مورد استفاده توسط مدیران شبکه می‌باشند، جزو ابزارهای پروتکل ICMP محسوب می‌شود.

با توجه به اینکه مهاجمان شبکه می‌توانند از پیام‌های ICMP برای دستیابی به مقاصد پلید! خود سوء استفاده نمایند، IOSهای سیسکو امکاناتی را در جهت فیلتر این پیام‌ها بر اساس نام، نوع(Type) و کد آنها از طریق ACLها فراهم آورده است.

به عنوان مثال در ACL زیر امکان ping توسط ایستگاه‌های کاری قابل اعتماد (مدیریت و سرورهای NMS) امکانپذیر بوده ولی برای سایر ایستگاه‌های موجود در شبکه، غیر قابل دسترس می‌باشد.

```
ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!
 permit icmp host <trusted-management-stations> any echo
 permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!
 permit ip any any
!
```

ویژگی Management Plane Protection

ویژگیManagement Plane Protection که باختصارMPP نیز نامیده می‌شود، از نسخه 12.4(6)T توسط IOSهای سیسکو ارائه گردیده است. ویژگیMPP به مدیر شبکه اجازه می‌دهد تا ترافیک مدیریتی دستگاه را به یک اینترفیس خاص منحصر نماید. این قابلیت مدیر شبکه را قادر می‌سازد کنترل‌های اضافی روی تجهیزات اعمال نموده و مشخص نماید که آنها به چه صورت می‌توانند قابل دسترس باشند.

برای استفاده از این ویژگی می توانید مراحل زیر را بر روی تجهیزات اعمال نمایید:

Configuring a Device for Management Plane Protection		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**control-plane host** **Example:** Router(config)# control-plane host	Enters control-plane host configuration mode.
Step 4	**management-interface** *interface* **allow** *protocols* **Example:** Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp	Configures an interface to be a management interface, which will accept management protocols, and specifies which management protocols are allowed. *interface*—Name of the interface that you are designating as a management interface. *protocols*—Management protocols you want to allow on the designated management interface. • BEEP • FTP • HTTP • HTTPS • SSH, v1 and v2 • SNMP, all versions • Telnet • TFTP
Step 5	**Ctrl z** **Example:** Router(config-cp-host)# Ctrl z	Returns to privileged EXEC mode.

Configuring a Device for Management Plane Protection		
Step 6	**show management-interface** [*interface*| **protocol** *protocol-name*] **Example:** Router# show management-interface FastEthernet 0/0	Displays information about the management interface such as type of interface, protocols enabled on the interface, and number of packets dropped and processed. *interface*—(Optional) Interface for which you want to view information. **protocol**—(Optional) Indicates that a protocol is specified. *protocol-name*—(Optional) Protocol for which you want to view information

رمز گذاری نشست‌های مدیریتی

بطور معمول مدیران شبکه برای برقراری ارتباط با تجهیزات شبکه از Telnet استفاده می‌نمایند که در این حالت اطلاعات بین آنها به صورت متن واضح تبادل می‌گردد. در این حالت اگر اطلاعات تبادل شده بین مدیر شبکه و تجهیزات شنود شود، فرد خرابکار به راحتی می‌تواند تمام اطلاعاتی که برای نابودی یک شبکه نیاز دارد را به دست آورد.

برای حفظ امنیت دیتای تبادل شده در نشست‌های مدیریتی، باید اقدام به رمزگذاری آنها نموده تا در صورت شنود توسط افراد خرابکار، از افشای اطلاعات جلوگیری به‌عمل آید. به همین منظور IOSهای سیسکو با پشتیبانی از پروتکل هایSSH[1] و HTTPS، اطلاعات نشست‌های مدیریتی را بصورت رمز شده انتقال می‌دهند.

پروتکل‌های SSHv1(SSH Version 1)، SSHv2 و HTTPS، از SSL(Secure Socket Layer) و TLS(Transport Layer Security) برای احراز هویت و رمزگذاری داده‌ها استفاده می‌نمایند. لازم به ذکر است که پروتکل های SSHv1 و SSHv2 با یکدیگر سازگاری ندارند!

سیسکو همچنین از پروتکل SCP(Secure Copy Protocol) نیز برای ایجاد یک ارتباط امن و رمز شده جهت انتقال فایلهای پیکربندی و IOS تجهیزات بهره می‌برد. عملکرد پروتکل SCP نیز بر اساس SSH می‌باشد.

پیکربندی SSH دارای روشهای متنوعی[2] جهت اجرا بر روی تجهیزات سیسکو می‌باشد، که در ادامه نحوه اجرای یکی از مرسوم ترین این روشها، توضیح داده شده است:

---

[1] Secure Shell

[2] http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html

Configuring a Router for SSH Using a Hostname and Domain Name		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**hostname** *hostname* **Example:** Router(config)# hostname MTR	Configures a hostname for your router.
Step 4	**ip domain-name** *name* **Example:** MTR(config)# ip domain-name example.com	Configures a domain name for your router.
Step 5	**crypto key generate rsa** **Example:** MTR(config)# crypto key generate rsa	Enables the SSH server for local and remote authentication.
Step 6	**ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*] **Example:** MTR(config)# ip ssh time-out 120	(Optional) Configures SSH control variables on your router.
Step 7	**ip ssh version** [**1** | **2**] **Example:** MTR(config)# ip ssh version 1	(Optional) Specifies the version of SSH to be run on your router.

پس از فعال سازی پروتکلSSH بر روی تجهیزات، باید محل استفاده از آنرا نیز مشخص نمایید. برای مثال در دستور زیر استفاده از پروتکلSSH جهت برقراری ارتباط از طریق vty اجبار گردیده است:

```
Device(config)#line vty 0 4
Device(config-line)#transport  input  ssh
```

پورت‌های کنسول و AUX

تجهیزات سیسکو دارای دو پورت فیزیکیAsynchronous به نام‌هایConsole و Auxiliary می‌باشند که جهت دسترسی محلی و راه دور مورد استفاده قرار می‌گیرند. همانطور که می‌دانید پورت کنسول به دلیل داشتن امتیازات ویژه از اهمیت بالایی برخوردار است، چراکه بعضی از

اعمال حیاتی مثل Password Recovery فقط از طریق این پورت امکان پذیر می‌باشد. اگر یک مهاجم بخواهد عمل بازیابی کلمه عبور را بر روی تجهیزات انجام دهد ضمن دسترسی فیزیکی باید امکان قطع و وصل برق آنها را نیز داشته باشد.

با توجه به اهمیت پورت کنسول، دسترسی به آن باید به شیوه‌ای امن و مطمئن انجام پذیرد. این روش‌های امن باید شامل استفاده از AAA، exec-timeout و تنظیم کلمه عبور برای مودم (در صورت استفاده)، باشد. همچنین در صورتی که بازیابی کلمه عبور مورد نیاز نباشد، می‌توان همانطور که قبلا گفته شد اقدام به غیر فعال نمودن این سرویس نمود.

یادگیری این نکته ضروریست که با استفاده از اتصالات معکوس از طریق خطوط tty می‌توان از تجهیزات دیگر به پورت کنسول دستگاه دسترسی پیدا نمود. برای جلوگیری از بر پایی اتصالات معکوس می‌توان به صورت زیر عمل نمود:

```
Router(config)#line console 0
Router(config-line)#transport input none
```

همچنین در اغلب موارد از پورت‌های AUX برای دسترسی راه دور به روترها استفاده نمی‌گردد. در این صورت بهتر است توسط دستورات زیر، اقدام به غیرفعال نمودن این پورت نمایید:

```
Router(config)#line aux 0
Router(config-line)#transport input none
Router(config-line)#transport output none
Router(config-line)#no exec
Router(config-line)#exec-timeout 0 1
Router(config-line)#no password
```

اعلامیه هشدار[1]

در برخی از حوزه‌های قضایی، امکان پیگرد قانونی افراد خرابکار مقدور نمی‌باشد مگر آنکه آنها را به طریقی از غیر قانونی بودن اعمالشان مطلع کرده باشید. در این صورت است که استفاده از اعلامیه‌های هشدار می‌تواند راهگشا باشد.

نحوه نگاشت اعلامیه هشدار کاری پیچیده بوده و نسبت به قوانین قضایی هر منطقه می‌تواند متفاوت باشد. بهترین راه برای انتخاب جملات مورد نظر، مشورت با یک وکیل متبحر در حوزهIT است. اما در مجموع یک اعلامیه هشدار می‌تواند شامل یک یا همه این موارد باشد:

[1] Warning Banner

- اعلامیه خاص قوانین محلی.
- توجه داشته باشید هر گونه استفاده غیر مجاز از این سیستم، پیگرد قانونی دارد.
- توجه داشته باشید که سیستمی که قصد ورود به آن را دارید، فقط می‌تواند توسط کاربران مجاز مورد استفاده واقع شود.
- توجه داشته باشید که تمام فعالیت شما در هنگام ورود و استفاده از این سیستم در فایل‌های رویداد نگاری ذخیره شده و می‌تواند بر علیه شما مورد استناد قرار گیرد.

(به قول فیلم‌های پلیسی خارجی: هر حرفی بزنی تو دادگاه بر علیه خودت استفاده می‌شه!)

از نظر امنیتی به این نکته مهم نیز توجه داشته باشید که اعلامیه‌ها نباید شامل اطلاعات خاصی در مورد تجهیزات مثل: مدل، نرم افزار، مالکیت و محل قرارگیری آنها باشد. به دلیل اینکه این اطلاعات می‌تواند کمک خوبی به افراد مهاجم در جهت اعمال مخرب باشد.

دستورات متنوعی جهت ایجاد Banner وجود دارند[1] که در ادامه به ذکر یک نوع آن بسنده می کنیم. دستور banner incoming جهت نمایش آگهی هشدار در زمان ورود به سیستم مورد استفاده قرار می‌گیرد:

Device(config)#**banner incoming *d message d***

حرف d در دستور فوق جهت مشخص نمودن ابتدا و انتهای پیام، مورد استفاده قرار گرفته است. شما می‌توانید به جای حرف d از هر کاراکتر دیگری مثل $ یا # نیز استفاده کنید. فقط به این نکته توجه داشته باشید که حرف مورد نظر نباید در پیام وجود داشته باشد.

منظور از Message در دستور فوق، پیام مورد نظر شما است که می‌خواهید در هنگام ورود کاربر نمایش داده شود.

مقاوم سازی پروتکل SNMP

با توجه به اینکه اطلاعات مهمی از طریق پروتکلSNMP بین تجهیزات با سرورهای مدیریت شبکه تبادل گردیده و حتی در برخی مواقع امکان تغییر پیکربندی از طریقSNMP نیز ممکن می‌باشد، لذا باید برای استفاده امن از این پروتکل به نکات زیر توجه داشته باشیم:

[1] http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf004.html

- **استفاده از Community String**

رشته ارتباط(Community String)، کلمه عبور مورد استفاده در پروتکلSNMP است که جهت اعمال محدودیت دسترسی خواندن/نوشتن مورد استفاده واقع می‌شود. برای انتخاب رشته ارتباط باید همان موارد گفته شده درباره کلمات عبور را مدنظر قرار داده و همچنین در بازه‌های زمانی مشخص اقدام به تغییر آنها نمود.

ضمن مشخص نمودن رشته ارتباط می‌توان سطح دسترسی را نیز تعیین کرد. دو سطح دسترسی فقط خواندنی (Read Only) و خواندن/نوشتن (Read/Write) در پروتکل SNMP قابل تعریف می‌باشد.

- **Community String همراه با ACL**

با استفاده از ACL می‌توان حتی استفاده از رشته ارتباط را محدود به آدرس‌هایIP خاص نمود.

- **استفاده از ACL در زیر ساخت SNMP**

در اینصورت می‌توان اطمینان حاصل نمود که فقط میزبان‌های قابل اطمینان امکان ارسال ترافیک پروتکلSNMP را به تجهیزات شبکه دارند.

