فصل ششم

Active Directory Site and Services

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتـدای هـر فصل به بررسی مطالب ساده‌تری پرداخته شده که در اسـتاندارد 411-70 وجـود دارد و در قسـمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری که در استاندارد 411-70 و 412-70 وجـود دارد پرداختـه شده است. لذا توصیه می‌شود ابتدا قسمت مباحث ابتـدایی را مطالعـه کـرده و در صـورتی‌کـه بـه مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

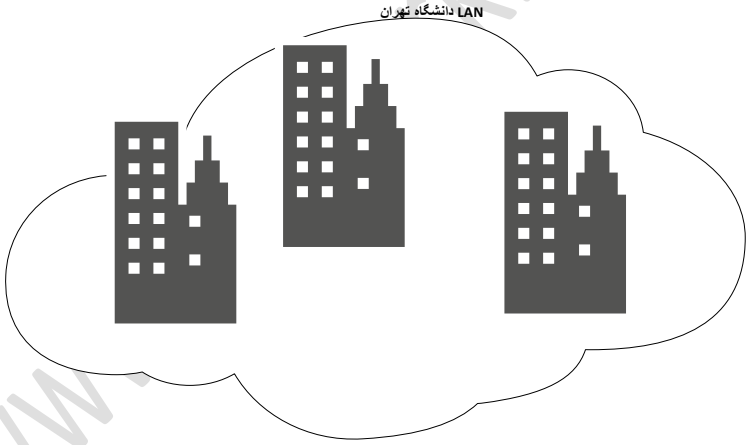
مقدمه

در زمان طراحی شبکه مدیران شبکه براساس نحوه اتصال کلاینت‌ها به سرور از مقایسه زیر استفاده می کنند.

شبکه‌های محلی LAN

به مجموعه کامپیوترهایی که در یک ساختمان یا چندین ساختمان درون یک محوطه مثل دانشگاه به‌هم متصل هستند شبکه محلی یا LAN گفته می‌شود. به‌عنوان مثال LAN دانشگاه تهران یا LAN شهرداری تبریز و ... .

در شکل زیر یک شبکه LAN را مشاهده می‌کنید که ابعاد آن درحد یک محوطه دانشگاه و سه ساختمان است. به‌طور معمول در شبکه LAN ارتباط بین کلاینت‌ها ازطریق کابل‌های UTP و استاندارد اترنت استفاده می‌شود. کامپیوترها به‌وسیله سوئیچ‌ها و کابل اترنت به یکدیگر متصل می‌شود. در رابطه با ساختار اتصال کامپیوترها در فصل 1 کتاب شبکه‌های مبتنی بر سیسکو صحبت کرده‌ایم.



