
- **SUBNETTING**

زمانی که میخواهیم عملیات subnetting را بر روی یک ای پی انجام دهیم باید پنج سوال زیر را مد نظر داشته باشیم

۱.چه مقدار subnets میتوانیم داشته باشیم
۲.چه مقدار هاست در هر subnet موجود می باشد
۳.چه subnet هایی قابل قبول هستند
۴.تعیین broad cast address
۵.چه هاست هایی قابل قبول است

در IP 192.168.10.10 و subnet mask 255.255.255.0 میخواهیم ۵۵ هاست (دستگاه) به هم شبکه کنیم ,عملیات subnetting به قرار زیر می باشد

به دلیل اینکه IP ما در کلاس C میاشد عملیات subnetting را در بیت آخر انجام میدهیم و آن را بسط میدهیم

192.168.10.2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

با توجه به اینکه ۵۵ هاست میخواهیم و ۵۵ بین ۶۴ و ۳۲ است ۲^۶ را انتخاب میکنیم در نتیجه ۶ بیت به host address تعلق میگیره و ۲ بیت به network address

(2^0=1 , 2^1=2 , 2^2=4 , 2^3=8 , 2^4=16 , 2^5=32 , 2^6=64 , 2^7=128 , 2^8=256)

۱.چه مقدار subnet میتوانیم داشته باشیم

برای بدست آوردن تعداد subnet از فرمول زیر استفاده میکنیم,n تعداد بیتهای تعلق گرفته به قسمت network address است

2^n ---> 2^2=**4**

۲.چه مقدار هاست در هر subnet موجود میباشد

برای بدست آوردن هاست از فرمول زیر استفاده میکنیم

2^n-2 ----> 2^6-2=**62**

در هر subnet شصت و دو هاست موجود میباشد و ۲- همان network address و broad cast address میباشد که not valid هستند

۳.چه subnet هایی قابل قبول هستند

برای بدست آوردن subnet های قابل قبول (block size)از فرمول زیر استفاده میکنیم

256 - subnet mask = **block size**

با توجه به اینکه الگوی استاندارد را به الگوی غیر استاندارد تبدیل کردیم subnet mask به غیر استاندارد تبدیل میشود و به آن (**CSN** (Customize Subnet Mask میگوییم

طریقه بدست آوردن آن به اینصورت است که بیتهایی را که به network address در بیت آخر تعلق دارد را جمع میکنیم

2^7 + 2^6 = 128+64 = **192** ---> **CSN**

256 - 192 = **64** --> **Block size**

۴.تعیین broad cast address برای هر subnet

پیامی است که به تمامی ایستگاهها توزیع میشود

این آسانترین قسمت است , broad cast address در هر subnet میشود block size - 1 مثلا اگر block size ما ۶۴ باشد broad cast ما میشود ۶۳ و بطور کامل میشود ۱۹۲.۱۶۸.۱۰.۶۳

۵.چه host هایی قابل قبول است

همیشه اعدادی که بین subnet address و broad cast address می باشند هاستهای قابل قبول هستند

با توجه به عملیات بالا subnetting به قرار زیر می باشد

network address	**192.168.10.0**	**192.168.10.64**	**192.168.10.128**	**192.168.10.192**
Valid IP	192.168.10.1	192.168.10.65	192.168.10.129	----------
	192.168.10.2	192.168.10.66	192.168.10.130	
	ادامه	ادامه	ادامه	
	ادامه	ادامه	ادامه	
	192.168.10.62	192.168.10.126	192.168.10.190	
broad cast address	**192.168.10.63**	**192.168.10.127**	**192.168.10.191**	
customize subnet mask	**255.255.255.192**	**255.255.255.192**	**255.255.255.192**	**255.255.255.192**

۲.۲. شبکه Workgroup و Domain

در workgroup برای اینکه بتوان از جای دیگر به سیستم دسترسی داشت باید نام کاربری روی آن سیستم نیز تعریف شده باشد در کل مدیریت هر سیستم به همان سیستم وابسته است.
مثلا اگر ۲۰ تا سیستم داشته باشیم و ۲۵ کاربر که جای آنها ممکن است تغییر کند باید هر کاربر برای وارد شدن به هر سیستم یک usernameروی همان سیستم تعریف کرده باشد تا بتواند وارد سیستم شود، ولی در domain تمامی username های کاربران روی یک سیستم تعریف می گردد و آن سیستم مسئول کنترل کاربران و منابع شبکه می باشد.
مزیت هم همین که بتونی کل سیستمها رو به شکل متمرکز کنترل کنه و بتونی برای رفتار و کار کاربرانت تصمیم بگیری بهترین مزیت می باشد.

امنیت domain خیلی بیشتر از work group و هر کسی نمی تواند به گروه متصل شده و از اطلاعات استفاده کند.