- **SNMP Views**

SNMP View ها ویژگی‌های امنیتی هستند که می‌توانند دسترسی مجاز یا غیر مجاز به یک SNMP MIB خاص را مشخص نمایند.

- **SNMPv3**

در نهایت توصیه می‌شود در صورت امکان ازSNMPv3 در شبکه استفاده شود. نسخه سومSNMP که توسط RFC 3410, 3411, 3412, 3413, 3414 تعریف گردیده دارای ویژگی‌های امنیتی بارزی نسبت به نسخه‌های قبلی خود می‌باشد.

مرجع دستورات استفاده از SNMP و ویژگی های فوق، در ادامه ذکر گردیده است:

Creating or Modifying Access Control for an SNMP Community		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

Step 3	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*] **Example:** Router(config)# snmp-server community comaccess ro 4	Defines the community access string. You can configure one or more community strings.
Step 4	**no snmp-server community** *string* **Example:** Router(config)# no snmp-server community comaccess	Removes the community string from the configuration.
Step 5	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 6	**show snmp community** **Example:** Router# show snmp community	(Optional) Displays the community access strings configured for the system.

Configuring SNMP Version 3		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**snmp-server group** [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read***readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*] **Example:** Router(config)# snmp-server group group1 v3 auth access lmnop	Configures the SNMP server group to enable authentication for members of a specified named access list. In this example, the SNMP server group *group1* is configured to enable user authentication for members of the named access list *lmnop*.
Step 4	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 5	**show snmp group** **Example:** Router# show snmp group	Displays information about each SNMP group on the network.

بهترین شیوه‌های رویداد نگاری[1]

رویدادنگاری رخدادها، نظارت جامعی از نحوه عملکرد اشخاص و تجهیزات شبکه را برای شما فراهم می‌آورد. سیسکو با ارائه گزینه‌های انعطاف پذیری جهت رویداد نگاری، شما را در جهت دستیابی به مدیریت شبکه و اهداف نظارتی سازمان، کمک می‌کند.

در ادامه به بررسی بهترین شیوه‌های رویداد نگاری با کمترین تاثیر بر روی عملکرد تجهیزات شبکه می‌پردازیم.

- **ارسال رویدادها به یک مکان مرکزی**

در این حالت اطلاعات وقایع به یک سرور Syslog ارسال گردیده و توسط آن سرور ذخیره می‌شوند. با وجود یک سرور مرکزی و ثبت تمام وقایع بصورت متمرکز، امکان مدیریت و نظارت بهتر برای مدیر شبکه فراهم می‌گردد.

توجه داشته باشید که بصورت پیش فرض اطلاعات بصورت متن واضح و از طریق پورتUDP برای سرور ارسال می‌گردد. لذا باید تمهیدات امنیتی از قبیل رمزگذاری اطلاعات مورد توجه قرار گیرد.

- **سطح واقعه نگاری**

هر پیامی که توسط OSهای سیسکو ایجاد می‌گردد در یکی از هشت سطح زیر با نوع و درجه اهمیت متفاوت خواهد بود.

Level	System	Description
Emergency	**0**	System unusable messages
Alert	**1**	Immediate action required messages
Critical	**2**	Critical condition messages
Error	**3**	Error condition messages
Warning	**4**	Warning condition messages
Notification	**5**	Normal but significant messages
Information	**6**	Informational messages
Debugging	**7**	Debugging messages

[1] Logging Best Practices

شما می‌توانید در زمان پیکربندی، نوع پیام‌های مورد نظر خود را جهت ایجاد و ارسال توسط تجهیزات مشخص نمایید.

توجه داشته باشید که ایجاد پیام‌های سطح هفتم (Debug) مقدار زیادی از منابع تجهیزات را به خود اختصاص می‌دهد. لذا توصیه می‌شود جز در موارد خاص از این سطح واقعه نگاری استفاده نکنید.

- **عدم ارسال رویداد به نشست‌های کنسول و نظارت**

تجهیزات سیسکو می‌توانند پیام‌های رویداد نگاری را بر روی نشست‌های کنسول و نظارت ارسال کنند. در اینصورت مقدار زیادی از منابع تجهیزات صرف ارسال این پیام‌ها می‌گردد. لذا توصیه می‌شود که از ارسال پیام‌های مربوط به وقایع بر روی نشست‌های نظارت و کنسول، توسط دستورات زیر جلوگیری نمائید.

```
Device(config)#no logging console
Device(config)#no logging monitor
```

- **استفاده از بافر[1]**

تجهیزات سیسکو به مدیر شبکه اجازه می‌دهند تا با استفاده از بافر، اقدام به بررسی رویدادها بصورت محلی بر روی تجهیزات نماید. استفاده از این روش مخصوصا به جای روش قبل (ارسال رویدادها بر روی نشست نظارت و کنسول) توصیه می‌گردد.

- **تعیین اینترفیس مبدا جهت واقعه نگاری**

بصورت پیش فرض آدرسIP پیام‌ها، آدرس اینترفیسی است که پیام از طریق آن دستگاه را ترک نموده است. به همین دلیل امکان دارد پیام‌های مربوط به یک دستگاه دارای آدرس‌هایIP متفاوتی باشند. برای اینکه بتوانید به راحتی تمام وقایع مربوط به یک دستگاه را تشخیص دهید، بهتر است اقدام به مشخص نمودن اینترفیس مبدا جهت واقعه نگاری نمایید. در این صورت تمام وقایع مربوط به دستگاه با یک آدرسIP مبدا بر روی سرورSyslog ذخیره می‌شوند تا به آسانی قابل تشخیص و طبقه بندی باشند.

- **ثبت وقایع به همراه زمان**

مهم است که تاریخ و زمان دقیق وقایع اتفاق افتاده مشخص باشد. برای تصمیم گیری درباره پیشگیری یا رفع یک ایراد، زمان رویداد آن می‌تواند از درجه اهمیتی بالایی برخوردار باشد. لذا تجهیزات سیسکو این امکان را دارند تا وقایع را همراه با تاریخ و زمان با دقت میلی ثانیه به ثبت رسانند.

---

[1] Buffer

دستورات مورد استفاده جهت رویداد نگاری در تجهیزات سیسکو به صورت زیر می‌باشد:

Setting the Syslog Destination	
Command	**Purposes**
Router(config)# **logging buffered** [*size*]	Logs messages to an internal buffer.
Router(config)# **logging** *host*	Logs messages to a syslog server host.

Enabling Time-Stamps on Log Messages	
Command	**Purposes**
Router(config)# **service timestamps log uptime** or Router(config)# **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	Enables log time stamps.

Limiting the Error Message Severity Level and Facilities	
Command	**Purposes**
Router(config)# **logging console** *level*	Limits the number of messages logged to the console.
Router(config)# **logging monitor** *level*	Limits the number of messages logged to the terminal lines.
Router(config)# **logging trap** *level*	Limits the number of messages logged to the syslog servers.

Setting the Syslog Source Address	
Command	**Purposes**
Router(config)# **logging source-interface** *type number*	Sets the syslog source address.

مدیریت پیکربندی

سیسکو درOSهای خود امکاناتی را جهت مدیریت پیکربندی ارائه نموده تا مدیر شبکه را قادر به آرشیو فایل‌های پیکربندی جهت جایگزینی و عقب گرد پیکربندی نماید.

- **ویژگی‌های جایگزینی[1] و عقب گرد[2]**

سیسکو از نسخه12.3(7)T به بعد، ویژگی‌های جایگزینی و عقب گرد را از طریق آرشیو نمودن پیکربندی تجهیزات، به OSهای خود افزوده است. پیکربندی‌های ذخیره شده بصورت دستی یا خودکار در این آرشیوها می‌توانند به منظور جایگزینی با پیکربندی فعلی مورد استفاده قرار بگیرند.

[1] Replace
[2] Rollback

می‌توان توسط دستورReplace اقدام به جایگزینی فایل مورد نظر با Running-config فعلی نمود و در مقابل با استفاده از دستور Copy می‌توان فایل پیکربندی مورد نظر را با فایل Running-config موجود ادغام کرد.

به عنوان مثال توسط دستور زیر مشخص می‌نماییم حداکثر۱۴ کپی از فایلهای پیکربندی را در مسیر حافظه فلش دستگاه و با نام Archive نگهداری نماید. همچنین مدت زمان تناوب ساخت کپی از فایل پیکربندی را ۱۴۴۰دقیقه (یک شبانه روز) تنظیم می‌کنیم:

```
Device(config)#archive
Device(config-archive)#path Flash:Archive
Device(config-archive)#maximum 14
Device(config-archive)#time-period 1440
Device(config-archive)#write-memory
```

دستور write-memory نیز مشخص می‌کند، پس از آنکه مدیر شبکه اقدام به write پیکربندی نمود، از فایل پشتیبان تهیه گردد.

- **انحصار دسترسی در زمان اعمال تغییرات**

سیسکو از نسخه12.3(14)T ویژگی انحصار دسترسی در زمان اعمال تغییرات را به IOSهای خود افزود تا تضمین نماید اعمال تغییرات در فایل پیکربندی در یک زمان معین فقط توسط یک مدیر شبکه امکان پذیر می‌باشد. این ویژگی از تاثیرات نامطلوب اعمال تغییرات همزمان توسط چند مدیر شبکه جلوگیری به عمل می‌آورد. این ویژگی می‌تواند به دو صورت خودکار و دستی، پیکربندی گردد.

به عنوان مثال برای اجرای خودکار این ویژگی از دستور زیر استفاده می‌نمائیم:

```
Device(config)#configuration mode exclusive auto
```

- **ویژگی ارتجاعی**

ویژگی(Resilient Configuration) را سیسکو از نسخه12.3(8)T جهت ذخیره امن یک نسخه از IOS و فایل پیکربندی جاری، به امکانات خود افزوده است. وقتی این ویژگی در حالت فعال قرار دارد، تغییر یا حذف فایل‌های پشتیبان مذکور غیرممکن می‌باشد. توصیه می‌شود برای جلوگیری از حذف غیر عمدی یا خرابکارانه فایلها، این ویژگی را بصورت فعال نگه دارید.

دستورات زیر جهت ذخیره امن IOS و فایل پیکربندی مورد استفاده قرار می گیرند:

```
Device(config)#secure boot-image
Device(config)#secure boot-config
```

- **امضاء دیجیتال**[1]

این ویژگی در روترهای سری 1900، 2900 ، 3900 و از نسخه 15.0(1)M به OSهای سیسکو اضافه گردیده است. ویژگی امضاء دیجیتال تسهیل کننده استفاده از OSهای قابل اطمینان سیسکو می‌باشد. سیسکو از رمزنگاری نامتقارن برای ایجاد امضاء دیجیتال استفاده می‌نماید.

- **رویداد نگاری و هشدار تغییرات در پیکربندی**

ویژگی رویداد نگاری و هشدار تغییرات را سیسکو از نسخه12.3(4)T به OSهای خود افزوده است. این ویژگی امکان رویداد نگاری اعمال تغییرات در پیکربندی را فراهم می‌آورد. در این فایل(log File) مشخصات کاربرانی که به سیستم وارد شده‌اند، دستوراتی که توسط هر یک از آنها به دستگاه اعمال گردیده و زمان انجام تغییرات، ذخیره می‌شود.

دستورات مورد استفاده برای این ویژگی به صورت زیر می‌باشد:

Configuring the Configuration Change Notification and Logging Feature		
	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**Configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**archive** **Example:** Router(config)# archive	Enters archive configuration mode.
Step 4	**log config** **Example:** Router(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	**logging enable** **Example:** Router(config-archive-log-config)# logging enable	Enables the logging of configuration changes. • Logging of configuration changes is disabled by default.
Step 6	**logging size** *entries* **Example:**	(Optional) Specifies the maximum number of entries retained in the configuration log.