شکل 6- 1

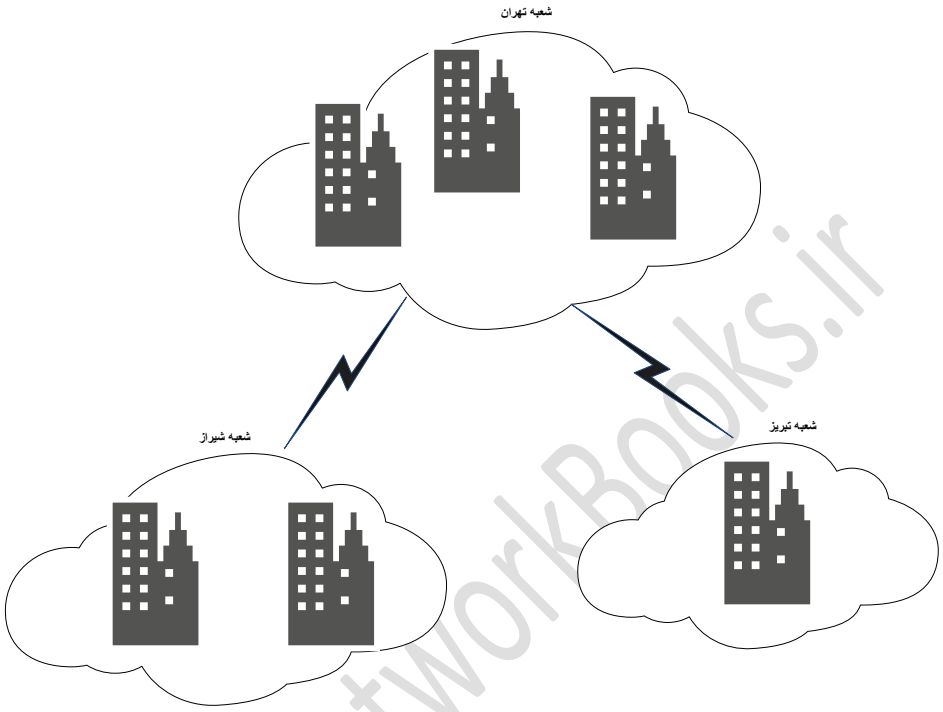
شبکه‌های گسترده یا WAN

زمانی که چند LAN را که از همدیگر دارای فاصله جغرافیایی هستند به‌هم متصل کنید در واقع یک WAN یا شبکه گسترده ایجاد کرده‌اید.

به دقت کنید فرض‌کنید شرکت زرافه دارای سه شعبه در ایران می‌باشد، شعبه‌های شرکت در تهران، تبریز و شیراز می‌باشد. که از اتصال این سه شعبه به‌هم یک WAN ایجاد شده است.

معمولاً ارتباط بین شبکه‌های LAN به‌وسیله یک شرکت مخابرات یا ISP فراهم می‌شود و شرکت

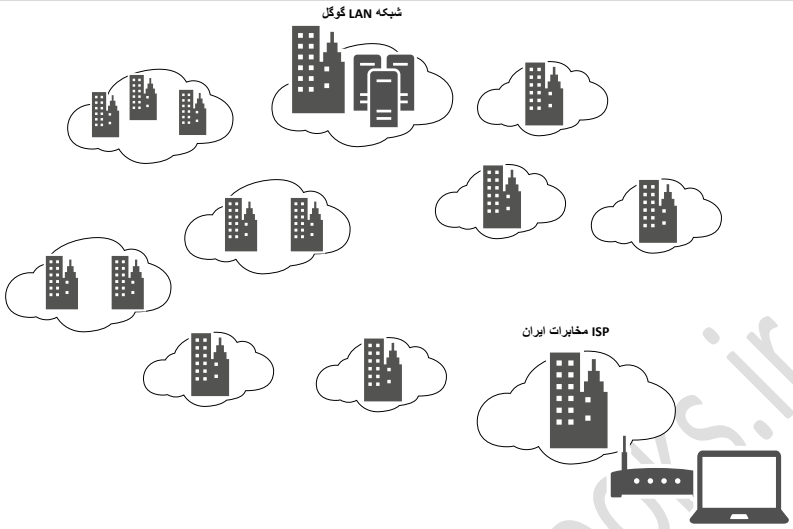
زرافه بابت اتصالی که مخابرات بین شعبه‌هایش ایجاد کرده است هزینه‌ای به مخابرات پرداخت می‌کند. سرعت لینک‌های WANمعمولاً خیلی کمتر از ارتباطات درون LAN است.



شکل 6 - 2

شبکه اینترنت Internet

به شکل 6- 3 دقت کنید، فرض‌کنید تمام LANهای روی کره‌زمین در شکل قراردارند که به این شبکه خیلی‌بزرگ اصطلاحاً اینترنت گفته‌می‌شود. اتصال شما به اینترنت به این‌صورت اتفاق می‌افتد که شما هم به‌وسیله یک مودم DSL به شبکه محلی ISP متصل شده‌اید و درواقع به تمام LANهای کره‌زمین دسترسی خواهید داشت.



