آموزش مقدماتی شبکه

مقدمه

لایه های شبکه

سخت افزارهای شبکه

کابلهای شبکه

شبکه Ethernet

شبکه VPN

شبکهWireLess

عیب یابی شبکه ها

امنیت شبکه ها

معرفی نرم افزار شبکه

مدارک بین المللی شبکه

شبکه با WI-Max

مدرس: دکتر برادران

بخش اول
مفاهیم، تعاریف و کلیات شبکه های کامپیوتری

1-انواع شبکه

به طور مرسوم شبکه‌ها را براساس وسعت و توپولوژی دسته بندی می کنند.

(1-1انواع شبکه از جنبه وسعت

1-شبکه محلی یا Local Area Network, LAN

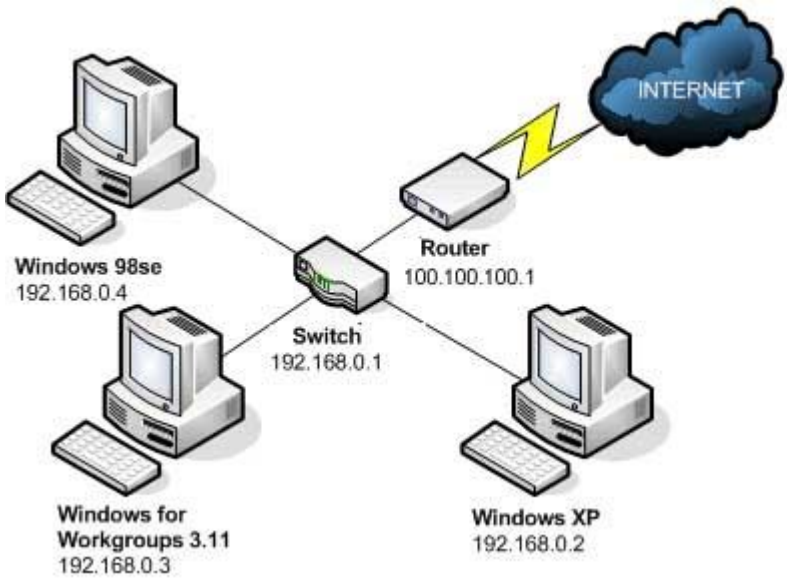
2-شبکه گسترده یاWide Area Network, WAN

شبکه محلی نوعی از شبکه است که از لحاظ محیط ، محدود میباشد. برای نمونه سایت آموزشی یک دانشگاه یک نمونه از شبکه محلی است. شبکه اترنت یا Ethernet یک نمونه آشنا از شبکه محلی است که در ادامه نصب و برپائی آن تشریح خواهد شد
در شبکه گسترده، کامپیوترهای موجود در این نوع شبکه محدود به منطقه خاصی نیستند. شبکه‌های بانکی که در کل کشور پراکنده اند یا اینترنت نمونه‌های آشنائی از شبکه گسترده می باشند.

.

(2-1انواع شبکه از جنبه توپولوژی

۱. شبکه خطی یا Bus
۲. شبکه ستاره‌ای یا Star
۳. شبکه حلقه‌ای یا Ring
۴. شبکه سرند یا Mesh



شکل ۱: توپولوژی مرسوم شبکه محلی

(1-2-1توپولوژی باس یاBus Topology

در این نوع از اتصال فیزیکی شبکه از کابلهای هم محور یا Coaxial استفاده میشود. کابلهای) coaxial همان سیم آنتن تلویزیون) که در شبکه باس بکار میرود دو نوع کلی دارد Thin : و Thick که نوع دوم دیگر استفاده نمیشود. برای اتصال این کابل به کارت شبکه از کانکتور های BNC و T connector استفاده میشود حداکثر طول کابل در شبکه Thin net برابر ۱۸۵ متر و در شبکه Thick net برابر ۵۰۰ متر است. در صورتی که طول کابل بیشتر از مقدار تعریف شده باشد، به علت مقاومت موجود در کابل، جریان ایجاد شده در آن رفته رفته ضعیف شده به گونه ای که کامپیوتر مقصد قادر به تشخیص جریان نخواهد بود که به این پدیده Attenuation میگویند. در این شبکه وقتی کامپیوتری شروع به ارسال Data میکند، جریان وارد کابل شده و در هر دو جهت پیش میرود تا به انتهای کابل برسد در این فاصله جریان به تمام کامپیوترها میرسد ولی تنها کامپیوتر مقصد از آن استفاده میکند. وقتی جریان به انتهای کابل برسد برگشت پیدا میکند (Bouncing) و با جریان داخل سیم تداخل پیدا میکند collision)رخ میدهد). برای جلوگیری از بروز چنین مشکلی در انتهای کابل از Terminator استفاده میکنیم که در واقع مقاومتی است که در Thin net معادل ۵۰ اهم و در Thick netبرابر ۷۵ اهم میباشد. حد اکثر تعداد کامپیوترها در شبکه Bus برابر ۳۰ عدد میباشد. مشکل اصلی این پیکربندی این است که اگر یک مشکل کوچک در یکی از کانکتورها، ترمیناتور یا کابل شبکه وجود بیاید کل شبکه بهم میریزد شبکه (done) میشود.

(2-2-1شبکه ستاره‌ای یاStar

در این نوع topology از یک وسیله مرکزی برای کابل کشی استفاده میشود که هاب یا تمرکز دهنده (concentrator) نامیده میشود در یک شبکه star هر یک از کامپیوترها توسط یک کابل مجزا به هاب وصل می شوند .اغلب LAN های ایترنتی امروزی از این topologyاستفاده می کنند. اولین مزیت star topology این است که به دلیل اینکه هر کامپیوتر با کابل جداگانه ای با هاب متصل میشود، اول اینکه تحمل خطا در چنین شبکه های بالاتر است و دیگر این که اگر یک کابل یا کانکتور دچار مشکل شود فقط ان سیستمی که با ان کابل یا کانکتور دچار مشکل بوده تحد تاثیر قرار میگیرد و دیگر اسیبی به کل شبکه نمیرساند ، بر خلاف .bus عیب این Topology در نیاز به سخت افزار اظافی یعنی هاب میباشد و اگر هاب دچار مشکل شود کل شبکه done میشود که البته چنین مشکلی به ندرت پیش می آید.

(3-2-1شبکه حلقه‌ای یاRing

در این نوع پیکربندی هر کامپیوتر منطقاً به کامپیوترهمسایه خود متصل است مانند شبکه‌های bus اما با این تفاوت که در این نوع شبکه بجای اینکه دو انتهای کابل شبکه بسته باشد به همدیگر متصل میشوند و یک حلقه را تشکیل میدهند به اینصورت که سیگنالی که از یک کامپیوتر تولید شده است بعد از گذر از تمام کامپیوترها دوبره به کامپیوتر تولید کننده بر می گردد و خودش ان را از شبکه حذف می کند. البته این پیکربندی حلقه یک ساختار منطقی است نه فیزیکی، به عبارت ساده تر حلقه در سیم کشی شبکه وجود دارد نه کابل کشی آن.

(4-2-1شبکه سرند یاMesh

در این نوع شبکه تمامی کامپیوترها با یکدیگر رابطه مستقیم دارند. توضیح بیشتر در مورد این شبکه‌ها از حوصله این جزوه آموزشی خارج است.

(2تجهیزات سخت افزاری شبکه

-1کارت شبکه
-2هاب یا سوئیچ (Hub or Switch)
-3کابل یا محیط انتقال

(2-1انواع کارت شبکه

برخی مهمترین مارکهای کارت شبکه عبارتند ازCompex - 3Com - Dlink - Acton - Acorp - Compack :
کارتهای شبکه از نظر سرعت ۱۰و ۱۰۰ یا ۱۰۰۰ مگابایت بر ثانیه (mg/s)هستند. اکنون همه مادربوردها دارای کارت شبکه onboard هستند و نیازی به خریداری کارت شبکه نیست.

(2-2هاب و سوئیچ

هاب گذرگاهی است که پایانه‌ها و سوکت‌های هر کامپیوتر عضو شبکه به آن وارد می‌شود و زمانی استفاده می‌شود که بیش از دو کامپیوتر را شبکه کنیم. سوئیچ نیز یک نوع هاب پیشرفته است.

(2-3انواع کابل شبکه

۱. کابل کواکسیال یا Coaxial
۲. کابل های زوجی یا هشت سیمی
۳. فیبر نوری

لازم به توضیح است در یک شبکه وایرلس رسانه انتقال هوا است و امواج در هوا پراکنده می شوند.

مقایسه لایه های مدل OSI و مدل TCP/IP

چکیده

مدل مرجع OSI و مدل مرجع TCP/IP نقاط مشترک زیادی دارند. هر دوی آنها مبتنی بر مجموعه‌ای از پروتکل های مستقل هستند، و عملکرد لایه‌ها نیز تا حدی شبیه یکدیگر است. مدل OSI ثابت کرده که بهترین ابزار برای توصیف شبکه‌های کامپیوتری است. اما پروتکل های TCP/IP در مقیاس وسیعی مورد استفاده قرار می‌گیرد. این دو مدل تفاوت هایی با هم دارند که در زیر به برخی از آنها اشاره می کنیم:

- در مدل TCP/IP تفاوت سرویس ها، واسط ها و پروتکل ها واضح و مشخص نمی‌باشد .
- پروتکلهای OSI بهتر از TCP/IP مخفی شده است.

- قبل از ایجاد مدل OSI پروتکلهای آن طراحی و ابداع شد. در نتیجه این مدل وابستگی و تعامل خاصی با هیچ مجموعه پروتکلی ندارد. اما در TCP/IP مسئله برعکس بود و این خود باعث شده که مدل TCP/IP تنها برای شبکه‌های تحت خود مناسب باشد.
- مدل OSI دارای هفت لایه است اما مدلTCP/IP ، چهار لایه دارد و از لایه ارائه و لایه نشست خبری نیست .
- لایه شبکه در مدل OSI اتصال گرا و غیر مستقیم است و لایه انتقال آن تنها اتصال گرا است اما در TCP/IP لایه شبکه الزاما غیر متصل و لایه انتقال آن اتصال گرا (TCP)یا غیر متصل (UDP)است.

مدل OSI

مدل OSI یا Open System Interconnectionیک مدل مرجع برای ارتباط بین دو کامپیوتر می باشد که در سال ۱۹۸۰ طراحی گردیده است. هر چند امروزه تغییراتی درآن به وجود آمده اما هنوز هم کاربردهای فراوانی در اینترنت و به خصوص در معماری پایه شبکه دارد. این مدل بر اساس لایه بندی قراردادهای برقراری ارتباط که همزمان روی دو سیستم مرتبط اجرا شده اند پایه ریزی شده است که این امر بسیار سرعت و دقت ارتباط را افزایش می دهد و این قراردادها بصورت طبقه طبقه در هفت لایه تنظیم شده اند که در زیر بررسی خواهند شد .

بررسی هفت لایه مدلOSI

لایه فیزیکی

این لایه که تنها تشکیل شده از سخت افزار می باشد و قراردادهای سخت افزاری در آن اجرا می شود وظیفه انتقال نهایی اطلاعات را دارد که این انتقال بصورت سیگنال و به صورت صفرو یک می باشد .

لایه پیوند داده ها

در این لایه اطلاعات، کشف خطا و اصلاح می شوند و بدون خطا و به صورت مطمئن به سوی مقصد ارسال می شوند.وظیفه دیگر این لایه مطمئن شدن از رسیدن اطلاعات به مقصد است که این کار توسط بیتهای (Parity check , checksum ,crc) انجام می پذیرد.که در صورت بروز خطا مجددا اطلاعات ارسال خواهند شد .

لایه شبکه

و اما پیچیده ترین لایه یعنی لایه شبکه که در آن قراردادهای شبکه بندی تعریف شده است. وظیفه این لایه انتقال تکنولوژی برقراری ارتباط برای دیگر شبکه های مستقل است که این امر این امکان را به osi می دهد که بتواند در زیر شبکه های مختلف فعالیت کند .

لایه انتقال

در این لایه قبل از ارسال اطلاعات یک بسته به سمت مقصد فرستاده می شود تا مقصد را برای دریافت اطلاعات آماده کند. همچنین این لایه وظیفه تکه تکه کردن بسته ها، شماره گذاری آنها و ترتیب و نظم دهی آنها را بر عهده دارد. که البته بسته ها در طرف گیرنده دوباره در همین لایه نظم دهی و قابل استفاده برای لایه های بالاتر خواهند شد .

لایه جلسه

در این لایه بر کارهایی از قبیل زمان ارسال و دریافت بسته ها مقدار رسیده و مقدار مانده از بسته ها نظارت می شود که به مدیریت بسته ها بسیار کمک می کند .

لایه ارائه

در این لایه استانداردهای رمز نگاری و فشرده سازی اطلاعات تعریف شده است که این لایه در امنیت بسیار مهم می باشد .

لایه کاربرد

استانداردهای ارتباط بین نرم افزارهای شبکه در این لایه قرار دارد که می توان از FTAM, CMIP, MHS VT :نام برد .

مدل TCP/IP یاInternet protocol /Transmission Control Protocol

مفهومTCP/IP

TCP/IPمجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها در شبکه مورد استفاده قرار می گیرند .وبه تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد. مدل چهار لایه TCP/IP از لایه های زیر تشکیل شده است .

لایه کاربرد

لایه انتقال

لایه شبکه

لایه واسطه شبکه

لایه فیزیکی

لایه واسط شبکه

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بزرگ این لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه

در این لایه پروتکل IP آدرس دهی و تنظیم می شود.(توضیحات در قسمت (IP و همچنین دیگر پروتکل ها مانند ARP,ICMP,BOOTPکه در این میان نقش هیچکدام به اندازه IP , ICMP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده می کنند.

لایه انتقال

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست .و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سرعت برای آنها مهم تر است.

لایه کاربرد

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد .در این لایه برنامه های کاربردی قرار دارند و در کل این لایه لایه ی نرم افزارهای شبکه می باشد و همچنین لایه پروتکل های نرم افزاری نیز می باشد .از مهم ترین نکات در خصوص این لایه قرارداشتن: انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد.