[1] Digital Signature

Configuring the Configuration Change Notification and Logging Feature		
	Router(config-archive-log-config)# logging size 200	• Valid values for the *entries* argument range from 1 to 1000. The default value is 100 entries. • When the configuration log is full, the oldest entry is deleted every time a new entry is added. **Note** If a new log size is specified that is smaller than the current log size, the oldest log entries is immediately purged until the new log size is satisfied, regardless of the age of the log entries.
Step 7	**hidekeys** **Example:** Router(config-archive-log-config)# hidekeys	(Optional) Suppresses the display of password information in configuration log files. **Note** Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.
Step 8	**notify syslog** **Example:** Router(config-archive-log-config)# notify syslog	(Optional) Enables the sending of notifications of configuration changes to a remote syslog.
Step 9	**end** **Example:** Router(config-archive-log-config)# end	Exits to privileged EXEC mode.

سرویس AAA

سیسکو توسط سرویس AAA(Authentication, Authorization, Accounting)، اقدام به ارائه چارچوبی برای خدمات امنیت در جهت دسترسی به تجهیزات شبکه نموده است. این سرویس شامل احراز هویت، مشخص کردن حدود اختیارات و حسابداری می‌باشد که در مجموع به کنترل دسترسی منجر می‌گردد.

سرویس AAA خدمات زیر را بصورت ماژولار انجام می‌دهد:

- **احراز هویت (Authentication)**

این ماژول روش شناسایی کاربران، از جمله محاوره ورود به سیستم و درخواست کلمه عبور، بررسی و پاسخ، پشتیبانی از پیام و رمزنگاری بر اساس پروتکل امنیتی که شما مشخص نمودید، را فراهم می‌آورد.

- **مشخص کردن حدود اختیارات (Authorization)**

روش کنترل دسترسی راه دور از جمله مجوز یک بار مصرف[1] یا مجوز مخصوص هر سرویس، مشخصات[2] و فهرست حساب به ازاء هر کاربر، پشتیبانی از گروه‌های کاربری و پشتیبانی از پروتکل‌هایIP، IPX و Telnet، را فراهم می‌آورد.

پس از آنکه کاربر توسط سرویس Authentication، مورد شناسایی و احراز هویت قرار گرفت، سرویس Authorization مشخص می‌نماید که کاربر مورد نظر به چه منابعی امکان دسترسی خواهد داشت.

- **حسابداری (Accounting)**

ارائه دهنده روشی جهت جمع‌آوری و ارسال اطلاعات مورد استفاده برای صدور صورت حساب[3]، حسابرسی[4] و گزارش‌دهی، مثل هویت کاربر، زمان‌های شروع و توقف، اجرای دستورات، تعداد بسته‌ها و تعداد بایت‌ها، می‌باشد.

این سرویس شما را قادر به ردیابی کاربران در دسترسی به سرویس‌ها و همچنین مقدار استفاده آنها از منابع شبکه، می‌نماید.

دستورات مورد استفاده جهت راه اندازی اولیهAAA، بر روی تجهیزات بصورت زیر است:

Configuring Default Login Authentication Methods		
	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**Configure terminal** Example: Router# configure terminal	Enters global configuration mode.
Step 3	**aaa authentication login default** {**group** *group-list* [**none**]| **local** | **none**} **Example:** switch(config)# aaa authentication login default group radius	Configures the default authentication methods. The *group-list* argument consists of a space-delimited list of group names. The group names are the following: • **radius**—Uses the global pool of RADIUS servers for authentication. • ***named-group***—Uses a named subset of

[1] One-time authorization
[2] Profile
[3] Billing
[4] Auditing

Configuring Default Login Authentication Methods		
		TACACS+ or RADIUS servers for authentication. The **local** method uses the local database for authentication. The **none** method uses the username only. The default login method is **local**, which is used when no methods are configured or when all the configured methods fail to respond.
Step 4	**exit** Example: switch(config)# exit	Exits configuration mode.
Step 5	**show aaa authentication** Example: switch# show aaa authentication	(Optional) Displays the configuration of the console login authentication methods.
Step 6	**copy running-config startup-config** Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring AAA Accounting Default Methods		
	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**Configure terminal** Example: Router# configure terminal	Enters global configuration mode.
Step 3	**aaa accounting default {group** *group-list* **|local}** Example: switch(config)# aaa accounting default group radius	Configures the default accounting method. The *group-list* argument consists of a space-delimited list of group names. The group names are of the following: • **radius**—Uses the global pool of RADIUS servers for accounting. • *named-group*—Uses a named subset of TACACS+ or RADIUS servers for accounting. The **local** method uses the local database for accounting. The default method is **local,** which is used when no server groups are configured or when all the configured server groups fail to respond.

Configuring AAA Accounting Default Methods		
Step 4	**exit** Example: switch(config)# exit	Exits configuration mode.
Step 5	**show aaa accounting** Example: switch# show aaa accounting	(Optional) Displays the configuration AAA accounting default methods.
Step 6	**copy running-config startup-config** Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring AAA Authorization Using Named Method Lists		
	Command	**Purpose**
Step 1	Router(config)# **aaa authorization**{**auth-proxy** | **network** | **exec** |**commands** *level* | **reverse-access** |**configuration** | **ipmobile**} {**default** |*list-name*} [*method1* [*method2*...]]	Creates an authorization method list for a particular authorization type and enable authorization.
Step 2	Router(config)# **line** [**aux** | **console**| **tty** | **vty**] *line-number* [*ending-line-number*] or Router(config)# **interface** *interface-typeinterface-number*	Enters the line configuration mode for the lines to which you want to apply the authorization method list. Alternately, enters the interface configuration mode for the interfaces to which you want to apply the authorization method list.
Step 3	Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** |**reverse-access**} {**default** | *list-name*} or Router(config-line)# **ppp authorization** {**default** | *list-name*}	Applies the authorization list to a line or set of lines. Alternately, applies the authorization list to an interface or set of interfaces.

☑ مبحث دوم

امنیت سوئیچینگ

مبنای امنیت سوئیچینگ بر حصول اطمینان از در دسترس بودن عملیات سوئیچینگ لایه دو شبکه استوار می‌باشد. باید ضمن استفاده از پروتکل‌های مورد نیاز در لایه دو، تمهیدات امنیتی مربوط به آنها را نیز مدنظر قرار داد تا افراد مهاجم نتوانند از این پروتکل‌ها سوء استفاده نمایند. در ادامه به ذکر مراحل کلیدی تامین امنیت و حفظ زیرساخت‌های سوئیچینگ می‌پردازیم.

محدود کردن حوزه پخش همگانی

طبق تعریف سوئیچ‌هایLAN عهده‌دار ارسال فریم‌های ناشناخته، فریم‌های Multicast و Broadcast در بخش مشخصی از شبکه و ایجاد یک دامنه پخش می‌باشند. هرچند دامنه پخش همگانی تسهیل کننده ارتباط لایه دو بین سیستم‌های شبکه می‌باشد، ولی بزرگ شدن بی اندازه این دامنه می‌تواند باعث بوجود آمدن اشکالات بزرگی در شبکه گردد.

اولین ایرادی که در شبکه‌های بزرگ دارای دامنه پخش یکنواخت پیش می‌آید، راه افتادن سیل ناشناخته‌ای از فریم‌های Multicast و Broadcastای می‌باشد که ممکن است باعث کاهش کارآیی یا حتی منجر به شکست[1] کامل اتصال گردد. علاوه بر این، دامنه پخش همگانی تعریف کننده یک دامنه خرابی[2] نیز می‌باشد که به موجب آن بروز هر گونه خلل یا خرابی، تمام دستگاه‌های موجود در آن دامنه را تحت الشعاع خود قرار خواهد داد. بنابراین دامنه پخش همگانی بزرگتر احتمال بوجود آوردن یک شکست بزرگتر را افزایش می‌دهد.

بهترین شیوه برای جلوگیری از چالش‌های فوق، تقسیم شبکه‌های بزرگ به شبکه‌های کوچک‌تر دارای آدرسIP با زیر شبکه‌های مختلف و یا تبدیل آن بهVLANها با توجه به طراحی سلسله مراتبی می‌باشد.

همانطور که ان‌شاءاله به یاد مبارکتان مانده! در فصل‌های گذشته به طور مفصل درباره طراحی بر اساس مدل سلسله مراتبی و همچنین نحوه پیکربندیVLANها توضیح داده شده است.

---

[1] Break
[2] Failure Domain

امنیت پروتکل STP

پروتکلSTP یک پروتکل مدیریت لینک می‌باشد که برای جلوگیری از ایجاد حلقه لایه دوم در شبکه کاربرد دارد. هر چند کهSTP یک پروتکل ارزشمند در سوئیچینگ می‌باشد اما متاسفانه در این پروتکل حداقل‌های امنیتی رعایت نشده و در مقابل حملات بسیار آسیب پذیر می‌نمایاند. پروتکلSTP هیچ نوع رمزنگاری را برای محافظت از تبادل پیام‌هایBPDU در نظر نگرفته که این اشکال در کنار فقدان احراز هویت در این پروتکل، باعث گردیده افراد خرابکار به راحتی بتوانند با تزریق پیام‌های جعلیBPDU، تجهیزات را مجبور به محاسبه مجدد توپولوژی و حتی تغییر توپولوژی شبکه نموده و در نهایت باعث منع ارائه خدمات توسط تجهیزات شبکه و یا حملات مرد میانی[1] گردند. علاوه بر موارد فوق، به دلیل رمزنگاری نشدن پیام‌هایBPDU، فرد مهاجم با دستیابی به این پیام‌ها می تواند توپولوژی شبکه را به راحتی به دست آورد.

جدول زیر حملات و آسیب پذیری‌های پروتکلSTP به همراه ویژگی‌های ارائه شده توسط سیسکو برای جلوگیری از آنها را نمایش می‌دهد.

STP Attacks and Vulnerabilities	Attack Objectives and Risk	Possible Countermeasures
Illegitimate trunk		• Disable Dynamic Trunking
STP spans VLANs	Attack on one VLAN impacts all other VLANs	• Restrict STP domain using Per-VLAN Spanning Tree (PVST)
Unauthorized spanning tree participation Bogus BPDU packets Superior BPDUs sent to become root bridge	Network instability Attacker sees frames he should not Can be used for MITM, DoS, etc	• BPDU guard • Root Guard

با توجه به جدول فوق، برای اینکه این پروتکل ابزاری جهت سوء استفاده افراد خرابکار قرار نگیرد، طبق بهترین شیوه ارائه شده توسط سیسکو، باید موارد زیر را در جهت امن کردن پروتکلSTP رعایت نمائید:

- **غیرفعال سازی Dynamic Trunking**

همانطور که می‌دانید، سوئیچ‌های سیسکو بصورت پیش فرض از ویژگی Dynamic Trunking، جهت قرارگیری اتوماتیک پورت سوئیچ در حالت Trunk پشتیبانی می‌کنند. برای اینکه پورت Trunk مورد سوء استفاده قرار نگیرد، باید خاصیت فعال سازی

[1] Man-In-The-Middle (MITM)

اتوماتیک آن را بر روی پورت‌های سوئیچ (مخصوصا پورت‌های در نظر گرفته شده برای کاربر نهایی) غیر فعال گردد. برای انجام این کار می‌توان از دستورات زیر بهره برد:

```
Switch(config)#interface type slot/number
Switch(config-if)#switchport mode access
```

البته علاوه بر تامین امنیت STP، بطور کلی نیز پیشنهاد می‌گردد که عملTrunk کردن پورت‌ها بصورت دستی توسط مدیر شبکه و بر روی پورت‌های مورد نظر انجام گرفته و ویژگی Dynamic Trunking بر روی تمام پورت‌های سوئیچ همواره بصورت غیرفعال نگاه داشته شود.

- **استفاده از PVST**

در صورتی که سوئیچ مورد استفاده شما قابلیت پشتیبانی از پروتکلPVST را دارد، بهتر است از این پروتکل جهت راه اندازی STP در شبکه خود استفاده نمائید. در این حالت به ازاء هر VLAN یک پروسه STP در شبکه اجرا می‌شود و در صورت رخداد مشکل، فقط یک VLAN تحت تاثیر قرار گیرد.

