به نام خدا

دانشگاه کردستان

گروه مهندسی کامپیوتر و فناوری اطلاعات

درس آزمایشگاه شبکه

تهیه:

صادق سلیمانی

< ویرایش دوم >

پاییز ۸۹

فهرست

پیشگفتار

شبکه‌های کامپیوتری از معدود دروسی است که مفاهیم نظری و عملی آن به هم آمیخته است. آشنایی با مفاهیم فنی و عملی مرتبط با شبکه با تنوع مکفی، علاوه بر کمک به درک آموخته‌های کلاسی، سبب آمادگی برای انجام پروژه‌های حرفه‌ای و ورود به باز کار می‌شود. همچنین زمینه شرکت در دوره‌های تأییدیه‌ی شرکت‌هایی مانند مایکروسافت و سیسکو (از قبیل MCSE و CCNA) و کسب مدارک معتبر این شرکت‌ها نیز فراهم خواهد شد.

این مستند که بر اساس تجربیات عملی مؤلف در سمت کارشناس، مدیر و مشاور شبکه در شرکت‌های خصوصی آسانرم‌افزار و ردان سیستم و مدیریت فناوری دانشگاه کردستان تدوین گردیده است، حول سه محور اساسی زیر از مدل TCP/IP بنا شده است:

- فراگیری خدمات لایه‌ی کاربرد بر اساس سیستم عامل Windows 2003 شرکت مایکروسافت و با کمک نرم‌افزار شبیه‌ساز Microsoft Virtual PC
- فراگیری خدمات زیرساخت لایه‌های حمل، شبکه و تا حدی میزبان به شبکه[1] بر اساس Cisco CLI[2] با کمک شبیه‌ساز Cisco Packet Tracer
- فراگیری بخشی خدمات لایه‌ی میزبان به شبکه با عنوان کابل‌کشی ساختیافته بر اساس آموزه‌های شبکه Bicsi بر اساس استانداردهای EIA/TIA

از طرفی در دوره‌ی کارشناسی مهندسی فناوری اطلاعات، درس آزمایشگاه شبکه با محدودیت‌های مهمی روبرو است که باید در تدوین مستندی بدین منظور، مد نظر قرار گیرد تا بهره‌وری هرچه بیشتری برای دانشجویان به همراه داشته باشد. به عنوان مثال زمان ارائه برای چنین درسی یک واحد عملی معادل با دو ساعت در نظر گرفته شده است که مجال عرضه‌ی بسیاری مفاهیم به صورت پیوسته را محدود می‌نماید. اما در دانشگاه کردستان، ساعات اختصاصی به هر آزمایش، به سه ساعت افزایش یافته و آزمایش‌ها نیز متناسب با همین تعداد ساعت تدوین شده است. همچنین اشتراک کامپیوترهای مورد استفاده برای آزمایشگاه شبکه با سایر دروس در بسیاری از دانشگاه‌ها و عدم امکان تأمین تجهیزات گران‌قیمت مربوط به شبکه به خصوص در بحث زیرساخت، ممکن است امکان تغییرات مهم و سیستمی مرتبط را از دانشجویان

[1] Host to Network، پایین‌ترین لایه در مدل TCP/IP

[2] Command Line Interface

سلب نماید. خوشبختانه ظهور شبیه‌سازهای کارآمد، در زمینه‌های مختلف شبکه، امکان انجام و فراگیری بسیاری از آزمایش‌ها را علیرغم محدودیت‌های اشاره شده، فراهم نموده است.

تنوع مسایل موجود در حیطه‌های مختلف شبکه، امکان انجام ده‌ها آزمایش را میسر کرده است، اما با توجه به محدودیت زمانی و تعداد تقریبی ده جلسه برای آزمایش‌های هر ترم، یازده آزمایش مدون شده است و در صورت کمتر بودن تعداد جلسات، مربی مختار است آزمایش‌های آخر را حذف نماید. بر کسی پوشیده نیست که به دلیل شرایط خاص حق کپی[1] در ایران، پرطرفدارترین و پرکاربردترین سیستم‌عامل مورد استفاده، نسخه‌های مختلف سیستم‌عامل ویندوز محصول شرکت مایکروسافت است. همچنین بیشترین تجهیزات مورد استفاده در زیرساخت برای مسیریاب‌ها و سوییچ‌ها، از محصولات شرکت سیسکو هستند. از این‌رو جهت تسهیل و تسریع آزمایش‌ها و استفاده‌ی حداکثری از آن‌ها در خارج از محیط آزمایشگاه، بر این فناوری‌ها بیشتر تأکید شده است.

۱-۱- نسخه الکترونیکی کتاب و راهنمای مربی

نسخه‌ی الکترونیکی این مستند از طریق ایمیل قابل عرضه است و مؤلف، پیشاپیش از نظرات و پیشنهادات ارسالی شما به آدرس ایمیل info@ITVirtualLab.com استقبال می‌نماید. خواهشمند است ایمیل‌های خود را تحت عنوان LAN-Lab Manual ارسال نمایید.

همچنین نسخه‌ی راهنمای مربی برای اساتید محترمی که قصد استفاده از این مستند را به عنوان مرجع یا کمک درسی در نظر دارند، در حال آماده شدن است و ایشان در صورت تمایل می‌توانند در ایمیلی با عنوان LAN-Lab Manual Guide، راهنمای مذکور را دریافت دارند.

[1] Copy Right

۱-۲- برنامه‌درسی

برای برگزار شدن هرچه بهتر این درس و دستیابی به اهداف آموزشی مورد نظر آن، موارد زیر پیشنهاد می‌شود. لازم به ذکر است پیشنهادهای مذکور بر اساس تجربه عملی برگزاری درس و گرفتن بازخوردهای مثبت، تدوین شده است:

- آزمایش‌ها در گروه‌های حداکثر سه نفره و حداقل دو نفره باید انجام شود و گروه یک نفره قابل قبول نیست.
- در صورت عدم استفاده از نرم‌افزار شبیه‌ساز، دانشجو موظف است پس از هر آزمایش در پایان ساعت، تغییرات سیستم را به حالت اول برگرداند. دانشجو مجاز نیست رمز عبور کاربر اصلی (Administrator) را در نرم‌افزارهای شبیه‌ساز تغییر دهد. این کار سبب بروز اختلال در آزمایش گروه‌های بعدی خواهد شد.
- پیش از حضور در هرجلسه باید پیش‌آگاهی آزمایش آن جلسه خوانده شود و در ابتدای کلاس از آن کوییز گرفته خواهد شد.
- به ازای هر جلسه، باید گزارش کار برای آزمایش‌هایی که دارای گزارش‌کار هستند پر شود و تحویل داده شود. دانشجویان مجاز به بردن و پرکردن گزارش کار به خارج از آزمایشگاه و یا تحویل آن در ساعاتی دیگر نیستند.
- برخی پرسش‌های تکمیلی با رعایت مهلت تعیین شده، برای تکمیل درک آزمایش‌های انجام پذیرفته، بایستی تحت عنوان تکلیف، تحویل داده شود. به خاطر اهمیت تکالیف در فهم دروس پیشین و پسین، اکیداً توصیه می‌شود، تکالیف در زمان مقرر تحویل داده شود.
- به خاطر محدود بودن تعداد جلسات آزمایشگاه، می‌توان برخی موضوعات مهم دیگر را تحت عنوان پروژه‌ی مکمل همراه با درس تعریف نمود. به عنوان مثال، بررسی و تحلیل سرآیندهای بسته‌های شبکه با نرم‌افزار تحلیل‌گر بسته WireShark می‌تواند یکی از مواردی باشد که چندین آزمایش را به خود اختصاص دهد. یا بررسی مسایل مشابه در سیستم عامل لینوکس خود می‌تواند به آزمایش‌های مختلف تقسیم شود که در صورت انجام آزمایش‌های مربوط به لینوکس در درس آزمایشگاه سیستم‌عامل، می‌توان این موضوع را به آن درس موکول نمود.
- جلسه‌ی آزمون نهایی نظری و عملی، آخرین جلسه‌ی کلاس‌ها از نظر آموزش دانشگاه است. جلسه‌ی آزمون عملی در همان ساعت کلاس و آزمون نظری به مدت نیم ساعت و به صورت هماهنگ برای تمام گروه‌هاست.

- حداکثر تعداد غیبت‌های موجه ۲ جلسه است و بیش از آن به صورت خودکار دانشجو حذف خواهد شد. جلسه‌ی پیش از آزمون نهایی، جلسه‌ی جبرانی است و دانشجویانی که یک یا دو غیبت مجاز داشته‌اند موظف‌اند، آزمایش‌های انجام نشده را در این جلسه انجام داده و گزارش‌کار مربوطه را تحویل دهند. همچنین دانشجویانی برخی آزمایش‌ها را ناقص انجام داده باشند یا در انجام برخی آزمایش‌ها پرسش یا ابهام داشته باشند، می‌توانند در جلسه‌ی جبرانی، آن را مطرح سازند.

۱-۳- سپاسگزاری

بدینوسیله از زحمات آقای محسن رمضانی دانشجوی کارشناسی مهندسی فناوری اطلاعات دانشگاه کردستان که در تهیه‌ی پیش‌نویس برخی آزمایش‌ها همکاری نمودند، تشکر می‌نمایم.

صادق سلیمانی
info@ITVirtualLab.com
دانشگاه کردستان

مهر ماه ۱۳۸۹

آزمایش اول

راه‌اندازی ساده‌ترین شبکه (Workgroup)

۲-۱- مقدمه

درس شبکه ۱ در رشته مهندسی فناوری اطلاعات به صورت هم‌نیاز با درس آزمایشگاه شبکه عرضه می‌شود، اما بهتر آن است که به عنوان پیش‌نیاز آن در نظر گرفته شود، زیرا مفاهیم متعددی در آزمایشگاه شبکه ارائه می‌گردد که تنها در جلسات آخر درس شبکه ۱ و حتی شبکه ۲ مطرح می‌شود.

بدین ترتیب در آزمایش‌های کنونی به خاطر عدم آشنایی دانشجو با برخی مفاهیم نظری پیش‌نیاز، به تشریح ساده و حتی گاهی غیر علمی آن‌ها پرداخته شده است تا در انجام آزمایش‌ها و انتقال مفاهیم، مشکلی برای دانشجو ایجاد نشود.

در راستای درس شبکه، یادگیری نحوه‌ی راه‌اندازی یک شبکه‌ی ساده‌ی محلی، مقدمات تنظیم کامپیوترها، دستورات مهم خط فرمان و ... ضروری است. آشنایی با مبانی شبکه به شیوه‌ای کاربردی، همواره از اولویت‌های مورد نظر دانشجویان در نظرخواهی‌ها بوده است.

در این جلسه هدف آن است که سریع‌ترین و آسان‌ترین راه برای راه‌اندازی یک شبکه بررسی گردد، تا هم پیش‌زمینه‌ای برای مباحث پیشرفته‌تر گردد و هم کمترین امکانات و نیازمندی‌های راه اندازی یک شبکه (بیشتر از دید نرم‌افزاری) در یک جلسه کوتاه مطرح گردد. در این جلسه استفاده از شبیه‌ساز نیاز نیست.

۲-۲- هدف

آشنایی با حداقل‌ها برای راه‌اندازی یک شبکه و آشنایی با دستورات کارای خط فرمان در زمینه شبکه

۲-۳- پیش آگاهی

کامپیوترهای مختلف در سراسر جهان برای برقراری ارتباط با هم نیاز به آدرس‌های یکتا دارند، برای درک این مطلب می‌توانید آدرس‌های یکتا را که آدرس IP[1] نامیده می‌شوند مانند شماره تلفن تصور کنید، هر دستگاه تلفن برای ارتباط با سایر دستگاه‌های تلفن در هر جای دنیا تنها کافی است که شماره آن‌ها را داشته باشد و این شماره‌ها همه یکتا هستند.

آدرس IP یک عدد چهار بایتی است که نحوه‌ی نمایش آن مشابه به x.x.x.x است که هر x بیانگر یک بایت است. یعنی می‌توان از 0.0.0.0 تا 255.255.255.255 شماره داشت (چرا؟). پس کامپیوترها برای یافتن همدیگر از آدرس IP استفاده می‌کنند، گرچه جزییات بسیار زیادی در همین وهله ممکن است در ذهن شما سبب ایجاد ابهام شوند، اما همین مقدار دانستن برای آدرس IP با توجه به آن‌چه در پایین خواهد آمد، کافیست.

البته به خاطر داشته باشید که تنها آدرس مورد استفاده در یک کامپیوتر نیست و یک کامپیوتر ممکن است از آدرس‌های متعدد یکتای دیگری استفاده کند، همانند یک فرد که علاوه بر نام دارای شماره ملی، شماره دانشجویی، شماره تلفن‌همراه و ... است. آدرس‌های مختلف در سطوح مختلف شبکه از دیدگاه مدل OSI (مدل هفت لایه‌ای برای پرداختن به مسایل شبکه) مطرح هستند، به عنوان مثال آدرس MAC که شماره یکتای هر کارت شبکه برای ارتباط سیستم‌ها در شبکه‌های محلی (LAN) است در لایه‌ی ۲ مطرح است که بر کارت شبکه حک شده است و قابل تغییر نیست. اما LANها محدود به تعداد کمی کامپیوتر هستند و برای ارتباط در سطح کل شبکه جهانی ازآدرسIP استفاده می‌شود که در مدل لایه‌ای OSI در لایه سه مطرح می‌شود و از طرف مسوول شبکه منتسب می‌شود و قابل تغییر می‌باشد. لازم به ذکر نیست که هر دوی این آدرس‌ها بایستی دست‌کم در سطح LAN یکتا باشند.

آدرس MAC، که گاهی از آن به آدرس فیزیکی نیز یاد می‌شود، از لحاظ ظاهری شش بایتی است که مقادیر بایت‌ها در مبنای هگزادسیمال نوشته می‌شود و مقادیر بایت‌ها با علامت : یا – از هم جدا می‌شوند.

[1] Internet Protocol

به عنوان مثال 0f:23:2d:11:56:90:22 یک آدرس MAC است. این آدرس برای هر کارت شبکه در سطح جهان یکتا است.

آدرس IP همانند یک شماره تلفن دارای مفهوم مشخصی است و پس از آشنایی با آن می‌توان اطلاعات مهمی را از ظاهر آن کسب نمود. به عنوان مثال شماره تلفن ۰۰۹۸۲۱۸۸۷۵۳۴۵۲ به کشور ایران تعلق دارد و شهرستان تهران و حتی می‌توان منطقه‌ی مرتبط با آن را نیز در تهران یافت. یک آدرس IP نیز دارای دو بخش است، شماره شبکه و شماره‌ی کامپیوتر در شبکه. اما برای تفکیک این دو از یک عدد کمکی دیگر به نام Subnet Mask یا الگوی زیر شبکه نیز استفاده می‌شود.

پس هر کامپیوتر در شبکه با دو عدد شناسایی می‌شود؛ آدرس IP و Subnet Mask. فعلاً و با دانش سطحی کنونی، اعداد معادل با 255های Subnet Mask در آدرس IP، تعیین کننده‌ی بخش شماره شبکه‌ی آدرس آن هستند. به عبارت ساده‌تر، هرگاه بخواهیم از روی Subnet Mask داده شده، بخش مربوط به آدرس شبکه را در آدرس IP بیابیم، بایت‌های متناظر با 255های Subnet Mask را در آدرس IP جدا می‌کنیم.[1]

بدین ترتیب دو کامپیوتر تنها در صورتی در یک شبکه LAN قرار دارند که دارای شماره شبکه یکسان باشند، همانند اینکه بگوییم دو شماره تلفن تنها در صورتی نیاز به گرفتن کد شهرستان ندارند که در یک شهرستان باشند. بخش دیگر آدرس IP که عبارت است از شماره کامپیوتر در شبکه، یکتاست تا با کامپیوتر دیگری دارای موجودیت مشترک نباشد. پس شماره شبکه کامپیوتری با آدرس IP معادل با 217.219.31.58 و الگوی زیرشبکه‌ی 255.255.255.0 برابر است با 217.219.31.0. به عنوان مثال از چهار کامپیوتر زیر، تنها PC1 و PC4 با دارا بودن آدرس شبکه‌ی 192.168.11.0 در یک شبکه هستند (چرا؟).

PC1 IP Address:192.168.11.7 Subnet Mask:255.255.255.0	**PC2** IP Address:192.168.121.7 Subnet Mask:255.255.255.0
PC3 IP Address:192.168.11.7 Subnet Mask:255.255.0.0	**PC4** IP Address:192.168.11.231 Subnet Mask:255.255.255.0

چند کامپیوتر دیگر می‌توانند در شبکه‌ایی باشند که کامپیوتر PC3 قرار دارد؟ چرا؟

[1] این تفسیر البته از لحاظ فنی و به صورت دقیق، خالی از ایراد نیست، اما برای دانشجویی با سطح دانش کنونی کفایت می‌کند.

گرچه یک کامپیوتر هم آدرس MAC و آدرس IP دارد، اما هر یک برای مقاصد مختلف استفاده می‌شوند، مانند اینکه یک فرد دارای شماره ملی و شماره دانشجویی باشد، که شماره ملی عمومیت و کاربرد بیشتری دارد. آدرس IP که توسط عامل انسانی تنظیم می‌شود برای مقاصد برقراری و تست ارتباط در سطح LAN وWAN کاربرد دارد و کاربر بیشتر با آن کار می‌کند تا آدرس MAC، زیرا آدرس MAC از پیش منتسب شده و غیرقابل تغییر است.

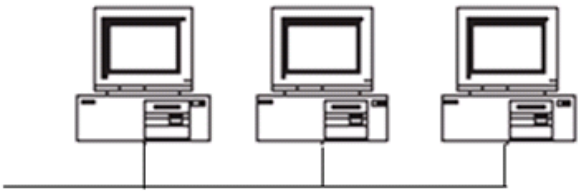
در Windows 2000 advanced Server و Windows 2003 Server و Windows 2008 Server از دیدگاه منطقی دو نوع شبکه می‌توان راه‌اندازی نمود:

۱. Workgroup
۲. Domain

تفاوت‌های ذاتی این دو شیوه که هم‌اکنون مورد بررسی قرار خواهد گرفت، نشان می‌دهد که هر یک از آن‌ها برای موارد به‌خصوصی مفید است.

۲-۳-۱- Workgroup

در این چیدمان از کامپیوترها، تمام سیستم‌های موجود در یک سطح‌اند، یعنی همه نسبت به هم وضعیت مشابه دارند، بانک اطلاعاتی مربوط به کاربران و مشخصه‌های هر یک از سیستم‌ها جداگانه و در همان سیستم ذخیره می‌شود[1] و البته هیچ تبادل اطلاعاتی مابین این بانک‌ها صورت نمی‌گیرد. پس اگر بخواهیم کاربری بتواند بر تمام سیستم‌های موجود در شبکه از نوع Workgroup، Login کند، باید بر تمام آن‌ها برایش User تعریف کرده باشیم. این امر در شبکه‌های کوچک و ساده می‌تواند مؤثر باشد، اما با افزایش تعداد کامپیوترها کارایی خود را از دست می‌دهد (چرا؟). با این توصیفات برای کامپیوترهای منفرد و برای Serverهای تکی این شیوه مناسب است و البته از بدیهیات آن عدم نیاز به تنظیمات پیچیده است.



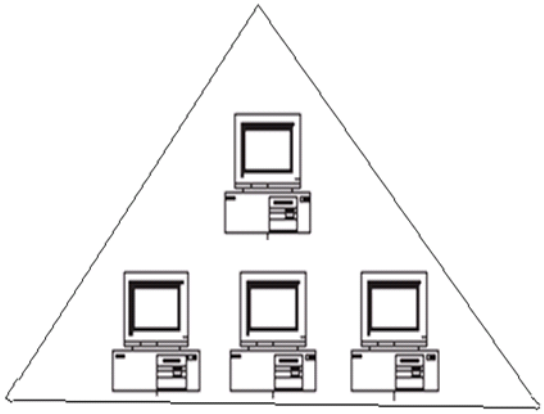
[1] منظور از بانک اطلاعاتی، اطلاعاتی مانند اسامی کابران، رمزعبور آن‌ها و تنظیمات هر یک از آن‌هاست و منظور از این که اطلاعات در همان سیستم ذخیره می‌شود، این است که نمی‌توان انتظار داشت با داشتن Usernameو Password بر سیستمی در Workgroup به سیستم‌های دیگر در Workgroup، Login کرد.