شکل 6- 3

شبکه خصوص مجازی یا VPN

شرکت‌ها از اینترنت برای ارائه سرویس‌های عمومی استفاده می‌کنند به‌عنوان مثال گوگل سرویس‌های ایمیل، موتور جستجو، نقشه و ... را در اختیار عموم قرار می‌دهد یا دانشگاه تهران سایت خودش را در اختیار عموم قرار می‌دهد. همان‌گونه که قابل برداشت است بستر اینترنت کاملاً عمومی بوده و تمامی افراد خواهند توانست به ترافیک‌های ردوبدل شده بین شبکه‌ها دسترسی داشته باشند و این موضوع برای شرکت‌هایی که می‌خواهند اطلاعات خصوصی خود را بین شعبه‌هایشان ردوبدل کنند خوشایند نیست، بنابراین شبکه‌ای با نام "شبکه خصوصی مجازی" (یا VPN) ایجاد شد.

"شبکه خصوصی مجازی" (یا VPN) چیست؟ فرض کنید که شرکت زرافه برای ارتباط بین دفاتر خود از شبکه اینترنت استفاده می‌کند و سه شعبه‌اش را به یکدیگر متصل می‌کند و سپس برروی بستر اینترنت یک شبکه خصوصی‌مجازی ایجاد کرده و تمام ترافیک‌های بین دفاتر خود را رمزنگاری می‌کند. بنابراین اگر در بستر اینترنت اطلاعات این شرکت به دست کسی برسد، به‌صورت رمزگذاری شده بوده و قابل استفاده نیست.

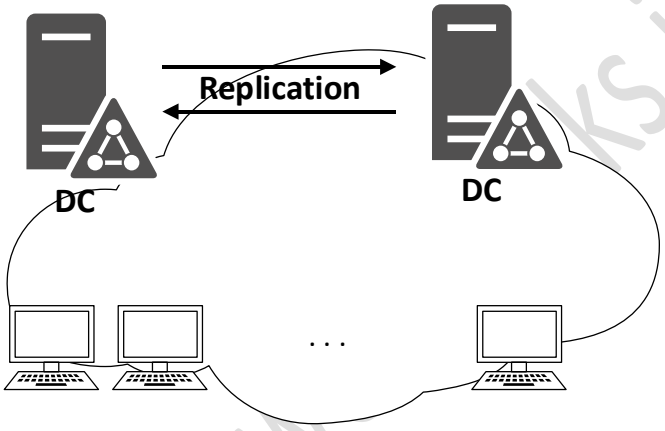
Replication Active Directory

همان‌گونه که از قبل می‌دانید AD محل ذخیره‌سازی اشیاء و ویژگی‌های آن‌ها می‌باشد.

در یک شبکه کاربران نیاز دارند که از منابع شبکه مثل فایل، پرینتر و ... که به اشتراک گذاشته‌شده

است استفاده کنند، در شبکه های بزرگ این منابع توسط AD یا همان Active Directory مدیریت می‌شوند. Active Directory به‌عنوان یک سیستم مرکزی (یا پایگاه داده) درنظر گرفته شده که قابل گسترش و توزیع است.

در شبکه‌های کوچک حداقل نیاز به دو سرور DC می‌باشد چراکه اگر یکی از سرورها دچار مشکل شد، شبکه با اختلال مواجه نشود. همچنین درصورت ازدیاد کلاینت‌ها نیاز است تا دو سرورAD وجود داشته باشد تا به درخواست‌های کاربران پاسخ دهند و این باعث افزایش سرعت می‌شود.