پروتکل اینترنت یاIP

حتما همه شما عزیزان واقف به این موضوع هستید که IP یکی از مهمترین قسمتهای TCP/IP و شاید بتوان گفت مهمترین قسمت آن زیرا تقریبا شما برای هر کاری نیاز به آن خواهید داشت لذا بسیار ضروری و حیاتی می باشد که شما اطلاعات خود را در زمینه این

مهم افزون کنید IP .یک آدرس عددی است که برای ارتباط با شبکه به هر ماشینی در شبکه اختصاص داده می شود (چون IP برای وسایلی از قبیل ROUTER و MODEM و LAN و ... استفاده می شود ما اصطلاحا به جای نام بردن تک تک آنها همه را ماشین می نامیم.(

وظیفه IP

وظیفه پروتکل IP حمل و تردد بسته های حاوی اطلاعات و همچنین مسیر یابی آنها از مبدا تا مقصد است IP .پس از دریافت اطلاعات از TCP شروع به قطعه قطعه کردن آن به قطعه های کوچک به اسم FRAGMENT می نماید، پس از این مرحله برای هر FRAGMENTیک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه می باشد و بسته IP را به بسته TCP اضافه می کند و شروع به ارسال بسته های تیکه تیکه شده (FRAGMENT)می نماید حال مسیر یابها بر اساس تنظیمات قسمت IP بسته ها را به مقصد خود هدایت می کنند و آن را داخل زیر شبکه ها هدایت می کنند.

خصوصیات IP

بسته IP حد اکثر ۶۴ کیلوبایت فضا را اشغال خواهد کرد و بیشتر از آن نمی تواند باشد ولی موضوع جالب اینجاست که در حالت عادی حجم بسته حدود ۱۶۰۰ بایت بیشتر نمی شود IP .در تمامی سیستم های عامل با ساختار استانداردی که دارد به درستی کار می کنند و نیاز به هیچ نوع سخت افزار ندارد .بسته IP ساخته شده از تعدادی فیلد مجزا می باشد که هر کدام اطلاعاتی را در خود دارند که در زمان مورد نیاز این اطلاعات از داخل بسته ها استخراج می شود و مورد استفاده قرار می گیرد این اطلاعات شامل مواردی مثل:آدرس IPفرستنده. آدرس IP گیرنده و ..... می باشد .

آدرس های ویژه IP

این آدرسها نمونه هائی از آدرس های IP خاص هستند که از قبل برای مقاصد خاصی در نظر گرفته شده اند و در تعریف شبکه نمی توان از آنها به عنوان IP برای ماشینها استفاده کرد. از این آدرس در مواردی استفاده می شود که ماشین میزبان از IP خود بی اطلاع است.البته اگر از این آدرس به عنوان آدرس فرستنده استفاده شود هیچ جوابی برای فرستنده پس فرستاده نمی شود.

HostId.0

ین آدرس برای زمانی است که از آدرس خود در زیرشبکه بی اطلاع باشیم

255.255.255.255

از این آدرس برای ارسال پیامهای به صورت عمومی و فراگیر در شبکه استفاده می شود البته با استفاده از این آدرس می توان در زیر شبکه خود پیام فراگیر ارسال کرد .

NetId.255

از این آدرس برای ارسال پیامهای فراگیر در دیگر شبکه ها از خارج از آنها استفاده می شود.البته این سرویس تقریبا در بیشتر اوقات از سوی مدیران شبکه غیر فعال می شود .

مقایسه مدلهای OSI وTCP/IP

شاید بزرگترین دستاورد مدل OSIروشن ساختن مفاهیم فوق (و تفکیک آنها) باشد.هر لایه سرویس هایی در اختیار لایه های بالاتر از خود قرار می دهد.تعریف این سرویس ها فقط می گوید که یک لایه چه کاری انجام می دهد، و هیچ حرفی در مورد نحوه انجام آنها و چگونگی استفاده از سرویس ها نمی زند .

تعریف چگونگی دسترسی به سرویس های یک لایه بر عهده واسط است.واسط پارامتر های ورودی لازم ، و نتیجه ای را که باید منتظر آن باشید، تعریف می کند.حتی واسط هم نمی گوید که یک لایه کار خود را چگونه انجام می دهد. و بالاخره، کاری را که یک لایه انجام می دهد را پروتکل های آن لایه تعریف می کنند.یک لایه مادامی که کار خود را درست انجام دهد، می تواند از هر پروتکلی استفاده کند.تغییر پروتکل های یک لایه هیچ تاثیری روی ارتباط آن با لایه های بالاتر نخواهد گذاشت.

ایده های فوق بسیار شبیه به مفاهیم مدرن برنامه نویسی شئ گرا هستند.هر شئ، مانند یک لایه، متدها (عملکردها) یی دارد که اشیا دیگر از آن استفاده می کنند.نحوه استفاده از این متدها در واقع همان سرویس هایی است که این شئ در اختیار دیگران می گذارد.ورودی ها و خروجی های شئ واسط آن با دنیای خارج هستند. کد اجرایی شئ نیز شبیه همان پروتکل است، که نحوه عملکرد آن از دید دیگران مخفی است.

در مدل اولیه TCP/IP تمایز بین سرویس ها، واسطها و پروتکل ها واضح و مشخص نبود، اگر چه افرادی (با توجه به تجربه موفق OSI (سعی کرده بودند آن را هر چه بیشتر شبیه OSI کنند.برای مثال لایه اینترنت فقط دو سرویس واقعی به نامهای SEND IP PACKETو RECEIVE IP PACKET داشت.با توجه به این وضع، پروتکل های OSI نهتر از TCP/IP مخفی شده اند، و امکان تغییر آنها به راحتی وجود دارد، چیزی که هدف غایی طراحی لایه ای محسوب می شود .مدل OSI قبل از اختراع پروتکل های آن طراحی و ابداع شد.این بدان معناست که مدل OSI وابستگی و تمایل خاصی به هیچ مجموعه پروتکلی ندارد، چیزی که در سایر مدل ها بسیار دیده می شود. البته این وضعیت یک نقطه ضعف نیز داردو آن این است که طراحان تجربه چندانی در زمینه موضوع کار ندارند، و واقعا نمی دانند کدام عملکرد را باید در کدام لایه قرار دهند.برای مثال ،لایه پیوند داده در ابتدا فقط برای شبکه های نقطه-به-نقطه طراحی شده بود، وقتی شبکه های بخشی وارد بازار شد، مجبور شدند یک زیر لایه به آن اضافه کنند .

وقتی که افراد شروع به طراحی شبکه با استفاده از مدل OSI و پروتکل های موجود کردند، به زودی دریافتند که این شبکه ها با سرویس های مورد نیاز انطباق ندارند.بنابر این مجبور شدند زیر لایه های زیادی به آن وصله پینه کنند.بالاخره، کمیته استاندارد مقرر کرد که هر کشور برای خود یک مدل منطبق با مدل) OSI تحت نظارت دولت) داشته باشد،شبکه ای که به هیچ عنوان آینده (اینترنت) در آن دیده نشده بود.خلاصه، کارها آنطوری که انتظار داشتند از آب در نیامد .در مورد TCP/IP وضع بر عکس بود:اول پروتکل ها اختراع و توسعه داده شدند، و سپس مدلی برای توصیف آنها ساخته شد.هیچ مشکلی در زمینه انطباق پروتکل ها با مدل وجود نداشت.همه چیز جفت و جور بود،تنها مشکل این بود که این مدل با هیچ مجموعه پروتکل دیگری جور در نمی آمد.

این بدان معنا بود که مدل TCP/IP به درد توصیف شبکه های غیر TCP/IP نمی خورد .جدای از مسایل فلسفی قضیه، تفاوت دیگر در تعداد لایه های این دو مدل است: مدل OSI هفت لایه دارد و مدل TCP/IP چهار لایه.لایه های شبکه، انتقال و کاربرد در هر دو مشترک اند، ولی لایه های دیگر فرق دارند. تفاوت دیگر در زمینه اطلاعات اتصال-گرا و غیر متصل است.مدل OSIاز هر دو نوع ارتباط اتصال-گرا و متصل در لایه شبکه پشتیبانی می کند، ولی در لایه انتقال فقط سرویس اتصال-گرا دارد (چون این سرویس در معرض دید کاربران است). مدل TCP/IP در لایه شبکه فقط سرویس غیر متصل دارد، ولی درلایه انتقال از هر دو نوع ارتباط پشتیبانی می کند، و دست کاربر را برای انتخاب باز می گذارد (که به ویژه برای پروتکل های ساده درخواست – پاسخ بسیار مهم است.(

نقد مدل OSI و پروتکل های آن

مدل OSI و) TCP/IP و پروتکل هایشان) هیچکدام کامل نیستند و جا دارد برخی از نقاط ضعف آنها را برشماریم.در این قسمت، برخی از نقاط ضعف مدل های OSI و TCP/IP را برسی خواهیم کرد.با مدل OSI شروع می کنیم. در سال ۱۹۸۹، بسیاری متخصصان برجسته شبکه بر این باور بودند که آینده در بست متعلق به مدل OSI و پروتکل های آن است، و هیچ چیز نمی تواند در مقابل پیشرفت آن مقاومت کند.اما این اتفاق نیفتاد.چرا؟ نگاهی به گذشته درسهای بسیاری را برای چشمان عبرت بین دارد،که می توان آنها را چنین خلاصه کرد .1 :زمان نا مناسب .2تکنولوژی نامناسب .3پیاده سازی نامناسب .4سیاست های نامناسب

زمان نامناسب

اولین عامل شکست مدل OSI زمان نامناسب بود.زمانی که یک استاندارد وضع می شود، اهمیت حیاتی در موفقیت و عدم موفقیت آن دارد.دیوید کلارک از دانشگاه M.I.T فرضیه ای در زمینه استانداردها دارد که ملاقات فیل ها معروف استد .این نظریه میزان فعالیت های حول یک موضوع جدید را نشان می دهد.وقتی موضوعی برای اولین بار کشف می شود، گرداگرد آن سیلی از فعالیت های تحقیقی (به شکل بحث، مقاله و سخنرانی) فرا می گیرد.بعد از مدتی این فروکش می کند و بعد از اینکه صنعت به این موضوع علاقه مند شد، موج سرمایه گذاری ها از پی می آید .بسیار مهم است که در محل تلاقی این دو فیل (موج تحقیق و موج سرمایه گذری) استانداردها به طور کامل وضع شوند.اگر استاندارد زودتر از موعد(قبل از پایان تحقیقات) نوشته شود، خطر آن هست که موضوع به درستی درک نشده باشد و استاندارد ضعیف از آب در آید.اگر استاندارد دیرتر از موعد(بعد از شروع موج سرمایه گذاری) نوشته شود، شرکتهای بسیاری قبلا –از مسیرهای مختلف- در آن سرمایه گذاری کرده اند،و این خطر هست که استانداردهای آنها را نادیده بگیرد. اگر فاصله این دو فیل خیلی کم باشد (همه عجله داشته باشند که کار را زودتر شروع کنند)، خطر آن هست که استاندارد نویسان بین آنها له شوند .اکنون

معلوم شده است که پروتکل های استاندارد OSI بین فیل ها له شده اند.وقتی که پروتکل های OSI پا به عرصه وجود گذاشتند، پروتکل های رقیب (TCP/IP) مدت ها بود که در مراکز تحقیقاتی و دانشگاه ها پذیرفته شده بودند.با اینکه هنوز موج سرمایه گذاری صنعتی در TCP/IP شروع نشده بود.اما بازار آکادمیک آنقدر بزرگ بود که شرکتهای بسیاری را تشویق به تولید محصولات TCP/IP کند.و وقتی OSI بالاخره از راه رسید،کسی نبود که داوطلبانه از آن پشتیبانی کند.همه منتظر بودند دیگری قدم اول را بر دارد.، قدمی که هرگز برداشته نشد دOSI در نطفه خفه شد .

تــکنولوژی نامناسب

دلیل دیگری که OSI هرگز پا نگرفت آن بود که، این مدل و پروتکل های آن هر دو ناقص و معیوب بودند.انتخاب هفت لایه برای این مدل بیشتر یک انتخاب سیاسی بود تا فنی، و در حالی که دو لایه آن (نشست و نمایش) تقریبا خالی بودند،در لایه های دیگر (لینک داده و شبکه) جای نفس کشیدن نبود .مدل) OSI و سرویس ها و پروتکل های آن) به طور باور نکردی پیچیده است.اگر کاغذهای چاپی این استاندارد را روی هم بچینید.ارتفاع آن از نیم متر هم بیشتر خواهد شد.پیاده سازی پروتکل های OSI بسیار دشوار، و عملکرد آنها ناقص است.در این رابطه، نقل جمله جالبی از پاول موکاپتریس (۱۹۹۳، (Roseخالی از لطف نیست :سوال: از ترکیب یک گانگستر با یک استاندارد بین المللی چه چیزی بدست می آید؟ جواب: کسی پیشنهادی به شما می کند که از آن سر در نمی آورید .مشکل دیگر مدل OSI ،علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکرد های آن (مانند آدرس دهی، کنترل جریان داده ها و کنترل خطا)در تمام لایه ها تکرار می شود.برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد،بنابراین تکرار آن در لایه های پائین تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد.

بخش دوم

معرفی سخت افزارهای شبکه

مقدمه

در اولین بخش به بررسی سخت افزار شبکه خواهیم پرداخت . این مباحث معمولآ در دوره network plus مورد بحث قرار می گیرد. این مقاله برای آشنا شدن افراد مبتدی و تازه کار با سخت افزار شبکه LAN مفید است.

تجهیزات سخت افزاری شبکه بسیار متنوع هستند. با این وجود به هنگام پیکربندی سخت افزاری شبکه های محلی اترنت و شبکه های بدون سیم در عمل با تعداد محدودی سخت افزار سرو کار خاهید داشت. این تجهیزات عبارتند از: کارت شبکه، هاب یا سوئیچ، کابلهای شبکه، روتر و اکسس پوینت. در این بخش توضیحات در مورد این سخت افزارهای ارائه شده است .

کارت شبکه

کارت شبکه، یکی از مهمترین عناصر سخت افزاری در زمان پیاده سازی یک شبکه کامپیوتری است .هر کامپیوتر موجود در شبکه، نیازمند استفاده از یک کارت شبکه است. کارت شبکه، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل ها ی مسی و یا فیبر نوری) را فراهم می نماید. اکثر مادربردهای جدیدی که از آنان در کامپیوترهای شخصی استفاده می گردد ، دارای کارت شبکه onboard می باشند.

کارت شبکه با پورتRJ-45

کارت شبکه PCMCIA بیسیم

کارت شبکه بی سیم

به کارت شبکه ، کارت اینترفیس شبکه و یا NIC مخفف Network Interface Cards نیز گفته می شود . وظیفه اصلی کارت شبکه ، اتصال فیزیکی یک کامپیوتر به شبکه است تا امکان مبادله اطلاعات برای وی فراهم گردد . هر کارت شبکه دارای یک آدرس فیزیکی (MAC) است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم، شماره سریال کارت شبکه است.

کارت شبکه می بایست با نوع محیط انتقال مطابقت و به نوعی با آن سازگار باشد . اترنت ، Token ringو Arcnet نمونه هائی از استانداردهای مختلف شبکه می باشند . شکل زیر یک نمونه کارت شبکه را نشان می دهد .