شکل ۱- قرارگیری منطقی کامپیوترها در شبکه‌های Workgroup

Domain -۲-۳-۲

روشی دیگر از راه‌اندازی شبکه است که امنیت و سازماندهی مناسبی برای کاربران متعلق به یک قلمرو یا محدوده یا Domain فراهم می‌کند. Domain نامگذاری شبیه به www.yahoo.com دارد، با این تفسیر که در Domain با نام yahoo که از نوع تجاری است (com)، یک Server برای دسترسی به وب داریم که نام آن www است، و در mail.yahoo.com نیز mail نام Server دیگری از Domain yahoo است، که Mail نام دارد.

در این حالت برای مدیریت و سازماندهی کاربران یک یا چند کامپیوتر با نقش Domain Controller نیاز داریم که اطلاعات کاربران و سازماندهی را به‌طور متمرکز نگه‌داری می کنند و تمام کامپیوترها از اطلاعات بانک اطلاعاتی مرکزی استفاده می‌کنند. به این ترتیب کافیست بر روی Server برای یک کاربر Username و Password تعریف کنید و این کاربر می‌تواند در صورت مجاز بودن، بر تمام کامپیوترهای شبکه که متعلق به آن domain هستند، login کند و تغییر Password آن کاربر در یک سیستم (Domain Controller) کافیست و لزومی به Login کردن بر تک تک سیستم‌ها و تغییر Password آن نیست. این روش برای کنترل مرکزی و اعمال سیاست‌های جامع به تمام Client ها مفید است، اما دارای پیچیدگی‌های خاص خود است و زمان بیشتری هم برای راه‌اندازی می‌برد.



شکل ۲- قرارگیری منطقی کامپیوترها در شبکه‌های Domain که Domain Controller در رأس هرم قرار می‌گیرد

با همه توصیفاتی که گفته شد، تاکنون فقط پیش‌زمینه‌ای برای ورود به مطلب عرضه گردید و مطالب مفصل‌تر در آینده عرضه خواهد شد.

۲-٤- راه‌اندازی سریع شبکه

پیش از هر چیز می‌دانیم که شبکه مورد نظر از نوع Workgroup خواهد بود، زیرا که براساس آنچه تاکنون گفتیم، ساده‌ترین روش است.

۲-٤-۱- نیازهای سخت‌افزاری

سپس به نیازهای سخت‌افزاری می‌پردازیم، آنچه در حالت حداقل لازم است:

برای شبکه‌ای با تعداد دو کامپیوتر

۱. دو کارت شبکه
۲. یک کابل (Cat 5e) از نوع Cross (در این حالت به Hub یا Switch نیاز نداریم) که دو انتهای آن به‌طور مستقیم به دو کارت شبکه موجود متصل‌اند.

برای شبکه‌ای با تعداد بیش از دو کامپیوتر

۱. یک یا چند hub یا Switch
۲. چند کابل (Cat 5e) از نوع عادی یا Straight
۳. به تعداد سیستم‌ها، کارت شبکه (هر کامپیوتر دارای یک کارت شبکه باشد)

۲-٤-۲- تنظیمات منطقی

پیش از هر چیز باید کامپیوترها بتوانند اصطلاحاً همدیگر را ببینند، یعنی اینکه آدرس‌های IP آن‌ها از یک محدوده[1] باشد، یعنی اینکه دارای یک شماره شبکه باشند. برای این منظور فعلاً بدون توضیح علت، یک محدوده‌ی به‌خصوص را برای این منظور پیشنهاد می‌کنیم.

مورد دیگری که باید در نظرداشته باشید این است که برای دسترسی کاربران به منابع همدیگر بر سیستم‌های مختلف، بایستی منابع مورد نظر را برای همدیگر به اشتراک بگذارید[2] و از طرف دیگر باید اجازه لازم را به کسانی که می‌خواهند از آن منابع استفاده کنند، لحاظ کنید و در نهایت برای اینکه بتوان به سیستم شخص دیگری به‌طور کامل دسترسی داشت، باید Username و Password کاربر آن سیستم را داشته باشید.

[1] Range
[2] Sharing

۲-۵- تکلیف جلسه‌ی بعد

۱. درحالی که از اینترنت تلفنی (Dial up) استفاده می‌کنید، با دستور ipconfig /all تمام تنظیماتی را که از طرف مرکز خدمات اینترنت به مودم شما داده شده است، یادداشت کنید و ضمن بیان تفاوت‌های آن با آنچه در این آزمایش در شبکه محلی دانشگاه دیدید، علت را شرح دهید.

۲. درحالی که از اینترنت تلفنی (Dial up) استفاده می‌کنید، دستورات ping www.yahoo.com و tracert www.yahoo.com را در خط فرمان اجرا کنید و خروجی هر یک را یادداشت نموده و نتیجه‌ی ping را با نتیجه‌ی آزمایش جاری مقایسه نمایید و علت را ذکر کنید. همچنین کاربرد tracert را بیان نمایید.

توجه: برای دانشجویان خوابگاهی که به اینترنت تلفنی دسترسی ندارند، این تکلیف اختیاری است.

۲-٦- دستور کار

توجه۱: پیش از شروع آزمایش، از مربی بخواهید که برای شما شماره گروه معین کند.

توجه۲: پیش از هر پرسش دیگری از مربی، راهنمایی‌های احتمالی ادامه‌ی سوال را بخوانید.

۱. پس از اینکه از اتصال کامپیوترها به Switch اطمینان حاصل کردید به

Start -> Settings -> Control Panel-> Network Connections

بروید و با کلیک راست بر کارت شبکه و انتخاب سربرگ[1] General و سپس انتخاب Internet Protocol(TCP/IP) و زدن کلید Properties، مشخصات زیر را برای آن تنظیم کنید:

IP address: 192.168.1.**شماره گروه‌تان**

Subnet mask: 255.255.255.0

کلید OK را بزنید و پس از بازگشت به سربرگ General، این بار سربرگ Advanced را انتخاب نمایید و Firewall را Off نمایید و OKهای بعدی را بزنید تا در آزمایش‌های امروز اختلال ارتباطی احتمالی ایجاد ننماید.

۲. به Start، Run بروید و در آن Cmd بنویسید و سپس دستور زیر را بنویسید:

ipconfig /all

به طوری کلی این دستور چه اطلاعاتی در اختیار قرار می‌دهد؟ (به عنوان مثال IP Address، Subnet Mask و ...)

آدرس IP، آدرس فیزیکی (MAC) و آدرس‌های DNS و Gateway را (در صورت وجود) بنویسید.

۳. برای اطلاع از امکان دسترسی به سیستم‌های مجاورتان دستور زیر را در خط فرمان تایپ کنید:

Ping 192.168.1.**شماره گروه سیستم مجاور**

چه می‌بینید؟ یک سطر از چهار سطر ظاهر شده را بنویسید. دقیقاً و جزء به جزء تا جاییکه می‌فهمید آن را شرح دهید. خطوط آخر پاسخ این دستور را که محتوی برخی آمارها (statistics) است، تفسیر کنید و مفهوم آن را بنویسید.

راهنمایی: بین دستور Ping و **شماره گروه**.192.168.1 یک فاصله باید وجود داشته باشد وگرنه با خطای زیر مواجه خواهید شد:

[1] Tab

'ping192.168.1.' is not recognized as an internal or external command,
operable program or batch file.

۴. ابتدا در خط فرمان دستور زیر را بنویسید:

Ping –t 192.168.1. **شماره گروه سیستم مجاور**

(توجه داشته باشید که در دو طرف t– دو فاصله خالی وجود دارد)

الف) حال بیان کنید که خروجی این دستور، چه تفاوتی با خروجی دستور آزمایش پیش دارد.

ب) در خط فرمان ping /? را تایپ نمایید و بگویید که چه گزینه‌های دیگری غیر از t– می‌توان با دستور ping همراه کرد و از روی ترجمه‌ی یک سطری آن‌ها، دو مورد دلخواه را شرح دهید. می‌توانید برای اطمینان از فهم خود آن را آزمایش نیز بکنید. به هر یک از این گزینه‌ها، یک **سوییچ** برای آن دستور، گفته می‌شود. موارد n–، l- و a– برای شما ملموس‌تر هستند. آن‌ها را تشریح و امتحان کنید. عملکرد سایر موارد به تنظیماتی وابسته است که خارج از کنترل شماست و ممکن است جوابی نگیرید.

۵. الف) پوشه‌ایی دلخواه ایجاد کنید و نام آن را همان شماره گروه‌تان بگذارید، با کلیک راست بر آن و انتخاب سربرگ[1]، Sharing و فعال‌سازی گزینه Just Enable File Sharing، آن را به اشتراک بگذارید. چه تغییری در ظاهر پوشه ایجاد شد؟ یک فایل دلخواه در آن قرار دهید تا برای استفاده‌های بعدی گروه‌های دیگر بتوانند از آن استفاده کنند.

ب) در قسمت آدرس My computer، شمار گروه سیستم‌مجاور .192.168.1\\ را تایپ کنید، چه می‌بینید؟ آیا می‌توانید فایلی را که ایشان به اشتراک گذارده است رویت کنید و بر کامپیوتر خود کپی نمایید؟

راهنمایی: این دستور اجازه‌ی دسترسی به فایل‌هایی را که سیستم مجاور به اشتراک گذارده است می‌دهد.

ج) حال در همان جا \\192.168.1.شماره گروه سیستم مجاور\c$ (مثلاً \\192.168.1.4\c$) را تایپ کنید، چه روی می‌دهد؟

راهنمایی: با این دستور می‌توان به درایوی از یک کامپیوتر دیگر دسترسی پیدا کرد.

د) شرح دهید که چرا در ورود به سیستم مجاور از شما رمز عبور خواسته می‌شود؟ مگر شبکه‌ی کنونی از چه نوعی است؟

[1] Tab

۶. الف) در خط فرمان تایپ کنید: hostname. خروجی چه خواهد بود؟

راهنمایی: به Start->Settings->Control Panel بروید و بر System کلیک دوگانه بکنید و از سربرگ Computer Name، گزینه‌ی Full Computer Name را بیابید و عبارت نوشته شده در جلوی آن را با خروجی دستور hostname مقایسه کنید.

ب) به جای آدرس IP در دستور ping، Hostname یک گروه دیگر را استفاده کنید و نتیجه‌گیری خود را بنویسید. این امر چه تسهیلی برای ما ایجاد می‌کند؟

۷. در پاسخ به دستور Ping چند حالت می‌تواند وجود داشته باشد (که هر کدام جواب مختص به خود را درپی خواهد داشت):

الف) سیستم مورد نظر دارای شماره شبکه‌ایی برابر با شماره شبکه‌ی کامپیوتر ما باشد و در دسترس هم باشد (یعنی اینکه خاموش نباشد و تنظیمات آن به نحوی باشد که بتوان با آن ارتباط برقرار کرد) مانند PC1 و PC4 در پیش‌آگاهی.

ب) سیستم مورد نظر دارای شماره شبکه‌ایی برابر با شماره شبکه‌ی کامپیوتر ما باشد، اما کامپیوتر مورد نظر در دسترس نباشد (یعنی اینکه خاموش باشد یا تنظیمات آن به نحوی باشد که نتوان با آن ارتباط برقرار کرد یا از شبکه قطع باشد)

ج) سیستم مورد نظر دارای شماره شبکه‌ایی برابر با شماره شبکه‌ی کامپیوتر ما نباشد اما به همان شبکه‌ی محلی ما وصل باشد و به صورت فیزیکی روشن و در دسترس باشد.

د) سیستم مورد نظر دارای شماره شبکه‌ایی برابر با شماره شبکه‌ی کامپیوتر ما نباشد و در دسترس هم نباشد.

دستور Ping برای هر یک از حالات بالا خروجی مخصوص به خود خواهد داشت، برای هر یک از موارد فوق مثال بزنید و Ping را انجام دهید و خروجی مرتبط را یادداشت کنید. به عنوان مثال برای حالت الف باید کامپیوتری را Ping کنید که هم‌اکنون در شبکه وجود دارد و خروجی مشابه به زیر خواهد بود:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

مورد ب و ج و د را شما انجام دهید. یعنی بنویسید چه آدرسی برای ping انتخاب کردید و چه خروجی‌ایی دیدید؟

تمرین اختیاری:

۸. در صورتی که امکان دسترسی به اینترنت را از داخل آزمایشگاه دارید، دستورات ping www.yahoo.com و tracert www.yahoo.com را در خط فرمان اجرا کنید و خروجی هر یک را یادداشت نموده و نتیجه‌ی ping را با نتیجه‌ی آزمایش جاری مقایسه نمایید و علت را ذکر کنید. همچنین کاربرد tracert را بیان نمایید.

آزمایش دوم

پشتیبان‌گیری (Backup)

۳-۱- مقدمه

از وظایف اصلی راهبرشبکه محلی، حفاظت و نگهداری از داده‌های ارزشمند سازمان و کارشناسان آن است. روش‌ها و نرم‌افزاری مختلفی برای پشتیبان‌گیری از فایل‌ها، برنامه‌ها و پوشه‌ها وجود دارد، اما نرم‌افزار سودمند[1] به نام NTBackup که در ویرایش‌های مختلف ویندوز ۲۰۰۰، XP، ۲۰۰۳ و ۲۰۰۸ لحاظ شده است نیز، علاوه بر امکانات متنوع، نکات حساس مرتبط با پشتیبان‌گیری را نیز آموزش می‌دهد.

در این جلسه علاوه بر آشنا شدن با چنین نرم‌افزاری، سیاست‌ها و رویکردهای صحیح مرتبط با پشتیبان‌گیری نیز تشریح خواهد شد. همچنین تفاوت بارز پیش‌آگاهی در این آزمایش، با آزمایش‌های پیشین، آن است که در بخش پیش‌آگاهی، اکثر نکات فنی استفاده از NTBackup بیان شده است و دانشجو در حین آزمایش باید این نکات را در خاطر داشته باشد. در نهایت، بازیابی[2] فایل‌های از دست رفته، نیز تشریح می‌گردد.

۳-۲- هدف

آشنایی با اصول پشتیبان‌گیری در شبکه‌های محلی و نحوه‌ی کار با نرم‌افزار سودمند NTBackup

[1] Utility
[2] Restore

۳-۳- پیش‌آگاهی

سیستم‌عامل ویندوز شرکت مایکروسافت دارای ابزار نیرومند و انعطاف‌پذیری به نام NTbackup است که در آن همه فرآیندهای Backup به صورت کاملا حرفه‌ای لحاظ شده است. این شکل Backup هم در سرورها[1] و هم در کلاینت‌های[2] مبتنی بر سیستم‌عامل ویندوز قابل اجراست و در همه نیز به یک شکل است.

دراین مجال سعی شده است که مبانی اصلی Backup، مفاهیم و اصطلاحات، ابزارها و استراتژی‌های آن به طور کامل تشریح شود. پس از این آزمایش، فرد با پشتیبان گرفتن بر روی کامپیوتر های محلی[3] و یا کامپیوترهای دیگر در شبکه[4] آشنا خواهد شد. شناخت انواع Backup نیز کمک خواهد کرد تا استراتژی مناسبی در ارتباط با پشتیبان گرفتن در هر شبکه کامپیوتری اتخاذ شود.

۳-۳-۱- کار با ابزار پشتیبان‌گیری

ابزار Backup در ویندوز، معمولا با نام اجرائی آن در کامپیوتر شناخته می‌شود یعنی همان NTbackup . برای وارد شدن به پنجره‌ی این ابزار می‌توان منوی Start را باز کرد و گزینه Run را انتخاب کرده و در آن عبارت ntbackup را تایپ نمود.

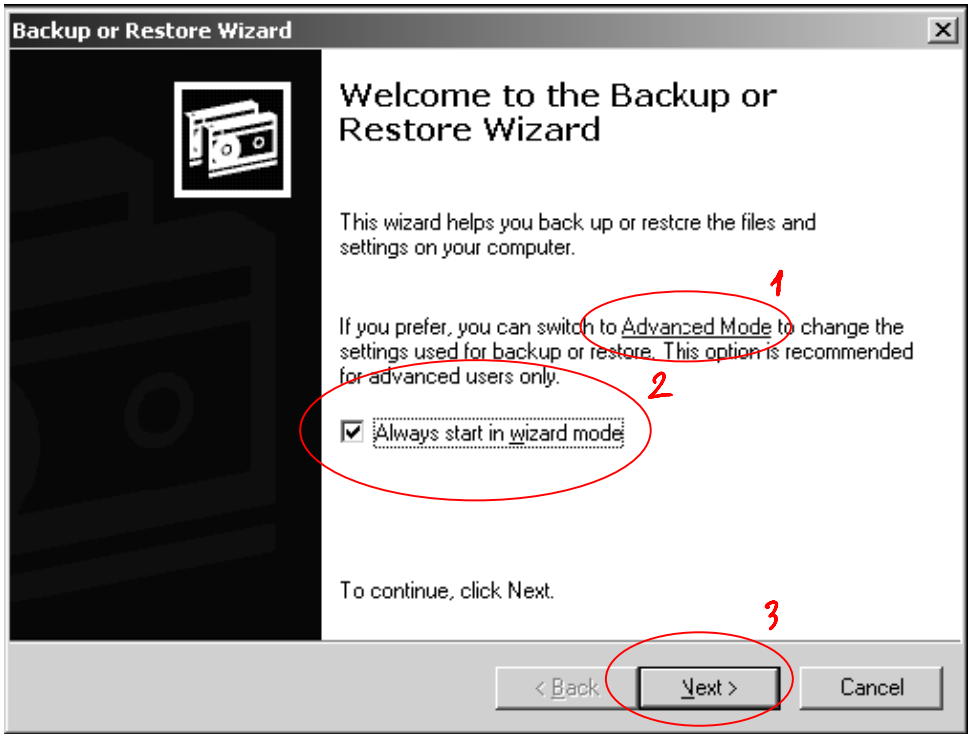
اولین بار که ابزار Backup باز می‌شود، به صورت یک Wizard مشاهده خواهد شد. اگر می‌خواهید مراحل ساده‌ای را طی کنید از دکمه NEXT استفاده کنید ولی برای دستیابی به تنظیمات پیشرفته بر روی پیوند موجود در Wizard با نام Advanced Mode کلیک کنید.

برای اینکه پنجره Wizard مجددا مشاهده نشود، تیک مربوط به Always start in wizard mode را بردارید. در غیر این صورت با هر بار باز شدن برنامه، Wizard مشاهده خواهد شد.

در این ابزار هم فرآیند پشتیبان گرفتن را به طور کامل خواهیم داشت و هم فرآیند بازیابی یا Restore را بعد از ازبین رفتن اطلاعات در یک سیستم. برای زمانبندی[5] تمامی فرآیند Backup نیز حتما باید از همین ابزار بهره برد.