با توجه به نحوه پیکربندی کامپیوترها در شبکه و نحوه دستیابی به اطلاعات ، شبکه ها را به دو گروه عمده تقسیم می شوند:

Workgroup و Domain:

در شبکه های Workgroup،سرویس دهنده اختصاصی وجود نداشته و سلسله مراتبی در رابطه با کامپیوترها رعایت نمی گردد. تمام کامپیوترها معادل و همتراز می باشند. هر کامپیوتر در شبکه هم بعنوان سرویس گیرنده وهم بعنوان سرویس دهنده ایفای وظیفه می کند. امنیت بصورت محلی و بر روی هر کامپیوتر ارائه می گردد . کاربر هر یک از کامپیوترها مشخص می نماید که چه داده ئی بر روی کامپیوتر خود را می بایست به اشتراک قرار دهد. برای مدیریت بیش از ۱۰ کامپیوتر استفاده از Workgroupمنطقی نیست و باید از دومین استفاده کرد.

Domain:

Domain ، یک گروه بندی منطقی از کامپیوترهای شبکه ای است که از یک محل مشترک بمنظور ذخیره سازی اطلاعات امنیتی ، استفاده می نمایند. استفاده از Domain ، تمرکز در مدیریت منابع شبکه را بدنبال خواهد داشت . بدین ترتیب پس از ورود کاربران به شبکه و تائید صلاحیت آنان ، زمینه استفاده از منابع به اشتراک گذاشته شده در سایر کامپیوترهای موجود در Domain ، با توجه به مجوزهای تعریف شده ، فراهم می گردد هر Domain توسط Contllore Domain ، مدیریت می گردد. بمنظور تسهیل در مدیریت چندین Domain ، می توان Domain ها را در ساختارهائی با نام درخت (Tree) و جنگل (Forest) ، گروه بندی کرد .

درخت (Tree) در Domain:

درخت، یک سازماندهی سلسله مراتبی از Domain های ویندوز ۲۰۰۰ بوده که یک نام را به اشتراک می گذارند . زمانیکه یک Domain به یک درخت موجود اضافه می گردد، بعنوان یک subDomain ، در نظر گرفته می شود. SubDomain ، یک Child domain نیز نامیده شده و Domain اضافه شده از طریق Parent domain مربوطه شناخته می گردد .

پس از اینکه Child Domain به درخت ملحق گردید نام Domain آن به نام Domain parent اضافه می شود. مثلا" زمانیکه یک Domain با نام Tehran به یک درخت موجود ملحق و بعنوان یک Chid Domain از Domain با نام Citys.com مطرح گردد ، نام

Domain مربوطه، بصورت Tehran.Citys.com خواهد بود.

جنگل (Forest) در Domain :

جنگل، شامل گروهی از درخت ها بوده که در مقابل استفاده از یک نام مشترک، از یک پیکربندی مشترک استفاده می نمایند. بمنظور مراجعه به جنگل ، بصورت پیش فرض از نام ریشه درخت و یا اولین درختی که در جنگل ایجاد می گردد ، استفاده می گردد . مثلا" در صورتیکه Citys.com اولین Domain در اولین درخت باشد و درخت دیگر به آن ملحق تا یک جنگل را ایجاد نمایند نام، جنگل Citys.com خواهد بود.

Domain Contllore :

کامپیوتری که برروی آن سرویس دهنده ویندوز ۲۰۰۰ اجراء و مدیریت Domain را برعهده می گیردDomain Contllore نامیده می شود .

Domain Contllor، تمام عملیاتی امنیتی مرتبط با کاربران و Domain را مدیریت می نماید.

اکتیو دایرکتوری (Active Directory):

Active Directory ، سرویس دایرکتوری ویندوز ۲۰۰۰ است . Active Directory ، اطلاعات مربوط به اشیاء شبکه را ذخیره و با ارائه یک ساختار سلسله مراتبی، زمینه سازماندهی Domain ها و منابع را بسادگی فراهم می نماید . بدین ترتیب کاربران بسادگی قادر به مکانیابی منابع شبکه نظیر فایل ها و چاپگرها ، خواهند بود Active Directoryدارای ویژگی های متعددی است :

Active Directory ، باعث سازماندهی دایرکتوری به بخش هائی خواهد شد که امکان ذخیره سازی حجم بالائی از اشیاء را فراهم می آورد . دستاورد ویژگی فوق ، توسعه Active Directory ، همزمان با رشد یک سازمان ، خواهد بود. بدین ترتیب، امکان رشد شبکه ای با صرفا" یک سرویس دهنده و کمتر از یکصد شی به شبکه ای با هزاران سرویس دهنده و میلیون ها شی فراهم خواهد شد .