کابل شبکه

از کابل های شبکه تحت عنوان محیط انتقال نیز یاد می شود. اما به خاطر داشته باشید ممحیط انتقال فقط کابل نیست. امواج مختلف مانند امواج رادیوئی، microwaveو infrared نیز محیط انتقال محسوب می شوند.

در شبکه های اترنت پیشرفته ، از کابل های بهم تابیده موسوم به twisted pair با هشت رشته سیم استفاده می شود که با یک نظم خاص سازماندهی می گردند . از یک کانکتور RJ-45 در دو سر کابل استفاده می گردد . کانکتور RJ-45 نظیر کانکتورهای استفاده

شده در خطوط تلفن است با این تفاوت که اندازه آن بزرگتر می باشد .در خطوط تلفن از کانکتورهای RJ-11 استفاده می شود . شکل زیر یک کابل اترنت به همراه یک کانکتور RJ-45 را نشان می دهد .ادامه مطلب ...

کابل اترنت به همراه یک کانکتور RJ-45

هاب و سوئیچ

با استفاده از کابل کراس نمی توان شبکه ای با بیش از دو دستگاه کامپیوتر را ایجاد نمود . هاب یک قطعه سخت افزاری است که در شبکه های محلی استفاده می شود و هر یک از کامپیوترهای عضو شبکه با اتصال به هاب با سرور شبکه ارتباط برقرار می کنند. استفاده از هاب در متن مباحث شبکه ستاره ای قرار دارد که قبلا توضیح داده شد .

بیشتر هابهای مورد استفاده در شبکه های محلی یک جعبه به همراه تعدادی پورت RJ-45 هستند. هر کامپیوتر موجود در شبکه از طریق یک کابل اترنت به هاب متصل می شود . شکل زیر یک نمونه هاب را نشان می دهد . سوئیچ نوعی هاب پیشرفته است که اکنون جای هابهای قدیمی را گرفته است .

یک نمونه هاب

وظیفه اصلی هاب ارائه یک نقطه مرکزی برای اتصال تمامی کامپیوترهای موجود در شبکه است. هر کامپیوتر موجود در شبکه به هاب متصل می گردد . در صورت نیاز می توان چندین هاب را به یکدیگر متصل تا بتوان کامپیوترهای بیشتری را به شبکه متصل نمود .

در صورت اتصال بیش از دو دستگاه کامپیوتر به هاب ، چگونه و بر اساس چه مکانیزمی داده به مقصد مورد نظر خواهد رسید . رمز این کار در کارت شبکه است . هر کارت شبکه اترنت در کارخانه تولید کننده برنامه نویسی شده و یک آدرس) MAC برگرفته از (Media Access Controlمنحصربفرد در آن نوشته می گردد. زمانی که یک کامپیوتر موجود در یک شبکه اترنت که شامل چندین دستگاه متصل به هاب است ، اقدام به ارسال داده می نماید ، داده برای هر یک از کامپیوترها ارسال خواهد شد. کامپیوترهای دریافت کننده پس از دریافت داده ، آدرس مقصد آن را با آدرس MAC خود مقایسه می نمایند و در صورت مطابقت دو آدرس (آدرس ارسالی موجود در بسته اطلاعاتی با آدرس کامپیوتر دریافت کننده) ، مقصد داده مشخص خواهد شد و در صورتی که دو آدرس اشاره شده با یکدیگر مطابقت ننمایند ، کامپیوتر دریافت کننده از داده صرفنظر خواهد کرد .

همانگونه که اشاره گردید ، در مواردی که کامپیوترهای موجود در یک شبکه از طریق هاب به یکدیگر متصل می گردند ، هر بسته اطلاعاتی برای هر یک از کامپیوترهای موجود در شبکه ارسال خواهد شد . یکی از نکات قابل تامل در این سناریو ، ارسال فرازمانی داده توسط هر کامپیوتر است (در هر زمان دلخواه امکان ارسال داده وجود خواهد داشت). این وضعیت مشابه طرح سوال همزمان از طرف دو دانشجو در یک کلاس درس است که قصد استفاده از یک منبع مشترک (معلم) را دارند . وضعیتی اینچنین بدفعات در شبکه اتفاق می افتد .

زمانی که یک کامپیوتر قصد ارسال داده را داشته باشد ، در ابتدا بررسی می نماید که سایر کامپیوترها چنین قصدی را نداشته باشند و در صورت آزاد بودن محیط انتقال ، اقدام به ارسال داده مورد نظر می نماید . در صورتی که کامپیوتری دیگر سعی در مبادله اطلاعات و در زمان مشابه را داشته باشد ، بسته های اطلاعاتی حاوی داده در طول شبکه با یکدیگر برخورد و از بین خواهند رفت . به همین علت است که به این نوع شبکه ها یک collision domain نیز گفته می شود . در صورت بروز تصادم ، دو کامپیوتر مجبور خواهند بود که پس از یک مدت زمان کاملا" تصادفی ، مجددا" تلاش نمایند تا داده خراب شده را ارسال نمایند .

به موازات افزایش کامپیوترهای موجود در یک collision domain ، احتمال بروز تصادم نیز افزایش خواهد یافت . وضعیت فوق کارآئی شبکه را به شدت کاهش خواهد داد . به همین علت است که سوئیچ در شبکه مطرح و جایگزین هاب گردید .

شکل زیر یک نمونه سوئیچ را نشان می دهد.

یک نمونه سوئیچ

عملکرد سوئیچ ، همانند هاب است و تمامی کارهای مشابه یک هاب را انجام می دهد با این تفاوت که زمانی که یک کامپیوتر نیازمند مبادله داده با کامپیوتر دیگر باشد ، سوئیچ از مجموعه ای مدارات منطقی داخلی به منظور ایجاد یک مسیر منطقی و اختصاصی بین دو کامپیوتر استفاده می نماید . این بدان معنی است که دو کامپیوتر بدون نگرانی در خصوص بروز یک تصادم می توانند با یکدیگر داده مبادله نمایند .

استفاده از سوئیچ بطرز کاملا" محسوسی افزایش کارآئی شبکه را به دنبال خواهد شد و باعث حذف تصادم در یک شبکه می گردد .

ویژگی فوق تنها مزیت سوئیچ محسوب نمی گردد و علاوه بر آن می تواند مسیرهای مبادله داده موازی را ایجاد نمایند . به عنوان نمونه زمانی که کامپیوتر A با کامپیوتر B ارتباط برقرار می نماید ، دلیلی ندارد که کامپیوتر C نتواند با کامپیوتر D داده مبادله نماید . در یک collision domain این نوع مبادله داده موازی امکان پذیر نمی باشد.

روتر یا مسیریاب

از روتر جهت اتصال شبکه ها به یکدیگر استفاده می شود. بویژه برای ارتباط اینترنت در یک شبکه محلی از روتر استفاده می شود. کار روتر مسیر یابی برای بسته های اطلاعاتی در شبکه است. روتر کوتاه ترین مسیر را برای رساندن اطلاعات به مقصد انتخاب می کند. یک

روتر هم چنین می تواند دو شبکه مجزا که هر کدام node هایی برای خودشان دارند به هم وصل کند.
به عبارت دیگر برای انتقال و مسیر یابی اطلاعات در شبکه از دستگاهی مسیر یاب به نام روتر استفاده می گردد. برای مثال روی شبکه اینترنت امکان ارسال اطلاعات از مسیرهای زیادی وجود دارد و انتخاب بهینه ترین مسیر به عهده روتر است.وظیفه اصلی روتر آن است که دو زیر شبکه را به هم متصل کند که لزوما از نظر فیزیکی مستقیما به هم متصل نیستند. معمولا از اصطلاح سوییچ لایه نیز برای روتر استفاده می کنند اما سوییچ کردن اصطلاح غیر فنی و بازاری است.روتر با هاب تفاوت دارد. هرچند که هاب ها بین دوشبکه مختلف قرار می گیرند اما مسیریابی صورت نمی دهند و تنها بسته ها را از یک شبکه به شبکه دیگر می فرستند.

روتر های سخت افزاری

براساس مدل مرجع OSI روترها دستگاههای لایه سوم می باشند. مسیریاب ها شبکه هایی که دارای یک رنج آدرس شبکه (IP Address)نیستند را به هم متصل می کنند. مانند ارتباط کامپیوترهای یک شبکه به سرورهای اینترنت.
هر روتر حداقل دارای یک پورت LAN جهت اتصال به شبکه محلی و یک پورت WAN جهت اتصال به شبکه دور دست می باشد.
مسیریابها بهترین مسیر را برای فرستادن بسته ها به مقصد انتخاب می کند و چک می کند تا ببیند آیا بسته ها به مقصد رسیده اند یا نه. بر اساس مقصد داده ها، بسته ها از یک مسیر یاب دیگر از طریق بهترین راه فرستاده می شوند. این موضوع باعث می شود تا به عنوان یک وسیله ی قدرتمند در شبکه های پیچیده مثل اینترنت استفاده شود، در واقع می توان اینترنت را به عنوان شبکه ای از مسیر یاب ها توصیف کرد. انواع مسیر یاب ها با جداول و پروتکل های مختلفی کار می کنند اما حداقل این که هر مسیر یاب در اینترنت باید با پروتکل TCP/IP کار کند .

یک نمونه روتر

روتر های نرم افزاری

روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهندهNT ، یک سرویس دهنده نت ور و یا یک سرویس دهنده لینوکس باشد. تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند .

در اکثر موارد از روترها به عنوان فایروال و یا gateway اینترنت، استفاده می گردد. در این خصوص لازم است به یکی از مهمترین تفاوت های موجود بین روترهای نرم افزاری و سخت افزاری ، اشاره گردد: در اکثر موارد نمی توان یک روتر نرم افزاری را جایگزین یک روتر سخت افزاری نمود، چرا که روترهای سخت افزاری دارای سخت افزار لازم و از قبل تعبیه شده ای می باشند که به آنان امکان اتصال به یک لینک خاص) WAN از نوع Frame Relay ، ISDNو یا (ATM را خواهد داد. یک روتر نرم افزاری (نظیر سرویس دهنده ویندوز) دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه های WAN از طریق روترهای سخت افزاری ، انجام خواهد شد.

پرینت سرور

این دستگاه جهت به اشتراک گذاشتن پرینترهایی که دارای پورت و کارت شبکه نمی باشند استفاده می شود. این دستگاه، یک وسیله کوچک است که به عنوان یک Node به شبکه متصل می شود (یعنی آدرس IP می گیرد) و چاپگر و یا چاپگرها به آن وصل می شود.

Access Point

نقطه دسترسی یا AP به عنوان یک پل ارتباطی بین شبکه های کابلی و دستگاههای بدون کابل عمل می نماید . با استفاده از سخت افزار فوق ، امکان ارتباط چندین دستگاه به منظور دستیابی به شبکه فراهم می گردد access point. می تواند دارای عملکردی مشابه یک روتر نیز باشد . در چنین مواردی انتقال اطلاعات در محدوده وسیعتری انجام شده و داده از یک access point به access pointدیگر ارسال می گردد.

یک نمونه اکسس پوینت

دقت کنید مواردی مانند داکت، سوکت، محفظه های فلزی و از این دست نیز بعضاً به عنوان سخت افزارهای کامپیوتری معرفی می شوند که به زعم نویسنده صحیح نیست .

بخش سوم

کابلهای شبکه و آموزش کابل کشی

مقدمه

امروزه استفاده از شبکه های بدون کابل در ابعاد وسیعی گسترش یافته است ولی هنوز بیشتر سازمان ها و موسسات از سیستم های شبکه مبتنی بر کابل، استفاده می نمایند. با وجود تنوع زیاد در کابلها و روشهای کابل کشی در اینجا ساده ترین و موثرترین راهکارها برای کابل کشی یک شبکه به صورت علمی و عملی بیان می شود .

انواع کابل شبکه

۱. کابل های هم محور یا Coaxial
۲. کابل های زوجی یا هشت سیمی
۳. فیبر نوری

کابلهای کواکسیال

این کابلها همان کابل آنتن تلویزیون خانگی هستند و در شبکه باس استفاده می شوند .کابلهای کواکسیال که در شبکه باس بکار میرود به دو نوع کلی Thin و Thick تقسیم می‌شود که نوع دوم دیگر استفاده نمی شود.برای اتصال این کابل به کارت شبکه از کانکتور های BNCو T connector استفاده میشود.

کابل زوجی یا هشت سیمی

این کابل ها مرسوم ترین کابل در ایجاد شبکه های کامپیوتری مانند اترنت هستند .این نوع کابل در هفت دسته بندی یا category که به اختصار cat نیز گفته می شود وجود دارند. کابل های زوجی ممکن است بدون محافظ باشند و به آنها UTP گویند. کابلهای دارای شیلد یا STP نیز در مکانهائی مانند اسانسور یا کنار کابل های فشارقوی برق که نویز وجود دارد استفاده می شود.

کانکتور استاندارد برای کابل های UTP ، از نوع RJ-45می باشد. این کانکتور شباهت زیادی به کانکتورهای تلفن (RJ-11) دارد. واژه RJ نیز مخفف Registered Jack است.

کانکتور استاندارد برای کابل های کواکسیال، از نوع BNC یا Bayone Neill Concelman می باشد.