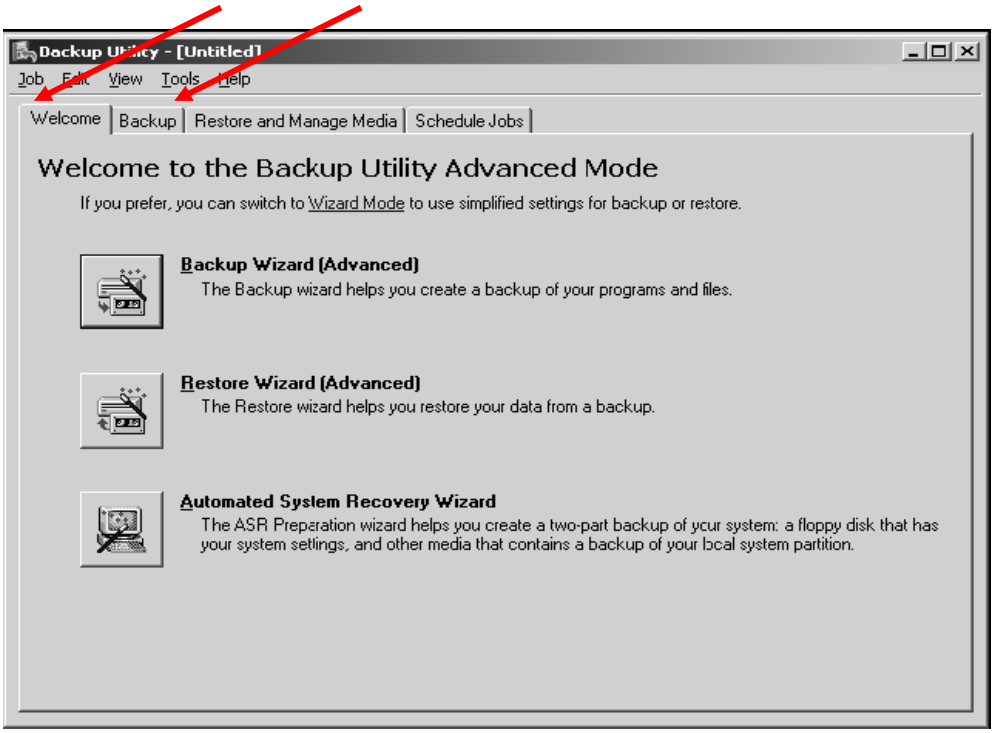
---

[1] servers
[2] Clients
[3] Local
[4] Remote
[5] Schedule

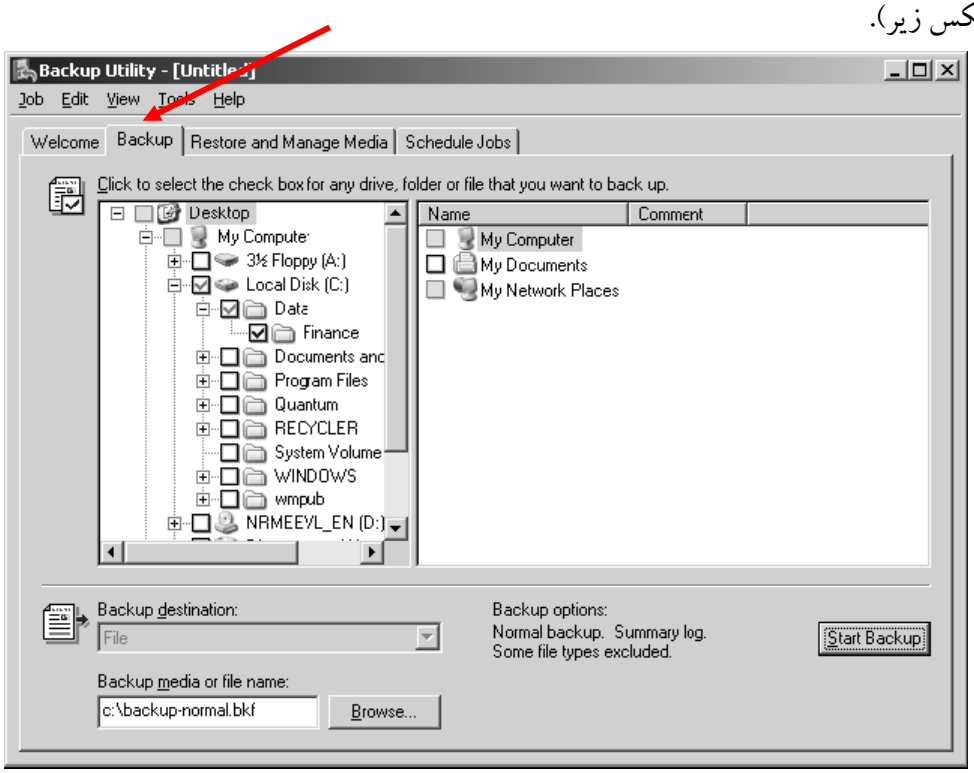


همانطور که در پنجره Backup Utility مشاهده می‌شود، می‌توان اطلاعات را به صورت دستی (در سربرگ[1] Backup) یا به صورت Wizardی پشتیبان گرفت. همچنین می‌توان با برنامه‌ریزی دقیق در بخش Backup، عملکردی برای آن لحاظ کرد که در زمان‌های تعیین شده‌ایی، بدون نیاز به راهبر، فرایند پشتیبان‌گیری به صورت خودکار انجام پذیرد. این عمل را با استفاده از زمانبندی یا Scheduling انجام می‌دهند. در ضمن عمل بازیابی یا Restore نیز می‌تواند هم به صورت دستی (در سربرگ با نام Restore and manage media) و هم به صورت خودکار (Wizard) انجام پذیرد.

[1] Tab



در ادامه ابتدا بر استراتژی‌های Backup و اجرای آن و ظرفیت‌های ابزار Backup Utility تمرکز خواهد شد (عکس زیر).



۳-۳-۲- انتخاب اطلاعات مهم برای پشتیبان‌گیری

در سربرگ Backup می‌توان فایل‌ها یا پوشه‌های مورد نظر برای پشتیبان‌گیری را انتخاب نمود. این فایل یا پوشه‌ها ممکن است در کامپیوتر کنونی یا بر یک کامپیوتر دیگر در شبکه ذخیره شوند . اگر پوشه به صورت کامل برای پشتیبان گیری انتخاب شود، یک علامت تیک به رنگ آبی در کنار آن ظاهر خواهد شد. ولی اگر فقط بخشی از آن برای پشتیبان گیری انتخاب شود، یک تیک به رنگ خاکستری کمرنگ در کنار آن پوشه ظاهر خواهد شد و نمایانگر آن است که فقط بخشی از پوشه پشتیبان گرفته خواهد شد که در داخل آن مشخص شده و نه تمام محتویات‌اش.

اگر Backup فایل‌ها یا پوشه‌های مورد نظر در کامپیوتر دیگری در شبکه است، مثلا از طریق My Network Places به سراغ آن رفته‌اید، ساختار آدرس آن در کامپیوترتان به صورت زیر مشاهده می‌شود:

\\Server1\ShareName\Path-To-Resource

۳-۳-۳- انتخاب مقصد فایل‌های Backup

سیستم‌عامل ویندوز اجازه می‌دهد فرآیند Backup بر انواع متفاوتی از رسانه‌ها[1] انجام شود. این رسانه‌های می‌توانند از انواع زیر باشند:

- Tape
- Removable Disk
- Local Disk Volume

به خصوص Tape برای شرکت‌ها و نهادهای بزرگ مانند بانک‌ها در فرایند آرشیو داده‌ها و اسناد الکترونیکی مورد استفاده قرار می‌گیرد.

فرآیند Backup یک فایل با پسوند bkf. تولید می‌کند که همچنین می‌توان برای امنیت از خطرات فیزیکی سیستم کنونی، آن را بر روی کامپیوتر دیگری در شبکه ذخیره کرد. انجام Backup همه سرورهای شبکه بر روی یک سرور مرکزی هم می‌تواند امنیت شبکه را بالا ببرد و هم تمام Backup ها را با نظم مشخصی قرار دهد. همچنین این امر مدیریت Backupها را در زمان بازیابی ساده‌تر می‌کند. عمل Backup بر روی سرور مرکزی در شبکه برای بسیاری از راهبران آن، ساده و معمول است.

[1] Media

توجه۱ : سرور مرکزی Backup می‌تواند یک کامپیوتر قوی (به خصوص از لحاظ حافظه) باشد که صرفاً فایل‌های Backup در آن نگهداری می‌شود و هیچ نقش دیگری در مدیریت شبکه نداشته باشد و تنها به عنوان یک Storage عمل کند.

توجه۲ : پشتیبان‌گیری همیشه با تهیه یک نسخه از فایل‌های حساس نیست و ممکن است که بر اساس اهمیت فایل‌ها، نسخه‌های متعدد در مکان‌های مختلف شبکه از آن‌ها نگهداری شود؛ به عنوان مثال

در یک شرکت برنامه‌نویسی، برنامه‌نویسان موظف هستند در پایان هر روز کاری، فایل‌های ایجاد شده و تغییر یافته در آن روز را در درایوی دیگر در کامپیوترشان و در مکانی مشخص با اسمی که دارای یک الگوی از پیش تعیین شده است، ذخیره کنند.

راهبر شبکه موظف است در آخر هر هفته از فایل‌های برنامه‌نویسان که در درایو مشخصی از کامپیوترشان قرار دارد، پشتیبان گرفته و آن را در سرور مخصوص Backup بریزد.

همچنین راهبر شبکه موظف است در آخر هرماه، محتویات سرور مخصوص Backup را در DVD یا Tape ریخته و به جایی امن در خارج از شرکت منتقل کند (مثلا گاوصندوق شرکتی دیگر).

به این ترتیب در بدترین شرایط و حوادث، بازهم داده‌هایی برای بازیابی وجود دارد. مکانیزم تشریح شده‌ی فوق، در پایین خلاصه شده است. نحوه‌ی پشتیبان‌گیری معمول راهبران حرفه‌ای مانند زیر است که به **نسل‌های Backup** موسوم است:

نسخه پدر بزرگ	نسخه پدر	نسخه پسر
تناوب کم	زیاد	خیلی زیاد
فاصله زیاد	کم	خیلی کم
مانند مکانیزم ماهیانه و انتقال فایل به جایی خارج از شرکت	مانند مکانیزم هفتگی و انتقال فایل‌ها به کامپیوتر دیگر	مانند مکانیزم روزانه و انتقال فایل‌ها به درایویی دیگر

توجه۳ : محدودیت‌های پشتیبان‌گیری از طریق کنونی، آن است که نرم‌افزار Ntbackup نمی‌تواند پشتیبان تهیه شده را بر CD یا DVD بریزد (Write کند) و نیز نمی‌تواند بر Removable Disk یا Tapeیی که به یک کامپیوتر دوردست متصل است بریزد.

۳-۳-٤- تعیین استراتژی Backup

بعد از انتخاب فایل‌ها و پوشه‌هایی که قرار است از آنها پشتیبان تهیه شود و معین کردن مقصدی که باید Backupها در آن ذخیره شوند، نوبت به تعیین استراتژی Backup می‌رسد؛ بدین معنی که چه نوعی از پشتیبان‌گیری و با چه برنامه‌ایی انتخاب شود تا بهترین کارایی حاصل شود. بدین ترتیب باید دکمه Start Backup را کلیک کرده و در پنجره باز شده دکمه Advance را انتخاب نمود. پنجره‌ی ظاهر شده، Advance Backup خواهد بود. در آن می‌توان نوع پشتیبان‌گیری را تعیین کرد. نوع Backup معین می‌کند که کدام یک از فایل‌های انتخابی باید به مقصد دخیره اطلاعات انتقال پیدا کند.آیا از همه فایل‌های انتخاب شده پشتیبان تهیه شود؟ آیا فقط فایل‌هایی که از زمان آخرین Backup تا به حال تغییر کرده‌اند پشتیبان تهیه شود؟

هر فایل Backup دارای یک خصیصه[1] به نام خصیصه آرشیو یا Archive است. این خصیصه را می‌توان پس از کلیک راست بر یک فایل و انتخاب کلید Advanced از سربرگ General رویت نمود. به عنوان مثال، پنجره‌ی زیر را که پس از کلیک راست بر یک فایل و انتخاب کلید Advanced از سربرگ General ظاهر شده است ببینید:

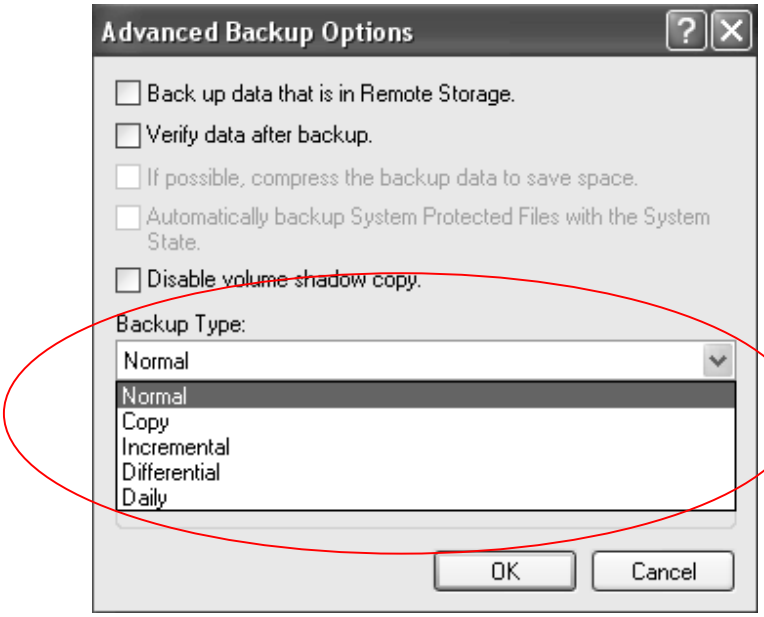
سیاست پشتیبان‌گیری به تیک (علامت) Archive وابسته است، بدین معنی که این تیک برای هر فایلی زده شده باشد یعنی اینکه آن فایل به تازگی ایجاد شده یا به تازگی تغییر کرده و سیستم با دیدن این تیک می‌فهمد که فایل از زمان پشتیبان‌گیری قبلی تا کنون تغییر کرده یا نه. پس اگر تغییر نکرده باشد (علامت

[1] Attribute

زده نشده باشد) در اکثر سیاست‌های پشتیبان‌گیری، فضای دیسک و توان پردازنده هدر داده نمی‌شود و پشتیبان‌گیری جدیدی روی نمی‌دهد. این امر به خصوص برای زمانی که حجم فایل Backup به چندین گیگابایت می‌رسد، حیاتی است.

انواع Backup همانطور که در شکل زیر دیده می‌شود عبارتند از:

1. Normal Backup
2. Incremental Backup
3. Differential Backup
4. Copy Backup
5. Daily Backup



که شرح کامل هریک از انواع Backup در ادامه خواهد آمد.

۱- Normal Backup

در این حالت از تمامی فایل‌هاو پوشه‌های انتخاب شده پشتیبان گرفته خواهد شد و تیک Archive را برمی‌دارد تا اعلام کند که از فایل‌ها پشتیبان گرفته شده است. Normal Backup از تیک Archive برای تعیین فایل‌هایی که باید پشتیبان گرفته شود استفاده نمی‌کند و همه موارد انتخاب شده را برای Backup به رسانه Media انتقال می‌دهد، چه این فایل‌ها از زمان آخرین پشتیبان‌گیری تغییری داشته باشند یا خیر. هر نوع طرح و سیاست Backup در ابتدا حتما از Normal Backup شروع می شود و Normal Backup پایه

همه انواع Backup هاست. پس در Normal Backup همه فایل‌ها و پوشه‌های انتخاب شده به عنوان فایل Backup به Media انتقال پیدا می‌کنند.

۲-Incremental Backup

در Normal Backup تیک Archive از تمامی فایل‌هایی که پشتیبان گرفته شده است برداشته می‌شود. در حالت Incremental Backup از همه فایل‌هایی که قبلا تیک Archive روی آنها تنظیم شده، پشتیبان تهیه می شود و بعد از این نوع Backup ، تیک Archive پاک می شود.

اگر Incremental Backup یک روز بعد از Normal Backup اجرا شود، فقط از فایل‌هایی پشتیبان تهیه می‌شود که در طول این یک روز تغییر کرده‌اند یا به تازگی ایجاد شده‌اند و اگر Incremental Backup رایک روز بعد از Incremental Backup دیگر اجرا کنید در این حالت نیز فقط از فایل‌هایی که در طول یک روز گذشته دچار تغییرات شده‌اند پشتیبان گرفته می‌شود.

Incremental Backup سریع‌ترین و در عین حال کم‌حجم‌ترین فایل در انواع Backup هاست. ولی در زمان بازیابی، کمترین کارایی را دارد. زیرا در زمان بازیابی کردن حتما باید ابتدا فایل Normal Backup بازیابی شود و بعد به ترتیب زمانی همه‌ی فایل‌های Backup از نوع Incremental بازیابی گردد. به‌طور خلاصه، این نوع پشتیبان‌گیری، تنها از تغییرات پشتیبان می‌گیرد و زمان انجام فرآیند Backup بسیار اندک ولی زمان بازیابی کردن فایل‌ها بسیار طولانی است.

۳- Differential Backup

همانند روش دوم، ازهمه فایل‌هایی که قبلا تیک Archive روی آنها تنظیم شده است پشتیبان تهیه می‌شود. ولی بعد از این نوع Backup، تیک Archive پاک نمی‌شود. Differential Backup هربار از این تیک استفاده می‌کند و فرآیند Backup فقط روی فایل‌هایی که بعد از آخرین Normal Backup یا Incremental Backup که تا به حال تغییر کرده اند یا جدید ایجاد شده‌اند انجام می‌شود. پس با توجه به اینکه Differential Backup تیک Archive را پاک نمی‌کند، اگر در۲ روز پشت سر هم از Differential Backup استفاده کنید، بدان معناست که Backup روز دوم شامل همه فایل‌هایی است که در Backup روز اول تهیه شده بود، بعلاوه‌ی تمام فایل‌هایی که در این ۲ روز تغییر کرده یا اخیرا ایجاد شده‌اند.

بنابراین Differential Backup فایلی با حجم بیشتر از Incremental Backup می‌سازد و زمان عملیات Backup طولانی‌تری نیز دارد ولی این زمان کمتر از پشتیبان گرفتن به شکل Normal Backup است.

Differential Backup در زمان بازیابی از Incremental Backup بهینه‌تر و سریعتر است. زیرا می‌توان Normal Backup را بازیابی کرده و بعد فقط وفقط آخرین Differential Backup را بازیابی نمود (چون دربردارنده تجمع تغییرات است).

۴- Copy Backup

در این نوع Backup ازهمه فایل‌ها و پوشه‌های انتخاب شده پشتیبان تهیه می‌شود. Copy Backup به هیچ وجه نه از تیک Archive استفاده می‌کند و نه آنرا پاک می‌کند. Copy Backup معمولا زمانی مفید است که اطلاعات یا فایل Backup یک کامپیوتر یا سرور را می‌خواهند به صورت کامل به کامپیوتر یا سرور دیگر در شبکه انتقال دهند و یا صرفا یک Backup را در سازمان خود می‌خواهند به صورت جداگانه و آرشیو نگهداری کنند. در این حالت می‌توان با آسایش از سیاست‌های Backup دیگر نیز استفاده کرد و استفاده از این نوع پشتیبان‌گیری باعث اختلال انواع دیگر Backup در سیستم نیست.

۵- Daily Backup

در این حالت از تمامی فایل‌ها و پوشه‌های انتخاب شده تنها آن‌هایی که امروز تغییر کرده‌اند، بر اساس آخرین تاریخ و ساعت تغییر (Modify)، پشتیبان تهیه می‌شود. در این حالت نیز نه تیک Archive استفاده می‌شود و نه پاک. اگر کاربر یا راهبر بخواهد از فایل‌ها و پوشه‌ها به صورت روزانهپشتیبان تهیه کند، بدون آنکه زمانبندی تعریف نماید یا در سایر سیاست‌های استفاده شده اختلال ایجاد کند، از این روش بهره می‌برد.

راهکار ترکیبی

گرچه ایجاد یک Normal Backup هر شب هم کاری مطمئن است و هم در هنگام بازیابی فقط یک فایل بازیابی می‌شود، ولی استفاده متوالی از این نوع Backup هم زمان زیادی نیاز دارد و هم حجم بسیار بالایی نیاز خواهد داشت. برای جلوگیری از این موارد و بهینه کردن فرآیند Backup از استراتژی‌های ترکیبی استفاده می‌شود و راهبران حرفه‌ایی نیز این راهکارهای ترکیبی را به کار می‌برند و شما نیز چنین کنید:

۱. استفا ده از ترکیب Normal Backup و Differential Backup

فرض کنید روز یکشنبه یک Normal Backup اجرا شده است و از روز دوشنبه تا جمعه شب Differential Backup اجرا شده است. با توجه به اینکه Differential Backup، نشانه Archive را پاک نمی‌کند، به این نتیجه می‌رسیم که هر Backup شامل همه تغییرات از روز یکشنبه تا به حال است. حال اگر اطلاعات در روز جمعه خراب شود فقط کافی است Normal Backup روز یکشنبه و Differential Backup روز پنج‌شنبه بازیابی شود. این استراتژی زمان زیادی برای اجرا نیاز دارد. یعنی اینکه در زمان Backup طولانی و زمان بر است ولی در زمان بازیابی ساده و سریع است زیرا به دو مرحله بازیابی نیاز دارد و نه بیشتر.