بر روی تجهیزات سیسکو بصورت پیش فرض PVST در حالت فعال قرار دارد و بهتر است که شما نیز این پروتکل را همواره در حالت فعال نگه دارید. اما در هر حال از دستور زیر برای فعال سازی این پروتکل می‌توانید استفاده نمائید:

```
Switch(config)#spanning-tree mode rapid-pvst
```

- **ویژگی PortFast**

با استفاده از ویژگی PortFast می‌توان پورت‌های مورد نظر (مثل پورت‌هایی که به کاربران نهایی متصل است) را از شرکت در فرآیندSTP معاف نمود. در این صورت علاوه بر افزایش سرعتSTP، سرعت آماده به کار شدن پورت‌ها نیز افزایش یافته و بدون نیاز به طی مراحل اضافی در وضعیتForwarding قرار می‌گیرند. برای فعال سازیPortFast بر روی اینترفیس مورد نظر، می‌توان از دستور زیر استفاده نمود:

```
Switch(config-if)#spanning-tree portfast
```

البته توجه داشته باشید که فعال سازی ویژگیPortFast به معنی غیرفعال کردنSTP بر روی اینترفیس نبوده و همچنان ممکن است پیام هایBPDU از این نوع اینترفیس‌ها دریافت گردد، لذا برای تامین امنیت از ویژگیBPDU Guard استفاده می‌شود.

- **ویژگی BPDU Guard**

با توجه به اینکه پروتکلSTP هیچ نوع رمزنگاری را برای پیام‌هایBPDU در نظر نگرفته، سیسکو برای جبران این نقیصه اقدام به معرفی ویژگیBPDU Guard نموده است. این ویژگی باعث اعمال محدودیت جهت مشارکت در پروتکلSTP میگردد.

از آنجا که هیچ نیازی نیست پورت‌های متصل به کاربر نهایی در فرآیندSTP شرکت نمایند، لذا ویژگیBPDU Guard در صورتیکه از این نوع پورت‌ها پیام BPDU دریافت نماید اقدام به Shutdown نمودن آن پورت می‌نماید.

ویژگی BPDU Guard را می‌توان هم بصورت عمومی و هم بر روی یک اینترفیس خاص فعال نمود. فقط توجه داشته باشید در صورتی که دستور مورد نظر بصورت عمومی بر روی سوئیچ اجرا گردد فقط پورت‌هایی تحت تاثیر قرار می‌گیرند که در حالتPort Fast قرار داشته باشند.

برای فعال سازی عمومیBPDU Guard باید از دستور زیر استفاده نمائید:

```
Switch(config)#spanning-tree portfast bpduguard default
```

برای فعال سازیBPDU Guard بر روی یک اینترفیس خاص نیز می‌توانید مراحل زیر را انجام دهید:

```
Switch(config)#interface type slot/number
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
```

- **ویژگی STP Root Guard**

همانطور که گفته شد پروتکلSTP برای تبادل پیام‌های خود از هیچ پروتکل رمزنگاری و احراز هویتی استفاده نمی‌کند، لذا سیسکو با ارائه ویژگیRoot Guard، از پورت‌های Designated محافظت کرده و اجازه نمی‌دهد سوئیچ دیگری که به سایر پورت‌ها متصل است، خود را به عنوان سوئیچ ریشه معرفی نماید. به عبارت دیگر، Root Guard سایر تجهیزاتی که بخواهند خود را به عنوان سوئیچ ریشه معرفی نمایند را مسدود می‌نماید. این ویژگی باید بر روی پورت‌هایی فعال گردد که قرار نیست هیچگاه به سوئیچ ریشه متصل گردند، مثل پورت‌های متصل به کاربران نهایی.

برای فعال سازی این ویژگی باید دستورات زیر را بر روی اینترفیس مورد نظر اجرا نمود. فقط توجه داشته باشید که ویژگیPortFast باید بر روی اینترفیس فعال باشد:

```
Switch(config)# interface type slot/number
Switch(config-if)#spanning-tree guard root
```

- **غیرفعال سازی پورت های بلااستفاده**

نه تنها برای حفاظت ازSTP، بلکه بصورت یک حفاظت کلی پیشنهاد می‌گردد تمام پورت‌های بلااستفاده سوئیچ را توسط دستور Shutdown، غیرفعال کرده و در نهایت نیز آنها را در یک VALN غیر فعال قرار دهید.

- **Loop Guard**

وجود اتصالات یکطرفه (اتصالی که فقط از یک طرف در حالتBlock قرار داشته باشد) در شبکه می‌تواند باعث بوجود آمدن چرخه لایه دو گردد. ویژگی Loop Guard با تشخیص این نوع اتصالات از ایجاد چرخه لایه دو جلوگیری به عمل می‌آورد.

ویژگیLoop Guard اقدام به پیگیری فعالیت پورت‌های Nondesignated می‌کند. مادامی که پیام‌هایBPDU دریافت می‌شوند، پورت بطور معمول رفتار می‌نماید، اما زمانی که پیام هایBPDU مفقود[1] شوند، این ویژگی وضعیت پورت را به حالت Loop-Inconsistent (حلقه متناقض) تغییر داده و پورت را ضمن نگه داشتن در نقش Nondesignated، در آن نقطه مسدود می‌نماید. در صورت دریافت مجدد پیام‌های BPDU، پورت به حالت فعال باز خواهد گشت.

بصورت پیش فرض ویژگیLoop Guard در وضعیت غیر فعال قرار دارد، برای فعال کردن آن بصورت عمومی می‌توان از دستور زیر استفاده نمود:

```
Switch(config)#spanning-tree loopguard default
```

دستور زیر نیز برای فعال کردنLoop Guard بر روی یک اینترفیس خاص می‌باشد:

```
Switch(config-if)#spanning-tree guard loop
```

- **UDLD**

در صورتی که یک اتصال در لایه فیزیکی دچار مشکل شده و قطع گردد، سوئیچ‌های هر دو طرف وضعیت را تشخیص داده و لینک را بصورت Not-Connected نمایش می‌دهند. اما اگر لینک فقط در یک طرف Transmit یا Receive دچار مشکل شود (مثل قطع شدن یکی از Coreهای اتصال فیبر نوری)، به نظر شما چه اتفاقی روی خواهد داد؟ بله! درست حدس زدید، در اینصورت نیز وجود لینک یک طرفه باعث ایجاد حلقه لایه دو در شبکه می‌گردد.

سیسکو ویژگی UDLD(UniDirectional Link Detection) را جهت تشخیص این نوع لینک‌ها ارائه داده است. این ویژگی با ارسال متناوب (هر ۱۵ ثانیه) پیام‌های UDLD، به

[1] Missing

نظارت بر روی پورت‌ها پرداخته و اقدام به تشخیص اتصالات یک طرفه می‌نماید. پس از تشخیص این نوع اتصالات، UDLD به یکی از دو روش عملیاتی زیر رفتار می‌نماید:

i. **Normal Mode**

در این صورت به پورت مربوطه اجازه داده می‌شود همچنان به فعالیت خود ادامه دهد ولی این پورت توسطUDLD به عنوان اتصال یکسویه علامت گذاری شده و یک پیام Syslog نیز صادر می‌گردد.

ii. **Aggressive Mode**

در اینصورت سوئیچ سعی به برقراری مجدد اتصال می‌نماید. سپس در هشت ثانیه، هشت بار پیام UDLD را ارسال می‌کند. اگر سوئیچ جواب پیام خود را دریافت نکند، تشخیص می‌دهد که ارتباط همچنان بصورت یکسویه می‌باشد؛ لذا پورت را در وضعیت Errdisable قرار می‌دهد تا استفاده از این پورت امکانپذیر نباشد.

برای فعال سازی عمومیUDLD از دستور زیر استفاده می‌شود:

Switch(config)# **udld {enable | aggressive | message time** *seconds***}**

برای فعال سازیUDLD بر روی یک اینترفیس خاص، از این دستور استفاده می‌گردد:

Switch(config-if)# udld {enable | aggressive | disable}

- **راه اندازی Port Security**

به دلیل کاربرد وسیع ویژگی Port Security، تشریح این ویژگی در همین مبحث بصورت مستقل انجام می‌شود.

- **فعال سازی Traffic Storm Control**

کنترل طوفان ترافیک یک ویژگی مهم است که در همین مبحث بصورت اختصاصی به تشریح آن پرداخته خواهد شد.

بهترین شیوه‌های امنیتی VLAN

برای حفاظتVLANها در برابر حملاتی چون VLAN Hopping اجرای مراحل زیر توسط سیسکو پیشنهاد گردیده است:

- ترجیحا از VLAN 1 برای هیچ کاری استفاده نکنید.
- همیشه VLAN IDهای مجاز برای انتقال را توسط پورت‌های Trunk مشخص نمائید.

- ضمن غیرفعال کردن پورت‌های بلا استفاده، بهتر است آنها را در یک VLAN غیرفعال نیز قرار دهید.
- بر روی تمام پورت‌های متصل به کاربر نهایی، ویژگی Dynamic Trunking (DTP Protocol) را غیر فعال نگاه دارید.
- اینترفیس‌هایTrunk را بصورت دستی پیکربندی نمائید. به عبارت دیگر بر روی پورت‌های Trunk هم بهتر است از ویژگیDTP استفاده نکنید.
- حتی برای Native VLAN نیز از حالت Tagged استفاده نموده و تمام فریم‌های Untagged را حذف نمائید.
- وضعیت پیش فرض پورت‌های سوئیچ را به حالت غیرفعال تغییر دهید.

ویژگی Port Security

ویژگیPort Security فراهم آورنده امنیت مورد نیاز در برابر آسیب پذیری‌های متعددی است که از جمله آنها می‌توان به موارد زیر اشاره نمود:

i. برقراری امنیت در پروتکلSTP

ii. مقابله با حملات MAC Flooding.

این نوع حمله با ارسال سیل آسای آدرس‌های MAC، باعث سرریز شدن حافظه CAM Table سوئیچ گردیده و عملا سوئیچ را به یک هاب تبدیل می‌نماید. در اینصورت سوئیچ همانند هاب دیتای دریافتی را بر روی تمام پورت‌های خود ارسال می‌نماید. فرد خرابکار هم که به یکی از پورت‌های سوئیچ متصل است، تمام اطلاعات تبادل شده توسط سوئیچ را به راحتی دریافت می‌نماید.

iii. جلوگیری از دسترسی افراد غیر مجاز به پورت سوئیچ با کنترل دسترسی بر اساس آدرسMAC .

برای مقابله با موارد فوق، سیسکو اقدام به معرفی ویژگیPort Security نموده است. توسط این ویژگی می‌توان اقدام به تعیین آدرس‌هایMAC مورد اعتماد نمود و یا اینکه تعداد آدرس‌هایMAC که سوئیچ می‌تواند از یک پورت قبول نماید را مشخص کرد.

در سوئیچ‌های سیسکو می‌توان از طریق راه‌های زیر اقدام به مشخص نمودن Secure MAC Address نمود:

- مشخص نمودن دستی آدرس‌هایMAC مورد اطمینان. در اینصورت آدرس‌های مورد نظر در فایل پیکربندی سوئیچ ذخیره و نگهداری می‌شوند. پس از مشخص نمودن این آدرس‌ها فقط دستگاه‌هایی می‌توانند به پورت سوئیچ متصل شوند که آدرسMAC آنها در جدول مربوطه موجود باشد.
- یادگیری پویای آدرسMAC تجهیزاتی که هم اکنون به پورت‌های سوئیچ متصل هستند. در این حالت اطلاعات این جدول پس از راه اندازی مجدد سوئیچ از بین رفته و باید پروسه یادگیری آدرس‌هایMAC مجددا انجام پذیرد.
- حالت سوم استفاده از روش چسبنده یا Sticky می‌باشد. این روش می‌تواند از طریق هر دو روش Static و Dynamic اقدام به یادگیری آدرس‌هایMAC مربوطه نموده و آنها را در فایل پیکربندی سوئیچ ذخیره نماید. در این صورت هر چند که ممکن است آدرس‌ها بصورت پویا جمع آوری شده باشد، ولی به دلیل ذخیره شدن آنها در فایل پیکربندی، پس از راه اندازی مجدد از بین نرفته و نیازی به اجرای مجدد فرآیند جمع آوری آدرس‌ها نمی‌باشد.