Active Directory ،یک مکان متمرکز بمنظور جمع آوری و توزیع اطلاعات در رابطه با اشیاء موجود در شبکه شامل کاربران، گروهها و چاپگرها بوده و امکان یافتن و استفاده از اطلاعات را آسان خواهد کرد.

تدابیر امنیتی در ارتباط با Active Directory ، پیش بینی و زمینه تحقق آن با استفاده از Log on و کنترل دستیابی به اشیاء موجود در دایرکتوری، فراهم می گردد . پس از فرآیند ورود به شبکه (یک log on به یک شبکه) ، مدیران شبکه قادر به مدیریت داده ها ی موجود در دایرکتوری می گردند . کاربران تائید شده نیز امکان دستیابی به منابع موجود درشبکه را از هر مکانی بدست خواهند آورد.

مقایسه شبکه دامین و شبکه گروهی (Workgroup & Domain):

معایب:

۱- هزینه بالا جهت مدیریت (حقوق بالا برای مدیر شبکه):

دامین: مدیر شبکه دامین فردی دانا و با علم اطلاعات و تجربه است بنابراین حقوق بالایی دریافت میکند.

گروهی: مدیریت این شبکه اطلاعات بسیار کمی نیاز دارد در نتیجه حقوق پایینی دارد.

۲- هزینه جهت خریداری کردن سرور:

دامین: باید تعدادی کامپیوتر بطور اختصاصی جهت سرویس دهی در شبکه تهیه شوند.

گروهی: چون هیچ کامپیوتری بطور اختصاصی سرویسی تحت شبکه ارائه نمیکند لذا نیازی به سرور نیست.

۳- هرینه جهت طراحی و پیاده سازی دامین:

دامین: نیاز به دانش مهندسی و فنی بالایی دارد لذا هزینه طراحی و پیاده سازی بالاست.

گروهی: نیاز به دانش کم و ابتدایی دارد لذا هزینه طراحی و راه اندازی کم است.

مزایا :

۱- نگه داری اطلاعات کاربران و موجودات شبکه بطور متمرکز:

دامین: کلیه اطلاعات کاربران مثل اسم و رمز و شماره تلفن و آدرس و غیره بطور متمرکز نگه داری میشوند و به همین دلیل قابلیت backup گیری و دسترسی سریع و مدیریت متمرکز را دارند.

گروهی: اطلاعات بطور پراکنده بر روی هر سیستم وجود دارد که علاوه بر امنیت بسیار ضعیف، قابلیت backup گیری تا حد زیادی مشکل و شاید غیر قابل انجام میشود و قابلیت مدیریت متمرکز را ندارد.

۲- مقیاس پذیری (Scalability):

دامین: به دلیل متمرکز بودن اطلاعات و مدیریت میتواند تعداد بسیار زیادی موجود مختلف را خود جا دهد و مدیریت کند.

گروهی: به دلیل پراکندگی اطلاعات توصیه میشود تعدا کاربران این نوع شبکه از ۱۰ عدد بیتشر نشود چون قابل مدیریت نیست.

۳- توسعه پذیری (Extensibility):

دامین: میتواند اشیا جدیدی را تعریف کرد (به جز اونهایی که بصورت پیش فرض تعریف شدند) و از آنها تحت شبکه استفاده کرد.

گروهی: فقط از اشیای تعریف شده میتوان استفاده کرد.

۴- قابلیت مدیریت (Managebility):

دامین: به دلیل تمرکز اطلاعات و مدیریت، میتوان به راحتی شبکه را در جهت هدف خاصی به پیش برد. مثلا در جهت ارتقای امنیت میتوان شبکه را هر هفته به قابلیت امنیتی جدیدی تجهیز کرد.

گروهی: به دلیل عدم تمرکز اطلاعات، مدیریت در حد حفظ وضعیت انجام می شود. مدیریت در جهت رسیدن به اهداف خاص وجود ندارد.

۵- یکپارچگی با DNS:

دامین: به دلیل هماهنگی با سیستم DNS به راحتی میتوان در شبکه به سرویس های مختلف دسترسی پیدا کرد. بر اساس ترتیب اسمی به حالت شاخه ای میتوان از بالا دستی ها، آدرس پایین دستی ها را گرفت.

گروهی: قابلیت دسترسی به دیگر موجودات شبکه بسیار ضعیف است مگر اینکه کاربر مقصد خود را با نام یا شماره IP بشناسد چون سیستم شاخه ای وجود ندارد و هیچ سرویسی آدرس دیگر اشیا شبکه را نمیداند.

۶- قابلیت مدیریت فعالیت کاربرها و کامپیوترها بطور متمرکز:

دامین: میتوان سطح فعالیت و دسترسی موجودات شبکه را در کل شبکه بصورت متمرکز تعریف کرد.