۲. استفاده از ترکیب Normal Backup و Incremental Backup

فرض کنید روز یکشنبه یک Normal Backup اجرا شده است و از روز دوشنبه تا جمعه شب Incremental Backup اجرا شده است. با توجه به اینکه Incremental Backup، نشانه Archive را پاک می‌کند، به این نتیجه می‌رسیم که هر Backup فقط و فقط شامل تغییراتی است که از Backup قبلی تا کنون ایجاد شده است. اگر اطلاعات در روز جمعه خراب شود، باید Normal Backup روز یکشنبه را بازیابی کرده و بعد هر یک از Incremental Backup ها را تک تک و به ترتیب از روز دوشنبه تا روز پنجشنبه بازیابی نمود. این استراتژی در پشتیبان گرفتن سریع ولی در بازیابی کند و کمی سخت و حساس است.

۳-۳-۵- بازیابی

بازیابی در محیط Ntbackup کار نسبتاً سرراستی است و مشتمل بر انتخاب مورد در نظر گرفته شده برای بازیابی و تعیین مکان آن و نیز نحوه‌ی برگشت آن است. پس از انتخاب سربرگ Restore and Manage Media و تیک زدن گزینه‌هایی که می‌خواهیم بازیابی شود، سه سیاست برای بازیابی پیش‌روی گذاشته می‌شود (در منوی پایین کشیدنی با عنوان Restore files to).

۱. **Original location**
   - بازیابی درست در مکان قبلی
   - این شیوه به‌خصوص برای برای حذف‌های ناخواسته مفید است
۲. **Alternate location**

- بازیابی در مکانی دیگر، اما با حفظ ساختار پوشه‌های محل پشتیبان‌گیری (غیر از درایو ریشه)
- به عنوان مثال اگر شما پیش از این از فایل‌های موجود در C:\Data\Finance پشتیبان گرفته‌اید و آن را در درایو D بازیابی می‌کنید، ترتیب تودرتویی پوشه‌های بازیابی شده در درایو D به شکل D:\Restore\Data\Finance. خواهد بود

۳. **Single folder**

- بازیابی در مکانی دیگر دلخواه
- اما بدون حفظ ساختار تودرتوی پوشه‌های اصلی، یعنی اینکه همه‌ی فایل‌ها فقط در یک پوشه‌ی تنها بازیابی می‌شوند

۳-٤- دستورکار

۱. ابتدا به سربرگ Backup بروید و از لیست فایل‌هایی که می‌توانید برای پشتیبان‌گیری انتخاب نمایید، گزینه‌ی System State را بیابید و نام فایل‌هایی را که در خود دارد بنویسید؟

۲. اگر شرکتی دارای کارمندهایی باشد که تنها در روزهای زوج به سرکار می‌آیند و از آن‌ها بخواهد که فایل‌هایشان را برای پشتیبان‌گیری در پوشه‌ایی به نام DailyWorks در درایو C بریزند و از شما بخواهد یک راه‌کار پشتیبان‌گیری مناسب از این فایل‌ها که کمترین حجم را ببرد، پیشنهاد کنید. راه‌کار خود را پیاده‌سازی کنید. فرض کنید که کارمندان از ساعت ۸ صبح تا ۲۰ شب کار می‌کنند. درضمن، تنظیماتی لحاظ کنید، که در زمان بازیابی، رمزعبور درخواست شود. فایل پشتیبان را در درایو D و در پوشه‌ایی دیگر به نام Backup بریزد.

روند کار بدین شرح است که نباید از حالت Wizard استفاده کنید، پس از انتخاب سربرگ Backup، پوشه مورد نظر را انتخاب نمایید، سپس محل ذخیره فایل پشتیبان را تعیین کنید، بعد بر کلید Start Backup کلیک کنید و سپس بر کلید Advanced و سیاست خود را تعیین کنید و پس از آن بر کلید Schedule کلیک نمایید و زمانبندی مورد نظر را تعیین و ذخیره کنید.

الف) طرح خود را برکاغذ و در جدولی مشابه به زیر بنویسید و به مربی نشان دهید و در صورت تأیید وی آن را عملیاتی نمایید.

شنبه	یکشنبه	دوشنبه	سه‌شنبه	چهارشنبه	پنج‌شنبه	جمعه
نوع Backup	نوع Backup	نوع Backup	نوع Backup	نوع Backup	نوع Backup	نوع Backup

ب) با رفتن به سربرگ Schedule، زمانبندی ایجاد شده را رویت کنید و صحت کار خود را بررسی کنید.

ج) راهکار پیاده‌سازی شده را به مربی نشان دهید.

د) آیا هم اکنون می‌توان از گزینه‌ی Restore استفاده نمود؟ چرا؟

راهنمایی: باید از راهکار ترکیبی مناسب برای پشتیبان‌گیری استفاده کنید.

۳. از پوشه My Pictures در My Documents کاربر جاری یک Normal Backup بگیرید و آن را در پوشه DailyWorks در درایو C بریزید. اکنون با استفاده از گزینه Alternate Location در بازیابی، آن را در پوشه Backup در درایو D بازیابی کنید. آدرس (مسیر) پوشه بازیابی شده‌ی My Picture را پوشه Backup در درایو D بنویسید.

راهنمایی: در صورتی که در زمان پشتیبان‌گیری، سیستم به حالت Hung up می‌رود، در گزینه‌ی Advanced تیک Disable volume shadow copy را بزنید. این مشکل به علت وجود نرم‌افزار Deep Freeze بر کامپیوترهای سایت است.

۴. فایلی در پوشه Works در درایو D با نام 1.txt با محتوی ۱۲۳ ایجاد کنید و پشتیبان بگیرید. سپس محتوی آن فایل را به ۱۲۳۴۵۶ تغییر دهید و فایل را با استفاده از گزینه Original Location بازیابی کنید.

الف) انتظار دارید محتوی فایل پس از بازیابی به چه تغییر کند؟

ب) محتوی فایل بازیابی شده چیست؟ چه تعمیمی می‌توانید از این رویداد بگیرید؟

ج) برای اینکه محتوی اصلی فایل بازیابی شود چه باید کرد؟

آزمایش سوم

میزبانی وب و انتقال فایل (IIS and FTP)

٤-١- مقدمه

در این جلسه علاوه بر اینکه به مفهوم Web Server می‌پردازیم، با مفاهیم مهم Hosting، Domain Name و Name Server برای وب‌سایت‌های اینترنتی که در چرخه ایجاد یک وب‌سایت غیرقابل اجتناب است، نیز آشنا خواهیم شد. همچنین به مکانیزم انتقال فایل در بستر اینترنت که با به اشتراک گذاردن آن (File Sharing) در بستر شبکه LAN متفاوت است نیز پراخته می‌شود.

اهمیت این درس از آن بابت است که همراه با آموزش شبکه، آشنایی با مراحلی از ایجاد وب‌سایت که معمولاً مورد توجه قرار نمی‌گیرند را نیز میسر می‌سازد. همچنین در رابطه با استفاده از دستورات خط فرمان از جمله telnet برای استفاده از خدمات مختلف، نیز آموزش‌هایی مطرح خواهد شد. به مفاهیم پیش‌نیازی مانند شماره پورت نیز اشاره می‌شود.

آزمایش کنونی بهتر است بر یکی از ویندوزهای نسخه Server مانند Windows 2003 Server یا Windows 2008 Server انجام پذیرد، اما به واسطه عدم وجود چنین ویندوزی بر تمام کامپیوترهای آزمایشگاه، می‌توان با محدودیت‌های قلیلی آن را بر Windows XP نیز انجام داد.

٤-۲- هدف

آشنایی با ایجاد و مدیریت Web-Server، Hosting و Name Server و FTP

٤-۳- پیش‌آگاهی

ابتدا به طرح مباحث پیش‌نیاز می‌پردازیم: ایجاد یک وب‌سایت از الف تا ی را می‌توان مشتمل بر ۶ گام در نظر گرفت، در گام اول بایستی هدف از ایجاد وب‌سایت مشخص باشد. به عبارت دیگر چه می‌خواهید در سایتتان داشته باشید؟ و پاسخ به این نیز با طرح پرسش زیر امکان‌پذیر می‌شود: می‌خواهید مخاطبان سایتتان چه کسانی باشند؟ به عبارت بهتر سایت را به چه هدفی می‌سازید؟ در گام دوم انتخاب نام مناسب برای سایتتان صورت می‌گیرد که به URL یا Domain Name معروف است.

در گام سوم تحلیل خواسته‌ها توسط افراد کارشناس، و بدین ترتیب تعیین نیازها و سپس طراحی مقدماتی و اصلی وب‌سایت صورت می‌گیرد، که جزییات فنی زیادی درپی دارد و در درس مهندسی فناوری اطلاعات ۱ به آن پرداخته خواهد شد. گام چهارم تعیین (کامپیوتر) میزبانی است که وب‌سایت بایستی بر آن قرارگیرد و امکان دسترسی تمام وقت به وب‌سایت شما توسط بازدید کنندگان را می‌دهد که ما در این جلسه بدان خواهیم پرداخت. گام پنجم معرفی وب‌سایت به دنیاست. زیرا اگر کسی از یک کشور به عنوان مثال آمریکای جنوبی بخواهد در زمینه‌های مورد فعالیت شما، با شرکتتان همکاری کند، بایستی بتواند از طریق جستجو در موتورهای جستجو (مانند www.google.com) شما را بیابد. پس در این گام سایت شما به موتورهای جستجوی معروف، معرفی می‌گردد تا قابل جستجو شود. از نکات مهم در این مرحله این است که اگر در مرحلهٔ طراحی تمهیدات مناسب برای این امر لحاظ نشده باشد بایستی تغییراتی در طراحی صورت گیرد و گام ششم یا آخر نیز عبارت است از نگهداری. امورات مطرح شده در این مرحله عبارتند از تمدید نام سایت، تمدید فضای رزرو شده برای آن، تغییر در محتوی سایت بر حسب نیاز و شرایط.

آن‌چه شما در این جلسه با آن آشنا خواهید شد مستقیماً با *مراحل دو و چهار* در ارتباط است و با مراحله ۶ نیز تا حدی رابطه دارد. سه مفهوم دیگر نیز که آشنایی با آن‌ها می‌تواند در جهت رفع ابهام مفید باشد، مفهوم Hosting وDomain Name و Name Server است:

٤-٣-١- میزبانی (Hosting)

هر وب‌سایت اینترنتی بایستی در تمام شبانه روز قابل دسترسی باشد و این امر از طریق نهادن آن بر سیستم‌هایی میسر است که به صورت تمام وقت روشن باشند. این امر، یعنی قرار دادن سایت بر یک Server به صورت تمام وقت را Hosting یا Web Hosting یا میزبانی وب می‌نامند، که با پرداخت مبلغی نیز به عنوان اجاره همراه است.

میزبانی وب در کشورهای مختلف جهان انجام می‌پذیرد و عرضه و پرداخت هزینه‌های آن از طریق اینترنت نیز امکان‌پذیر است. برای تبدیل یک سیستم به یک Web Host در سیستم‌عامل ویندوز، باید از سرویس IIS استفاده کنیم، که جزییات بیشتر آن در ادامه خواهد آمد. برای انتقال فایل‌های وب‌سایت به کامپیوتر Web Server نیز روش‌های مختلفی وجود دارد که کارآمدترین و ساده‌ترین آن، استفاده از FTP برای انتقال فایل بر بستر شبکه WAN یا اینترنت است، هرچند می‌توان از FTP برای اشتراک و انتقال فایل بر بستر شبکه LAN یا MAN نیز استفاده نمود. برای تبدیل یک کامپیوتر به FTP Server نیز از همان IIS استفاده می‌کنیم. File and Printer Sharing که در آزمایش‌های پیشین برای اشتراک و انتقال فایل در بستر شبکه LAN استفاده می‌شد، دارای محدودیت‌های عمده‌ایی از جمله از نظر امنیتی است. (بکوشید در پایان این آزمایش، هر چه می‌توانید تفاوت بین File and Printer Sharing و FTP نام ببرید.)

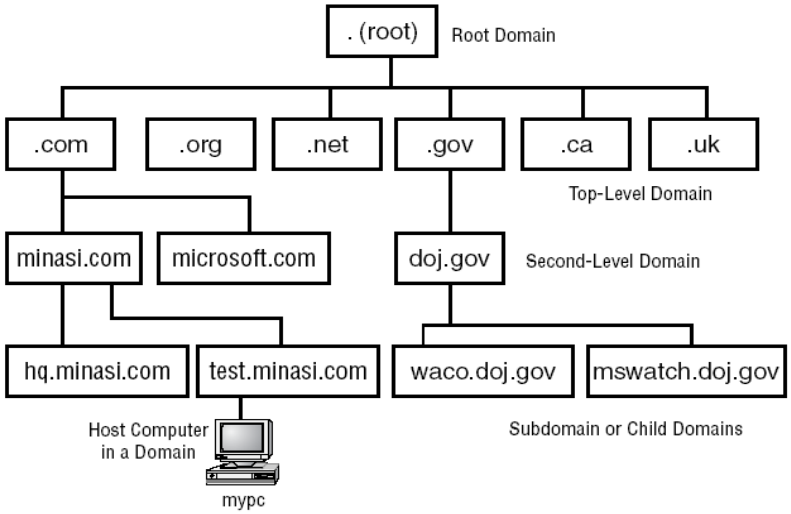
٤-٣-٢- Domain Name

همانگونه که در آزمایش اول فراگرفتیم، می‌توان به جای ارجاع به یک کامپیوتر با استفاده از آدرس IP مثلا در دستوری مانند Ping، می‌توان از Hostname آن استفاده نمود. چنین اسمی که در شبکه‌های ویندوز به NETBIOS Name نیز معروف است، علاوه بر داشتن ساختار مسطح (یعنی سلسله مراتبی نیست)، در شبکه‌های LAN مختلف ممکن است یکتا نباشد. در عوض برای ارجاع به یک کامپیوتر در شبکه جهانی، باید از یک اسم یکتا که به FQDN[1] موسوم است استفاده نمود. چنین مکانیزم نامگذاری‌ای به شبکه‌ها اسم می‌دهد و به اسم کامپیوترهای هر شبکه، اسم شبکه را نیز به عنوان پسوند اضافه می‌کند.

DNS Name که همان FQDN است نامی است یکتا و حرفی (متشکل از حروف الفبا)، که برای یک کامپیوتر در نظر گرفته می‌شود؛ البته می‌توان از آن برای ارجاع به وب‌سایتی که بر یک کامپیوتر قرار دارد نیز استفاده کرد، مانند www.iransport.net. همانطور که می‌دانیم کامپیوترها زمانی که با هم ارتباط برقرار می‌کنند از آدرس IP استفاده می‌کنند ولی هنگامی که ما می‌خواهیم به یک وب‌سایت متصل شویم از

[1] Fully Qualified Domain Name

Domain Name استفاده می‌کنیم. این دو دارای معنای یکسان هستند اما یکی را کامپیوتر استفاده می‌کند و دیگری را انسان. تبدیل بین این دو Name Resolution نام دارد و توسط DNS انجام می‌گیرد و در اینترنت جهانی اولین DNS معتبری که این تناظر برای یک وب‌سایت در آن ثبت می‌شود، Name Server نام دارد. نحوه عملکرد DNS به با توجه به ساختار سلسله مراتبی آن به شرح زیر است:



زمانی که نوشته می‌شود mail.yahoo.com یعنی Serverی در اینترنت وجود دارد که نام DNSی آن yahoo.com است و کامپیوتری در شبکه این Server واقع شده است که mail نام دارد و نام کامل آن mail.yahoo.com است. درخواست برای تبدیل Domain Name به IP Address از بالاترین رده‌ی DNS شروع شده و تا زمانی که به نتیجه نرسد، از DNSهای دیگر پرسیده می‌شود. این نحوه پرس و جو البته با یک ترتیب معین و دقیق و دور از دوباره‌کاری انجام می‌گیرد که شرح آن در درس مهندسی فناوری اطلاعات خواهد آمد.

٤-٤- Internet Information Service (IIS)

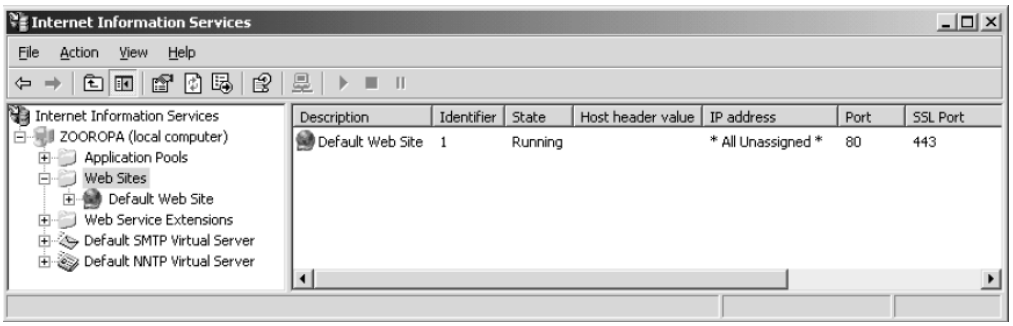
یک وب‌سایت برای اینکه به صورت ۲۴ ساعته در دسترس قرار گیرد، اولاً باید بر یک Server که همیشه روشن است، قرار گیرد و ثانیاً سرویسی[1] بر آن Server اجرا شود و امکان استفاده از برنامه‌ی وب را به ما بدهد، که این سرویس در ویندوز IIS (Internet Information service) نام دارد.

[1] Service به زبان ساده، برنامه‌ایی است که با شروع به کار ویندوز، اجرای آن شروع می‌شود و تا زمان اجرای ویندوز، در پیش‌زمینه در حال اجراست و این قابلیت را دارد که همواره در پس‌زمینه در حال اجرا باشد. به عنوان مثال، نحوه اجرای نرم‌افزارهای آنتی‌ویروس به صورت سرویس است.

Internet Information service در ویندوز ۲۰۰۳یک بستر (Platform) مشروح با توانایی سرویس‌دهی وب HTTP(Web)، FTP (file transfer)، NNTP(news) و SMTP (e-mail) برای یک سازمان است، اما استفاده از آن تنها منحصر به ویندوزهای Server نیست و می‌توان در ویندوز XP نیز از آن استفاده نمود و به این ترتیب امکان انجام آن نسبت به آزمایش‌هایی که تنها بر Windows 2003 Server قابل انجام است، بیشتر است. البته پر واضح است که این امکان در ویندوز XP بسیار محدودتر است.

IIS به خاطر همبستگی[1] آن با ویندوز، به سادگی قابل نصب، پیکربندی و مدیریت نیز است. IIS همچنین قابلیت گسترش برای پذیرش بیشترین میزبانی‌ها را داراست به عنوان مثال می‌تواند سایت بزرگی مانند مایکروسافت را میزبانی کند. با توجه به آمارهای Netcraft (www.netcraft.com/survey)، IIS دومین بستر برای web Serverها در دنیاست و مکان اول متعلق به Apache است، که یک ویرایش رایگان از Web Serverهای تحت یونیکس است.

IIS 5.0 مشکلات امنیتی زیادی داشت، Defaultهای ناامن فراوان سبب آسیب‌پذیری آن شده بود، اما ویرایش‌های بعدی آن، با تنظیمات پیش‌فرض امن، اطمینان بیشتری برای وب‌سایت‌ها فراهم کرده‌اند. همچنین از IIS می‌توان جهت ایجاد وب‌سایت داخلی برای یک موسسه نیز استفاده کرد و استفاده از آن تنها در اینترنت محدود نمی‌شود.