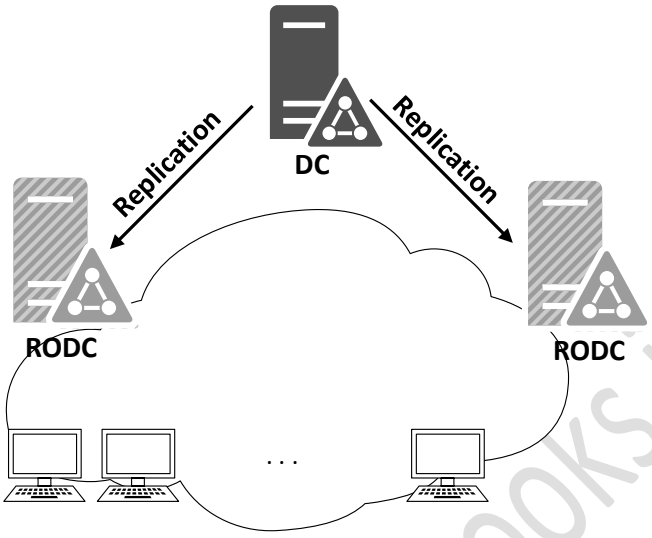


شکل 6- 4

در حالت‌های گفته‌شده نیاز است تا اطلاعات هردوسرور DC با یکدیگر همگام شود که برای این کار نیاز است تا پروسه Replication بین هردوسرور صورت پذیرد. زمانی که در هر سرور تغییراتی اتفاق بیفتد بلافاصله در دیگر سرور DC این تغییرات اعمال خواهد شد.

افزایش امنیت

گاهی اوقات به‌منظور افزایش امنیت سرویسAD ، از دو سرور استفاده می‌شود که یکی سرورDC و دیگری به‌عنوان سرورDC از نوع فقط‌خواندنی با نام RODC (یا Read Only Domain Controller) می‌باشد. ازاین‌رو تنها سرور RODC در معرض کاربران قرار داده می‌شود تا درصورت وجود هکر یا ویروسی که قصد نفوذ در سرور را داشته باشند نتوانند اطلاعاتی را تغییر دهند و یا پاک کنند چراکه ماهیت این سرور از نوع فقط‌خواندنی می‌باشد. توجه داشته باشید که RODC تنها اصلاحات خود را از DC اصلی دریافت می‌کند.



شکل 6- 5

با توجه به شکل 6- 5 فرآیند Replication زمانی صورت می‌پذیرد که سرورDC اصلی، اطلاعات خودش را با سایر RODCها یکسان‌سازی نماید.

توجه داشته باشید که DCها از لحاظ بعد جغرافیایی محدودیتی ندارند و می توانند خیلی نزدیک به هم و یا خیلی دور ازهم باشند. خواه خط ارتباطی بین DCها 1GB باشد یا 56kbps، در هرصورت عملیات Replication به‌منظور برقراری انسجام اطلاعات باید انجام شود.

مفهوم Active Directory Site

مفهوم سایت در Active Directory ساختار فیزیکی و توپولوژی شبکه می‌باشد. Active Directory از اطلاعات سایت استفاده می‌کند تا محل ذخیره‌سازی اشیاء و اتصال‌های بین شبکه فیزیکی را تشخیص دهد و هر شئ را در سرور Active Directory نزدیک به محل فیزیکی خود قرار دهد. با استفاده از کنسول Active Directory Site and Services می‌توان سایت‌ها و چگونگی اتصال بین آن-ها را تعریف کرد.

یکی از مهمترین مسائلی که هنگام پیاده ساختار یک سیستم Active Directory باید به آن توجه کرد جداسازی اجزاء منطقی و فیزیکی است.

در حالت معمول از AD (یا سرویس دامنه) برای دسته‌بندی منطقی اشیاء و منابع شبکه استفاده می‌شود، به‌عنوان‌مثال از AD برای دسته‌بندی اشیاء OU، کاربران و گروه‌ها استفاده شده و از Active Directory Site and Services برای دسته‌بندی ساختار فیزیکی شبکه مانند کامپیوترها و شیوه

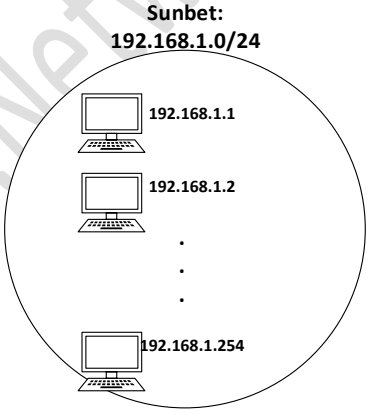
اتصال آن‌ها و لینک ارتباطی بین آن‌ها استفاده خواهیم کرد.
توجه داشته باشید که ارتباط مشخصی بین سرویس دامنه و سرویس سایت وجود ندارند بلکه سرویس دامنه از مفهوم سایت جهت اتصال به اجزاء فیزیکی استفاده می کند.
به صورت کلی یک سایت می‌تواند ترکیبی از چند Subnet باشند که به یکدیگر متصل شده است، و یک دامنه می تواند در چندین سایت توزیع شده باشد و همچنین یک سایت می تواند دارای چندین دامنه باشد.