شما باید اینترفیس‌های سوئیچ را طوری پیکربندی نمائید که واکنش مناسبی در برابر رخداد هر گونه تخلف امنیتی[1] از خود نشان دهد. منظور از تخلف امنیتی در Port Security، رخ دادن یکی از این شرایط می‌باشد: اول آنکه دستگاهی که آدرسMAC آن به عنوان دستگاه قابل اطمینان در جدول وجود ندارد، قصد اتصال به پورت سوئیچ را دارد. دوم اینکه، یک آدرسMAC که به عنوان آدرس قابل اطمینان در لیست قرار گرفته، بر روی دو پورت متفاوت سوئیچ در همانVLAN مشاهده گردد.

شما می‌توانید در زمان پیکربندی مشخص نمائید که در صورت رخ دادن یک تخلف امنیتی، کدام یک از چهار حالت زیر بر روی سوئیچ فعال گردد:

- **Protect**

هنگامی که تعداد آدرس‌هایMAC یک پورت به حد مجاز مشخص شده برسد، از آن پس بسته‌های دارای آدرسMAC مبدا ناشناخته توسط سوئیچ از بین می‌رود.
در این حالت هیچ پیامی جهت آگاه سازی مدیر شبکه، از سوئیچ صادر نمی‌گردد.

[1] Security Violations

- **Restrict**

هنگامی که تعداد آدرس‌هایMAC به حد مجاز مشخص شده برسد، از آن پس بسته‌های با آدرسMAC مبدا ناشناخته توسط سوئیچ از بین می‌رود.

در این حالت بر خلاف حالت Protect، سوئیچ از طریق SNMP Trap و Syslog، اقدام به آگاه سازی مدیر شبکه می‌نماید.

- **Shutdown**

در این حالت، در صورت رخداد تخلف امنیتی، پورت سوئیچ به حالت Error-disable وارد شده و بلافاصله Shutdown می‌گردد. چراغ LED پورت نیز خاموش می‌گردد.

- **Shutdown VLAN**

این حالت شبیه به حالت قبل بوده، با این تفاوت که حالت Error-disable و Shutdown به جای یک اینترفیس، بر روی یک VLAN اتفاق خواهد افتاد.

دستورات اجرای ویژگی Port Security به صورت زیر می‌باشد:

Enabling and Configuring Port Security		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**Interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 3	**switchport mode**{**access | trunk**}	Set the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.
Step 4	**switchport voice vlan** *vlan-id*	Enable voice VLAN on a port. *vlan-id*—Specify the VLAN to be used for voice traffic.
Step 5	**switchport port-security**	Enable port security on the interface.
Step 6	**switchport port-security**[**maximum***value* [**vlan**{*vlan-list* /{**access** /**voice**}}]]	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. (Optional) **vlan**—set a per-VLAN maximum value Enter one of these options after you enter the **vlan**keyword: • *vlan-list*—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified

Enabling and Configuring Port Security		
		VLANs, the per-VLAN maximum value is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.
Step 7	**switchport port-security [violation**{**protect | restrict | shutdown |shutdown vlan**}]	(Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these: • **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit. • **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. • **shutdown**—When a violation occurs, the interface is error disabled, the port LED turns off, and the violation counter increments. • **shutdown vlan**—Use to set the security violation mode per VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs. **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the**errdisable recovery cause psecure-violation**global configuration command. You can manually re-enable it by entering the **shutdown** and**no shutdown** interface configuration commands or by using the **clear errdisable interface vlan**privileged EXEC command.
Step 8	**switchport port-security**[**mac-address** *mac-address*[**vlan** {*vlan-id* | {**access/ voice**}}]	(Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned. **Note** If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to

Enabling and Configuring Port Security		
		the running configuration. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan**keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.
Step 9	**switchport port-security mac-address sticky**	(Optional) Enable sticky learning on the interface.
Step 10	**switchport port-securitymac-address sticky**[*mac-address* **|** **vlan** {*vlan-id* / {**access**/ **voice**}}]	(Optional) Enter a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration. **Note** If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan**keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show port-security**	Verify your entries.

Enabling and Configuring Port Security Aging		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.

Enabling and Configuring Port Security Aging		
Step 3	**switchport port-security aging**{**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	Enable or disable static aging for the secure port, or set the aging time or type. **Note** The switch does not support port security aging of sticky secure addresses. Enter **static** to enable aging for statically configured secure addresses on this port. For *time*, specify the aging time for this port. The valid range is from 0 to 1440 minutes. For **type**, select one of these keywords: • **absolute**—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time *(*minutes) specified lapses and are removed from the secure address list. • **inactivity**—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

کنترل طوفان ترافیک

ویژگیStorm Control از ایجاد اختلال در ترافیکLAN، توسط طوفان Unicast، Multicast یا Broadcast بوجود آمده از طریق یک اینترفیس فیزیکی، ممانعت به عمل می‌آورد. طوفانLAN زمانی رخ می‌دهد که سیل بسته‌هایLAN، ترافیک بیش از حدی ایجاد نموده و باعث کاهش کارآیی شبکه گردند. از جمله مشکلات بوجود آمده توسط طوفان ترافیک می‌توان از بروز خطا در پیاده سازی Protocol-Stack، اشتباهات پیکربندی شبکه و یا حمله منع خدمات، نام برد.

ویژگی کنترل طوفان (یا سرکوب[1] ترافیک)، بر روی بسته‌های عبوری از یک اینترفیس به سوئیچ نظارت کرده و مشخص می‌نماید که این بسته‌ها از نوع Unicast، Multicast و یا Broadcast هستند. سوئیچ نیز در بازه زمانی یک ثانیه اقدام به شمارش هر نوع از بسته‌های مشخص شده می‌نماید تا در صورتیکه تعداد بسته‌های مورد نظر از آستانه تعیین شده فراتر رود، اقدام به سرکوب آن ترافیک نماید.

کنترل طوفان با استفاده از یکی از روش‌های زیر اقدام به اندازه‌گیری فعالیت‌های ترافیکی می‌نماید:

[1] Suppression

- مشخص کردن درصد مورد نظر از کل پهنای باند یک پورت که می‌تواند برای ترافیک Unicast، Multicast و Broadcast مورد استفاده قرار گیرد.
- تعیین میزان[1] دریافت ترافیک بسته‌های Unicast، Multicast و Broadcast، بر اساس بسته بر ثانیه[2].
- تعیین میزان دریافت ترافیک بسته‌های Unicast، Multicast و Broadcast، بر اساس بیت بر ثانیه[3].
- تعیین میزان ترافیک بسته‌های کوچک بر اساس بسته بر ثانیه. این ویژگی به صورت عمومی فعال بوده و پیکربندی آستانه بسته‌های کوچک نیز به ازاء هر اینترفیس انجام می‌پذیرد.

در هر یک از روش‌های فوق، در صورتیکه ترافیک از آستانه مشخص شده فراتر رود ترافیک مسدود خواهد شد. این انسداد تا زمانی که مقدار ترافیک به پائین‌تر از آستانه مورد نظر برسد ادامه خواهد داشت و پس از آن مجددا تبادل ترافیک به حالت عادی باز خواهد گشت.

بصورت پیش فرض بر روی تجهیزات سیسکو کنترل طوفان در حالت غیرفعال قرار داشته و سطح سرکوب نیز بر روی 100% می‌باشد. در صورتی که بخواهید اقدام به پیکربندی این ویژگی نمائید باید از دستورات زیر بهره ببرید:

Configuring Storm Control and Threshold Levels		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**Interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 3	**storm-control**{**broadcast** | **multicast** | **unicast**} **level**{*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps*[*pps-low*]}	Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled. The keywords have these meanings: • For *level*, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00. • (Optional) For *level-low*, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when

[1] Rate
[2] Packet-per-Second
[3] Bit-per-Second

Configuring Storm Control and Threshold Levels		
		traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00. If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked. • For **bps** *bps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For *bps-low*, specify the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. • For **pps** *pps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For *pps-low*, specify the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to**10000000000.0. For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.
Step 4	**storm-control action**{**shutdown** |**trap**}	Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps. • Select the **shutdown** keyword to error-disable the port during a storm. • Select the **trap** keyword to generate an SNMP trap when a storm is detected.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show storm-control**[*interface-id*] [**broadcast** |**multicast** | **unicast**]	Verify the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, broadcast storm control settings are displayed.

لازم به ذکر است که فقط اینترفیس‌های فیزیکی از ویژگی کنترل طوفان ترافیک پشتیبانی می‌کنند. البته شما می‌توانید این ویژگی را بر روی EtherChannel نیز فعال نمائید که در این صورت، این ویژگی بر روی تمام پورتهای فیزیکی عضو گروهEtherChannel پخش می‌گردد.

ویژگی DHCP Snooping

برخی از هکرها حملات خود را با سوء استفاده از سرویسDHCP انجام می‌دهند. این حملات ممکن است با تزریق یک سرورDHCP جعلی به شبکه صورت گیرد؛ و یا اینکه هکر با ارسال پیام‌های جعلی درخواستIP از طریق یک کلاینت، باعث گردد رنج آدرس‌هایIP در نظر گرفته شده برای شبکه اشباع گردیده و سرور دیگر نتواند در جواب درخواست‌های مشروع کلاینت‌ها، آدرسIP به آنها اختصاص دهد.

ویژگی DHCP Snooping همانند یک فایروال بین سرورDHCP قابل اعتماد و کلاینت‌های غیرقابل اطمینان[1] در شبکه قرار گرفته و فعالیت‌های زیر را انجام می‌دهد:

- اعتبار سنجی پیام‌هایDHCP دریافت شده از منابع غیرقابل اطمینان و فیلتر پیام‌های غیر معتبر.
- محدود سازی میزان ترافیکDHCP از منابع قابل اعتماد و غیرقابل اعتماد.
- ایجاد و نگهداری پایگاه داده DHCP Snooping، شامل اطلاعاتی درباره کلاینت‌های غیرقابل اطمینان به همراه آدرس‌هایIP استیجاری[2] اختصاص داده شده به آنها.
- بهره‌گیری از پایگاه دادهDHCP Snooping برای اعتبار سنجی درخواست‌های بعدی کلاینت های غیرقابل اعتماد.

البته توجه داشته باشید ویژگی‌های امنیتی دیگر مثلDAI نیز برای انجام عملیات مربوط به خود، از اطلاعات موجود در پایگاه دادهDHCP Snooping استفاده می‌نمایند.

یکی از قابلیت‌هایی کهDHCP Snooping در اختیار مدیر شبکه قرار می‌دهد، قابلیت Option-82 Data Insertion می‌باشد. این قابلیت امکان استفاده چندین کلاینت از یک پورت سوئیچ را برای ارسال درخواست‌های دریافت آدرسIP فراهم می‌آورد، بطوریکه هر یک از کلاینت‌ها همچنان بصورت منحصر بفرد شناسایی می‌شوند. قابلیت Option-82 در شبکه‌های بزرگ کاربرد دارد.

بطور پیش فرض، ویژگیDHCP Snooping در حالت غیر فعال قرار دارد. اما شما می‌توانید آنرا بر اساس هرVLAN یا گروهی ازVLANها فعال نمائید. دستورات مورد استفاده برای فعال سازی ویژگی DHCP Snooping به همراه قابلیت Option-82 بصورت زیر می‌باشد:

---

[1] منظور از غیرقابل اطمینان کلاینت‌هایی هستند که به طور معمول به شبکه وصل می‌شوند و ممکن است فرد هکر نیز یکی از آنها باشد. پس توجه داشته باشید که غیرقابل اطمینان به منظور ناشناخته بوده و با غیرمجاز فرق می‌کند!