شکل ۱- نمایی از IIS در ویندوز 2003

٤-١-٤- پیکربندی IIS

در پیکربندی IIS چند تصمیم باید از پیش گرفته شود و آگهی‌هایی داشته باشید که برخی از آن‌ها در زیر آمده است:

[1] Integration

تنها پیش‌نیاز نصب IIS، نصب بودن پروتکل TCP/IP بر سیستم است، همچنین سیستم باید یک IP address ثابت داشته باشد. برای استفاده از نام‌های متعارف به جای آدرس IP در ارجاع به IIS، بایستی در شبکه‌تان DNS Server نیز داشته باشید (در حالت Intranet web server). همچنین اگر به اینترنت اتصال دارید، بایستی یک domain name برای سایتتان ثبت کنید و نیز بایستی دو Name Server داشته باشید یا از ISPتان بخواهید برایتان فراهم کند. در نهایت برای امنیت بیشتر توصیه اکید بر این است که سیستم‌فایل درایوی را که IIS بر آن قرار می‌گیرد، NTFS انتخاب کنید.

Port Number -۲-٤-٤

شماره پورت به‌طور خلاصه شماره‌ایی است که در سرآیند لایه چهار مدل OSI و لایه سه مدل TCP/IP قرار دارد و اشاره دارد به خدمتی که باید به بسته ورودی به کامپیوتر داده شود، به عنوان مثال شماره پورت ۸۰ برای خدمات وب (www)، ۲۱ برای خدمات FTP، ۲۵ برای ارسال ایمیل و ۱۱۰ برای دریافت ایمیل و ... است. بر این اساس، پس از ورود بسته به کامپیوتر، تشخیص داده می‌شود که به چه نوع برنامه‌ایی تحویل داده شود. شماره پورت‌های زیر ۱۰۲۴، که به پورت‌های استاندارد معروف هستند معمولا به یک خدمت متمایز اشاره دارند.

Http پروتکل (زبان یا قراردادی) است که بر طبق آن، کامپیوتر Client درخواست خود برای رویت یک صفحه وب را به Web Server ارسال می‌کند و کامپیوتر Web Server نیز در پاسخ، به همین زبان، فایل‌ها را به مرورگر کامپیوتر Client برمی‌گرداند. در زمان درخواست صفحه‌ی وب از یک Web Server، این عبارت به صورت خودکار پیش از آدرس وب‌سایت مقصد قرار می‌گیرد تا نوع درخواست را مشخص کند. بسته‌های HTTP که برای تبادل صفحات وب هستند و به عبارت دیگر، برای خدمات وب استفاده می‌شوند، دارای شماره پورت ۸۰ هستند.

٤-٥- دستور کار

توجه:

پیش از شروع به کار، از off بودن Windows Firewall اطمینان حاصل کنید.

مرور:

۱. پس از اینکه از اتصال کامپیوترتان به Switch اطمینان حاصل کردید به

Start -> Settings -> Network Connections

بروید و با کلیک راست بر کارت شبکه و انتخاب General Tab و سپس انتخاب Internet Protocol(TCP/IP) و زدن کلید Properties، مشخصات زیر را برای آن تنظیم کنید:

IP address: 192.168.0.**شماره گروه‌تان**

Subnet mask: 255.255.255.0

۲. به Start، Run بروید و در آن Cmd بنویسید و سپس دستور زیر را بنویسید:

Ipconfig

و از صحت تنظیمات انجام شده، اطمینان حاصل کنید.

۳. برای اطلاع از امکان دسترسی به سیستم‌های مجاورتان دستور زیر را برای یکی از گروه‌ها، در خط فرمان تایپ کنید:

Ping 192.168.0.**شماره گروه**

اگر جز Reply پاسخی می‌بینید، مشکل عدم ارتباط را برطرف کنید یا با گروه دیگری تست بگیرید.

آزمایش اصلی:

۴. پیش از هر چیز باید از نصب بودن IIS اطمینان حاصل کنید، بدین منظور ابتدا به مسیر زیر بروید و وجود IIS را تحقیق کنید.

Start -> Setting -> Control Panel -> Administrative Tools -> Internet Information Services

در صورتیکه وجود نداشته باشد با در اختیار داشتن Windows XP CD می‌توانید آن را از طریق زیر نصب نمایید:

از Add/Remove Programs در Control Panel استفاده کنید و Add/Remove Windows Components را انتخاب نمایید. در اینجا می‌توانید IIS را انتخاب و نصب کنید.

۵. اگر شرایط پیش‌فرض را پذیرفته باشید و تغییری در آن ایجاد نکرده باشید، تنظیمات وب‌سایت‌ها را به صورت زیر خواهید داشت:

Default web site (که دارای چند صفحه‌ی وب پیش‌فرض است) و به بسته‌های رسیده با شماره پورت ۸۰ TCP/IP به ازای تمام آدرس‌های IP تنظیم شده روی Web Server، پاسخ می‌دهد. Home directory یا مکانی که فایل‌های وب‌سایت شما در آن قرار می‌گیرد به صورت پیش‌فرض در c:\inetpub\wwwroot است.

الف)ابتدا در Notepad خطوط زیر را تایپ کنید و سپس آن را با نام "index.htm" ذخیره کنید و در c:\inetpub\wwwroot قرار دهید (در صورتیکه ویندوزتان در درایو دیگری غیر از C نصب شده است، اسم آن درایو را وارد کنید) و اگر فایل دیگری در آنجا وجود دارد آن را حذف نمایید.

```
<html>
<body>
<h1> Test Website شماره گروه </h1>
</body>
</html>
```

ب) سپس Internet Explorer را باز نمایید و در قسمت آدرس آن، عبارت زیر را تایپ کنید:

http:// آدرس IP سیستم‌تان

اگر IP Address کامپیوتر گروه‌های کناری را وارد کنید، چه خواهید دید؟

اگر صفحه ایجاد شده را ندیدید باید IIS را Start کنید (چگونه؟).

شیوه زیر را برای دسترسی امتحان کنید:

http:// آدرس IP سیستم‌تان:80

تصور می‌کنید، ۸۰ در اینجا چه نقشی بازی می‌کند؟ اگر نمی‌دانید می‌توانید در آزمایش هفت قسمت ب به آن برسید.

۶. بر Default Web Site کلیک راست کنید و Properties را انتخاب کنید. برای هر یک از Tabهای Web Site، Home Directory و Documents یک سطر توضیح بنویسید. (هر چه برداشت می‌کنید)

۷. به کارت شبکه‌تان بروید و در قسمت Internet Protocols با استفاده از کلید Advanced و IP Settings Tab، یک IP Address دیگر به کارت شبکه کامپیوترتان منتصب نمایید (شماره گروه+192.168.0.100). مثلاً اگر شماره IP شما 192.168.0.2 بود، اکنون باید 192.168.0.102 هم یکی دیگر از آدرس‌ها IP شما باشد.

(با استفاده از دستور ipconfig از درستی تنظیماتتان اطمینان حاصل کنید)

الف) حال بر اساس Web Site Tab از Default Web Site Properties بگویید چگونه می‌توان تنها با IP Address جدید به سایت‌تان دسترسی پیدا کرد؟

ب)از Web Site Tab از Default Web Site Properties، TCP Port را ۶۸۶۸ وارد کنید، حال خط زیر را در Address Bar از Internet Explorer وارد کنید:

آدرس IP سیستم‌تان://:http

آیا وب‌سایت‌تان نمایش داده می‌شود؟ چرا؟ چه باید کرد؟

ج) با استفاده از نتایج مورد ب حدس می‌زنید تغییر در شماره Port، چه کاربردی در جهان خارج برای دسترسی به وب‌سایت شما می‌تواند داشته باشد؟

۸. مربی بر یک کامپیوتر در آزمایشگاه، یک DNS Server برای تسهیل ارجاع به وب‌سایت‌ها از طریق نام و از طریق آدرس IP، راه‌اندازی کرده است. بر کارت شبکه‌تان در همان پنجره که آدرس IP را تنظیم می‌کنید، آدرس DNS Server را تنظیم کنید و از مربی بخواهید تا با ایجاد یک رکورد مرتبط در DNS Server ترتیبی فراهم نماید که بتوانید وب‌سایتتان را به صورت www.Your_Group_Name.com در Internet Explorer مشاهده نمایید.

شرح دهید که آیا این وب‌سایت به همین ترتیب و با همین نام از طریق اینترنت جهانی هم قابل دسترسی است؟ چرا؟

۹. با کلیک راست بر Default Web Site و سپس انتخاب New Virtual Directory یک وب‌سایت جدید ایجاد نمایید و که محتوی صفحه‌ی اول آن، کلمه Second Website باشد. حال توضیح دهید که چگونه می‌توان از کامپیوتری دیگر به این وب‌سایت وصل شد؟

راهنمایی: مفهوم Virtual Directory آن است که پوشه‌ایی بر آدرس کنونی وب‌سایت افزوده شود که وب‌سایت جدید در آن قرار گیرد. به عنوان مثال در آدرس http://eng.uok.ac.ir/sulaimany، Sulaimany یک Virtual Directory برای وب‌سایت http://eng.uok.ac.ir است.

۱۰. آیا می‌توانید بر اساس آنچه تا کنون آموختید، FTP Server راه‌اندازی کنید؟ پس از فعال‌سازی سرویس FTP، آدرس پوشه‌ی مرتبط با آن در c:\inetpub را بیابید.

۱۱. فایلی متنی با نام test.txt در پوشه‌ی مربوط به FTP قرار دهید. نحوه‌ی دسترسی به ftp خود یا دیگران از کامپیوتر شما به چه صورت خواهد بود؟ (باید در قسمت آدرس پنجره، چه عبارتی نوشته شود؟)

۱۲. برای اینکه با استفاده از خط فرمان وارد FTP گروهی دیگر شوید، نیاز به تعریف یک کاربر دارید، برای این امر به مسیر زیر بروید:

Start -> Setting -> Control Panel -> Administrative Tools -> Computer Management

از قسمت System Tools، Local Users and Groups و سپس Usersرا انتخاب نمایید و با کلیک راست در فضای خالی سمت راست پنجره و انتخاب New User کاربر جدیدی با مشخصات زیر ایجاد کنید:

User: ftpuser
Password: 123

۱۳. در خط فرمان دستور زیر را تایپ کنید تا به FTP گروهی دیگر وارد شوید:

ftp 192.168.0.شماره گروهی دیگر

برای نام کاربری و رمز عبور، موارد ایجاد شده در تمرین ۱۲ را استفاده کنید تا پیام زیر را دریافت کنید که نشان دهنده‌ی ورود موفق به FTP است:

User ftpuser logged in.

الف) با تایپ علامت ? دستورات مجاز برای استفاده را رویت کنید و سه مورد از آن‌ها را که می‌شناسید، هر کدام در یک سطر شرح دهید.

ب) با استفاده از دستور زیر فایل test.txt را به کامپیوتر خود انتقال دهید.

Get test.txt

بنویسید که فایل به چه آدرسی در کامپیوتر شما منتقل شده است؟

ج) حدس می‌زنید برای قرار دادن یک فایل در FTP کامپیوتری دیگر، باید از چه دستوری استفاده شود؟ بیازمایید و پاسخ را بنویسید و دلیل را شرح دهید. آیا لازم است که تنظیمی در Properties از FTP آن داده شود؟ چرا؟

آزمایش چهارم

Active Directory

۵-۱- مقدمه

طراحی ساختار IT یک سازمان از مهمترین دغدغه های مدیران آن به شمار می‌آید. شرکت‌ها و سازمان‌های کوچک پس از طی مراحل رشد مقدماتی به نحو خیره‌کننده‌ای تعدادکامپیوترهای خود را افزایش می‌دهند و دیگر راهکارهای قدیمی و محدود جوابگوی کیفیت خدمات و امنیت استفاده از شبکه نیست. بدین منظور لازم است تا نظم و کنترل متمرکزی بر تمام‌کامپیوترها وکاربران آن‌ها اعمال‌گرددکه این امر در ویندوز با استفاده از خدمتی[1] به نام Active Directory صورت می‌پذیرد. با کمک Active Directory شبکه‌هایی دارای کنترل متمرکز خواهیم داشت و بر خلاف شبکه‌های ساده‌ی Work Group، تمام کامپیوترهای و منابع تحت پوشش آن‌ها قابل کنترل و اعمال سیاست‌های دقیق است. این نوع شبکه در اصطلاح مایکروسافت Domain نامیده می‌شود که توسط کامپیوتر یا کامپیوترهایی که Active Directory بر آن‌ها نصب شده و Domain Controller نام دارند، کنترل می‌شود.

Active Directory پیوستگی عمیقی با DNS داردکه آن هم ارتباط مستقیم با ساختار IT سازمان داراست. به‌طور خلاصه، DNS خدمتی است که ساختار نامگذاری سلسله مراتبی برای اجزای فعال شبکه از قبیل کامپیوترها را فراهم می‌سازد.

بی‌تردید، امروزه یکی از نیازهای اصلی شرکت‌ها و سازمان‌ها به فردی است‌که بتواند با تسلط در رابطه با طراحی ساختار Active Directory اظهار نظر نماید و با برنامه‌ریزی درست در این زمینه، سازمان را از مشکلات آتی برهاند. در این آزمایش دانشجو با مبانی نظری اولیه و نحوه نصب و تنظیم مقدماتی و افزودن کامپیوتر به شبکه‌های Domain آشنا خواهد شد. با توجه به بحث بسیار گسترده‌ی مرتبط با Active Directory، در این آزمایش تنها تلاش شده است که دانشجو با کلیات آن و نحوه‌ی راه‌اندازی و تنظیم اولیه آشنا شود و ادامه‌ی بحث در رابطه با آن، خارج از محدوده‌ی این آزمایش است.

---

[1] Service

۵-۲- هدف

راه‌اندازی و تنظیمات اولیه شبکه‌های Domain در محصولات مایکروسافت

۵-۳- پیش آگاهی

سیستم‌عامل ویندوز در ویرایش‌های مختلف عرضه شده است. برخی از این ویرایش‌های دارای عنوان Server هستند، به عنوان مثال: Window 2000 Server، Window 2003 Server یا Window 2008 Server. سیستم‌عامل‌های Server تفاوت‌های بنیادی با سیستم‌عامل‌های معمولی یا Client مانند Windows XP دارند. از جمله اینکه می‌توان آن‌ها را برای عرضه انواع خدمات شبکه تنظیم نمود. به عنوان مثال، سیستم‌عامل Windows 2003 Server را می‌توان برای عرضه‌ی انواع خدمات شبکه از قبیل DHCP، DNS، RRAS، Active Directory، IIS با امکانات حرفه‌ای و ... تنظیم کرد. فعال‌سازی بسیاری از این خدمات مانند فعال‌سازی IIS از طریق گزینه‌های Add/Remove Windows Components از Control Panel امکان‌پذیر است.

Active Directory اصطلاحی است از شرکت مایکروسافت برای عرضه خدمت در حیطه‌ی دایرکتوری‌ها یا فهرست‌ها. یک خدمت از نوع فهرست[1] برای نگهداری اطلاعات مرتبط با اشیاء و کاربران مورد استفاده قرار می‌گیرد. به عنوان مثال یک شیء مانندکاربر می‌تواند در داخل یک خدمت از نوع فهرست، اطلاعاتی همچون شماره تلفن، آدرس الکترونیکی[2]، نام ساختمان و بسیاری از مشخصات را که یک راهبر[3] شبکه به آن ها نیازمند است، ذخیره نماید.

خدمات از نوع فهرست به عنوان یک لیست جامع از شبکه تلقی می‌گردند.که شامل تعاریفی ازکاربر، شیء و مدیریت هستند. این فهرست‌ها برای اعتبارسنجی کاربران وکنترل دستیابی به منابع استفاده می‌گردند. مثال‌هایی از فهرست‌های اولیه عبارتند از:

MVS PROFS (IBM), Grapevine's Reqistration Database, WHOIS

این فهرست‌ها تنها از طریق روش‌های دستیابی اختصاصی و در سطح محدود، قابل دستیابی بودند. برنامه‌های کاربردی‌که این نوع فهرست‌ها را مورد استفاده قرار می‌دادند عبارتند از:

Novel Groups Wise Directory, Lotus Notes, Unix Sendmail

[1] Directory Service
[2] Email
[3] Administrator

بیشترین توسعه خدمت از نوع فهرست درسیستم‌عامل Novel صورت گرفت. به طوری‌که در اوایل ۱۹۹۰ فهرست خدماتی ناول[1] به بازار عرضه گردید. این فهرست خدماتی توسط شرکت NetWare که متولی سیستم‌عامل Novel است ایجاد شد. سرانجام آن را طوری توسعه دادند تا بتواند ترکیبی از NT/NetWare را پشتیبانی نماید که NT اولین نسخه‌ی Windows Server است. زیرا ویندوز در آن‌زمان نیز محبوبیت زیادی داشت اما فهرست خدماتی در آن لحاظ نشده بود. از طرفی به علت عدم سهولت در اداره‌کردن نام‌های دامنه‌های در ویندوز NT و کنترل متمرکز برکاربران، سازمان‌ها مجبور شدند تا از فهرست‌های خدماتی ناول استفاده نمایند. وجود این‌گونه‌کمبودها در NT، موجب‌گردید تا شرکت مایکروسافت مقدمات ایجاد Active Directory را فراهم نماید.

۵-۳-۱- ویژگی‌های اصلی Active Directory

نظر به تلاش‌های صورت گرفته برای تطابق ساختار Active Directory با آخرین پروتکل‌ها و ساختار اینترنت، عملکرد آن با پنج جزء کلیدی و مرکزی گره خورده است:

- تطابق با TCP/IP

پروتکل TCP/IP برخلاف بسیاری پروتکل‌های خاص منظوره‌ی شرکت‌ها، برای عملکرد مستقل از سیستم‌عامل و در سطح جهانی طراحی شده است و فعالیت Active Directory نیز بر آن استوار است و از این پروتکل برای ایجاد ارتباط استفاده می‌نماید.

- پشتیبانی از LDAP[2]

این پروتکل به عنوان یک پروتکل استاندارد فهرست‌ها عرضه شده و وظایفی از قبیل به روزرسانی و جستجوی اطلاعات در فهرست را برعهده دارد. Active Directory نیز به‌طور مستقیم از آن استفاده می‌کند تا در بین هزاران رکورد، به سرعت و کارآمدی جستجو نماید.

- پشتیبانی از سیستم نامگذاری DNS

از زمانی‌که نیاز شدیدی به ترجمه‌ی آدرس IP به نام قابل فهم برای انسان احساس گردید، این امکان پدیدارگشت. اکتیودایرکتوری برای انجام صحیح فعالیت‌ها، به طور مؤثر به فضای نام نیازمند است. به عبارتی هر کامپیوتر در Active Directory دارای یک نام سلسله‌مراتبی مبتنی بر DNS است. مثلا اگر کامپیوتر یک کاربر با نام Ali به شبکه‌ی از نوع Active Directory با نام دامنه‌ی Uok.com محلق شود. زین پس نام آن کامپیوتر در چنین شبکه‌ای Ali.Uok.com خواهد بود.

[1] Novel Directory Service
[2] Lightwieght Directory Access Protocol

- امنیت

امنیت برای محیطی که امکان اتصال و ارتباط و کنترل متمرکز صدها، هزاران و حتی میلیون‌ها کامپیوتر و کاربر را در یک شبکه محدود یا پخش‌شده در سراسر جهان داشته باشد، بسیار مهم است. زیرا موجب انجام شدن فعالیت‌ها در محیطی کاملاً امن و مطمئن می‌گردد. ویندوز ۲۰۰۳ و Active Directory دارای امنیت در سطح بسیار بالا هستند. به طوری که از پروتکل‌ها و قابلیت‌های امنیتی زیرحمایت می‌نمایند:

IP Sec, Kerberos, SSL, Certificate Authorities

چنین قابلیت‌هایی سبب انتقال ایمن رمزعبور کاربران در ورود به سیستم‌های تحت Domain یا دامنه می‌شود و فعالیت‌های نفوذگری را در این رابطه، بی‌اثر می‌سازد.

- مدیریت آسان

استفاده از امکانات فهرست‌های خدماتی باعث سهولت در مدیریت و پیکربندی محیط و کاهش زمان و هزینه می‌شود. در سیستم‌عامل ویندوز به سادگی می‌توان با Active Directory آشنا شد و با آن کار کرد.