کابل های UTP: Unshielded Twisted Pair

کابل UTP یکی از متداولترین کابل های استفاده شده در شبکه های مخابراتی و کامپیوتری است . از کابل های فوق ، علاوه بر شبکه های کامپیوتری در سیستم های تلفن نیز استفاده می گردد .(CAT1) شش نوع کابل UTP متفاوت وجود داشته که می توان با توجه به نوع شبکه و اهداف مورد نظر از آنان استفاده نمود . کابلCAT5 ، متداولترین نوع کابل UTP محسوب می گردد.
با توجه به مشخصه های کابل های UTP ، امکان استفاده ، نصب و توسعه سریع و آسان آنان ، فراهم می آورد . جدول زیر انواع کابل های UTP را نشان می دهد:

گروه	سرعت انتقال اطلاعات	موارد استفاده
CAT1	حداکثر تا یک مگابیت در ثانیه	سیستم های قدیمی تلفن ، ISDN و مودم
CAT2	حداکثر تا چهار مگابیت در ثانیه	شبکه های Token Ring
CAT3	حداکثر تا ده مگابیت در ثانیه	شبکه های Token ring و BASE-T۱۰
CAT4	حداکثر تا شانزده مگابیت در ثانیه	شبکه های Token Ring
CAT5	حداکثر تا یکصد مگابیت در ثانیه	اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Token Ring (شانزده مگابیت در ثانیه)
CAT5e	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet
CAT6	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet

توضیحات :

- تقسیم بندی هر یک از گروه های فوق بر اساس نوع کابل مسی و Jack انجام شده است .
- از کابل های CAT1 ، به دلیل عدم حمایت ترافیک مناسب، در شبکه های کامپیوتری استفاده نمی گردد .
- از کابل های گروه CAT2, CAT3, CAT4, CAT5 و CAT6 در شبکه ها استفاده می گردد .کابل های فوق ، قادر به حمایت از ترافیک تلفن و شبکه های کامپیوتری می باشند .
- از کابل های CAT2 در شبکه های Token Ring استفاده شده و سرعتی بالغ بر ۴ مگابیت در ثانیه را ارائه می نمایند .
- برای شبکه هائی با سرعت بالا (یکصد مگا بیت در ثانیه) از کابل های CAT5 و برای سرعت ده مگابیت در ثانیه از کابل های CAT3 استفاده می گردد.
- در کابل های CAT4, CAT3 و CAT5 از چهار زوج کابل مسی استفاده شده است . CAT5 نسبت به CAT3 دارای تعداد بیشتری پیچش در هر اینچ می باشد . بنابراین این نوع از کابل ها سرعت و مسافت بیشتر ی را حمایت می نمایند .
- از کابل های CAT3 و CAT4 در شبکه هایToken Ring استفاده می گردد .
- حداکثر مسافت در کابل های CAT3 ، یکصد متر است .
- حداکثر مسافت در کابل های CAT4 ، دویست متر است .
- کابل CAT6 با هدف استفاده در شبکه های اترنت گیگابیت طراحی شده است . در این رابطه استانداردهائی نیز وجود دارد که امکان انتقال اطلاعات گیگابیت بر روی کابل های CAT5 را فراهم می نماید(CAT5e) .کابل های CAT6 مشابه کابل های CAT5 بوده ولی بین ۴ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار مگابیت در ثانیه را ارائه می نمایند.

کابل های کراس CAT5 UTP که از آنان با نام X-over نیز نام برده می شود ، یکی از متداولترین کابل های استفاده شده پس از کابل های Straight می باشند . با استفاده از کابل های فوق ، می توان دو کامپیوتر را بدون نیاز به یک هاب و یا سوئیچ به یکدیگر متصل نمود. با توجه به این که هاب عملیات X-over را به صورت داخلی انجام می دهد ، در زمانی که یک کامپیوتر را به یک هاب متصل می نمائیم ، صرفا" به یک کابل Straight نیاز می باشد . در صورتی که قصد اتصال دو کامپیوتر به یکدیگر را بدون استفاده از یک هاب داشته باشیم ، می بایست عملیات X-over را به صورت دستی انجام داد و کابل مختص آن را ایجاد نمود.

چرا به کابل های X-over نیاز داریم ؟

در زمان مبادله داده بین دو دستگاه (مثلا "کامپیوتر) ، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می نماید . تمامی عملیات ارسال داده از طریق کابل های شبکه انجام می شود .یک کابل شبکه از چندین رشته سیم دیگر تشکیل می گردد. از برخی رشته سیم ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می شود. برای ایجاد یک کابل-X overاز رویکرد فوق استفاده شده و (TXارسال) یک سمت به) RX دریافت (سمت دیگر، متصل می گردد . شکل زیر نحوه انجام این عملیات را نشان می دهد :

اتصال دو کامپیوتر به یکدیگر با استفاده از یک کابل X-over

کابل CAT5 X-over

به منظور ایجاد کابل های کراس CAT5 صرفا" از یک روش استفاده می گردد. همانگونه که قبلا" اشاره گردید ، یک کابل X-over پین TX یک سمت را به پین RX سمت دیگر متصل می نماید(و برعکس) . شکل زیر شماره پین های یک کابل CAT5 معمولی X-overرا نشان می دهد .

شماره پین های یک کابل CAT5 X-over .

همانگونه که در شکل فوق مشاهده می گردد در کابل های X-over صرفا" از پین های شماره یک ، دو ، سه و شش استفاده می گردد . پین های یک و دو بمنزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند . از پین های چهار ، پنج ، هفت و هشت استفاده نمی گردد . (صرفا" از چهار پین برای ایجاد یک کابل X-over ، استفاده می گردد) .

موارد استفاده از کابل های X-over

از کابل های X-over صرفا" به منظور اتصال دو کامپیوتر استفاده نمی شود و می توان از آنان در دستگاه های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود . در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نمائیم ، معمولا" از پورت uplink استفاده می گردد. پورت فوق ، بخش های tx و rx را کراس نمی نماید. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق پورت Uplink را نشان می دهد :

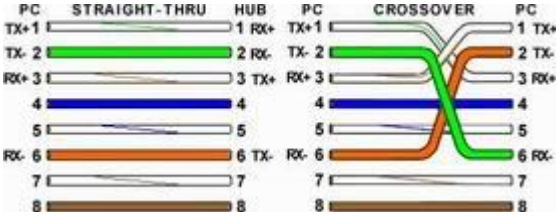
اتصال دو هاب با استفاده از پورت Uplink و یک کابل Straight

با توجه به وجود پورت uplink ، نیازی به استفاده از یک کابل x-over نخواهد بود . در صورتی که امکان استفاده از پورت uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از پورت های معمولی به یکدیگر متصل نمائیم ، می توان از یک کابل X-over استفاده نمود . شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل X-over را و بدون استفاده از پورت Uplink نشان می دهد :

اتصال دو هاب با استفاده از پورت معمولی و یک کابل X-over

شکل زیر تفاوت موجود بین شماره پین های یک کابل Straight و X-over را نشان می دهد :

تفاوت شماره پین های بین کابل Straight و X-over



کابل کشی شبکه : ایجاد کابل Straight

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت،ظرافت خاص و پایبندی به اصول کابل کشی ساختیافته ، انجام شود. برای ایجاد کابل های UTP از تجهیزات زیر استفاده می گردد :

تجهیزات مورد نیاز	
کابل UTP	کانکتورهای RJ-45
سیم لخت کن	آچار پرس RJ-45

یکی از عوامل تاثیر گذار در پشتیبانی و نگهداری یک شبکه ، نحوه کابل کشی آن است . با رعایت اصول کابل کشی ساختیافته ، در صورت بروز اشکال در شبکه ، تشخیص و اشکال زدائی آن با سرعتی مناسبی انجام خواهد شد .

مراحل ایجاد یک کابل : بدون هیچگونه توضیح اضافه !

مدل های متفاوت کابل کشی کابل های UTP

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت T-568Aو T-568B استفاده می گردد . نحوه عملکرد دو مدل فوق یکسان بوده و تنها تفاوت موجود به رنگ زوج هائی است که به یکدیگر متصل می شوند.در کابل های UTP از کانکتورهای استاندارد و چهار زوج سیم بهم تابیده استفاده می گردد :

- زوج اول : آبی و سفید/ آبی
- زوج دوم : نارنجی و سفید /نارنجی
- زوج سوم : سبز و سفید/ سبز
- زوج چهارم : قهوه ای و سفید / قهوه ای

در شبکه های ۱۰/۱۰۰ Mbit از زوج های دو و سه استفاده شده و زوج های یک و چهار رزو شده می باشند . در شبکه های گیگااترنت از تمامی چهار زوج استفاده می گردد. کابل های CAT5 متداولترین نوع کابل UTP بوده که دارای انعطاف مناسب بوده و نصب آنان بسادگی انجام می شود.

ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight)

اترنت عموما" با استفاده از هشت کابل هادی به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند . کانکتور استاندارد، RJ-45نامیده شده و مشابه کانکتور استاندارد RJ-11است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هائی خاص است . (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط . (به منظور تسهیل در امر نگهداری ، می بایست به اندازه ضروری سیم های بهم تابیده را از حالت پیچش خارج نمود (مثلا" حدود یک سانتیمتر) . زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند . از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود .
به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام) T-568Bیا (EIA و) T-568A یا AT&T ، (258A، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است .

شماره پین های استاندارد T568B

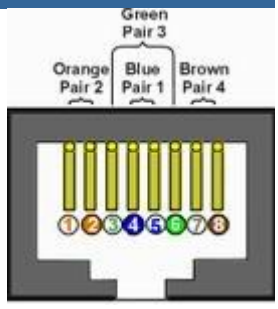
همانگونه که در جدول زیر مشاهده می گردد ، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند

.

کد رنگ ها در استاندارد T568B			
یک	سفید/ نارنجی	دوم	TxData
دو	نارنجی	دوم	-TxData
سه	سفید / سبز	سوم	RecvData
چهار	آبی	یک	
پنج	سفید /آبی	یک	

شش	سبز	سوم	RecvData-
هفت	سفید/قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

استاندارد T568B

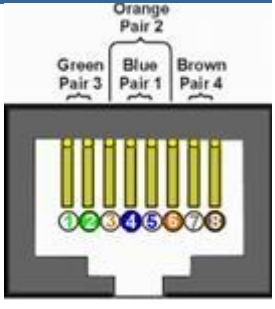


شماره پین های استاندارد T568A

در استاندارد T568A، اتصالات سبز و نارنجی برعکس شده است ، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند (سازگاری با اتصالات . (telco voice

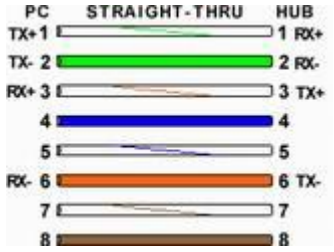
کد رنگ ها در استاندارد T568A			
یک	سفید/ سبز	سوم	RecvData
دو	سبز	سوم	RecvData-
سه	سفید / نارنجی	دوم	TxData
چهار	آبی	یک	
پنج	سفید /آبی	یک	
شش	نارنجی	دوم	TxData-
هفت	سفید/قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

استاندارد T568A



موارد استفاده

متداولترین کاربرد یک کابل straight ، اتصال بین یک کامپیوتر و هاب /سوئیچ است . در چنین مواردی ، کامپیوتر مستقیما" به هاب و یا سوئیچ متصل شده که به صورت اتوماتیک و با استفاده از مداراتی خاص، کابل cross overمی گردد.



شکل فوق یک اتصال استاندارد straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک PC به هاب استفاده می گردد . ممکن است با مشاهده شکل فوق انتظار داشته باشید که TXیک طرف به TX طرف دیگر متصل گردد(عملا "این اتفاق نیافتاده است) . زمانی که یک PC به هاب متصل می گردد ، هاب به صورت اتوماتیک و با استفاده از مدارات داخلی خود کابل را X-overنموده و بدین ترتیب ، پین شماره یک از کامپیوتر (TX) به پین شمار یک هاب (RX) متصل می گردد .
در صورتی که هاب عملیات x-over را انجام ندهد (در زمان استفاده از پورت (Uplink ، پین شماره یک کامپیوتر (TX) به پین شماره یک هاب (TX) متصل می گردد . بنابراین مهم نیست که چه نوع عملیاتی را با پورت HUB انجام می دهیم Uplink)و یا نرمال (، سیگنال های نسبت داده شده به هشت پین سمت PC ، همواره یکسان باقی مانده و هاب با توجه به نوع استفاده از پورت (نرمال و یا (Uplink عملیات لازم را انجام خواهد داد.

بخش چهارم

پیاده سازی و پشتیبانی شبکه اترنت

مقدمه

شبکه های اترنت شکل مرسوم شبکه های مورد استفاده در سایتهای دانشگاهی، ادارات و کافی نت ها است. پیاده سازی و پیکربندی این شبکه ها در زیر ارائه شده است. آرش حبیبی

تاریخچه

اترنت در سال ۱۹۷۰ توسط شرکت زیراکس و در مرکز تحقیقات Palo Alto در کالیفرنیا پیاده سازی گردید . در سال 1979شرکت های DEC و اینتل با پیوستن به زیراکس، سیستم اترنت را برای استفاده عموم ، استاندارد نمودند . اولین مشخصه استاندارد در سال

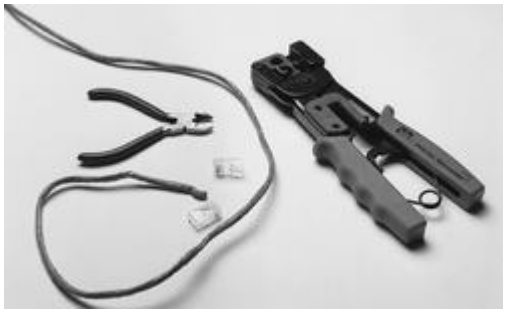
1980توسط سه شرکت فوق و با نام Ethernet Blue Book ارائه گردید . (استاندارد. (DIX
اترنت یک سیستم ده مگابیت در ثانیه است (ده میلیون صفر و یا یک در ثانیه (که از یک کابل کواکسیال بزرگ به عنوان ستون فقرات و کابل های کواکسیال کوتاه در فواصل ۵ / ۲ متر به منظور ایستگاههای کاری استفاده می نماید . کابل کواکسیالی که به عنوان ستون فقرات استفاده می گردد ، Thick Ethernetو یا ۱۰ 5Baseeنامیده می شود که در آن 10به سرعت انتقال اطلاعات در شبکه اشاره داشته (۱۰ مگابیت در ثانیه (و واژه Base نشاندهنده سیستم Base band است . در سیستم فوق ، از تمامی پهنای باند به منظور انتقال اطلاعات استفاده می گردد . در Broad band به منظور استفاده همزمان ، پهنای باند به کانال های متعددی تقسیم می گردد . عدد ۵ نیز شکل خلاصه شده ای برای نشان دادن حداکثر طول کابلی است که می توان استفاده نمود (در این مورد خاص 500 متر . (
موسسه IEEE در سال ۱۹۸۳ نسخه رسمی استاندارد اترنت را با نام IEEE 802.3 و در سال ۱۹۸۵ ، نسخه شماره دو را با نام IEEE 802.3aارائه نمود . این نسخه با نام Thin Ethernet و یا ۱۰ 2Baseمعروف گردید. (حداکثر طول کابل ۱۸۵ متر می باشد و عدد 2نشاندهنده این موضوع است که طول کابل می تواند تا مرز ۲۰۰ متر نیز برسد(
از سال ۱۹۸۳ تاکنون ، استانداردهای متفاوتی ارائه شده است که یکی از اهداف مهم آنان ، تامین پهنای باند مناسب به منظور انتقال اطلاعات است . ما امروزه شاهد رسیدن به مرز گیگابیت در شبکه های کامپیوتری می باشیم.

پیکربندی شبکه اترنت

پیکربندی شبکه اترنت در دو مرحله ارائه می شود. پیکربندی سخت افزاری و پیکربندی نرم افزاری.

پیکربندی سخت افزاری

تجهیزات مورد نیاز در این مرحله عبارتند از: هاب یا سوئیچ، کابل Cat5 به مقدار مورد نیاز، سوکت و آچار شبکه. در گذشته نیاز به تهیه کارت شبکه نیز بود که امروزه دیگر به صورت Onboard روی شبکه ها موجود است.