سایت Site

در AD سایت مجموعه‌ای از کامپیوترها بوده که درون یک شبکه LAN یا Campus با سرعت بالا به هم متصل شده‌اند و این سایت می‌تواند شامل یک یا چند زیرشبکه باشد.

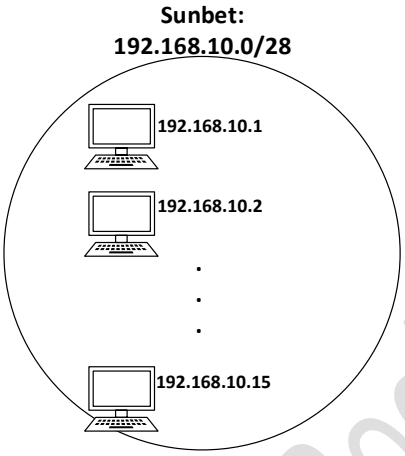
زیرشبکه یا Subnet

زیرشبکه یک تقسیم‌بندی براساس آدرس IP می‌باشد. درواقع مجموعه کامپیوترهایی که دارای آدرس شبکه یکسان هستند در یک زیرشبکه قرار دارند، به‌عنوان مثال:
در شکل 6- 6 یک زیرشبکه با آدرس شبکه 192.168.1.0/24 قابل مشاهده است که درکل می‌تواند 254 آدرسIP برای دستگاه‌ها فراهم آورد.



شکل 6- 6

در شکل 6- 7 یک زیرشبکه با آدرس شبکه 192.168.10.0/28 قابل مشاهده است که درکل می‌تواند 14 آدرس IP برای دستگاه‌ها فراهم آورد.

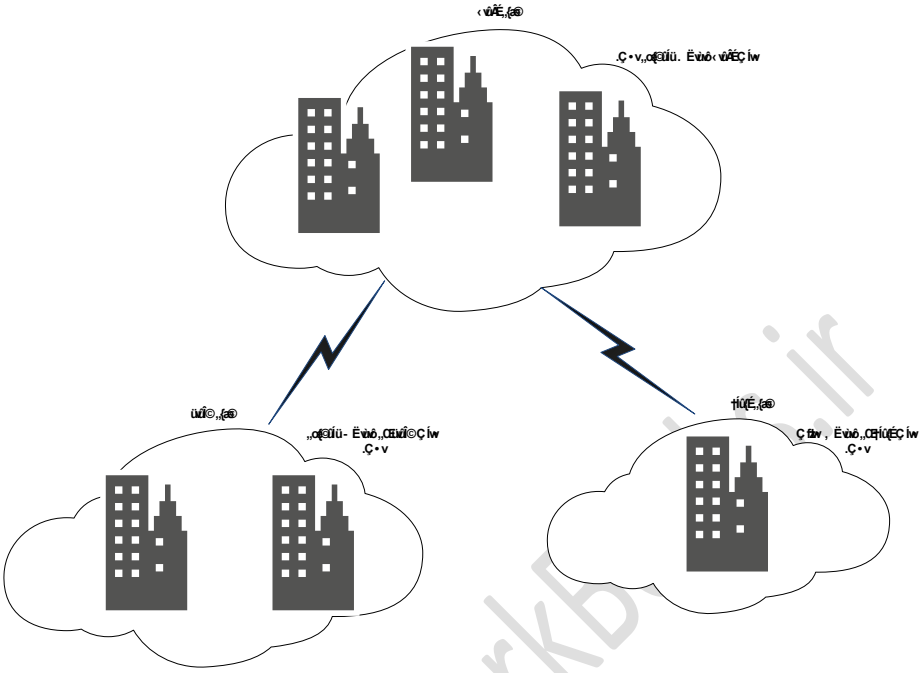


شکل 6- 7

برای آشنایی بیشتر با آدرس‌هایIP، فصل TCP/IP جلد اول از همین کتاب را بررسی نمایید.
در شبکه LAN پس از پیاده‌سازی ساختار دامنه باید زیرشبکه‌ها و سایت‌ها را شناسایی و ایجاد کنید.