گروهی: حداکثر میتوان دسترسی کاربر را در کامپیوتر خودش تعریف کرد. تحت شبکه این امکان وجود ندارد.

۷- سیاست پذیری (system Policy based):

دامین: میتوان با اعمال سیاست های مختلف تحت شبکه، شبکه را در جهت هدف خاصی پیش برد.

گروهی: اعمال سیاست فقط در حد یک کامپیوتر تعریف میشود و نه تحت شبکه.

۸- قابلیت تبادل اطلاعات بین سرورها در سطح شبکه های بزرگ:

دامین: اطلاعات بین سرورهای مختلف رد و بدل میشود لذا کلیه سرورها با آخرین تغییرات شبکه آشنا هستند و سرویس به روز ارائه میشود. مثلا کاربر تازه وارد به محض ورود، توسط کلیه سرورها قابل شناسایی و اهراز هویت است لذا میتواند به محض ورود از کلیه سرویسها استفاده

کند.

گروهی: هیچ اطلاعاتی جابجا نمیشود زیرا اصولا سروری وجود ندارد. به همین دلیل کاربر تازه وارد مجبور است برای درخواست هر سرویس از طرف مدیر شبکه به آن سرویس معرفی شود.

۹- انعطاف پذیری در امنیت و تعیین هویت موجودات شبکه:

دامین: قابلیت شناسایی هر موجودی در هرجایی از شبکه را دارد و میتواند با مدل ها و روش های مختلف اهراز هویت کند (Security Protocols).

گروهی: هر کامپیوتر فقط قابلیت شناسایی موجودی را دارد که در همان کامپیوتر تعریف شده باشد.

۱۰- امنیت یکپارچه و گسترده:

دامین: با ورود به دامین، برخی مسائل امنیتی بطور پیش فرض اعمال میشوند و در ادامه مدیر میتواند امنیت شبکه را تا حد غیر قابل تصوری بال ببرد.

گروهی: به دلیل نبود مدیریت و اطلاعات بطور متمرکز قابلیت امنیتی در حد ابتدایی و ضعیف و منحصر به هر کامپیوتر تعریف میشود (امنیت در حد کاربر خانگی!).

۱۱- قابلیت تبادل اطلاعات بین سرویس های ثالث تحت سیستم تبادل اطلاعات دامین (امنیت-راحتی):

دامین: چنانچه از سرویس یا نرم افزاری استفاده کنید که قابلیت ادغام با Active Directory partition را داشته باشد، میتوانید بطور بسیار امن و سریع، اطلاعات آن نرم افزار را همراه با اطلاعات ActiveDirectory بین سرورها جابجا کنید.

۱۲- قابلیت اتصال و برقراری ارتباط با دیگر ActiveDirectory از جنس دیگر:

دامین: به دلیل اینکه Win 2003 ActiveDirectory برا اساس LDAP ver3 و NSPI که استاندارد جهانی هستند نوشته شده، میتواند با ActiveDirectoryهایی که بر این اساس نوشته شده اند ارتباط برقرار کند. حتی اگر این ActiveDirectory ها توسط شرکتی غیر از خود مایکروسافت نوشته شده باشد.

۱۳- نشانه گذاری دیجیتالی اطلاعات تبادلی:

دامین: اطلاعات بصورت رمز شده بین سرورها جابجا میشود لذا دارای امنیت بسیار مطلوبی است

گروهی: اطلاعات بین سرورها جابجا نمیشود.

البته در مقایسه سیستم Domain و Workgroup میتوان موارد شماره ۹/۶/۴/۲/۱ را در نظر گرفت. بقیه موراد تقریبا از مشخصات اختصاصی Windows 2003 Active Directory هستند.

شرایطی که می توان تحت عنوان موارد استفاده از مدل شبکه ایی Domain نامبرده شوند عبارتند از:

نیاز به یک مدیر شبکه برای پیاده سازی این بستر می باشد.

می توان تمامی قابلیت های شبکه ایی و سرویس ها را در حد بالاو پیشرفته ایی دربستر فوق اجرا نمود.

امکان به وجود آمدن مدیریت متمرکز Centralized)) برای تمامی منابع شبکه و کاربران.

امکان تدوین سیاست های دسترسی به منابع و سرویس های شبکه برای تمامی کاربران در دامین.

به وجود آوردن سطح بالایی از امنیت اطلاعات و ارتباطات برای تمامی کاربران و کامپیوترهای داخل دامین.

مشخص کردن نحوه دسترسی به اینترنت، چگونگی استفاده و نظارت بر آن.

فصل سوم

آشنایی با سرویس های متداول

۳.۱ نصب Active directory

ابتدا در run کامند dcpromo را تایپ کرده و اینتر میکنیم