۵-۳-۲- اعتبارسنجی[1] یا شناسایی در Active Directory

ویندوز NT که ویرایش‌های قدیمی ویندوزهای Server مایکروسافت است از روشی به نام NT LAN Manager یا NTLMبرای اعتبارسنجی یا شناسایی کاربر استفاده می‌نمود. این روش کلمه عبور را به صورت درهم[2] در شبکه ارسال می‌نمود. مشکل این روش آن بود که مهاجم می‌توانست از کلمه‌ی رمز درهم‌سازی عبوری از شبکه آگاهی پیداکرده، آن‌ها را جمع آوری نموده و با استفاده از ابزارهای رمزگشایی به واژه‌ی استفاده شده به عنوان کلمه عبور و فنون رمزگذاری پی ببرد.

ویندوز ۲۰۰۰ و ۲۰۰۳ از الگوریتم امنیتی محکمی به نام Kerberos برای اعتبارسنجی استفاده می‌نمایند که این روش اطلاعات مربوط به‌کلمه‌ی عبور را در سطح شبکه ارسال نمی‌نماید و نسبت به NTLM مطمئن‌تر است. Kerberos به طور پیش فرض در Active Directory استفاده نمی‌شود، زیرا Active Directory به صورت پیش‌فرض قابلیت تطابق با ویرایش‌های امنیتی پیشین را دارد.

[1] Authentication
[2] Hash

۵-۳-۳- ساختار Active Directory

ساختار منطقی Active Directory از عناصر زیر تشکیل شده است:

۵-۳-۳-۱- دامنه[1]

محدوده‌های اصلی در یک Active Directory را دامنه می‌نامند. کاربران، کامپیوترها و به طور کلی اشیا در داخل دامنه‌ها قرارمی‌گیرند و به‌صورت متمرکز مدیریت می‌گردند. دامنه‌ها با استفاده از سیاست‌های امنیتی به مدیریت اشیا می‌پردازند. به عنوان مثال دامنه‌های مختلف می‌توانند شامل سیاست‌های مختلف کلمه عبور، برای کاربران باشند. بایستی این نکته مهم را به یاد داشت که هردامنه، یک سازمان منطقی از اشیا است که به راحتی چندین ناحیه فیزیکی را به یکدیگر مرتبط می‌نماید. اگر قرار باشد برای شرکتی با نام ariatech یک ساختار IT متمرکز ایجاد کنیم. یک دامنه‌ی پیشنهادی برای آن، ariatech.com است. آدرس یک کامپیوتر در این دامنه، به عنوان مثال می‌تواند pc1.ariatech.com باشد، یعنی اسم دامنه در اکتیودایرکتوری، همیشه به عنوان پسوند اسم کامپیوتر اضافه خواهد شد.

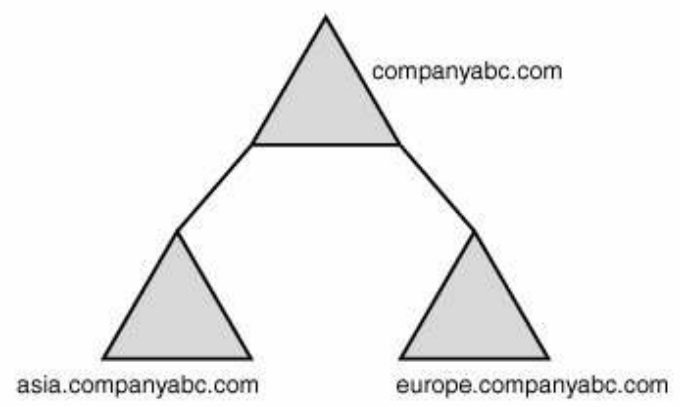
۵-۳-۳-۲- درخت[2]

یک درخت از ترکیب چند دامنه به وجود می‌آید. این دامنه‌ها از طریق اعتماد انتقالی دوطرفه[3] با یکدیگر ارتباط برقرار می‌نمایند. منظور نوعی از اعتماد در ارتباطات است که اگر یک دامنه به نام x اجازه دهد کاربران دامنه‌ی y از منابعش استفاده کند و دامنه‌ی z نیز به کاربران دامنه‌ی x اجازه‌ی استفاده دهد آنگاه کاربران دامنه‌ی y اجازه‌ی استفاده از دامنه‌ی z را خواهند داشت. دامنه‌های موجود در یک درخت خصوصیات کلی آن را به اشتراک می‌گذارند. در شکل زیر دامنه‌ی ریشه Companyabc.com نام دارد. زیر شاخه‌های این دامنه asia.companyabc.com و euro.companyabc.com هستند.

اعتماد دوطرفه مطمئن از نسخه‌ی ویندوز ۲۰۰۳ به بعد به صورت خودکار تنظیم می‌شود. یعنی نیاز به تنظیم دستی توسط راهبر شبکه ندارد. در اینجا نیز ارتباط دامنه asia و euro با companyabc، سبب انتقال ارتباط بین asia و euro می‌شود. درخت معمولا در مواردی مورد استفاده قرار می‌گیرد، که شرکت بزرگ و دارای چند شعبه باشد. در این حالت برای هر دامنه در درخت، یک Server جدا اختصاص داده شده و یک Active Directory نصب می‌شود.

---

[1] Domain
[2] Tree
[3] Two-Way Transitive Trust



شکل ۵-۱ مثالی از یک درخت متشکل از دو دامنه

۵-۳-۳-۳- جنگل[1]

جنگل‌ها ترکیبی از درخت‌های مرتبط به یکدیگر هستند. درخت‌ها در داخل یک جنگل از طریق ریشه‌هایشان به یکدیگر متصل هستند. چنین ساختاری فقط در مورد سازمان‌های بسیار بزرگ و گسترده در یک محدوده‌ی جغرافیایی وسیع نیاز خواهد شد. تمامی دامنه‌ها و درخت‌ها در یک جنگل به یکدیگر مرتبط هستند. دامنه و درخت‌ها نیازی به اشتراک‌گذاشتن فضای نام ندارند. به عنوان مثال Microsoft.com و Msn.com می‌توانند بدون نیاز به به اشتراک‌گذاشتن فضای نام خود، در بخشی از جنگل با یکدیگر مرتبط باشند و فضای نام خود را نیز حفظ نمایند.

در این حالت جنگل، مرجع سازمان‌دهی اصلی از نظر امنیتی در داخل Active Directory است. فرض بر این است‌که تمام راهبران در داخل جنگل به درجات مختلف با یکدیگر در ارتباط هستند. اگر راهبری با دیگر راهبران ارتباط برقرار ننماید، آن گاه باید در جنگلی دیگر قرار گیرد.

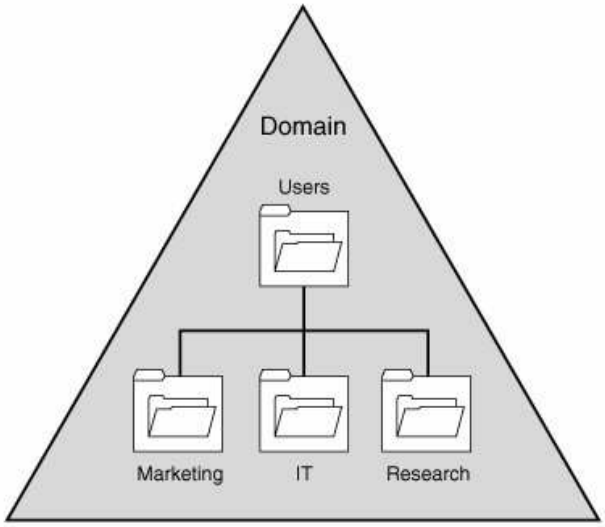
۵-۳-۳-۴- واحد سازمانی[2]

گاهی لازم است در یک سازمان کوچک که یک Active Dircetory محدود دارد، یعنی ساختار یک دامنه‌ای دارد، برخی واحدها را به صورت منطقی از هم جدا کنیم. مثلا واحد حسابداری به دلیل نیاز به اعمال سیاست‌های خاص، از واحد آموزش جدا شود. واحدهای سازمانی به عنوان صندوقچه‌هایی برای ذخیره اطلاعات دایرکتوری‌ها به صورت منطقی هستند. واحدهای سازمانی، اصلی‌ترین روش برای

[1] Forest

[2] - Organizational Unit (OU)

سازماندهی اطلاعات مربوط به‌کاربران،کامپیوترها و سایر اشیا در یک دامنه هستند. این سازماندهی در قالب لایه های قابل فهم صورت می‌گیرد. در شکل ۱-۷ یک واحد سازمانی ریشه‌که در آن سه واحد سازمانی تودرتو به نام های IT، Marketing، Research قرارگرفته است، نشان داده شده است. تودرتو بودن، سازمان را قادر می‌سازد تا کاربران را در چندین بخش(صندوقچه) تقسیم بندی نماید. این‌کار سبب نمایش ومدیریت آسان منابع برای شبکه می‌گردد. در داخل اکتیودایرکتوری می‌توان به سادگی، واحد سازمانی ایجاد کرد.



شکل ۱- ۷ : نمونه‌ای از سازماندهی واحدهای سازمانی در داخل یک دامنه

واحدهای سازمانی قادر به تقسیم بندی بیشتری برای منابع خواهند بود. این واحدها موجب مدیریت و سازماندهی آسان می‌گردند. دفاتر دوردست یک سازمان می‌توانند واحدهای سازمانی را برای مدیران خود در اختیار داشته باشند. هنگامی که سازمان نیاز به یک مدیریت‌کلی برتمامی مدیران دارد، یک واحد سازمانی ایجاد می‌نماییم. اگر یک شخص یا گروه بتواند یک دامنه را به درستی مدیریت نماید، نیازی به استفاده از واحدهای سازمانی نیست.

۵-۳-۳-۵- گروه

در اکتیودایرکتوری می‌توان کاربران را در سطوح مختلف دسترسی و قابلیت، قرار داد. به هر سطح، یک گروه گفته می‌شود. قوی‌ترین گروه در شبکه‌های مبتنی بر اکتیودایرکتوری، Administrators است. چنین کاربرانی توان ایجاد تنظیمات و اعمال تغییرات در هر سطحی را دارند. این در حالی است که یکی از

ضعیف‌ترین گروه‌ها در اکتیودایرکتوری، Users است که امکان نصب برنامه و تغییر تنظیمات مهم در سیستم را ندارد. هر کاربر که ایجاد می‌شود به صورت پیش‌فرض در گروه Users عضو می‌شود.

۵-۳-۳-۵-۱- قواعد مربوط به‌گروه‌ها در محیط اکتیودایرکتوری

گروه مکانیزمی برای مدیریت هر چه بهتر امنیت بر روی کاربران است. بدون‌گروه، سازماندهی منطقی‌کاربران و اعطای مجوز دسترسی به اشیای موجود در شبکه، بایستی به صورت دستی صورت گیرد. یعنی اگر تمام‌کاربران یک اتاق نیاز به چاپگر داشته باشند، هرکاربر باید به صورت دستی وارد لیست مجوزهای دسترسی به چاپگر شود. بنابراین ابداع گروه باعث راحتی راهبران می‌شود. حال اگر برای کاربران همان اتاق، دسترسی به چاپگر را با کمک مکانیزم گروه تنظیم کنیم، کافی است همه‌ی آن‌ها را در یک گروه خاص عضو کرده و تنها برای آن گروه، مجوز دسترسی صادر کرد، و نه هر یک ازکاربران موجود درآن.

در اکتیودایرکتوری دو نوع‌گروه امنیتی و توزیعی وجود دارد. اصولاً یک‌گروه امنیتی برای اعطای مجوزهای دسترسی به اعضای‌گروه به‌کار می‌رود و یک‌گروه توزیعی به عنوان یک شی برای ارسال اطلاعات به اعضای‌گروه استفاده می‌گردد.

۵-٤- پیش‌نیاز

جزوه‌ی مربوط به کار با نرم‌افزار شبیه‌ساز Virtual PC را از صفحه‌ی درس در وب‌سایت دانلود کنید و برای انجام سریعتر آزمایش، حتما قبل از انجام آزمایش، آن را مرور کنید.

۵-۵- تکلیف

مفهوم Schema در AD را بنویسید.

۵-٦- منابع

بخش های چهارم و پنجم کتاب:

Microsoft® Windows Server 2003 Unleached, R2 Edition, By Rand Morimoto, Michael Noel, Alex Lewis, : Sams Publisher, May 10, 2006.

دستور کار

توجه ۱: در این آزمایش از نرم‌افزار شبیه‌ساز Microsoft Virtual PC استفاده خواهد شد. دو سیستم عامل Windows XP و Windows 2003 Server برای انجام این آزمایش لازم است که مربی، مکان آن‌ها و نحوه‌ی فعال‌سازی و استفاده از آن‌ها در محیط Microsoft Virtual PC را آموزش خواهد داد.

توجه ۲: نظر به اینکه، محیط فراهم شده توسط نرم‌افزار شبیه‌سازی Microsoft Virtual PC، کاملا مانند محیط طبیعی رفتار می‌کند، برای جلوگیری از تداخل احتمالی آدرس‌های IP تنظیم شده توسط گروه‌ها، پیش از اجرای سیستم‌عامل‌های موجود در نرم‌افزار Microsoft Virtual PC، بر گزینه‌ی Stteings در آن کلیک نموده و کار کارت شبکه (Networking) را در حالت Local Only تنظیم کنید.

۱. همانگونه که از مربی آموختید، دو سیستم‌عامل XP و Winodows 2003 را به کمک Microsoft Virtual PC فعال و آماده‌ی استفاده نمایید. برای سیستم‌عامل Windows XP، اختصاص 64 MB حافظه RAM و برای سیستم‌عامل Windows 2003 Server، اختصاص 192 MB حافظه RAM کفایت می‌کند.

۲. پیش از راه‌اندازی و تنظیم شبکه با کنترل متمرکز، لازم است محدوده‌ی آدرس دو سیستم‌عامل XP و Winodows 2003 را به درستی تنظیم نمایید و از امکان ارتباط بین این دو، مطمئن شوید. انتخاب آدرس IP مناسب برای هر سیستم عامل، به اختیار گروه است. آدرس‌های انتخابی را در برگه گزارش کار یادداشت کنید. با دستور Ping از صحت ارتباط آن‌ها اطمینان حاصل کنید.

۳. الف) پیش از شروع به نصب Active Directory، از گزینه‌های موجود در آدرس زیر در سیستم‌عامل Windows 2003 Server، با کمک کلید Print Screen بر صفحه کلید، عکس گرفته و با کمک محیط Paint، عکس گرفته شده را در Desktop آن سیستم عامل کپی کنید:

Start -> Programs -> Administratrive Tools

ب) در پنجره‌ی RUN در Windows 2003 Server، کلمه‌ی DCPromo را بزنید تا تبدیل شدن سیستم‌عامل جاری به Domain Controller شروع شود. مراحل نصب را همانند آنچه مربی آموزش داده است، طی کنید و منتظر بمانید تا فرایند نصب، تکمیل شود. در مرحله‌ی پنجم نصب، Full DNS

Name را ITGroup.com انتخاب کنید. در پایان نصب، سیستم عامل مربوطه را متعاقبا Restart نمایید.

ج) در ورود به سیستم عامل جدید، چه تغییری روی داده است؟

د) گزینه‌های موجود در آدرس Administrative Tools را با گزینه‌های بخش الف همین سوال مقایسه کنید و موارد افزوده شده در اثر نصب Active Directory را در برگه‌ی گزارش کار، یادداشت نمایید.

و) در تنظیمات کارت شبکه‌ی Windows 2003 Server، در بخش آدرس DNS، همان آدرس IP Windows 2003 Server جاری را بنویسید. برای ویندوز XP نیز، آدرس DNS را آدرس سیستم Windows 2003 Server لحاظ نمایید.

ی) برای ایجاد یک کاربر که بتواند در سراسر کامپیوترهای متعلق به این دامنه امکان ورود داشته باشد، در Administrative Tools در Windows 2003 Server، به Active Directory Users and Computers بروید و پوشه‌ی Users را از دامنه‌ی ITGroup.com، انتخاب نموده و با کلیک راست، نام کاربری جدید testuser را با رمز عبور 1234Abc ایجاد کنید.

۴. الف) اکنون امکان پیوستن کامپیوتر Windows XP به دامنه‌ی ITGroup.com فراهم است. با کلیک راست بر My Computer در ویندوز XP و انتخاب سربرگ Computer Name، برای اتصال آن به دامنه، کلید Change را انتخاب کرده و انتخاب Member of Domain را با نوشتن نام دامنه‌ی ITGroup.com، تکمیل کرده و کلیدهای OK را پیاپی بزنید تا سیستم نیاز به Restart پیدا کند و آن را Restart کنید.

ب) با بررسی محتوی DNS و محتوی پوشه‌ی Computers در Active Directory Users and Computers در ویندوز ۲۰۰۳، حدس می‌زنید چه مواردی پس از پیوستن ویندوز XP به دامنه‌ی ITGroup.com، در این بخش‌ها اضافه و ثبت شده است؟

۵. الف) در ورود به ویندوز XP از حالت دامنه استفاده کنید و نام کاربری ایجاد شده در بخش **ی** از سوال ۳ را مورد استفاده قرار دهید. سعی کنید پس از ورود تحت دامنه، ساعت سیستم را تغییر دهید. چه اتفاقی روی می‌دهد؟ بر این اساس آیا حدس می‌زنید امکان نصب یا پاک کردن برنامه‌های کامپیوتر جاری را دارید؟ چرا؟

ب) Logoff کنید و با نام کاربری و رمزعبور Administrator ویندوز ۲۰۰۳ که اکنون Administrator کل دامنه به حساب می‌آید، به ویندوز XP وارد شوید. نتیجه‌ی فعالیت‌های بخش

الف همین سوال، با چنین نام‌کاربری‌ای، چیست؟ آیا می‌توانید رمز کاربر Administrator محلی ویندوز XP را نیز عوض کنید؟ چه نتیجه‌ای می‌گیرید؟

۶. با کلیک بر کاربر ایجاد شده در اکتیودایرکتوری در Windows 2003 Server، شرح یک سطری بر هر یک سطری بر هر یک از سربرگ‌های General، Member of و Account بنویسید. اگر زمان آزمایش شما هنوز تمام نشده است، گزینه‌ی Logon Hours را از سربرگ Account تست کنید.

آزمایش پنجم

پیکربندی خودکار پویای ماشین میزبان (DHCP)

٦-١- مقدمه

در ایـن آزمـایش بـه معرفـی DHCP پرداختـه خواهـد شـد. DHCP کـه مخفـف Dynamic Host Configuration Protocol است در واقع پروتکلی برای پیکربندی پویای ماشین میزبان از جهت آدرس IP و آدرس DNS و Default Gateway و موارد مشابه است. DHCP به صورت یک خدمت یا سـرویس در ویندوزهای سرور لحاظ شده است.

در این آزمایش همچنین به معرفی ویرایش ۶ از آدرس‌های IP پرداختـه خواهـد شـد کـه انتظـار مـی‌رفـت تاکنون، جای آدرس‌های IPv4 که ۳۲ بیتی هستند را بگیرند و محدودیت‌های مرتبط با آن‌ها را رفع نمایند اما هنوز چنین نشده است ولی به زودی در حیطه‌ی وسیعی از کاربردهای شبکه، خود را نشان خواهند داد.