[2] Leased

Enabling DHCP Snooping and Option 82		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp snooping**	Enable DHCP snooping globally.
Step 3	**ip dhcp snooping vlan** *vlan-range*	Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Step 4	**ip dhcp snooping information option**	Enable the switch to insert and to remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.
Step 5	**ip dhcp snooping information option allow-untrusted**	(Optional) If the switch is an aggregation switch connected to an edge switch, enable the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default setting is disabled. **Note** Enter this command only on aggregation switches that are connected to trusted devices.
Step 6	**Interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 7	**ip dhcp snooping trust**	(Optional) Configure the interface as trusted or as untrusted. Use the **no** keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.
Step 8	**ip dhcp snooping limit rate** *rate*	(Optional) Configure the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured. **Note** We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN with DHCP snooping.
Step 9	**exit**	Return to global configuration mode.
Step 10	**ip dhcp snooping verify mac-address**	(Optional) Configure the switch to verify that the source MAC address in a DHCP packet received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.

IP Source Guard

ویژگی امنیتی IPSG جهت محدود سازی ترافیک مربوط به اینترفیس‌های لایه دو می‌باشد و عمل فیلتر ترافیک شبکه را بر اساس جدولIP Source Binding انجام می‌دهد. وقتی می‌توان از این ویژگی استفاده نمود که DHCP Snooping بر روی اینترفیس‌های غیرقابل اعتماد فعال گردیده باشد. با ادغام این دو ویژگی، سوئیچ تمام ترافیک دریافتی یک اینترفیس را بلوکه می‌کند مگر آنکه ترافیک از سویDHCP Snooping مجاز شناخته شده باشد.

جدول IP Source Binding، شامل آدرس‌های یاد گرفته شده از طریقDHCP Snooping و یا پیکربندی شده بصورت دستی(Static IP Source Binding) می‌باشد. هر ورودی این جدول شامل آدرسIP به همراه آدرسMAC اختصاص داده شده و شماره VLAN مربوطه می‌باشد. سوئیچ تنها زمانی از جدولIP Source Binding استفاده می‌نماید که ویژگیIP Source Guard بر روی آن فعال گردیده باشد.

ویژگی امنیتیIPSG فقط روی پورت‌های لایه دو پشتیبانی گردیده و هر دو نوع پورت Access و Trunk را شامل می‌گردد. پیکربندیIPSG را می‌توان بر اساس فیلتر آدرسIP مبدا و یا بر اساس فیلتر آدرس‌های IP و MAC مبدا انجام داد.

در ادامه حداقل دستورات مورد نیاز جهت راه اندازی این ویژگی آمده است:

Enabling IP Source Guard		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 3	**ip verify source** or **ip verify source port-security**	Enable IP source guard with source IP address filtering. Enable IP source guard with source IP and MAC address filtering. **Note** When you enable both IP source guard and Port Security by using the **ip verify source port-security** interface configuration command, there are two caveats: • The DHCP server must support option 82, or the client is not assigned an IP address. • The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.
Step 4	**exit**	Return to global configuration mode.
Step 5	**ip source binding** *mac-address* **vlan** *vlan-id ip-*	Add a static IP source binding. Enter this command for each static binding.

Enabling IP Source Guard		
	address **interface** *interface-id*	
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show ip verify source**[**interface** *interface-id*]	Verify the IP source guard configuration.
Step 8	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**inteface** *interface-id*] [**vlan** *vlan-id*]	Display the IP source bindings on the switch, on a specific VLAN, or on a specific interface.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

ویژگی DAI

پروتکلARP را که به خاطر دارید؟! پروتکلی است که کلاینت‌ها از آن برای پیدا کردن آدرس MAC متناظر با IP مورد نظر، استفاده می‌کنند. اما در صورتیکه از این پروتکل محافظت نگردد، می‌تواند توسط هکرها برای حمله به شبکه، مورد استفاده قرار گیرد.

از جمله موارد سوء استفاده از پروتکلARP می‌توان به حملات ARP Spoofing اشاره نمود. هکرها در این نوع حملات با جعل پیام‌هایARP، سیستم خود را بجای دستگاه قربانی معرفی می‌نمایند. در اینصورت تمام دیتای ارسال شده به دستگاه مورد نظر به سیستم فرد مهاجم تحویل داده می‌شود. حملهARP Spoofing می‌تواند یک میزبان، سوئیچ و یا روتر متصل شده به شبکه لایه دو را هدف قرار دهد.

ویژگی امنیتی DAI(Dynamic ARP Inspection) برای مقابله با تهدید فوق، اقدام به اعتبار سنجی بسته‌هایARP تبادل شده در شبکه می‌نماید. ویژگیDAI با رهگیری، ثبت وقایع و حذف بسته‌هایARP که شامل آدرس‌های IP-to-MAC نامعتبر هستند، از حملات مرد میانی(MITM) جلوگیری به عمل می‌آورد.

ویژگیDAI را می‌توان مبتنی بر سرورDHCP و یا غیر مبتنی بر سرورDHCP راه اندازی نمود. همچنین این ویژگی دارای پارامترهای متعددی برای پیکربندی می‌باشد. در ادامه حداقل دستورات مورد نیاز جهت راه اندازیDAI در شبکه مبتنی بر سرورDHCP آورده شده است.

Configuring Dynamic ARP Inspection in DHCP Environments		
	Command	**Purpose**
Step 1	**show cdp neighbors**	Verify the connection between the switches.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**ip arp inspection *vlan*** *vlan-range*	Enable dynamic ARP inspection on a per-VLAN basis. By default, dynamic ARP inspection is disabled on all VLANs. For *vlan-range*, specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.
Step 4	**Interface** *interface-id*	Specify the interface connected to the other switch, and enter interface configuration mode.
Step 5	**ip arp inspection trust**	Configure the connection between the switches as trusted. By default, all interfaces are untrusted.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show ip arp inspection interfaces** **show ip arp inspection vlan** *vlan-range*	Verify the dynamic ARP inspection configuration.
Step 8	**show ip dhcp snooping binding**	Verify the DHCP bindings.
Step 9	**show ip arp inspection statistics vlan** *vlan-range*	Check the dynamic ARP inspection statistics.

شبکه مجازی شخصی(PVLAN)

بصورت معمول کلاینت‌های موجود در یک شبکه فیزیکی یا منطقی امکان تبادل اطلاعات با یکدیگر را دارند. به عنوان مثال اگر یکی از کلاینت‌ها اقدام به ارسال یک پیامBroadcast نماید، تمام کلاینت‌هایی که در آن شبکه قرار دارند، این پیام را دریافت خواهند نمود.

ممکن است در برخی مواقع به دلایل امنیتی بخواهید بعضی از پورتهای حساس یک VLAN را بدون تغییر در آدرسIP و VLAN مربوطه، از سایر پورت‌های موجود در آن شبکه جداسازی نمائید. به عنوان مثال شما در شبکه دارای یک VLAN به عنوان Server Farm هستید و تمام سرورهای شبکه نیز در این VLAN قرار دارند. ممکن است بنا به دلایل امنیتی بخواهید بعضی از

این سرورها با هم در ارتباط نباشند ولی همچنان بتوانند از Gateway شبکه نیز استفاده کنند. در اینصورت می توان از PVLAN استفاده نمود.

شبکه مجازی شخصی (Private VLAN)، امکان جداسازی بین پورت‌های سوئیچ که در یک Broadcast Domain یکسان قرار دارند، را فراهم می‌آورد؛ بدون آنکه نیاز به ایجاد شبکه‌ای جدا با رنج آدرسIP متفاوت وجود داشته باشد. پورت‌هایPVLAN در یکی از سه حالت زیر پیکربندی می‌گردند:

- **Promiscuous**

یک پورت بی قاعده(Promiscuous) می‌تواند با تمام اینترفیس‌های Isolated و Community موجود در یک PVLAN ارتباط برقرار نماید.

- **Isolated**

پورت ایزوله، بصورت کاملا جدا شده از سایر پورت‌های لایه دو واقع در یک PVLAN قرار می‌گیرد. این نوع پورت از ترافیک ارسالی به سایر پورت‌ها جلوگیری به عمل آورده و در این حالت تنها پورتی که امکان تبادل دیتا با پورت ایزوله را دارد، پورتهای بی قاعده می‌باشند.

- **Community**

پورت‌های Community امکان برقراری ارتباط با پورت‌های هم نوع خود و همچنین با پورت‌های بی قاعده را دارند. این نوع پورت‌ها از سایر پورت‌های لایه دو موجود درPVLAN و پورت‌های Isolated کاملا جدا شده و امکان برقراری ارتباط بین این پورت‌ها وجود نخواهد داشت.

ویژگی PVLAN فقط در برخی از سوئیچ‌های سیسکو پشتیبانی می‌گردد و در سایر سوئیچ‌ها ممکن است به جایPVLAN، از ویژگی پورت حفاظت شده پشتیبانی گردد. لذا قبل از تصمیم‌گیری برای استفاده ازPVLAN یا پورت حفاظت شده، باید مدل تجهیزات موجود در شبکه و نسخه IOS آنها را مورد بررسی قرار دهید.

پورت حفاظت شده

برخی از برنامه‌های کاربردی نیاز دارند تا ترافیک مربوط به آنها در لایه دوم شبکه و بین پورت‌های همان سوئیچ قابل تبادل نباشد؛ بطوریکه ترافیک ایجاد شده یک همسایه قابل دیدن توسط همسایه‌های دیگر نباشد. در چنین محیطی استفاده از پورت‌های حفاظت شده می‌تواند

تضمین نماید که هیچ ترافیک Unicast، Multicast و Broadcastای بین این پورت‌های سوئیچ تبادل نخواهد گردید.

پورت‌های حفاظت شده دارای ویژگی‌های زیر می‌باشند:

- یک پورت حفاظت شده هیچ ترافیکی(Unicast, Broadcast, Multicast) را به هیچ پورت حفاظت شده دیگری ارسال نخواهد کرد. ترافیک دیتا نمی‌تواند در لایه دوم شبکه بین پورت‌های حفاظت شده تبادل گردد، مگر ترافیک کنترلی مثل بسته‌هایPIM که توسطCPU پردازش شده و برای نرم افزارها ارسال می‌گردد.
- تمام ترافیک عبوری بین پورت‌های حفاظت شده باید از طریق یک دستگاه لایه سه تبادل گردد.
- تبادل دیتا بین پورت‌های حفاظت شده با پورت‌های حفاظت نشده نیز بطور معمول انجام می‌پذیرد.

شما می‌توانید ویژگی پورت حفاظت شده را هم بر روی پورت‌های فیزیکی و هم بر روی EtherChannel پیکربندی نمائید. برای اجرای این ویژگی می‌توانید از دستورات زیر بهره ببرید:

Configuring a Protected Port		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 3	**switchport protected**	Configure the interface to be a protected port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces***interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

استاندارد IEEE 802.1X

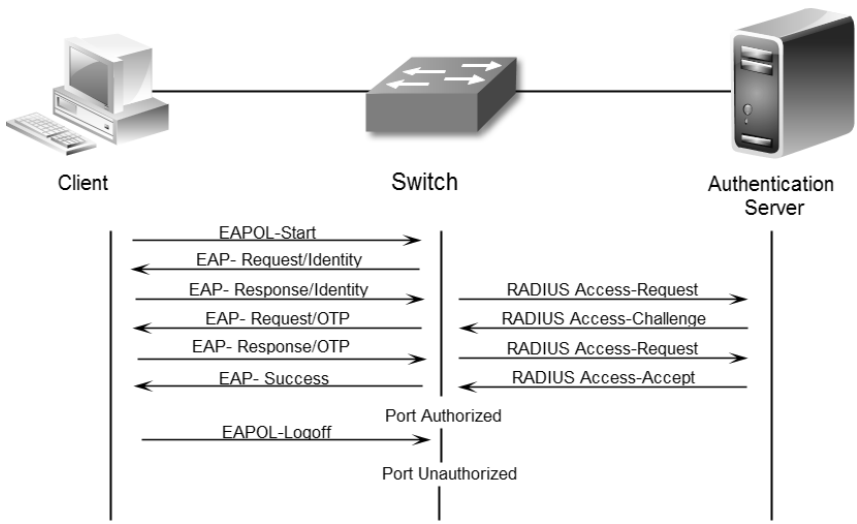
سازمان IEEE برای امنیت شبکه اقدام به معرفی استاندارد802.1X نموده است. این استاندارد احراز هویت کلاینت‌ها را جهت دسترسی به شبکه بر اساس هر پورت سوئیچ انجام می‌دهد.[1]

[1] Port-Base Authentication

استانداردIEEE 802.1X (به اختصار dot1x گفته می‌شود) کنترل دسترسی به شبکه را در سطح رسانه (Media Level) انجام داده و صدور اجازه یا رد دسترسی به شبکه را در همان سطح صادر می‌نماید. این استاندارد کنترل دسترسی و اعمال سیاست‌های ترافیکی را مبتنی بر هویت کاربر یا ماشین انجام می‌دهد.