اگر بیش از دو کامپیوتر را شبکه می‌کنید ابتدا سیم‌های زوجی را لخت کنید. هشت رشته سیم رنگی را به صورت دوبه‌دو زوج کنید و با آچار سوکت بزنید. برای اینکار هیچ گونه قانونی جهت رنگهای زوج شده سیمها وجود ندارد. تنها هر گونه ترتیب رنگی را که در یک سوکت اعمال کردید در کل شبکه استفاده کنید. به این الگو، کابل کشی Patch گویند. مراحل سوکت زنی در شکل زیر ترسیم شده است.

بعد از این مرحله یک سر کابل Patch را به پورت شبکه کامپیوتر و سر دیگر را وارد هاب کنید. اگر عملیات سخت افزاری درست انجام شده باشد یک هاب سبز می‌شود.

پیکربندی نرم افزاری

در این مقاله مبانی لازم جهت پیکربندی نرم افزاری براساس سیستم عامل ویندوز XP ارائه شده است. انجتم عملیات پیکربندی نرم افزاری در ویندوز ویستا و نسخه ۷ نیز بسیار مسابه است.

در این مرحه هر کامپیوتر باید یک نام منحصر به فرد و یک آدرس IP منحصر به فرد داشته باشد. بعلاوه همه کامپیوترها باید عضو گروه واحدی باشند. برای دریافت فایل آموزشی مروبط به پیکربندی نرم افزاری از لینک زیر کمک بگیرید.

جهت تخصیص آدرس IP منحصر به فرد به هر کامپیوتر از طریق کنترل پنل وارد network connection شوید. روی آیکون Local area connectionکلیک راست کرده و وارد Properties شوید. در کادر ظاهر شده روی گزینه Internet protocol کلیک کرده و دکمه properties را بزنید تا کادر جدیدی باز شود. در این کادر برای IP از بازه ای مانند ۱۹۲.۱۶۸.۰.۱ استفاده کنید. تنظیمات دیگری در این کادر لازم نیست .

اشتراک گذاری یا Sharing

بعد از این مرحل به سادگی می توانید اقدام به Share کردن پوشه ها، درایوها و یا پرینتر خود نمائید. مطالب مربوط به share کردن را در سایر بخش های آموزش شبکه دنبال کنید.

عیب یابی شبکه های اترنت

مقدمه

پیکربندی و برپائی شبکه های اترنت کاری تقریباً ساده است که پیشتر نحوه آن توضیح داده شد) ادامه مطلب .(...با پیکربندی یک شبکه کار آن شبکه به پایان نرسیده است. پشتیبانی و رفع عیب شبکه گام مهم دیگری است که متخصص شبکه باید با آن آشنا باشد. دقت کنید مسائل مربوط به امنیت شبکه هم در زمان برپائی و هم در زمان پشتیبانی باید با آن آشنا باشید.

موضوع عیب یابی که شامل تشخیص و تعیین نوع مشکل و رفع آن می شود نیز از مباحث مهم نگهداری شبکه ها به شمار می رود. منشأ این عیب می تواند نرم افزاری، سخت افزاری، عدم تطابق تجهیزات، ناهماهنگی بین اجزا، تنظیمات نادرست و ... باشد. افراد دست اندرکار رفع مشکلا ت شبکه در تمامی موارد، الزاماً نباید مدارک علمی چندان سطح بالا یی داشته باشند. چون در این میدان تجربه و کارآزمودگی حرف اول را می زند و معمولاً داشتن اطلا عات اولیه و زیربنایی از شبکه ها کافی به نظر می رسد. عیب یابی یک شبکه بسیار شبیه حل معما است. اگر یک ایده کلی در مورد نحوه عملکرد شبکه به دست آورده اید و می دانید کدام بخش ها به یکدیگر وابسته هستند.چنانچه در هنگام راه اندازی شبکه به مشکلاتی برخورده اید، رهنمودهای زیر برای تست سریع شبکه راه گشا خواهد بود؛ بسیاری از این مشکلات به سادگی برطرف می شوند. اما به شرط آن که قبلا با راه حل ها آشنا شده باشید .در این بخش عیب یابی شبکه های کامپیوتری توضیح داده می شود. به خاطر داشته باشید به عنوان یک تکنیسین شبکه داشتن ابزارهائی مانند Link Runnerشناسائی و رفع عیب شبکه ساده تر خواهد شد .

-1اتصال پذیری

شاید بدیهی به نظر برسد،اما در قدم اول باید مشخص شود که آیا همه کامپیوترها، سرویس دهنده ها، چاپگرها و دیگر دستگاه های متصل به شبکه می توانند با یکدیگر ارتباط برقرار کنند یا خیر. برای این منظور، در شبکه ی باسیم، باید مطمئن شد که میان هر دستگاه و هاب یا سوییچ مرکزی یک کابل ارتباطی مطمئنی وجود دارد که به ترتیب درستی متصل شده باشند، چرا که وجود دو نوع کابل شبکه مختلف و اتصال نادرست آنها مشکل ساز می شود. اکثر کابل های مدرن) UTP جفت های تابیده بی حفاظ) اتصال دهنده هایی دارند که در هر دو انتها به یکدیگر متصل می شوند. در خود این اتصال دهنده ها، چندین سیم مجزا هست که ممکن است به همان پین های اتصالی در همان انتها وصل شوند یا به صورت ضربدری اتصال یابند. کابل های مستقیم، یک کامپیوتر شخصی، سرویس دهنده یا دیگر وسایل شبکه را به هاب یا سویچ متصل می کنند. کابل های ضربدری، اتصال دو کامپیوتر شخصی به یکدیگر را ممکن می سازند و در اتصال سریالی یک هاب یا سو ییچ به هاب یا سوییچ دیگر کاربرد دارند .استفاده غلط از کابل ها(که غالباً هیچ علامتی هم ندارند) باعث می شود سیگنال ها به مقصد نرسد. اگر به ترتیب رنگ های اتصال یک کابل اطمینان ندارید، ساده ترین راه وصل کردن کابل مذکور و سپس بررسی LED اتصال در آداپتور یا انتهای سوییچ است. اکثر کابل ها یک) LED دیود نوری) کوچک سبز رنگ دارند که در صورت برقراری اتصال قبل از روشن شدن دستگاه، روشن می شود. در بعضی کابل ها این دیود نوری به دو رنگ زرد یا نارنجی در می آید تا اتصال ۱۰۰ مگابایت در ثانیه یا گیگابایت باشد (در بعضی دیگر، چراغ های راهنمای ۱۰۰ مگابایتی جداگانه ای وجود دارد.) اما اگر هیچ نوری به چشم نخورد، مطمئناً کابل نادرستی را به کار برده اید. در این صورت چاره ی کار تعویض کابل است، هر چند در برخی از سوییچ ها، دگمه هایی در کنار پورت های خاص معمولا با علامت Uplink وجود دارد که امکان استفاده از یک کابل مستقیم برای برقراری اتصال با هاب یا سوییچ دیگر را فراهم می کند. برخی از جدیدترین سوییچ ها می توانند به طور خودکار کابل های مورد استفاده را بررسی کنند و از داخل ترتیب رنگ های پورت را به شکلی مناسب تغییر دهند.

-2چشمک زدن LED

در برخی از موارد ممکن است LED اتصال به عوض آنکه دائماً روشن باشد، چشمک بزند. حالت اخیر به این معناست که فعالیت هایی در این خط ارتباطی انجام شده اما در نصب پورت ناسازگاری هایی وجود داشته است. مثلاً فرض کنید که آداپتور کامپیوتر شخصی روی ۱۰۰ مگابایت در ثانیه و پورت سوییچ روی ۱۰ مگابایت در ثانیه تنظیم شده باشد. خوشبختانه در حال حاضر تقریباً تمامی وسیله ها، به منظور اجتناب و عدم سازگاری سرعت در دو طرف، از تشخیص خودکار (auto Sensing) سرعت پورت و نصب دو طرفه پشتیبانی می کنند. با این حال در هنگام استفاده از وسایل کارخانه های مختلف به مشکلاتی برخورده ایم که تنها با تنظیم دستی پارامترهای فوق بر طرف می شود.

-3اتصال های بی سیم

بررسی اتصالات بی سیم اندکی سخت تر است، چونکه برقراری اتصال، نشانه ی مشخصی ندارد. با این حال، در کنار اکثر آداپتورهای بی سیم، نرم افزارهایی به بازار عرضه شده که برقراری اتصال را به شما اعلام می کند و فارغ از فروشنده مربوطه با تسهیلات مشابهی در ویندوز XP عرضه می شود. برای عیب یابی اتصالات بی سیم، در وهله نخست مطمئن شوید که کلیه گزینه های امنیتی یا رمز گذا، غیر فعال شده اند. سپس اطمینان یابید که آداپتور روی حالت صحیح تنظیم شده باشد. اکثر آداپتورها یک حالت ad hoc برای اتصال دو وسیله همانند دارند و برای کاربرد در یک access point به پیکر بندی جداگانه ای مجهز هستند. مطمئن شوید که در سراسر شبکه از یک کانال و SSID واحد ID) مجموعه سرویس دهنده که Lan بی سیم را شناسایی می کند) استفاده می شود.

4-پیکر بندی IP

بعد از اینکه ثابت کردید وسایل شما به لحاظ فیزیکی به یکدیگر متصل هستند،در قدم بعد مطمئن شوید که آنها می توانند با یکدیگر ارتباط برقرار کنند. در اکثر شبکه هایی که با TCP/IP کار می کنند، برای برقراری ارتباط باید نشانی IP یگانه ای به تک تک وسیله ها اختصاص یابد. نشانی ها را می توان به صورت دستی پیکر بندی نمود، اما بهتر آن است که از پروتکل پیکربندی دینامیک میزبان (DHCP)استفاده شود که در آن یک سرویس دهنده DHCP ، نشانی های IP را از محل یک مخزن تعیین شده، توزیع می کند. به این ترتیب هیچ وقت دو یا چند سیستم، نشانی های یکسانی نخواهند داشت. بیشتر مسیریاب ها و پل های ارتباطی، یک سرویس دهنده DHCPداخلی دارند. همچنین می توان سرویس دهنده ویندوز را طوری پیکر بندی نمود که این عملیات را انجام دهد و پس از پیکربندی نیاز به کاردیگری نداشته باشد. باتمام این حرف ها ممکن است اشتباهاتی رخ دهد. هنگامی که مشکلی پیش آمد در ابتدای کار عیب یابی، مطمئن شوید که نشانی های درستی به کار رفته است. تمامی کارهای فوق را می توان با استفاده از برنامه خدماتی ipconfigموجود در ویندوز و از طریق یک پنجره فرمان در کامپیوتر شخصی یا سرویس دهنده آزمایش نمود. در هر پنجره فرمان، ipconfigرا تایپ کنید تا نشانی IP اختصاص یافته به هر رابط شبکه را ببینید. با اضافه کردن" all"به انتهای فرمان، دیگر اطلاعات شبکه همچون نشانی MAC ، نشانی سرویس دهنده DHCP به کار رفته و پل ارتباطی پیش فرض و نشانی های DNS به نمایش در می آید،اطلاعاتی که در هنگام اشکال زدایی از شبکه می تواند مفید واقع شود. اگر تنظیمات DHCP را تغییر داده اید اما کامپیوتر شخصی یک سرویس گیرنده هنوز آن را اعمال نکرده است، می توانید با اضافه کردن elease به فرمان ipconfig ، کامپیوتر مذکور را وادار به استفاده از نشانی جدید نمایید و با اضافه کردن renew به انتهای فرمان، ipconfigرا دوباره اجرا کنید. چنانچه ipconfig هیچ نوع نشانی را به نمایش نگذارد، این احتمال هست که سرویس دهنده DHCP ، غیر فعال یا غیر قابل دسترسی باشد.این احتمال هم وجود دارد که کامپیوتر شخصی یا سرویس دهنده، طوری پیکربندی نشده باشد که بتواند با استفاده از DHCP به نشانی یابی خودکار خود دست یابد. در این وضعیت کافی است تنظیمات کامپیوتر شخصی را تغییر دهید. در برخی از سیستم های ویندوز ممکن است به نشانی هایی برخورد کنید که با ۱۶۹ شروع می شود (۱۶۹ (xxx.xxx.xxx.و این در صورت است که تخصیص خودکار پیکربندی شده اما هیچ سرویس دهنده DHCP وجود ندارد، اما از لحاظ عیب یابی باید آن را یک خطا به حساب آورد.

5-بررسیPing

یکی دیگر از ابزارهای اصلی برای عیب یابی، نرم افزار خدماتی ping است Ping .پرکاربردترین ابزار عیب¬یابی شبکه ها است و تقریباًهمه کسانی که درگیر رفع اشکال شبکه هستند با این دستور و نحوه استفاده از آن آشنا می باشند, اما چرا این ابزار ساده, این قدر مفید است؟

Pingکردن موفقیت آمیز سرویس های اصلی شبکه نظیر Web applicationها و User authentication نشان خواهد داد که سرویس ها به تنهایی از محل کلاینت ها قابل دسترسی هستند. در واقع موفقیت انجام یک ping ساده نشان می دهد که ارتباط مستقیم یا End-to-End بین دو دستگاه درلایه ۳ مشکلی ندارد. انجام کامل این عمل در شبکه می تواند نمایی کامل از وضعیت شبکه را به دست بدهد. البته درخواست های ICMP در ترافیک داده ها اولویت پایینی دارند و اگر روتری در مسیر دستگاههای پر کاربرد باشد , ممکن است آن دستگاهها را به موقع ارسال ننماید. سرورهای خارج از شبکه یک سازمان بزرگ نیز می تواند از جانب کلاینت ها به عنوان مقصد Ping برای بررسی صحت ارتباط شبکه WAN مورد استفاده قرار گیرند. اگر سرورهای سمت داخلی فایروال به ping پاسخ دهند اما سرورهایی که پشت فایروال هستند, تقاضای ping را نادیده بگیرند, تکنسین های شبکه را به این نتیجه می رسانند که باید نگاهی به مسیریاب ها یا سایر ادوات مربوط به زیر ساخت شبکه بیندازند و اشکال را در آنها جستجو کنند اگر نتیجه برعکس باشد یعنی سرورهای پشت فایروال به ping پاسخ می دهند ولی سرورهای سمت داخل, تقاضای ping را نادیده می گیرند, آنگاه تکنسین شبکه باید در پی پاسخ این سؤال باشد که چرا بعضی از بخشهای شبکه در دسترس نیستند. اگر حالت سوم روی دهد یعنی همه سرورهای دو طرف فایروال به ping پاسخ دهند, اما کلاینت ها به درستی پاسخ نمی دهند , نتیجه می گیریم که در نقل و انتقال فیزیکی داده ها اشکالی وجود دارد.