٦-٢- هدف

- آشنایی با فعال‌سازی و تنظیم DHCP در سیستم‌عامل Windows Server
- آشنایی و کار با آدرس‌های IPv6

٦-٣- پیش‌آگاهی

مکانیزم دستی تنظیم آدرس‌های IP برای شرکت‌ها و مؤسساتی که تعداد کامپیوترهای آن‌ها در حد انگشتان دست باشد، کفایت می‌کند. اما برای شرکت‌ها و سازمان‌ها بزرگ با چند صد یا چندین هزار کامپیوتر، بسیار دشوار خواهد بود اگر بخواهیم تک تک کامپیوترها را به صورت دستی تنظیم کنیم. زیرا همانطور که می‌دانیم آدرس‌های IP دارای یک سازمان‌دهی خاص هستند و زمانی که برای تعداد زیاد و متنوعی از کامپیوترها در بخش‌های مختلف سازمان، آدرس‌های با محدوده‌های متفاوت تعریف کنیم، بایستی همیشه در افزودن کامپیوتر جدید یا در تغییر تنظیمات یک کامپیوتر جاری، تمام جزییات تنظیمات را مرور کنیم و از اشتباهات احتمالی پرهیز کنیم. از طرفی، ممکن است بارها در سازمان یا شرکت، مواردی پیش آید که نیاز به تغییر پارامترهای مرتبط با تنظیمات آدرس IP همه یا بخش بزرگی از کامپیوترها باشیم. به عنوان مثال اگر در یک سازمان بزرگ که تنظیمات آدرس IP از طریق دستی ایجاد شده است، آدرس Default Gateway که متولی فراهم ساختن دسترسی به اینترنت یا شبکه‌ی خارجی برای کامپیوترهاست یا DNS که متولی ترجمه‌ی آدرس‌های اینترنتی (URL) به آدرس IP برای استفاده‌ی کامپیوترهاست، تغییر کند، کارشناسان شبکه بایستی روزهای متوالی برای انجام تغییرات به تک تک کامپیوترها مراجعه کنند (شکل زیر را ببنید).

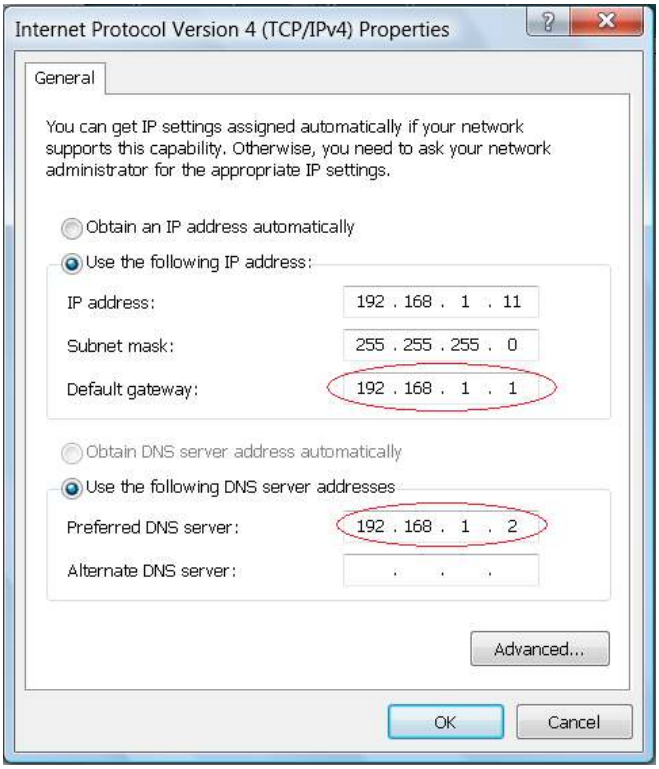
از این‌رو خدمتی یا سرویسی در شبکه به وجود آمده است که متولی ارائه‌ی تنظیمات متنوع به کارت شبکه‌های کامپیوترهاست. چنین تنظمیاتی تنها به کارت شبکه‌هایی داده می‌شود که از گزینه‌ی Obtain an IP address automatically استفاده می‌کنند(شکل زیر را ببینید).

چنین گزینه‌ای را مدیر شبکه از پیش و به عمد انتخاب کرده، تا در شروع به کار این کامپیوترها، اولین درخواستی که به صورت همه‌پخشی[1] از تمام شبکه محلی انجام می‌دهند آن باشد که آیا کامپیوتر ویژه‌ای وجود دارد که تنظیمات آدرس IP را به آن‌ها نسبت دهد و برای آن‌ها رزور نماید؟ این کامپیوتر ویژه، براساس پروتکل DHCP که مخفف Dynamic Host Configuration Protocol یا **پیکربندی پویای**

[1] Broadcast

ماشین میزبان است کار می‌کند و وظیفه‌ی آن انتساب تنظیمات متنوع به کامپیوترهایی است که در حالت انتساب خودکار تنظیمات شبکه هستند.

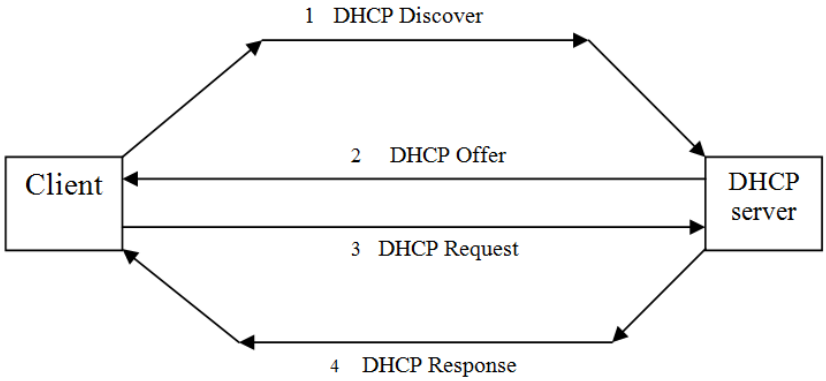
حال سوال این است که کامپیوتری که آدرس IP ندارد، چگونه می‌تواند با دیگران در شبکه‌ی محلی ارتباط برقرار کند؟ مگر نه اینکه مبنای ارتباطات کامپیوترها، آدرس IP است؟



شکل ٦-١ نمای تنظیمات اولیه‌ی کارت شبکه

لازم به یادآوری است که هر کامپیوتر در شبکه دارای چندین آدرس با کاربری‌های مختلف است. به عنوان مثال آدرس MAC که در زمان ساخت، بر کارت شبکه حک شده است، شماره‌ی یکتایی است که امکان ارتباط کامپیوترها در شبکه‌های LAN و در حالتی که آدرس IP نداشته باشند را فراهم می‌سازد. بنابراین در شروع به کار یک سیستم که دارای آدرس IP نیست، از آدرس MAC برای ارتباط با دیگران استفاده می‌شود. همانطور که اشاره شد، ارتباط از طریق MAC در این حالت، همه‌پخشی است. یعنی تمام کامپیوترهای شبکه محلی، درخواست تنظیمات را از سایرین مشاهده می‌کنند.

کامپیوتر یا به زبان بهتر، Serverیی که متولی رسیدگی به درخواست‌های تنظیمات خودکار آدرس IP و موارد مشابه است، DHCP Server نام دارد که می‌توان از سیستم‌عامل ویندوز Server برای ایجاد آن استفاده کرد. روند درخواست و رسیدگی به آن مطابق با شکل زیر است:



شکل ٦-۲ روند درخواست و رسیدگی به آن در پروتکل DHCP

کامپیوتر Server که از پیش برای این کار مهیا شده است، دارای مجموعه‌ای از آدرس‌هاست که می‌تواند به هر کامپیوتر درخواست دهنده، یکی از آن‌ها را اختصاص دهد. این آدرس‌های اختصاص داده شده، دایمی نیستند و پس از مدت زمان مشخصی، که زمان اجاره نام دارد، در صورت عدم ارجاع کامپیوتر اجاره گیرنده، آزاد می‌شوند و قابل اختصاص به سایرین هستند.

برخی واژه‌ها و تنظیمات که همه‌ی DHCP Serverها دارا هستند، در زیر به صورت خلاصه توضیح داده شده‌اند:

- lease duration :مدت زمان اجاره یک آدرس IP
- Reservation: اختصاص همیشگی یک IP به یک MAC خاص؛ برای مثال زمانی که مایل هستیم در شبکه، مثلا به یک دوربین مداربسته‌ی خاص، همیشه یک آدرس مشخص IP اختصاص یابد تا برای کار با آن و اتصال به آن از طریق شبکه، مجبور به مکاشفه و بررسی آدرس اختصاص نباشیم.
- Exclusion : آدرس‌های تنظیم شده به صورت دستی (به عبارتی آدرس‌هایی که در محدوده‌ی مستثنی شده‌اند). مثلا ممکن است مایل نباشیم برخی Serverهای خاص، از DHCP تنظیمات خود را دریافت کنند. اما برای اینکه محدوده خاصی از آدرس‌های تحت کنترل DHCP را مجزا کنیم، از این امکان استفاده می‌کنیم.
- Address Pool : مجموعه آدرس‌های آماده برای اختصاص
- Scope:محدوده آدرس‌های اختصاص یافته به کامپیوترها را مشخص می‌کند. به‌طور مثال محدوده‌ی 192.168.1.1 تا 192.168.1.253 ارای ۲۵۳ آدرس جهت اختصاص است. البته در داخل DHCP چندین محدوده‌ی مختلف برای چندین شبکه‌ی LAN تعریف کرد. یعنی به عبارت دیگر ، چندین Scope داشت که این امر برای سازمان‌های بزرگ رایج است.

- Scope Option: گزینه های اضافی همراه با آدرس IP، مانندDNS, Default Gateway و....
- Server Option: زمانی که چندین Scope متفاوت تعریف کرده باشیم و بخواهیم تنظیماتی یکسان را به همه‌ی آن‌ها اعمال کنیم، از این گزینه استفاده می‌کنیم.

٦-٤- آدرس IPv6

به صورت خلاصه و غیرفنی، یکی از مهمترین معایب آدرس‌های IP جاری مورد استفاده که آدرس‌های ویرایش ۴ یا IPv4 نام دارند، محدودیت تعداد کامپیوترهایی است که می‌توانند تحت پوشش قرار دهند. آدرس‌های IPv4 که ۴ بایتی هستند، می‌توانند حدود ۴ میلیارد آدرس در اختیار ما قرار دهند که این تعداد اکنون کفاف تمام کامپیوترهای دنیا که متصل به شبکه جهانی اینترنت هستند را نمی‌دهد به همین دلیل ویرایش جدیدی از این آدرس‌ها که ۱۲۸ بیتی یا شانزده بایتی است عرضه شده است. به دلیل تعداد بیت‌های زیاد، نحوه‌ی نمایش این آدرس‌ها در مبنای هگزادسیمال است. نحوه‌ی نمایش این آدرس‌ها متشکل از ۸ تا ۲ بایتی است که یک نمونه از آن را نیز در زیر آمده است:

DF2D:1893:1389:1351:4513:2B2E:1897:FFFF

به جهت مختصر نویسی، رقم‌های هگز متناظر با صفر از ظاهر آدرس حذف می‌شود. یعنی وجود علامت :: در یک IP Address به معنای صفر بودن ۴ یا ۸ یا ۱۲ یا بیشتر رقم صفر هگز است. گرچه جزییات بسیار زیادی در رابطه با این آدرس‌ها قابل بررسی است، اما در این آزمایش که هدف آن، صرفا آشنایی با این آدرس‌ها و نحوه‌ی کار با آن‌هاست، به همین توضیح مختصر اکتفا می‌شود.

٦-٥- تکلیف جلسه بعد

۱. پس از انجام آزمایش، تحقیق کنید آیا مکانیزم تمرین ۲ که به APIPA معروف است، برای لینوکس یا سایر سیستم‌عامل‌های غیر از ویندوز نیز برقرار است؟ اگر بلی، محدوده‌ی آدرس داده شده به Clientهای آن‌ها چیست؟
۲. تحقیق کنید که آیا می‌توان همزمان در یک شبکه که تمام کامپیوترهای آن با یک یا چند سوییچ معمولی به هم متصل هستند و به صورت فیزیکی با هم در ارتباط‌اند، بیش از یک DHCP Server داشت؟ اگر چنین است، چه توجیهی برای وجود همزمان این دو وجود دارد؟ تنظیمات این دو باید چگونه باشد؟

٦-٦- دستور کار

توجه ۱: به خاطر دامنه نفوذ DHCP و تحت تأثیر قرار گرفتن سایر کامپیوترهای شبکه توسط آن، پیش از اجرای سیستم‌عامل‌های موجود در نرم‌افزار Microsoft Virtual PC، بر گزینه‌ی Stteings در آن کلیک نموده و کار کارت شبکه (Networking) را در حالت Local Only تنظیم کنید.

توجه ۲: آزمایش‌های جاری نیز با استفاده از نرم‌افزار Microsoft Virtual PC و دو سیستم عامل Windows XP و Windows 2003 انجام خواهد شد.

۱. ابتدا در صورتیکه Active Directory از مرحله قبل برجا مانده است، بهتر است به منظور فراگیری نحوه از Domain در آوردن Windows XP و سریعتر شدن اجرای ویندوز ۲۰۰۳ و نیز فراگیری روش حذف Active Directory:

الف) بر My Computer در ویندوز XP کلیک راست کرده و آن را از Domain خارج کنید.

ب) در Run، دستور dcpromo را بزنید. نوشتن مجدد این دستور سبب شروع روند حذف آن خواهد شد. روند را تا آخر پی‌گیری کنید و Windows 2003 را در انتها Restart کنید.

توجه: می‌توانید آزمایش ۲ را به موازات این بخش پیش ببرید.

ج)پس از حذف Active Directory، آدرس Windows 2003 را 192.168.i.1 تنظیم کنید که i شماره گروه است.

۲. در زمان حذف Active Directory از ویندوز ۲۰۰۳، به سراغ ویندوز XP بروید و بر کارت شبکه آن گزینه‌ی Obtain an IP Address Automatically و Obtain DNS Server address automatically را انتخاب کنید و منتظر بمانید تا انیمشن جستجوی تنظیمات کارت شبکه، ساکن شده و بر آن علامت مثلث زرد رنگی پدیدار شود. سپس با دستور ipconfig آدرس IP کنونی کارت شبکه را بیابید.

الف) شماره شبکه جاری Windows XP شما چند است؟

ب) از دو گروه مجاور خود نیز شماره شبکه Windows XP مربوط به آزمایش ۲ را بپرسید و یادداشت کنید.

ج) آیا این کامپیوترها با کامپیوتر شما در یک شبکه هستند؟ آیا اگر تنظیماتی برای کارت شبکه Windows XP لحاظ نکنیم، به صورت پیش‌فرض تمام ویندوزهای XP در یک شبکه خواهند بود؟ چنین پدیده‌ایی در سیستم‌عامل ویندوز APIPA (Automatic Private IP Addressing) نام دارد.

۳. الف) با استفاده از آموخته‌های دو جلسه پیش، نحوه نصب Service جدید به نام DHCP را در Windows 2003 بیان کنید و انجام دهید.

ب) سپس به Administrative Tools رفته و DHCP را باز کنید و با کلیک راست بر نام کامپیوتر جاری، گزینه New Scope را انتخاب کنید و مراحل را به ترتیب طی نمایید:

a. ابتدا نام و شرح برای محدوده جدید تعریف کنید.
b. در گام بعد، محدوده آدرس‌های IP را 192.168.i.10 تا 192.168.i.240 تعیین کنید
c. گزینه‌های Add Exclusion و Lease Duration را خالی بگذارید و Configure DHCP Options را نیز No انتخاب کنید. در نهایت و پس از Finish. با کلیک راست، Scope جاری را که علامت قرمز رنگی به نشانه توقف دارد، Activate کنید. به ویندوز XP بروید و در خط فرمان دستور ipconfig /release را بزنید. چنین دستوری چه کاری انجام می‌دهد؟ پس از آن دستور ipconfig /renew را نیز بزنید و آدرس جدید ویندوز xp را یادداشت کنید.
d. به ویندوز ۲۰۰۳ بروید و بنویسید که در بخش Address Lease چه می بینید.

۴. پس از اینکه آدرس IP کامپیوتر مورد نظر را از طریق DHCP دریافت کردید، در Windows 2003 با کلیک راست بر Address Pool و استفاده از Exclusion آن را مثتنی کنید و مجددا با دستورات ipconfig /release و ipconfig /renew از Server آدرس جدیدی طلب کنید و ببینید آیا آدرس قبل به ویندوز XP شما اختصاص داده می‌شود یا خیر؟ چرا؟

۵. با استفاده از Scope Options تنظیمات DNS و Default Gateway خودکار را نیز به Windows XP انتقال دهید و با دستور ipconfig /all خروجی را تأیید کنید. هردوی این آدرس‌ها را آدرس کارت شبکه‌ی Windows 2003 قرار دهید.

۶. برای نصب ویرایش جدید آدرس‌های IP، یعنی IPv6 در خط فرمان دستور netsh را بزنید و سپس interface ipv6 را در ویندوز xp زده و کلمه install را تایپ کنید، سپس خروجی دستور show interface را در برگه گزارش کار بنویسید.

۷. با دستور exit از حالت netsh خارج شده و مجددا با دستور ipconfig آدرس IP ویرایش ۶ را که به کامپیوتر شما منتسب شده است بنویسید.

۸. اگر در سوال ۶ یک interface با مشخصه (Connected (State مشاهده می‌کنید که به عنوان مثال نام آن test است، می‌توانید در حالی که در <netsh interface ipv6 هستید به شکل زیر به آن آدرس بدهید:

set address "test" 2001:4188:2::20

اگر موفق به انجام این کار شدید در برگه گزارش‌کار، سوال مربوطه را OK بنویسید.

تمرین اختیاری:

۹. اگر Active Directory نصب باشد و بخواهیم DHCP را تنظیم کنیم به نحوی که Clientها، از جمله ویندوز XP، اضافه بر بودن در Domain، آدرس و تنظیمات خود را از Server دریافت کنند، چه مورد اضافه‌ای نسبت به آزمایشات پیشین در تنظیم DHCP لازم خواهد شد؟

آزمایش ششم

مقدمه‌ای بر Cisco

۷-۱- مقدمه

Router و Switch از مهمترین تجهیزات مورد استفاده در زیرساخت، برای ایجاد شبکه‌های WAN و LAN هستند. چنین تجهیزاتی توسط شرکت‌های مختلف تولید می‌شود و گرچه در مبانی نظری عملکرد، شباهت‌های بسیاری بین محصولات شرکت‌های مختلف است اما در سیستم‌عامل کار با چنین تجهیزاتی، تفاوت‌های زیاد به چشم می‌خورد. سیسکو (Cisco) از معتبرترین شرکت‌های عرضه چنین تجهیزاتی است که بازار فراگیری در سراسر جهان و از جمله ایران دارد. از این‌رو، شروع کار با تجهیزات ایجاد زیربنای شبکه، با تجهیزات سیسکو در نظر گرفته شده است.

طراحی زیربنا از اهمیت خاصی برخوردار است و شاید یکی از دشوارترین قسمت‌های شبکه‌بندی باشد چرا که به تسلط زیادی نیازدارد. طراحی شبکه باید به گونه‌ای باشد که بتوان در آینده هنگام مواجه با نیازهای جدید آن را گسترش‌داد و این کار به تقبل هزینه‌های سنگین منجر نشود. با برنامه‌ریزی درست و پیش‌بینی کافی، شبکه طراحی‌شده باید پایداری و کارایی مناسبی فراهم‌آورد. برای انجام چنین امر خطیری، بایستی مقدمات را به درستی فراگرفت. بدین منظور از یک نرم‌افزار شبیه‌ساز بسیار قوی و بدون خطا که از طرف شرکت سیسکو عرضه شده است و Cisco Packet Tracer نام دارد، استفاده شده است.

۷-۲- هدف

آشنایی با مبانی کار با تجهیزات سیسکو (Router و Switch) با کمک شبیه‌ساز Cisco Packet Tracer

۷-۳- پیش آگاهی

چرا مسیریاب و سوئیچ هر دو برای استفاده در دسترس است؟ چرا فقط یکی از آنها به تنهایی استفاده نمی‌شود؟ پاسخ این است که مسیریاب و سوئیچ هریک جایگاه خاص خود را در زیربنای شبکه‌ی دارد. ابتدا لازم است یادآوری شود که هر یک از انواع تجهیزات در کدام لایه از مدل OSI کار می‌کند. مسیریاب‌ها در لایه۳ (لایه شبکه) کار می‌کنند و سوئیچ‌ها به طور معمول در لایه۲(لایه پیوند) کار می‌کنند. از آنجاکه مسیریاب‌ها و سوئیچ‌ها در دو لایه متفاوت مدل OSI کار می‌کنند، به ترتیب بسته و فریم را انتقال می‌دهند. بسته‌ها از طریق مسیریاب‌ها بنابه آدرس مقصد لایه۳ یا آدرس شبکه عبور داده می‌شوند، درحالی‌که فریم‌ها توسط سوئیچ‌های لایه۲ براساس آدرس MAC[1] یا آدرس فیزیکی عبور داده می‌شوند. تفاوت دیگربین مسیریاب‌ها وسوئیچ‌ها این است که مسیریاب‌ها وابسته به پروتکل هستند اما سوئیچ نه. مسیریاب‌ها برای متصل کردن شبکه های مختلف و دامنه های همه‌پخشی[2] جداگانه استفاده می‌شوند، در حالی‌که سوئیچ‌ها برای دامنه‌های برخورد[3] جداگانه استفاده می‌شوند زیرا هر پورت آن‌ها مانند یک سگمنت جدای شبکه تلقی می‌شود.