در صورت فعال بودن dot1x، یک ماشین در زمان اتصال به پورت سوئیچ قبل از هر کاری مورد احراز هویت قرار می‌گیرد. پایگاه داده مربوط به احراز هویت نیز معمولا بر روی یک سرورAuthentication قرار گرفته که توسط پروتکل RADIUS[1] با سوئیچ در ارتباط می‌باشد. سوئیچ پس از تبادل اطلاعات کاربر مورد نظر با سرور، در نهایت اقدام به تصمیم گیری درباره صدور یا عدم صدور مجوز دسترسی به کلاینت می‌نماید.

قبل از اتمام پروسه احراز هویت، کلاینت‌ها تنها قادر به تبادل پیام‌های EAPOL[2] با سوئیچ هستند و پس از اتمام موفقیت آمیز پروسه Authentication، تبادل ترافیک بصورت عادی انجام خواهد پذیرفت. در غیر اینصورت سوئیچ اقدام به بلوکه کردن پورت مربوطه می‌نماید.



استانداردdot1x امکان پشتیبانی از دو نوع توپولوژی شبکه را دارد:

- **Point-to-Point**

در حالت Point-to-Point، از طریق یک پورت سوئیچ فقط یک کلاینت می‌تواند با احراز هویتdot1x به شبکه متصل گردد. سوئیچ وجود کلاینت جدید را با تغییر حالت

[1] Remote Authentication Dial In User Service
[2] Extensible Authentication Protocol Over LAN

پورت به Up تشخیص داده و اقدام به اجرای پروسه Authentication می‌نماید. در صورتیکه دستگاه متصل شده خاموش شود و یا اقدام به جابجایی نماید، سوئیچ حالت پورت خود را بهDown تغییر داده و مجددا در حالت Unauthorized قرار می‌گیرد.

- **Wireless**

در این حالت با توجه به اتصال بی سیم کلاینت‌ها به یک Access Point، امکان اتصال چند کلاینت از طریق یک پورت مهیا گردیده است. در اینصورت پس از احراز هویت یک کلاینت، پورت به حالت Authorized رفته و تمام کلاینت‌هایی که پس از آن بهAP متصل می‌شوند نیز بدون احراز هویت امکان دسترسی به شبکه را خواهند داشت.

برای جلوگیری از ایراد فوق باید از APای استفاده شود که قابلیت پشتیبانی از استاندارد dot1x را داشته باشد. به عبارت دیگر وظیفه Authentication کلاینت‌های بی سیم باید بر عهده AP گذارده شود.

استاندارد dot1x را بر اساس نیازهای شبکه می‌توان به روش‌های مختلف و با استفاده از سرورهای احراز هویت متفاوت راه اندازی نمود. به هر حال حداقل دستورات مورد نیاز برای فعال سازی این استاندارد بصورت زیر می‌باشد:

Enabling 802.1X Authentication		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication** dot1x {default}*method1* [*method2*...]	Create an 802.1X authentication method list. To create a default list that is used when a named list is*not* specified in the **authentication** command, use the**default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: • **group radius**—Use the list of all RADIUS servers for authentication. • **none**—Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client.
Step 4	**Interface** *interface-id*	Enter interface configuration mode, and specify the interface to be enabled for 802.1X authentication.
Step 5	**dot1x port-control auto**	Enable 802.1X authentication on the interface.
Step 6	**end**	Return to privileged EXEC mode.

Enabling 802.1X Authentication		
Step 7	**show dot1x**	Verify your entries. Check the Status column in the 802.1X Port Summary section of the display.

Configuring the Switch-to-RADIUS-Server Communication		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server host**{*hostname* |*ip-address*}**auth-port***port-number***key** *string*	Configure the RADIUS server parameters on the switch. For *hostname* | *ip-address,* specify the host name or IP address of the remote RADIUS server. For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1812. For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the**radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. If you want to use multiple RADIUS servers, re-enter this command.

☑ مبحث سوم

امنیت مسیریابی

امنیت مسیریابی شامل دو بخش اصلی می‌گردد. بخش اول مربوط به راهکارهای کنترل دسترسی کاربران بخش‌های مختلف جهت امکان تبادل دیتا با یکدیگر بوده و بخش دیگر نیز مربوط امن کردن پروتکل‌های مورد استفاده در مسیریابی می‌باشد.

Access Control List

یکی از مهمترین مباحث امنیتی لیست کنترل دسترسی یا Access Control List می‌باشد، که به اختصار ACL نامیده می‌شود. ACL دارای طیف کاربردی وسیعی است. از جمله موارد استفاده از ACL می‌توان به کنترل دسترسی جهت مدیریت تجهیزات شبکه، کنترل دسترسی کلاینت‌های شبکه‌های مختلف با یکدیگر، امن کردن سرورها، اعمال محدودیت استفاده از سرویس‌ها، فیلتر ترافیک و موارد دیگر اشاره نمود.

فارغ از اینکه از ACL در کجا و برای چه کاری استفاده می‌گردد، نحوه ایجاد آن بین تمام موارد مشترک است. لذا در این قسمت تمرکز اصلی بر روی آموزش نحوه ایجاد ACL می‌باشد.

انواع ACL

ACLها دارای انواع مختلفی هستند که توسط شماره یا نحوه تعریف در زمان نام گذاری مشخص می‌گردند. جدول زیر شامل لیستی از مرسوم ترین انواع ACL ها می‌باشد:

Protocol	Range
Standard IP	1–99 and 1300–1999
Extended IP	100–199 and 2000–2699
DECnet and extended DECnet	300–399
AppleTalk	600–699
Source-route bridging (protocol type)	200–299
Source-route bridging (vendor code)	700–799
Extended 48-bit MAC address	1100-1199
IPX Summary Address	1200-1299

همانطور که در جدول فوق ملاحظه می‌کنید ACL دارای انواع مختلفی است. اما به هر حال ما فقط به بررسی دو نوع مورد استفاده آن که در شبکه‌هایTCP/IP مورد استفاده قرار می‌گیرد، می‌پردازیم:

- **Standard Access List**

این نوع ACL که در رنج‌های 99-1 و 1999-1300 قرار دارد، فقط امکان Permit یا Deny نمودن جریان ترافیک مربوط به یک آدرسIP خاص را دارد. در این حالت شما نمی‌توانید بر اساس پورت یا آدرس مقصد اقدام به اعمال فیلترینگ نمائید.

- **Extended Access List**

این نوع ACL که در رنج‌های 199-100 و 2699-2000 قرار دارد، امکان Permit و Deny ترافیک را بر اساس آدرس مبدا، آدرس مقصد و پورت مورد نظر فراهم می‌آورد. همچنین Extended ACL ها مدیر شبکه را قادر می‌سازند تا فیلتر ترافیک را حتی بر اساس نوع پروتکل (مثل UDP، TCP و ICMP) اعمال نماید.

قوانین و نکات ACL

در هنگام ایجاد و استفاده از ACL باید قوانین و نکات زیر را مد نظر قرار دهید:

- تا قبل از تعریف و اختصاصACL، بصورت پیش فرض تمام ترافیک اجازه عبور دارند.
- صرف ایجاد ACL هیچ تاثیری بر روی ترافیک ورودی یا خروجی نداشته و حتما باید ACL به فرآیند مورد نظر اختصاص داده شود.
- روتر برای تطبیق بسته‌های اطلاعاتی با ACL، بررسی خطوط ACL را به ترتیب از بالا به پائین انجام داده و در صورت تطبیق با یک شرط همان را به بسته اعمال نموده و از بررسی سایر خطوط صرفنظر می‌نماید.
- بصورت پیش فرض در پایان لیستACL، تمام درخواست‌ها Deny می‌شوند. مثل اینکه شما شرط Deny any را به آخرACL اضافه کرده باشید. به عبارت دیگر اگر بسته مورد نظر با هیچ یک از شروط ACL تطابق نداشته باشد، در آخر فرض بر Deny گرفته می‌شود.

  توجه داشته باشید که در زمان مشاهدهACL، این پیش فرض (Deny any) نمایش داده نمی‌شود.
- در ACL به جای استفاده از Subnet Mask از Wildcard Mask برای مشخص کردن زیر شبکه استفاده می‌شود.

- باید شروط لیست ACL را از خاص[1] به عام[2] وارد نمایید. به عبارت دیگر باید در ابتدای ACL، شروط مد نظر برای میزبان‌های خاص و در انتها شروط مربوط به گروه‌ها و یا شروط عمومی را وارد نمائید.
- خطوط جدید همیشه به انتهای ACL اضافه می‌شوند. ترتیب قرار گرفتن خطوط ACL دقیقا وابسته به ترتیب وارد نمودن آنها می‌باشد و شما نمی توانید یک شرط جدید را به اواسط لیستACL اضافه نمائید.
- همیشه ابتدا ACL را بطور کامل ایجاد و سپس به فرآیند فیلترینگ، Route Map یا Redistribute مورد نظر اعمال نمائید.
- یک ACL در جواب فرستنده بسته‌هایی که Deny می شوند، پیام Host Unreachable فرستاده و سپس اقدام به دور ریختن بسته‌ها می‌نماید.
- ACL مربوط به فیلتر ترافیک باید نزدیک به مبدا ایجاد کننده آن ترافیک، اعمال گردد.
- بصورت معمول فیلترهای امنیتی در ورودی (Inbound) و فیلترهای ترافیک در خروجی (Outbound) اعمال می‌گردند.
- فیلترهای اعمال شده به Outbound هیچ تاثیری بر روی ترافیک ایجاد شده توسط روتر نخواهد داشت.
- اعمال و حذف ACL به اینترفیس‌ها را به دقت انجام دهید تا خللی در عملکرد روتر ایجاد نگردد.

نحوه ایجاد و اعمال ACL

مراحل نوشتن لیست کنترل دسترسی Standard و Extended و نحوه اعمال آن در ادامه آمده است:

Creating Standard ACL		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip access-list standard** *name*	Define a standard IP access list using a name or number, and enter access-list configuration mode. Note The name can be a number from 1 to 99.
Step 3	**deny** {source [source-wildcard] |**host** source | **any**} [**log**]	In access-list configuration mode, specify one or more conditions denied or permitted to determine

[1] Specific
[2] General

Creating Standard ACL		
	or **permit** {source [source-wildcard] |**host** source | **any**} [**log**]	if the packet is forwarded or dropped. • host *source*—A source and source wildcard of *source* 0.0.0.0. • any—A source and source wildcard of 0.0.0.0 255.255.255.255.
Step 4	end	Return to privileged EXEC mode.
Step 5	**show access-lists** [number | name]	Show the access list configuration.