در خط فرمان داس ping را تایپ می کنید و این بار در انتهای آن، نشانی IP یا نام DNS دیگر سیستم های دلخواه خود برای برقراری ارتباط را اضافه می کنید. بعضی از مسیریاب ها و دیگر وسایل شبکه امکان صدور فرمانهای ping را هم فراهم می کنند. در هر دو حالت مجموعه ای از بسته های ارتباطی) ICMP پروتکل کنترل پیام ای اینترنتی) به نشانی مورد نظر فرستاده می شود. اگر سیستم هدف پاسخ دهد مدت زمان لازم برای مجموع رفت و برگشت مشخص خواهد شد. در این شکل،هدف اول (۱۹۲.۹۲.۱۹۵.۲۲۲) در شبکه LAN است و بسیار سریع (با سرعت یک متر بر ثانیه) پاسخ می دهد. هدف دوم (۱۹۲.۹۲.۱۹۵.۲۲۲)یک سرویس دهنده DNSعمومی (در این مورد، (Freeاست و مدت زمان بیشتری می طلبد. اگر هیچ پاسخی در کار نباشد یا کامپیوتر میزبان غیر قابل دسترسی است و یا قبل از دریافت پاسخ، مدت مهلت زمانی به پایان رسیده است. در هر صورت ایراد کار مشخص نمی شود اما کاربرد ping، سرنخ های مهمی را به همراه می آورد.بهتر است در عیب یابی مشکلات مربوط به اتصال به اینترنت قبل از همه، پل ارتباطی را بررسی کنیم. اگر پل ارتباطی پاسخی ندهد، احتمالاً مشکل درهمین قسمت است یعنی یا مسیر یاب از کار افتاده و یا خط ارتباطی غیر فعال است. اما اگر بتوانیم پل ارتباطی را ping کنیم، همچنین یک نشانی اینترنتی را ping کنیم و اگر به این شیوه بتوانیم به اینترنت راه پیدا کنیم اما امکان مرور وب یا بازیابی email فراهم نباشد، مشکلی در DNS خواهد بود یا سرویس دهنده DNS غیرفعال است که با استفاده از برنامه nslookup آن را بررسی می کنیم و یا در کامپیوتر سرویس گیرنده، نشانی اشتباهی پیکر بندی شده است که با کاربرد ipconfig آن را پیدا می نمایم. حصارهای امنیتی (Firewalls) را به گونه ای می توان پیکر بندی نمود که مانع ورود ICMPشود، به همین خاطر ناتوانی در پینگ کردن یک وسیله راه دور الزاماً به معنای مشکل ارتباطی نمی باشد. اکثر مسیریاب های

خانگی یا تجاری کوچک به گونه ای پیکر بندی خواهند شد که به درخواست های Ping دریافتی از طریق اینترنتی پاسخ ندهند، اما پینگ های محلی را همچنان باید پاسخ گفت.

-6ردیابی مسیر

پینگ های ارسالی به یک میزبان اینترنتی، بیشر از پینگ های محلی طول می کشد، زیرا ممکن است میان سیستم های مبدا و هدف، چند مسیر یاب موجود باشد. با استفاده از یک برنامه خدماتی ویندوز موسوم به tracert (traceroute) برای کاربران لینوکس) می توان تعداد این قبیل "توقفگاه ها (hops) "و نشانی های مسیریاب های واسط را تعیین کرد. پس از تایپ tracert نشانی IP هدف (یا نام (DNS را اضافه کنید. بسته های ارتباطی برای رسیدن به نشانی IP مورد نظر (۱۹۵.۹۲.۱۹۵.۲۲۲)، نخست از طریق یک مسیریاب محلی به نشانی ۱۹۲.۱۶۸.۰.۲۲۲ ارسال می شوند و سپس قبل از رسیدن به مقصد نهایی، چند نقطه ی دیگر را پشت سر می گذارند. در مورد عیب یابی محلی، معمولاً فقط به اولین "توقفگاه " توجه می کنیم، هر چند در صورت بروز مشکلات اجرایی و دیگر اطلاعات راه گشاه خواهد بود.

-7تبدیل نام ها

ممکن است با استفاده از یک نرم افزار خدماتی موسوم به nslookup ، به بررسی طرف DNS شبکه خود واتصال آن به اینترنت بپردازید. همان طور که قبلاً گفته شد این کار در هنگامی ضرورت می یابد که پس از پینگ کردن یک آدرس در اینترنت، نتوانسته باشید به یک URL بروید یا نام های DNS را ping کنید. با این حال nslookup که یک نرم افزار خدماتی خط فرمان است، امکان تبدیل نام های DNS به نشانی IP و بالعکس را مستقیماً فراهم می کند. در خود نرم افزار nslookup ، چندین گزینه ی دیگر هم وجود دارد و برای دیدن تمامی گزینه های اختیاری کافی است پس از تایپ nslookup ، علامت "؟" را درج کنید. اما ساده ترین راه برای استفاده از این نرم افزا، تایپ nslookup و سپس تایپ نام DNS یا نشانی IP مورد نظر است. بعد از این کار، با استفاده از تنظیمات پیش فرض سرویس دهنده DNS در سیستم میزبان، عملیات جستجو (lookup) انجام خواهد شد. اگر نام یا نشانی درج شده را درست فرض کنیم، اختلال در تبدیل، نشان دهنده مشکلی در همان قسمت خاص است که معمولاً یک ورودی ناصحیح سرویس دهنده DNS می باشد. در هنگام تفسیر نتایج حاصل از nslookup و دیگر ابزار معرفی شده در این مقاله باید احتیاط کرد، ما ابزار فوق هیچ ضرر و زیان جدی به شما وارد نمی کند، پس ارزش یکبار آزمایش را دارند.

-8تست کابل

اولین کابلی که باید سلامت آن مورد بررسی قرار گیرد Patch Cable است که ارتباط ایستگاه کاری یا هرگونه تجهیزات شبکه را با پریز دیواری برقرار می کند. برای این کار, یک طرف Patch Cable را به پورت شبکه دستگاه Link Runner و طرف دیگر آن را به پورت Wiremap متصل می کنیم تا سلامت آن بررسی شود. قدم بعدی دنبال کردن مسیر کابل ها برای یافتن ,ایراد است .
در این وضعیت به سوییچ و رک می رسیم. اگر رک بزرگ و شلوغ باشد, معمولاً یافتن کابل مورد نظر در آن مشکل است خصوصاً اگر به درستی نیز علامت گذاری نشده باشند. برای رفع این مشکل, دستگاه Link Runner دو گزینه دارد. اول آنکه دستگاه یک آوای صوتی را روی کابل منتشر میکند.این صدا با tone probe قابل شنیدن است. از این طریق می توان کابل مرتبط را یافت و به خصوص برای موقعی مناسب است که نمی دانیم کابل به سوییچ متصل است یا خیر. به غیر از این وقتی طرف دورتر کابل مشخص است, آداپتور Wire mapدستگاه می تواند برای بررسی سلامت کابل افقی و نحوه اتصالات آن مورد استفاده قرار گیرد. در همین حال, دستگاه اقدام به ارسال سیگنال نیز میکند. در این صورت چراغ مربوط به آن پورت روی سوییچ, هر ۳ ثانیه یک بار چشمک می زند و به این طریق می توان فهمید که کدام پورت از سوییچ به کابل مورد نظر ما متصل است. وقتی محل پورت مشخص شد, کابل را می توان روی پورت بدون استفاده دیگری تست کرد. اگر اشکال از پورت روی سوییچ باشد, ممکن است با تغییر کابل از پورتی به پورت دیگر , مشکل شبکه حل شود. اگرپورت های هاب یا سوییچ نیز سالم باشند, آنگاه باید به سراغ ایستگاههای کاری رفت, با اتصال مستقیم Link Runnerبه کارت شبکه می توان به درستی کارکرد آن را بررسی کرد Link Runner .با اتصال به کارت, لینکی را برقرار می کند و نوع و سرعت لینک را بررسی و گزارش می کند.اگر کارت شبکه سالم باشد, باید ایستگاه کاری را بوت کرد و از خط فرمان وبا استفاده از دستوری مانند ping این امکان را فراهم کرد که Link Runner ترافیک شبکه را مشاهده کند. اگر دستگاه وجود هیچگونه ترافیکی را گزارش نکرد باید به تنظیمات خود PC دقت کرد که ممکن است اشکال در آنجا نهفته باشد. اگر گزارش لینک و ترافیک همه چیز را به خوبی نشان دهد, آن گاه باید به تنظیمات شبکه ای PC مشکوک شد .

9-بررسی فعالیت کلی سگمنت ها(Segment)

در یک شبکه اترنت یک طرفه یا Half Duplexبه علت وجود تعداد ایستگاه هایی که می توانند به طور همزمان داده ها را ارسال کنند و همچنین محدودیت اندازه frame ها اگر تعداد زیادی از ایستگاهها به طور همزمان شروع به تبادل داده بنمایند, به علت تکرار تصادم یا ,Collision کار آیی کل شبکه به شدت افت خواهد کرد.

البته بروز تعداد متعادلی پدیده تصادم در شبکه های اترنت Half Duplex امری طبیعی است ولیکن هنگامی که تعداد این تصادم ها رو به افزایش می گذارد, ترافیک شبکه نیز بالا می رود و بالا رفتن ترافیک شبکه که به علت ارسال مجدد پکت ها می باشد, افت کیفی شبکه را به دنبال دارد .در چنین شبکه ای منحنی کارآیی شبکه به یک باره سقوط می کند و نحوه تغییر این منحنی به تعداد فریم های ارسالی , تعداد تصادم ها و تعداد پکت هایی که به ارسال مجدد نیاز دارد, بستگی دارد. با کاهش کارآیی شبکه ,کار کردن برای کاربران شبکه مشکل می شود و انتقال داده ها نیز با وقفه و کندی صورت می گیرد. برای رفع این عیب, شناخت Segment های شبکه و بررسی ترافیک شبکه ضروری است. با استفاده از LinkRunner می توانید تست مربوط و اقدام بهینه را انجام دهید. اگر ترافیک شبکه در جریان باشد LinkRunner آن را به صورت نوارهایی روی صفحه نمایش خودش نشان می دهد .

10-استفاده از DHCP

اگر لینک شبکه برقرار باشد و به آزمونهای اولیه پاسخ دهد, در نتیجه کاربر می تواند آزمایشهایی را با ping انجام دهد. اگر از Link Runnerاستفاده می کنید, این دستگاه در اینجا سعی می کند که ابتدا یک IP Address از سرور DHCP شبکه به دست بیاورد . DHCPدر واقع یکی از معمولترین روشهای مبتنی بر انتشار (Broadcast) است. به طور معمول, برای هر ,subnet یک سرور DHCPمجزا نیاز است(که این امر پر هزینه است و از نظر مدیریت نیز مشکل می باشد) و یا اینکه DHCP رله کننده پراکسی هایی است که وظیفه نقل وانتقال در خواست ها را بین کلاینت ها وسرورها برعهده دارند(هنگامی که کلاینت ها و سرورها به طور فیزیکی در یک subnet قرار ندارند). این انتشار جهت دار می تواند راهنمای خوبی برای اطلاع از اوضاع ترافیک شبکه باشد. عدم موفقیت هر کلاینت یا Link Runner در اتصال خودکار به DHCP می تواند نشانه ای از بروز مشکل در سیستم رله کننده DHCP باشد . DHCPدر اغلب شبکه های امروزی وجود دارد و دستگاه نیز می تواند با پیکر بندی IP دستی یا ایستا نیز کار کنند. پروسه کاری نیز شامل به دست آوردن یک نشانه DHCP برای سنجش صحت کار کرد کابل های محلی, هاب محلی, پورت سوییچ و نهایتاً کل زیر ساخت شبکه باشد.

11-تست پیشرفته تر

اگر ایستگاه کاری می تواند با شبکه لینک برقرار کند, باید بررسی کنید که آدرس دهی ایستگاه کاری متناسب با subnet مرتبط با آن است یا خیر. سپس بررسی اینکه از protocol stack درستی استفاده می کند و به درستی نیز پیکربندی شده است یا نه. سپس باید همه اجزای برنامه های مورد نیاز را بررسی نمود. این کار معمولاً از طریق حذف کردن پروتکل ها یا حذف تنظیمات کارت شبکه و نصب مجدد آنها صورت می گیرد تا از صحت کارکرد آنها اطمینان حاصل شود. اگر همه این موارد نیز به درستی کار میکنند, احتمالاً رفع مشکل به دانش تخصصی بیشتر و پیشرفته تری نیاز دارد .

ابزارهای مدیریت و تست شبکه همچون PLC’s Smart Bits TeraMetrics XD وActerna DA ۳۴۰۰ Ethernet Data Network Analyzerنیز نقشی مهم در عیب یابی و شناسایی شبکه ها ایفا می کنند. مدیریت شبکه در واقع در بهترین شکل آن، شامل ترکیب بندی و دیده بانی دوردست Remote Monitoring شبکه می شود که به شما امکان می دهد علا وه بر انجام اصلا حات نهایی از راه دور، سالم بودن شبکه خود را نیز ارزیابی کنید.

امنیت شبکه های کامپیوتری

امنیت شبکه های کامپیوتری از مهمترین مسائل مبتلا به شبکه های کامپیوتری است. مهمترین رکن برپائی یک شبکه پس از پیکربندی صحیح سخت افزاری مساله تضمین امنیت شبکه است. این مساله در محورهای زیز بررسی شده است :

کلیات امنیت شبکه کامپیوتری

حفاظت، پشتیبانی و نگهداری از داده‌های رایانه‌ای، اطلاعات مهم، برنامه‌های حساس، نرم‌افزارهای مورد نیاز و یا هر آنچه که در حافظه جانبی رایانه مورد توجه بوده و با اهمیت می‌باشد، امنیت رایانه‌ای نامیده می‌شود. تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از راز داری و امانت داری(Confidentiality) ، یکپارچگی (Integrity)و در نهایت در دسترس بودن همیشگی .(Availability) این سه عامل (CIA) اصول اساسی امنیت اطلاعات - در شبکه و یا بیرون آن - را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است .

Confidentiality

به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و اینگونه تعریف شده است .بعنوان مثال از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات .

Integrity

بیشتر مفهومی است که به علوم سیستمی باز می گردد و بطور خلاصه می توان آنرا اینگونه تعریف کرد:
-تغییرات در اطلاعات فقط باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد.
-تغییرات بدون اجازه و بدون دلیل حتی توسط افراد یا پروسه های مجاز نباید صورت بگیرد .
-یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج آن باید یکسان باشد و اگر تغییر می کند باید همزمان درون و برون سیستم از آن آگاه شوند .