درک مفهوم Subnet، Site و Domain

برای درک بهتر این مفاهیم Subnet، Site و Domain به مثال شرکت زرافه که داری سه شعبه در شهرهای مختلف است توجه کنید.
این شرکت در تهران دارای یک شبکه LAN یا همان Site بوده و دارای 3 زیرشبکه است. در شیراز دارای یک Site بوده و درون آن سایت 2 زیرشبکه قرار دارد و در تبریز دارای یک Site و درون سایت 1 زیرشبکه وجود دارد.



شکل 6 - 8

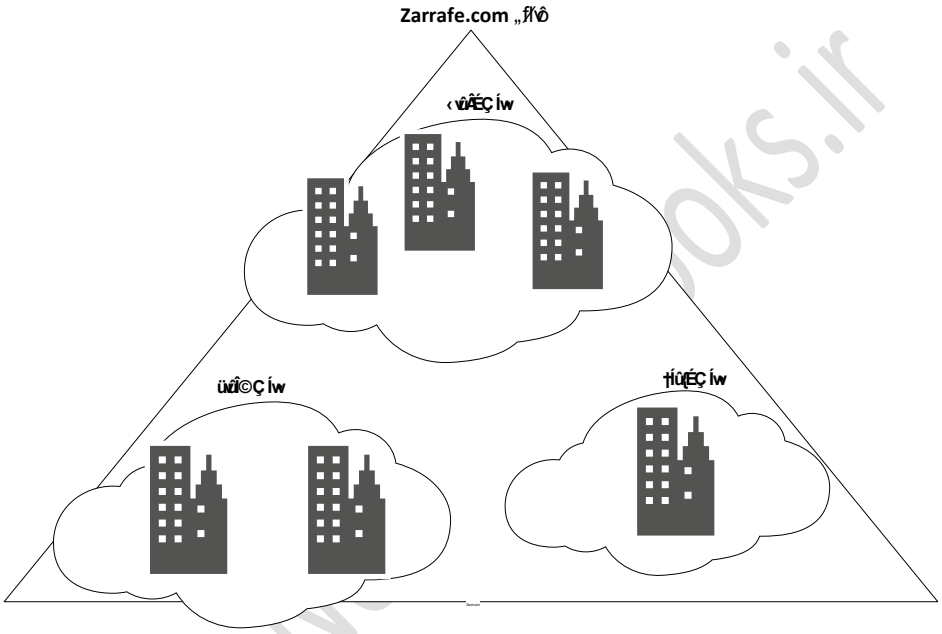
در ساختار Active Directory، site نقشه فیزیکی شبکه شما را مشخص می‌کند در حالی که Domain نقشه منطقی یا ساختار مدیریتی سازمان شما را مشخص می‌کند.

جدایی بین ساختار فیزیکی و منطقی مزیت‌های زیر را دارد:

- نگهداری و مدیریت ساختار فیزیکی و منطقی کاملاً بی‌نیاز ازهم می‌شود.
- می‌توان چند دامین درون یک سایت ایجاد کرد.
- می‌توان یک دامین را برای چند سایت ایجاد کرد.

چندین سایت درون یک دامنه

در مثال بعد برای هر سه شعبه شرکت زرافه یک دامنه تعریف کرده‌ایم. یعنی از لحاظ فیزیکی سه سایت وجود دارد اما از لحاظ منطقی مدیریت آن‌ها تحت یک دامنه با نام Zarrafe.com انجام خواهد شد.



شکل 6- 9