Creating Extended ACL		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip access-list extended** name	Define an extended IP access list using a name and enter access-list configuration mode. **Note** The name can be a number from 100 to 199.
Step 3	{**deny | permit**} protocol {source [source-wildcard] | **host** source | **any**} {destination [destination-wildcard] | **host** destination |**any**} [**precedence** precedence] [**tos** tos] [**established**] [**log**] [**time-range** *time-range-name*]	In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations. • host *source*—A source and source wildcard of *source* 0.0.0.0. • host *destination*—A destination and destination wildcard of *destination* 0.0.0.0. • any—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.

Applying an IP ACL to a Terminal Line		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**line** [**console** |**vty**] *line-number*	Identify a specific line for configuration, and enter in-line configuration mode. • console—Enter to specify the console terminal line. The console port is DCE. • vty—Enter to specify a virtual terminal for

Applying an IP ACL to a Terminal Line		
		remote console access. The *line-number* is the first line number in a contiguous group that you want to configure when the line type is specified. The range is from 0 to 16.
Step 3	**access-class** access-list-number {**in** | **out**}	Restrict incoming or outgoing connections between a virtual terminal line (into a device) by using the conditions in the specified access list.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Display the access list configuration.

Applying an IP ACL to an Interface		
	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** interface-id	Identify a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL) or a Layer 3 interface (router ACL).
Step 3	**ip access-group** {access-list-number | name} {**in** | **out**}	Control access to the specified interface by using the IP access list. You can enter a standard or extended IP access number or name. Note The out keyword is not valid for Layer 2 interfaces. Port ACLs are supported only in the inbound direction.

Route-Maps

Route-Maps را می‌توان نوعیACL پیشرفته دانست که برای فیلتر کردن مسیرها و تغییر پارامترهای آنان در فرآیند توزیع مجدد (Redistribution) کاربرد دارد. دستور پیکربندی پویای پروتکل توزیع مجدد، به شما اجازه استفاده از هر دو ویژگی ACL یا Route-Map را می‌دهد. لذا شناسایی شباهت‌ها و تفاوت‌های ACL با Route-Map می تواند کمک قابل توجهی برای شما در زمان طراحی شبکه به شمار آید.

شباهت ACL با Route-Map

- هر دو دارای دستورات پی در پی هستند که هر کدام از آنها می‌تواند باعث Permit یا Deny دیتای مورد نظر گردد.

- در نحوه بررسی و تشخیص تطابق نیز عملکردی شبیه به یکدیگر دارند. پس از تطبیق با اولین شرط، همان را اعمال نموده و از بررسی سایر خطوط صرفنظر می‌کنند.
- هر دو دارای یک مکانیسم کلی هستند: تطابق معیارها[1] و تفسیر تطابق[2] بر اساس روش اعمال شده مشخص می‌شوند. به عبارت دیگر یک Route-Map یکسان اعمال شده به وظایف[3] مختلف ممکن است تفاسیر متفاوتی داشته باشد.

تفاوت ACL با Route-Map

- غالبا Route-Mapها از ACL جهت تطابق معیارها استفاده می‌نمایند.
- نتیجه اصلی بررسی یک ACL، رسیدن به جواب بلی یا خیر است که مشخص می‌نماید دیتای ورودی باید Permit یا Deny شود. و با اعمال ACL به فرآیند توزیع مجدد، می‌توان تعیین نمود که آیا مسیر مورد نظر امکان توزیع مجدد را دارد یا خیر.
  اما معمولاRoute-Map ها علاوه بر Permit و Deny مسیرها، اقدام به تغییر اطلاعات مربوط به مسیرها در زمان توزیع مجدد آنها در یک پروتکل دیگر نیز می‌نمایند.
- Route-Map انعطاف بیشتری نسبت به ACL داشته و می‌تواند اقدام به بررسی مسیرها بر اساس معیارهایی نماید که ACL قادر به انجام آنها نیست. به عنوان مثال یک Route-Map می‌تواند بررسی کند که آیا نوع مسیر داخلی است یا اینکه دارای علامت خاصی است؟
- بر اساس قرارداد در پایانACL همه چیز Deny خواهد شد. اما Route-Map قراردادی شبیه به ACL نداشته و اگر تلاش برای تطبیق تا انتهای Route-Map ادامه یابد، نتیجه به کاربرد خاص آن Route-Map بستگی خواهد داشت.
  اما خوشبختانه Route-Map در توزیع مجدد رفتاری شبیه به ACL دارد: اگر مسیری با هیچ شرطی از Route-Map تطابق پیدا نکند، توزیع مجدد نخواهد یافت؛ درست مثل اینکه Route-Map در پایان دارای Deny any می‌باشد.
- اعمال ACL به هر دو ترافیک ورودی و خروجی امکانپذیر است. اما Route-Map را فقط می‌توان بر روی ترافیک ورودی اعمال نمود.
- نحوه ایجاد ACL ساده تر از ایجاد Route-Map است.

---
[1] Criteria Matches
[2] Match Interpretation
[3] Tasks

- بر خلاف ACL، درRoute-Map امکان حذف یک شرط بدون تاثیر گذاری بر روی سایر شروط و همچنین امکان اضافه نمودن یک شرط جدید در بین شرط‌های موجود وجود دارد.

با توجه به شباهت‌ها و تفاوت‌های فوق، نهایتا می‌توان به این نتیجه رسید که اگر می‌خواهید اطلاعات مسیرها را در هنگام توزیع مجدد تغییر دهید و یا اینکه نیاز به توانایی‌های قویتری جهت تطبیق شروط مورد نظر دارید، بهتر است از Route-Map استفاده کنید. و بر عکس اگر شما فقط می‌خواهید اقدام به یک فیلترینگ ساده مسیرها بر اساس Prefix آدرس آنها نمائید، سیسکو پیشنهاد می‌کند که از ACL بهره ببرید.

دستورات Route-Map

هر شرط موجود در Route-Map می‌تواند توسط یکی از دستورات زیر تعریف گردد:

- **Match**

از این دستور جهت انتخاب مسیرهایی استفاده می‌شود که این شرط باید به آنها اعمال گردد.

- **Set**

برای تغییر اطلاعات مورد نظر در مسیرها قبل از انجام توزیع مجدد، از دستورSet استفاده می‌گردد.

در هر شرط دستورات Match و Set، ممکن است استفاده نشده و یا بر عکس، چندین بار مورد استفاده واقع شده باشند. با توجه به شرایط یکی از حالات زیر روی خواهد داد:

- اگر چند دستورMatch در یک شرط وجود داشته باشد، در صورتی آن شرط اعمال می‌شود که همه آنها با مسیر مورد نظر تطابق داشته باشند. به عبارت دیگر، از منطق AND برای بررسی دستورات Match پی در پی استفاده می‌گردد.
- اگر در یک دستور، یکMatch به چند شیء[1] اشاره داشته باشد، کافیست با یکی از آنها تطابق پیدا نماید تا شرط اعمال گردد. به عبارت دیگر در این حالت از منطق OR استفاده می‌شود.
- اگر هیچ دستورMatchای وجود نداشته باشد، تمام مسیرها با شرط تطابق پیدا خواهند نمود.

[1] Object

- اگر هیچ دستور Setای در شرط Permit یک Route-Map وجود نداشته باشد، توزیع مجدد مسیرها بدون هیچ تغییری در پارامترهایشان، انجام خواهد پذیرفت.

پیکربندی Route-Map بنا بر پروتکل‌های مسیریابی مختلف، می‌تواند شامل ویژگی‌های متفاوتی باشد. لذا برای استفاده از این ویژگی باید به مرجع دستورات در آن پروتکل خاص مراجعه نمائید.

ویژگی Passive Interface

بصورت پیش فرض تمام اینترفیس‌هایی که آدرسIP آنها در فرآیند مسیریابی پویا معرفی می‌شوند اقدام به ارسال و دریافت پیام‌های مسیریابی می‌نمایند. هر چند که این عمل برای درست انجام شدن فرآیند مسیریابی لازم است اما ممکن است بر روی بعضی از اینترفیس‌ها مخصوصا اینترفیس‌هایی که به شبکه‌های خارجی متصل هستند، این ویژگی منجر به یک ضعف امنیتی گردد.

اگر فرد خرابکار از طریق شبکه دیگری که با سازمان شما در ارتباط است قادر به دریافت پیام‌های مربوط به بروزرسانی پروتکل‌های مسیریابی پویا باشد، می‌تواند به راحتی توپولوژی و آدرس‌های شبکه مورد استفاده در سازمان شما را به دست آورد.

برای جلوگیری از این اتفاق می‌توان از ویژگی Passive Interface بهره برد. در صورتیکه این ویژگی بر روی یک اینترفیس فعال باشد، پیام‌های بروز رسانی مربوط به مسیریابی پویا از طریق آن اینترفیس دریافت و ارسال نخواهد شد.

برای پیکربندی ویژگی Passive Interface باید ابتدا به محیط پیکربندی پروتکل مسیریابی پویا وارد شده و سپس با استفاده از دستور زیر اقدام به معرفی اینترفیس مورد نظر نمائید:

Router(config-router)#**passive-interface** *interface-type interface-number*

ترجمه آدرس شبکه

به ویژگی ترجمه آدرس شبکه در بخش مسیریابی این کتاب بطور مفصل پرداخته شده است. ویژگی ترجمه آدرس شبکه یا NAT علاوه بر ترجمه آدرس‌های Private به آدرس‌های Public و برقراری امکان استفاده از اینترنت برای کاربران فاقد آدرس‌های عمومی، یک ویژگی امنیتی نیز محسوب می‌گردد.

ترجمه آدرس شبکه می‌تواند با تبدیل آدرس‌های مورد استفاده در داخل شبکه به یک سری آدرس IP خاص، از افشای آدرس‌های IP و زیر شبکه‌های مورد استفاده در سازمان شما جلوگیری به عمل آورد.

استاندارد RFC 2827

نوعی از حملات منع خدمت که توسط افراد خرابکار انجام می‌پذیرد، حمله بر اساس جعل آدرس IP مبدا می‌باشد. سازمان IETF برای جلوگیری از این نوع حملات و فیلترینگ نفوذ به شبکه اقدام به معرفی استاندارد RFC 2827 نموده است.

این استاندارد که معمولا در مرز شبکه با اینترنت اعمال می‌شود، جهت محافظت شبکه در برابر سیل حملاتی است که از آدرس IP جعلی استفاده می‌نمایند. لذا استاندارد برای جلوگیری از این نوع مخاطرات، به رعایت دو مورد زیر تاکید می‌نماید:

۱) جلوگیری از ورود بسته‌هایی که آدرس مبدا آنان در شبکه داخلی وجود دارد.

۲) جلوگیری از خروج بسته‌هایی که آدرس مبدا آنان در شبکه داخلی وجود ندارد.

سیسکو در جهت تکمیل فیلترینگ بسته‌های دارای آدرس IP مبدا جعلی، پیشنهاد می‌کند موارد زیر در مرز شبکه توسط ACLها یا فایروال اعمال گردد:

i. رعایت موارد گفته شده در RFC 2827.

ii. فیلتر آدرس‌های موجود در RFC 1918.

RFC 1918 شامل فضای آدرس‌های Private است که جهت استفاده در شبکه‌های خصوصی توسط سازمان IANA در نظر گرفته شده و قابلیت مسیریابی در اینترنت را نیز ندارند.

iii. فیلتر رنج آدرس‌های معرفی شده در RFC 3330.

RFC 3330 شامل آدرس‌هایی است که توسط سازمان IANA به موارد خاصی اختصاص داده شده و امکان مسیریابی در اینترنت را نیز ندارند.

منابع:

www.ieee.org
www.ietf.org
www.iana.org
www.iso.org
www.iec.ch
www.itu.int
www.icann.org
www.w3c.org
www.isoc.org
www.ansi.org
www.tiaonline.org
www.ecma-international.org
www.ibm.com
www.apple.com
www.xerox.com
www.novell.com
www.intel.com
www.cisco.com
www.ciscopress.com
www.protocols.com
www.microsoft.com
www.itil-officialsite.com
www.sri.com

Network

Zero to Hundred