Availability

این پارامتر ضمانت می کند که یک سیستم - مثلا اطلاعاتی - همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مد نظر باشد اما عواملی باعث خوابیدن سیستم شوند - مانند قطع برق - از نظر یک سیستم امنیتی این سیستم ایمن نیست .

اما جدای از مسائل بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می شوند برای خود شخصیت جداگانه ای پیدا کرده اند. در این میان می توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authenticationبه معنی مشخص کردن هویت کاربر، Authorizationبه معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountabilityبه معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد .

امنیت در یک شبکه به ۲ روش صورت می پذیرد. ۱- برنامه های نرم‌افزاری ۲- قطعه‌های سخت‌افزاری. در بهترین حالت از برنامه های نرم افزاری و قطعات سخت افزاری بطور همزمان استفاده می گردد. عموماً برنامه‌های نرم‌افزاری شامل برنامه‌های ضدمخرب (مخرب‌ها شامل ویروس، کرم‌های مهاجم، اسب‌های تراوا، مخفی‌شده‌ها و ....) و دیوار آتش می‌باشد. قطعات سخت‌افزاری نیز عموماً شامل دیوار آتش می‌شود. این قطعه‌ها موجب کنترل درگاه‌های ورودی و خروجی به رایانه و شناخت کامل از حمله‌کننده‌ها بخصوص نشانه‌های خاص مهاجم را ایجاد می نماید .

فراموش نکنیم که شرکت مایکروسافت به عنوان عرضه‌کننده سیستم های عامل نسل) Windows که در حال حاضر پرمصرف ترین گروه سیستم‌های عامل را تشکیل می دهد)، به یک برنامه نرم افزاری دیوار آتش بصورت پیش فرض مجهز می باشد، که می‌تواند تا امنیت را هر چند کم، برای کاربران سیستم‌های عامل خود فراهم نماید اما قطعاً این نرم افزار به تنهایی کفایت امن سازی رایانه را تأمین نمی نماید. اما در اولین مرحله امن سازی یک شبکه ابتدا باید سازمان را به یک برنامه ضدمخرب قوی مانندَ Antivir, Symantec, Kaspersky, Nod32, BitDefender, Norton, Pandaو Mac با قابلیت بروزآوری مجهز نمود، تا بتواند در مقابل حمله برنامه های مخرب واکنش مناسبی ارائه نماید. برنامه Antivir می تواند یک انتخاب مناسب در این زمینه باشد. چرا که این برنامه قابلیت بروزآوری را بطور مداوم دارا می‌باشد و خود برنامه نیز هر ۶ ماه یکبار ویرایش می‌گردد تا از موتور جستجوگر قوی تر و بهینه‌تری برای یافتن برنامه های مخرب بهره گیرد. خرید نسخه اصلی این نرم‌افزار توصیه می‌گردد، چرا که در صورت بروز مشکل شرکت اصلی نسبت به پشتیبانی از رایانه‌های شما اقدام لازم را در اسرع وقت به انجام می‌رساند.

در مرحله دوم امن سازی یک شبکه باید از دستگاه تقسیم‌کننده استفاده نمود. دستگاه های فوق خود بر دومدل قابل تنظیم و پیکربندی و غیرقابل تنظیم و غیر قابل پیکربندی تقسیم می شوند. ممکن است در گروه اول نیز قطعاتی یافت شود که تنظیمات جزئی پیکربندی را انجام دهند اما بطور کامل و با تمامی امکاناتی که در گروه دوم قطعات دیده می شوند، مجهز نمی‌باشند. عموماً این دستگاه تقسیم کننده از مدل Core و برای ارتباط سرویس‌دهنده‌های مرکزی به یکدیگر و انجام خدمات به شبکه داخلی یا دنیای اینترنت تهیه می‌شود و در لایه اصلی تقسیم ارتباط شبکه، از طرف سرویس‌دهنده‌های مرکزی به سرویس گیرنده های داخلی و بالعکس قرار گیرد. این قطعه می تواند از تکثیر یک برنامه ضدمخرب و همچنین ورود و خروج مهاجمان پنهان، در درون شبکه داخلی از یک رایانه به رایانه دیگر تا حد بسیار زیادی جلوگیری نماید. اما اگر تعداد کاربران و سرویس‌گیرنده‌های یک سازمان بیش از تعداد درگاههای خروجی یک تقسیم‌کننده مرکزی Core Switch باشد، در این صورت از تقسیم کننده های دیگری که قابلیت پیکربندی را دارا بوده و مقرون به صرفه نیز می‌باشند، می‌توان استفاده نمود، تا کنترل ورودی و خروجی های هر طبقه یا واحد را بیمه نماییم. در مورد قطعات سخت افزاری تقسیم کننده Cisco Switch گزینه مناسبی می باشد که برترین نام جهانی را در این زمینه به خود اختصاص داده و با بروزآوری قطعات خود و همچنین آموزش متخصصان خود سهم بزرگی در این بحث ایفا می نماید .

در مرحله سوم امن سازی، نیاز به خرید برنامه نرم افزاری و یا قطعه سخت افزاری دیوار آتش احساس می شود. بیشترین تأکید بر روی قطعه سخت افزاری استوار است زیرا که از ثبات، قدرت بیشتر و ایرادات کمتری نسبت به نرم افزارهای مشابه خود برخوردار است. قطعه سخت‌افزاری دژ ایمن می بایست در مسیر ورودی اینترنت به یک سازمان قرار گیرد. دقیقاً همانجایی که اینترنت غیرامن به یک سازمان تزریق می گردد. پیشنهاد ما، قطعه سخت‌افزاری Cisco ASAو یا Astaro Firewall می باشد. فراموش نشود استفاده از دو دستگاه همزمان موازی قطعاً نیاز ارجح هر سازمان می باشد چرا که با ایست، و توقف سرویس‌دهی یکی از قطعه‌ها، دستگاه دیگر کنترل ورودی ها و خروجی ها را بدست می‌گیرد. اما در برنامه نرم‌افزاری نیاز به نصب نرم‌افزار بر روی یک سرویس‌دهنده مرکزی دیوار آتش بوده که ورود اینترنت ناامن تنها از مسیر این سرویس‌دهنده مرکزی انجام پذیرد. باید توجه داشت در صورت تهیه قطعه‌های سخت‌افزاری خاصی استفاده نمود تا در قبل و بعد از قطعه مسیریاب‌ها قرار گیرد که در این صورت بهتر است تا از قطعه های Cisco ASA در دیواره داخلی و بعد از قطعه مسیرباب‌ها استفاده نمود .

در مرحله چهارم امن سازی نیاز به وجود قطعه سخت‌افزاری دیگری به نام مسیریاب برای شبکه داخلی می‌باشد که ضمن قابلیت پیکربندی، برای نشان دادن مسیر ورودی ها و خروجی ها، اشتراک اینترنت، تنظیم ورودی ها و خروجی های دیوار آتشین، و همچنین خروج اطلاعات به شکل اینترنتی از سازمان به رایانه های شهری و یا بین شهری از طریق خطوط تلفن و ... استفاده نمود. پیشنهاد ما نیز محصولات شرکت معتبر Cisco میباشد .

در مرحله بعدی امن سازی یک سازمان نیاز به وجود دستگاه های تنظیم جریان برق و دستگاه های پشتیبان جریان برق اضطراری برای ارائه خدمات به صورت تمام وقت، بدون قطعی و تنظیم جریان برق، تمامی قطعه‌های سخت افزاری راهبر یک شبکه شامل تقسیم‌کننده‌ها، مسیریاب ها ، سرویس‌دهنده‌هامی باشد. این سیستم به دلیل ایجاد خطرات احتمالی ناشی از قطع جریان برق نظیر از بین رفتن اطلاعات در حال ثبت بر روی سرویس‌دهنده ها، تقسیم کننده ها، مسیریاب ها می‌باشد.

به عنوان آخرین مرحله امن سازی، تهیه از اطلاعات و فایلهای مورد نیاز به صورت پشتیبان از برنامه‌های اصلی نرم‌افزاری بر روی یک سرویس‌دهنده پشتیبان ، آخرین لایه امن سازی درون سازمانی را تکمیل می نماید .

امنیت در شبکه های بی سیم

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این بخش به «امنیت در شبکه های بی سیم» بپردازیم.

سه روش امنیتی در شبکه های بی سیم عبارتند از:

- WEP: Wired Equivalent Privacy

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می آید که مناسب برای شبکه های کوچک بوده زیرا نیاز به تنظیمات دستی (KEY)مربوطه در هر Client می باشد .اساس رمز نگاری WEP بر مبنای الگوریتم RC4 بوسیله RSA می باشد.

- SSID: Service Set Identifier

شبکه های WLAN دارای چندین شبکه محلی می باشند که هر کدام آنها دارای یک شناسه (Identifier) یکتا می باشند این شناسه ها در چندین Access Point قرار داده می شوند . هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSIDمربوطه را انجام دهد.

- MAC : Media Access Control

لیستی از MAC آدرس های مورد استفاده در یک شبکه به (AP (Access Point مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرسها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می کند MAC آدرس آن با لیست MACآدرس مربوطه در AP مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می گیرد .این روش امنیتی مناسب برای شبکه های کوچک بوده زیرا در شبکه های بزرگ امکان ورود این آدرسها به AP بسیار مشکل می باشد.

ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد .

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.

- اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند .
- حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به‌راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.
- در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد شبکه نیز وجود دارد.

راه کارهای افزایش امنیت سیستمها

-بررسی میزان امنیت مورد نیاز کامپیوترها با توجه به اطلاعات ذخیره شده روی آنها، محیطی که در آن قرار گرفته اند، موارد و روشهای استفاده از آنها

-بررسی تنظیمات موجود روی کامپیوترها و تشخیص آسیب پذیریها و سوراخهای امنیتی با استفاده از برنامه های جدید و حرفه ای

-انجام تنظیمات و نصب برنامه های لازم جهت ارتقای امنیت منطقی کامپیوترها پیاده سازی امنیت برای فایلها

-کنترل میزان دسترسی کاربران به فایلها بر اساس موارد زیر :الف -فقط خواندن ب -خواندن و ویرایش ج -خواندن، ویرایش و حذف د - خواندن، ویرایش، حذف و کنترل دسترسی دیگران

-ثبت دسترسی کاربران مورد نظر به فایلهای تعیین شده (برای مثال جهت تشخیص کاربری که فایلهای خاصی را ویرایش می کند - (پیاده سازی رمزگذاری فایلها (Encrypting File System) جهت جلوگیری از دسترسی کاربران دیگر (حتی مدیر شبکه) به آنها

دیواره آتش Firewall

دیواره آتش برای جدا کردن شبکه ها از همدیگر به کار می رود با استفاده از یک Firewall مناسب اهداف زیر محقق می گردد.

-1می توان سیاستها و سرویسهای ارائه شده در شبکه ها را از همدیگر بصورت مجرا نگهداری ، مدیریت و کنترل نمود.

-2انتخاب سرویس های داخلی ارائه شوند به بیرون از شبکه و یا بالعکس

- 3کنترل امنیت و مدیریت دسترسی های کاربران

-4حفاظت از اطلاعات در ماقبل کسانی که قصد نفوذ به شبکه داخلی را دارند .

دیوار آتش سیستمی است که در بین کاربران یک شبکه محلی و شبکه جهانی قرار می‌گیرد و ضمن نظارت بردسترسی‌ها در تمام سطوح ورود و خروج اطلاعات راتحت نظر دارد. در این ساختار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات را کنترل‌کند موظف است تمام ارتباطات مستقیم شبکه داخلی خود را با دنیای خارج قطع کرده و هرگونه ارتباط خارجی از طریق یک دروازه که دیوارآتش یا فیلتر نام دارد انجام‌شود. بسته‌های TCP و IPقبل از ورود به شبکه یا خروج ازآن ابتدا وارد دیواره آتش می‌شوند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند.

شبکه های با قابلیت بالا جهت ارتباط با اینترنت از سخت افزاری های تخصصی استفاده می نمایند ولی نرم افزارهایی هم به همین منظور تولید شده و روی دستگاه های PC نصب می شود برای اتصال مناسب و امن به اینترنت استفاده از نرم افزار firewall ضروری می باشد. ناگفته نماند که ویندوز XP در نسخه SP2 خود این قابلیت را دارا می باشد و دارای امنیت بسیار بالائی جهت اتصال به شبکه می باشد . علاوه بر این توصیه می شود که جهت اتصال به شبکه اینترنت علاوه بر استفاده از Firewall ، از نرم افزارهای مناسب ویروس کش و AntiSpy نیز استفاده شود.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود.بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

-1فایروالهای سطح مدار :(Circuit-Level) این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از (TCP را نیز نمی دهند.

-2فایروالهای پروکسی سرور : فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

-3فیلترهای : Nosstateful packet این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال مانند سرآیندهای TCPو UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

-4فیلترهایِ : Stateful Packetاین فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند.این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند.این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای .TCP بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانندعامل کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

-5فایروالهای شخصی : فایروالهای شخصی ، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند.آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولا از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست .

نصب و تنظیم فایروال

-تشخیص و تعیین کامپیوترهایی که نیاز به نصب فایروال روی آنها وجود دارد (مخصوصا سرورها(

-نصب نرم افزار فایروال مناسب روی کامپیوترها جهت جلوگیری از دسترسی های غیر مجاز

-انجام تنظیمات لازم در فایروالهای نصب شده بگونه ای که اختلالی در سرویسها و ارتباطات معمول ایجاد نگردد

-انجام آزمایشات لازم جهت کسب اطمینان از صحت و کارایی فایروال

نرم افزار Sunbelt Personal Firewall

قطع ترافیک ورودی و خروجی رایانه: بسیار مناسب برای زمانی که حرکات مشکوک و نا خوشایند بر روی شبکه رخ می دهد .نگارش وقایع: با ثبت تمامی ارتباطات شبکه به شما امکان مرور و پیدا کردن مشکل احتمالی را می دهد .مرور کلی ارتباط ها و آمارگیری از وقایع: آمارگیری دقیق از ارتباطات برقرار شده و پورت های باز توسط نرم افزارهای دیگر و موقعیت بلاک شده ها و زمان های حمله و جلوگیری را نمایش می دهد .به روز رسانی: با بروز شدن نرم افزار آخرین ویرایش و قویترین آن همیشه در دسترس خواهد بود .

مدارک بین المللی شبکه

مدارک مایکروسافت

هر شخص بعد از قبولی در اولین آزمون مایکروسافت به عنوان فرد مورد تائید مایکروسافت یا MCP شناخته می شود .دسترسی به بسیاری اطلاعات، بهره مندی از تخفیف های ویژه و امکان حضور در نشست‌های فنی این شرکت از مزایای دریافت این مدارک است. در زمینه شبکه نیز مدارک متعددی وجود دارد که در زیر به مهمترین آنها اشاره می شود.

گواهینامه+A

این گواهینامه از جمله مدارک بسیار متداول مایکروسافت است. آزمون +A دو زمینه سخت افزار و سیستم عامل را مورد سنجش قرار می‌دهد.

گواهینامه +Network

در این گواهینامه کلیه مطالب پایه و مقدماتی شبکه بررسی می‌شود. سرفصل‌های آزمون +Network عبارتند از: انواع شبکه‌ها از دید اندازه و توپولوژی، پروتکل‌های شبکه، سخت افزارهای شبکه، پیکربندی سخت افزاری و نرم افزاری شبکه، معماری لایه های شبکه، امنیت شبکه، پشتیبانی از شبکه و رفع عیب شبکه. در تدوین فصول آموزشی این سایت از سرفصل های همین آزمون استفاده شده است.

گواهینامه CISCO

شرکت سیسکو یکی از برجسته ترین شرکتها در زمینه شبکه است. در ایران موسسات متعددی به تدریس این دوره‌ها می‌پردازند اما چون شرکت سیسکو یک شرکت آمریکائی است و به علت مناسبات سیاسی دو کشور، هیچ یک از مدارک فوق در ایران صادر نمی‌شود و برای دریافت مدرک باید به کشور دیگری(به طور مرسوم دبی) رجوع نمائید.
گواهینامه های این شرکت در سه سطح ارائه می شود که عبارتند از .CCNA, CCNP, CCIE :دقت کنید این مدارک به صورت پلکانی است. برای نمونه پیش نیاز شرکت در آزمون داشتن مدرک CCNA است. در سطح عالی گواهینامه CCIE به فرد اعطا می-شود.

گواهینامهMCSE

گواهینامه MCSE یکی از مهمترین مدارک مایکروسافت است. این گواهینامه در ازای ارائه یک طرح تجاری، پیاده‌سازی زیرساختی مبتنی بر محصولات مایکروسافت یا ارائه راه‌حل‌هائی به مایکروسافت اعطاء می‌شود. این گواهینامه برای مهندسان سیستم، تحلیلگران شبکه و مشاوران فنی مناسب است.

مطالعه مطالب این سایت و کتابهای مشابه جهت کسب مدرک +Networkکارآمد است اما جهت دریافت گواهینامه MCSE تجربه و مهارت عملی الزامی است. گواهینامه MCSE دارای هفت آزمون است. چهار آزمون اول عبارتند از:

-1نصب، پیکربندی و مدیریت ویندوز ۲۰۰۰ حرفه‌ای
-2نصب، پیکربندی و مدیریت ویندوز ۲۰۰۰ سرور
-3بکارگیری و مدیریت زیرساختهای شبکه
-4بکارگیری و مدیریت زیرساختهای سرویس‌های دایرکتوری

سه آزمون دیگر نیز به صورت انتخابی از میان آزمونهای ارائه شده صورت می‌گیرد. برای کسب اطلاعات بیشتر به سایت مایکروسافت رجوع کنید.

مقدمه

واژه WiMAX مخفف Worldwide Interoperability for Microwave Accessبوده و یک تکنولوژی ارتباط راه دور است که دستیابی ثابت به اینترنت را فراهم می کند. سرعت کنونی WiMAX در حدود ۴۰ Mbpsاست. وایمکس براساس استاندارد IEEE 802.16است که Broadband Wireless Access نیز خوانده می شود. گروه وایمکس که در سال ۲۰۰۱ پایه ریزی شده است وایمکس را اینگونه تعریف کرده است: یک تکنولوژی استاندارد که دستیابی به اینترنت broadband را به جای استفاده از روشهای کابلی یا DSL میسر می کند.

مفهوم :broadband در فارسی به جای braodband از واژه پهنای باند بالا نیز استفاده می‌گردد. واژه braodband به مفهوم اینترنت پرسرعت است. اتصالات اینترنت پرسرعت یا braodband پهنای باندی بین ۶۴ Kbpsتا ۳۰۰ kbpsو یا بیشتر را ارائه می‌نمایند. دو مفهوم پهنای باند و broadband را با یکدیگر اشتباه نگیرید broadband .، نشاندهنده روش استفاده شده به منظور ایجاد یک ارتباط است در صورتی که پهنای باند، نرخ انتقال داده از طریق محیط انتقال را نشان می‌دهد .

تکنولوژی WIMAX وWi-Fi

تکنولوژی WiMAX که براساس استاندارد شبکه های بدون سیم IEEE 802.16 می باشد بسیار مشابه تکنولوژی Wi-Fi است که براساس استاندارد شبکه های بدون سیم IEEE 802.11 می باشد. اجازه استفاده از تجهیزات وایمکس توسط تولید کنندگان و فروشندگان مجاز است لذا امکان استفاده از این تکنولوژی در دستگاه های مختلف وجود دارد.

همانطور که در بحث استاندارد ۸۰۲.۱۱ در مباحث شبکه های بدون سیم اشاره شد استاندارد ۸۰۲.۱۶ نیز به دو صورت ۸۰۲.۱۶ dو ۸۰۲.۱۶ eدر بازار رواج دارد. استاندارد ۸۰۲.۱۶ dرا تحت عنوان وایمکس ثابت یا Fixed WiMAX می شناسند. استاندارد ۸۰۲.۱۶ e را نیز تحت عنوان وایمکس متحرک یا Mobile WiMAX می شناسند. استفاده از وایمکس متحرک رواج بسیار بیشتری دارد و آینده تکنولوژی وایمکس محسوب می شود .

مهمترین موارد استفاده وایمکس عبارت از اینترنت پرسرعت موبایل، اینترنت پرسرعت بی سیم جایگزین کابل و DSL و ایجاد شبکه های کامپیوتری بدون سیم است.

وایمکس در ایران

در ایران در پی مزایدهٔ فناوری وایمکس در تابستان و پاییز ۱۳۸۷ چهار شرکتِ صنایع ارتباطی پایا و مبین در ۳۰ استان، ایرانسل (اپراتور تلفن همراه سراسری) در استان‌های تهران، آذربایجان شرقی، اصفهان، خراسان رضوی، فارس و خوزستان، اسپادان (اپراتور تلفن همراه اصفهان) در استان اصفهان و رایانه دانش گلستان در استان گلستان مجاز به ارائهٔ خدمات وایمکس شدند. از میان این شرکت‌ها در حال حاضر تنها ایرانسل این خدمات را ارائه می‌دهد و بقیهٔ شرکت‌ها در حال تلاش برای راه‌اندازی آن هستند.

ویژگی‌ها و خصوصیات فنی

شبکه‌های بنا شده با تکنولوژیWiMAX ، جزء شبکه‌های wireless شهری محسوب می‌شوند که به راحتی می‌توانند با وجود منطقهٔ بسیار وسیعی که دکل‌های WiMAX تحت پوشش خود قرار می‌دهند، کل شهر و یا شهرک‌های صنعتی و مناطق استراتژیک را پوشش دهند و قابلیت استفادهٔ اینترنت بسیار پر سرعت را از طریق این تکنولوژی برای سازمان‌ها، ارگان‌ها و شرکت‌های تجاری و همچنین منازل مسکونی امکان پذیر سازند.

به کمکWiMAX ، سرعت داده‌هایی مانندWi-Fi ، پشتیبانی می‌شوند و موضوع تداخل امواج نیز کاهش می‌یابد. یکی از ویژگی‌های این تکنولوژی عدم نیاز به دید مستقیم بین مشترکان و دکل‌های BTS می‌باشد.از جمله خصوصیات WiMAX آن است که علاوه بر داده، صدا و تصویر را نیز به خوبی پشتیبانی می‌کند و سرویسی که ارائه می‌شود به صورت کاملاً نامحدود می‌باشد و هیچ گونه محدودیت حجمی و یا زمانی ندارد و این بدان معناست که کاربر می‌تواند بدون هیچ محدودیت زمانی، در تمام شبانه روز به هر مقدار و حجمی که پهنای باندش اجازه می‌دهد download و یا upload داشته باشد.

یکپارچگی مودم، فرستنده و گیرندهٔ رادیویی در سایز بسیار کوچک و قابل حمل و امکان نصب بسیار آسان آن نیز جزو برتری‌هایی محسوب می‌شود که نسبت به سایر فن آوری‌های مشابه خود داراست. امکان مدیریت مودم کاربر از راه دور توسط شرکت و کارشناسان فنی و قابلیت به روز رسانی نرم افزارهای مودم نیز در زمرهٔ این گونه موارد قرار می‌گیرند.

عدم نیاز به دید مستقیم میان مودم سمت کاربر و آنتن مرکزی و شعاع فوق العاده زیاد تحت پوشش آن در حین سرعت بالای انتقال داده نیز از جمله ویژگی‌های دیگر آن محسوب می‌شود. که توپولوژی‌های پیشرفته (شبکه‌های mesh و تکنیک‌های آنتنی-beam forming، STCو تنوع آنتن) می‌توانند برای پوشش برد بیشتری به کار روند که این تکنیک‌های پیشرفته همچنین می‌توانند برای افزایش کارایی طیفی، ظرفیت، استفاده مجدد، توان خروجی ماکزیمم و میانگین برای هر کانال) RF فرکانس رادیویی) مفید واقع گردند.

خصوصیت interoperability در این تکنولوژی، بدین معناست که کاربر می‌تواند هر محصول مورد علاقهٔ خود را خریداری کند (با ویژگی‌های مورد نظرش) و مطمئن باشد که این محصول با سایر محصولات مورد تایید مشابهش هماهنگی و سازگاری خواهد داشت که این امر رقابت بین شرکت‌ها، بهتر شدن کیفیت محصولات و کاهش قیمت‌ها را در پی خواهد داشت.

کاربردهای عملی وایمکس

مهم‌ترین خصوصیت و برتری WiMAX که باید عنوان گردد همان قابلیت سیار بودن آن است که موجب می‌شود که این تکنولوژی را وارد لپ تاپ‌ها، کامپیوترهای دستی و در نهایت گوشی‌های تلفن‌های همراه سازد و این امکان را به آن‌ها می‌دهد که دیگر کاربران برای استفاده از اینترنت پر سرعت نیاز به استقرار در یک مکان خاص و یا محدوده ٔ بسیار محدود نداشته باشند و بتوانند در هر حال و حتی در حال حرکت نیز با سرعت‌های بالا از این امکان بهره مند گردند.

دستگاه های مختلفی مانندLaptop, PDA, MP3 player ، تلفن های همراه، PCهای متحرک، دستگاههای بازی، همگی از مشتریان M-WiMAX هستند و قابل اتصال به شبکه M-WiMAX می‌باشند. ساختار شبکه مبتنی برIP ، قابلیت اتصال این وسایل متنوع را به شبکه ایجاد می‌کند .

منظور از M-WiMAX همان Mobile Wimax است که در بالا به آن اشاره شد.

یکی از مهمترین ویژگی‌های وایمکس بار گذاری اطلاعات بر روی گوشی‌های تلفن همراه می‌باشد که می‌تواند برای جنبه‌های تبلیغاتی بسیار موثر واقع گردد و آن هم بدین صورت است که مثلاً فردی که در حال گذر از یک پل هوایی است به یک باره حجمی از اطلاعات بر روی گوشی وی فرستاده می‌شود که می‌تواند در قالب تصویر، صوت و یا انیمیشن باشد که برای جنبه‌های تبلیغاتی بکار گرفته شود و یا تعداد قابل توجهی افراد که روزانه از مترو استفاده می‌کنند که در هر ایستگاه نوع خاصی از تبلیغات می‌تواند برای این افراد فرستاده شود که این جنبه‌ها موج جدیدی از این فن آوری فوق العاده را در دنیای امروزی نمایان می‌سازند.

تحلیل فنی وایمکس

سرعت بالای انتقال داده در حین حرکت
با وجود آنتن های پیشرفته MIMO و استفاده از روشهای کدینگ و مدولاسیون مبتنی برفن آوری OFDM ، M-WiMAXقادر به انتقال داده تا ماگزیمم نرخ 20 Mbps در دانلینک DL در هر سکتور و ۸ Mbpsدر آپلینک UL در هر سکتور برای یک کانال ۱۰ MHzمی‌باشد که ۱۰ برابر نرخ انتقال داده شبکه‌ها UMTS-HSDPA نسل ۳ موجود با بیشترین نرخ انتقال داده (۲ Mbps) می‌باشد و پایین آمدن تاخیر در سیستم شده و تمامی کاربری های یک اتصال توسط سیم شامل کاربری های بی‌درنگ(Real-Time)و کاربری های نیازمند باند وسیع را ارئه می‌دهد.

تضمین کیفیت سرویس (QoS)
ساختار لایه MAC استاندارد EEE802.16 به گونه‌ای است که ویژگی QoS را برای یک اتصال نقطه به نقطه در شبکه تضمین

می‌کند. این ویژگی پهنای باند مورد نیاز سرویس را در تمامی طول مسیر تضمین کرده و حداقل تاخیر مورد قبول هر سرویس را حفظ می‌کند. همچنین زیر کانالهای موجود مکانیسمی انعطاف پذیر جهت تخصیص بهینه منابع فضا، فرکانس و زمان در قسمت air interfaceموجب شده است.

مقیاس پذیری بر اساس نوع سرویس (Scalability)

تکنولوژی M-WiMAX به گونه‌ای طراحی شده است که در محدوده کانالهای ۲۰ MHzتا ۱.۲۵ قادر به کار کردن است. از نتایج این امر راحتی پیاده سازی شبکه با ایجاد تغییرات جزئی در قسمتAir Interface می باشد و بسته به مدل مصرف بر اساس نوع سرویس و طیف فرکانسی آزاد، M-WiMAXقابل پیاده سازی در فرکانس های متفاوتی می‌باشد. این خصوصیت همچنین باعث می‌شود که محدوده کشورها بر اساس نیازمندیهای منطقه‌ای مختلفشان برای مثال نیاز به دسترسی به اینترنت در شهر و با دسترسی پرظرفیت باند وسیع متحرک در متروها و حومه شهر قادر ، به استفاده موثر و چند منظوره‌ای از این فن آوری باشند.

ظرفیت ترافیکی بالاتر M-WiMAX

به علت به کارگیری تکنیک کدینگ OFDMA و وجود زیر کانال ها، نسبت به سایر تکنولوژی ها در کانلالهایی با پهنای باند مشابه M-WiMAXاز ظرفیت ترافیکی بیشتری برخوردار است.

شبکه تماما مبتنی بر IP M-WiMAX

M-WiMaxبر پایه فن آوری تماماً IP می‌باشد و از IP در ارتباطات ما بین کلیه اجزای شبکه از ابتدا تا انتها استفاده شده است. در حالیکه بسیاری از پروتکل های میانی G۳ تماماً IP نمی‌باشند.