نکته: سوئیچ‌ها می‌توانند در لایه‌های مختلف مدل OSI کار کنند(بعداً در این باره بحث می‌شود) اما اصل بحث ما در این آزمایشگاه، سوئیچ‌های سنتی است که در لایه۲ کار می‌کنند.

۷-۳-۱- عملکرد Router

هنگامی که یک Router روشن می‌شود مرحله POST[4] صورت خواهد گرفت، در صورت موفقیت‌آمیز بودن آن «IOS»[5] اجرا می‌شود. نرم‌افزار اصلی سوئیچ‌ها و مسیریاب‌های سیسکو، IOS است. بدون IOS، نمی‌توان از قابلیت‌های چنین سخت‌افزارهایی استفاده کرد. IOS عهده‌دار هر عملیاتی در دستگاه است، اعم

[1] Media Access Control
[2] Broadcast Domain
[3] Collision Domain
[4] Power On Self Test
[5] Internetwork Operating System

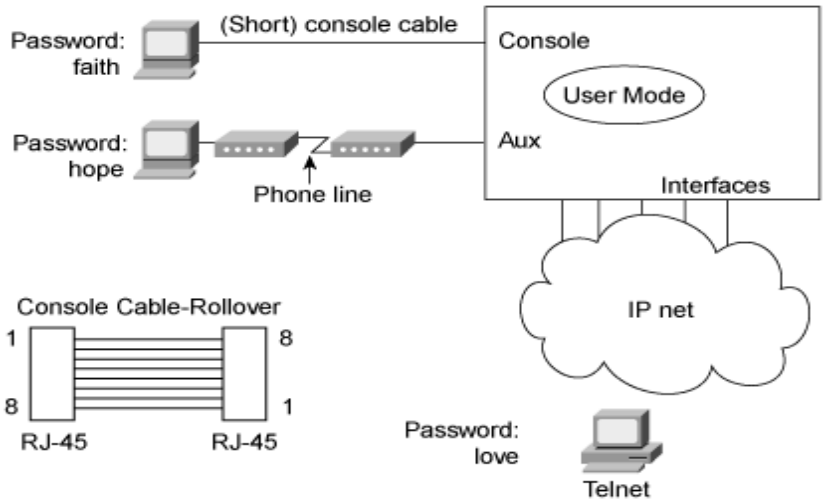
از اجازه دادن تنظیمات واسط (کارت شبکه یا Interface) تا امنیت لیست کنترل دسترسی [1] و هر تنظیم دیگر از قبیل رمزعبور، انتخاب و اجرای پروتکل، بایگانی برخی فعالیت‌ها و گزارشات تحت خط فرمان.
پس از POST موفق، IOS اقدام به یافتن و اجرای «Configuration file» خواهد کرد که در حافظه‌ی NVRAM قرار دارد. ولی اگر IOS موفق به یافتن فایل مربوطه نشد مرحله‌ای با نام« System Configuration Dialog» که معمولاً Setup mode هم خوانده می‌شود، اجرا خواهد شد که در طی اجرای آن به صورتی که خواهد آمد، سؤالاتی مبنی بر تنظیمات اولیه Router پرسیده می‌شود. البته برای مدیریت بیشتر بایستی وارد CLI[2] شد و پیکربندی Router را انجام داد.
رایج‌ترین روش محاوره (کار) با مسیریاب از طریق واسط خط فرمان (یا همان CLI) است که توسط نرم‌افزارIOS سیسکوفراهم می‌شود.هر مسیریاب سیسکو یک پورت کنسول داردکه مستقیماً می‌تواند به یک رایانه شخصی[3] یا پایانه وصل شود، بنابراین می‌توانید دستورات را توسط صفحه کلید تایپ کرده و خروجی را از صفحه نمایش دریافت کنید. بخشی از نرم‌افزار IOS سیسکو، که یک واسط کاربر فراهم می‌کند و دستوراتی که تایپ کرده‌اید را تفسیر می‌کند، EXEC یا اجرا کننده دستور نامیده می‌شود.
البته می‌توان از طریق پروتکل Telnet نیز به صورت راه دور و مبتنی بر شبکه، به تجهیزات سیسکو متصل شده و تنظیمات انجام داد که از این پس از این امکان استفاده‌های مکرر خواهیم کرد. البته به صورت کلی سه روش برای دسترسی به CLI سیسکو وجود دارد که عبارتند از:

- از طریق کنسول[4]
- از طریق دستگاه Dial-up با اتصال یک مودم به پورت کمکی[5]
- با استفاده از Telnet

هر کدام از سه روش دسترسی فوق باعث ورود به user exec mode می‌شود که حالتی از اجرای IOS است که امکانات محدودی در اختیار کاربر قرار می‌دهد. مسیریاب مکان‌های ارتباطی (پورت‌های) برای اتصال واسط RJ-45 دارد که هم برای پورت کمکی است و هم برای کنسول. کابلی که برای اتصال کنسول به PC استفاده می‌شود، یک کابل هشت سیمی مخصوص است که Rollover نام دارد و در آن پین ۱ به پین ۸ از انتهای دیگرِ کابل، پین ۲ به پین ۷ و... متصل می‌شود. شکل ۳-۱ رشته‌های کابل را نشان می‌دهد. برای اتصال مودم به پورت کمکی از کابل Straight – through استفاده می‌شود که دارای نوعی

[1] ACL: Access List Control
[2] Command Line Interface
[3] PC
[4] Console
[5] Auxiliary

همبندی است که دو دستگاه غیرمشابه را به هم متصل می‌کند و در آزمایش کابل‌کشی ساخت‌یافته به آن پرداخته خواهد شد.



شکل ۰-۱ روش‌های دسترسی به CLI

۷-۳-۲- حالت‌های[1] عملیاتی Cisco IOS

نرم افزار Cisco IOS دسترسی به چندین مد دستوری مختلف را فراهم می‌کند و هر مد دستوری یک گروه مختلف از دستورات وابسته به هم را عرضه می‌کند. جدول۳-۱ مدهایی که معمولاً بیشتر استفاده می‌شود، نحوه ورود به آن‌ها و اعلان‌های پی‌آمد آن‌ها را توصیف می‌کند. این اعلان‌ها کمک می‌کنند که شما تشخیص بدهید در کدام مد هستید و با توجه به آن چه دستوراتی در آن مد برای شما موجود است.

به منظور اهداف امنیتی، نرم‌افزار Cisco IOS دو سطح دسترسی به دستورات را فراهم ساخته است که عبارتند از : حالت کاربری بی‌امتیاز که User EXEC mode نامیده می‌شود. حالت ممتاز که Privileged EXEC mode نامیده می‌شود و نیازمند رمزعبور[2] است.

- User EXEC mode : هنگامی که شما به Router متصل می‌شوید وارد این مد می‌شوید. دستورات موجود در user EXEC زیرمجموعه‌ی دستورات موجود در privileged EXEC می‌باشد.
- Privileged EXEC mode : دستورات Privileged به شرح ذیل است:
  - Configure : پیکربندی را به صورت نرم‌افزاری تغییر می‌دهد.

[1] Modes
[2] Password

- Debug : پیغام‌های رخداد سخت‌افزار و فرآیند را نمایش می‌دهد.
- Setup : وارد کردن اطلاعات پیکربندی.

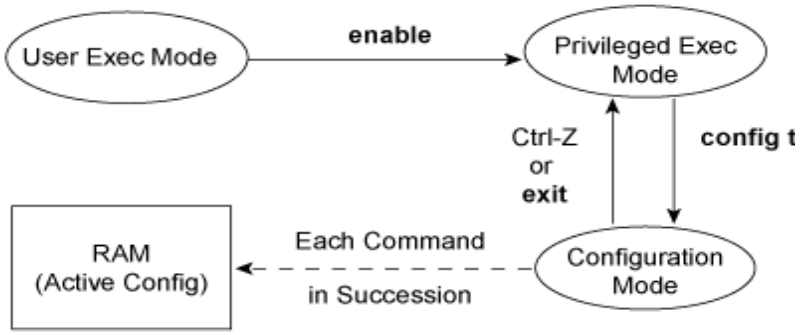
دستور disable برای خارج شدن از مد privileged EXEC و بازگشت به مد User EXEC می‌باشد.

جدول ۷-۱ مدهای عملیاتی Cisco IOS

مد عملیاتی	کاربرد	نحوه ورود به آن	نمایش اعلان
User EXEC	تغییر تنظیمات نهایی بصورت موقتی، اجرای تست‌های پایه و لیست کردن اطلاعات سیستم	اولین سطح دسترسی یافته شده می‌باشد.	Router>
Privileged EXEC	مدیریت سیستم، معین کردن پارامترهای عملیاتی	از مد user EXEC با دستور enable بدان وارد می‌شویم.	Router#
Global Config	اصلاح کردن پیکربندی که سیستم را سراسری تغییر می‌دهد.	از مد privileged EXEC با دستور Configure terminal بدان وارد می‌شویم.	Router(config)#
Interface Config	اصلاح کردن عملیات یک Interface	از مد Global با دستور Interface Type [slot#]port#	Router(config-if)#
Setup	ایجاد نخستین پیکربندی	از مد privileged EXEC با دستور setup	Prompted dialog

- Configuration mode : این مد شامل یک مجموعه از زیرمدهاست که برای اصلاح تنظیمات Interface ، تنظیمات پروتکل routing ، تنظیمات line و غیره به کار می‌رود. دستوراتی که در مد پیکربندی تایپ می‌شوند، فایل پیکربندی فعال را به‌روز می‌کنند. این تغییرات پیکربندی بلافاصله بعد از هر بار فشردن کلید Enter در پایان دستور، اعمال می‌شود. بنابراین هنگام تایپ دستورات پیکربندی باید مراقب بود.
- همان‌طور که در جدول آمده با دستور Configure terminal وارد این مد می‌شویم و توسط کلیدهای ctrl-z می‌توان از این مد خارج شد.

در شکل ۷-۲ مدهای مختلف Cisco IOS و ارتباط آن‌ها با هم نشان داده شده است.



شکل ۷-۲- حالات پیکربندی CLI به ازای هر حالت اجرا یا Exec mode

نکته: تقریباً هر دستور پیکربندی یک فرم منفی[1] نیز دارد. به‌طور معمول شکل منفی برای غیرفعال کردن یک ویژگی یا تابع به‌کار می‌رود. استفاده دستور بدون کلمه‌کلیدی no باعث می‌شود که یک ویژگی که غیرفعال شده بود دوباره فعال شود یا یک ویژگی که به‌طور پیش‌فرض غیرفعال است فعال شود.
به عنوان مثال ip routing به‌طور پیش‌فرض فعال است برای غیرفعال کردن آن دستور no ip routing را وارد می‌کنیم و برای اینکه آن را دوباره فعال کنیم دستور ip routing را وارد می‌کنیم.

۷-۳-۳- مشخصه‌های CLI Help

جدول ۷- ۲، گزینه‌های کمکی یادآوری دستور که در IOS در دسترس است را خلاصه کرده است.
اطلاعاتی که با استفاده از help به دست می‌آید بستگی به مد CLI دارد. برای نمونه، وقتی ؟ در مد کاربر تایپ شود، فقط دستوراتی که در مد privileged مجاز هستند، نشان داده نمی‌شوند. help در مد پیکربندی نیز بکار می‌رود و فقط دستورات پیکربندی هستند که در این مد عملیاتی نمایش داده می‌شوند.
توجه کنید که در ستون اول، کلمه "command" می‌تواند هر دستوری باشد. کلمه "parm"، پارامترهای دستور را ارایه می‌دهد. مثلاً در ردیف سوم Command? آمده است و به این معنی است که دستوراتی مثل show? و copy?، به ترتیب دستورات کمکی show و copy را لیست می‌کنند.

جدول ۷-۲ دستورات کمکی نرم‌افزار **Cisco IOS**

[1] No form

دستور	عملکرد
?	Help برای تمام دستورتی که در این مد در دسترس است.
help	متنی که توصیف می‌کند چگونه Help را استفاده کنیم.
command ?	متنی که تمام گزینه‌های پارامتر اول را برای دستور توصیف می‌کند.
com?	لیست تمام دستوراتی که با com شروع می‌شوند
command parm?	این مدل از help لیست تمام پارامترهایی را که با parm شروع می‌شود را می‌آورد توجه شود که بین parm و ؟ هیچ فاصله‌ای نباشد.
command parm<Tab>	اگر شما دکمه Tab را وسط کلمه نوشته شده فشار دهید، یا باقیمانده پارامتر را می‌نویسد یا هیچ کاری انجام نمی‌دهد.اگر هیچ کاری انجام ندهد یعنی این رشته از کاراکتر بیش از یک کاراکتر بعدی را نشان می‌دهد بنابراین CLI نمی‌داند که کدام است تا آن را بنویسد.
command parm1 ?	اگر در این دستور فاصله قبل از ؟ بیاید CLI تمام پارامترهای بعدی را لیست می‌کند و یک شرح کوتاه از هر کدام می‌دهد.

رشته‌کلیدها[۱] در جدول ۷- ۳، قسمتی از مد ویرایش پیشرفته[۲] هستند. **IOS**، به طور پیش‌فرض مد ویرایش پیشرفته را فعال می‌کند و به مدت طولانی آن را دارد. می‌توانید با دستور **no terminal editing** این ضربه‌کلیدها[۳] را خاموش کنید و با دستور **terminal editing** دوباره روشن کنید. یعنی با این دستورات می‌توان مد ویرایش پیشرفته را غیر فعال و فعال کرد.

[1] Key sequence
[۲] Enhanced editing mode
[۳] Keystroke

جدول ۷-۳ رشته کلیدها برای ویرایش و فراخوانی دستورات

رشته کلید	عملکرد
Up arrow or Ctrl-p	بیشتر دستورات استفاده شده اخیر را نشان می‌دهد. اگر دوباره فشار داده شوند دستور قبلی استفاده شده را نشان می‌دهد و تا زمانی این کار را می‌کند که بافر ظرفیت ذخیره کردن دستورات را دارد.
Down arrow or Ctrl-n	اگر شما به دستورات قبلی نگاه کرده‌باشید مثل بالا، این دکمه شما را به سمت دستورانی می بردکه به دستور آخر نزدیک است
Left arrow or Ctrl-b	این دکمه‌ها مکان نما را به سمت عقب فرمان جاری در حال نمایش می‌برد بدون این‌که کاراکتری را پاک کند.
Right arrow or Ctrl-f	این دکمه‌ها مکان‌نما را به سمت جلوی فرمان جاری می‌برد بدون این‌که کاراکتری را پاک کند.
Backspasce	این دکمه مکان‌نما را به سمت عقب دستور در حال نمایش می‌برد بدون این‌که کاراکتری را پاک کند
Ctrl-a	این دکمه‌ها مکان‌نما را مستقیماً به اولین کاراکتر فرمان جاری می‌برد.
Ctrl-e	این دکمه‌ها مکان‌نما را مستقیماً به آخرین کارکتر فرمان جاری می‌برد.
Esc-b	این دکمه‌ها مکان‌نما را یک کلمه عقب‌تر از دستور جاری می‌برد.
Esc-f	این دکمه‌ها مکان‌نما را یک کلمه جلوتر از دستور جاری می‌برد.
Ctrl-r	این دکمه‌ها یک *Command promt* جدید ایجاد می‌کند که شامل تمام کاراکترهای تایپ شده در آخرین *Command promt* است این کار مخصوص زمانی است که سیستم به هم می‌ریزد و صفحه نمایش واضح نیست.

۷-۳-۳-۱- نحوه نام‌گذاری Router:

به صورت پیش‌فرض نام دستگاه Router است ولی با دستور ذیل می‌توان نام مسیریاب را عوض کرد:

Router(config)# hostname MAH

با این دستور نام مسیریاب MAH می‌شود و به صورت زیر نمایش داده می‌شود:

MAH(config)#

۷-۳-۳-۲- **تنظیمات** مربوط به Interfaceهای Router :

شکل عمومی دسترسی به Interface های مسیریاب مثل دسترسی به Interface های سوئیچ است.

Router(config)# interface type [slot#/] port#

نکته: مسیریاب‌ها از انواع مختلفی از رسانه‌ها[1] استفاده می‌کنند مانند:

Serial ، FDDI ، Token Ring ، ATM ، ISDN ، Ethernet ، Fast Ethernet ، Gigabit Ethernet

مثال:

Router(config)# interface Ethernet 0/1

نمایش خط فرمان پس از دستور:

Route(config-if)#

نکته: در مسیریاب‌های کوچکتر، شماره واسط، یک تک شماره است. در بعضی دیگر، واسط ابتدا با slot ای که کارت قرار دارد و سپس یک خط مورب (/) و سپس شماره پورت آن کارت شماره‌گذاری می‌شود. مثلاً در اینجا، port 1 روی کارت در slot 0، interface 0/1 است. شماره‌گذاری با 0 برای کارت و 0 برای پورت‌های آن کارت شروع می‌شود. در بعضی موارد، واسط با سه شماره، معرفی می‌شود: ابتدا card slot، سپس daughter card (معمولاً port adapter نامیده می‌شود) و سپس یک شماره برای واسط فیزیکی روی port adapter.

نکته: بر خلاف سوئیچ‌ها تمامی Interface های مسیریاب به‌طور پیش‌فرض در حالت غیر فعال قرار دارند و برای فعال کردن آن‌ها بایستی از دستور no shutdown استفاده کرد. بصورت ذیل:

Router(config-if)# no shutdown

برای غیر فعال کردن دستور shutdown به کار می‌رود.

[1] Media

۷-۳-۳-۳- پیکربندی **مربوط** به LAN Interface

برخی از انواع مسیریاب‌ها قادر به پشتیبانی بیش از یک کارت شبکه Ethernet در روی هر یک از Interface های خود می‌باشند. با فرم کلی دستورات ذیل می‌توان این تنظیمات را انجام داد:

Router(config)# interface Ethernet [slot#/] port #
Router(config-if) # media-type media-type
Router(config-if) # speed 10|100|outo
Router(config-if) # [no] half-duplex

۷-۳-۳-۴- **پیکربندی** مربوط به Serial Interface :

هنگامی که کابل serial را در serial Interface قرار می‌دهیم عملیات clocking معمولاً به‌وسیله‌ی دستگاه‌هایی مثل مودم یا «CSU/DSU » انجام می‌پذیرد. مسیریاب‌ها به عنوان DTE و مودم‌ها یا CSU/DSU به عنوان DCE نامیده می‌شوند. چون مسیریاب‌ها به صورت پیش‌فرض به عنوان DTE شناخته می‌شوند نیاز به یک DCE داریم که عمل clocking انجام شود. در غیر این‌صورت Interface غیرفعال باقی خواهد ماند. برای این کار از دستور clock Rate استفاده می‌شود. با الگوی زیر:

Router(config)# interface serial [slot#/] port #
Router(config-if)# clock Rate rate-in-bit-per-second

نکته: مقادیر ممکن clock rate را می‌توان با استفاده از حالت context-sensitive در IOS به صورت ذیر دریافت:

Router # clock Rate ?

با استفاده از الگوی دستور «show connector» می‌توان از وضعیت اتصالات پورت‌های سریال آگاهی پیدا کرد، به صورت ذیل:

Router> show connector serial [slot# /] port#

۷-۳-۳-۵- **تخصیص** آدرس IP :

برخلاف سوئیچ‌ها که فقط یک آدرس را برای کل دستگاه استفاده می‌کنند، مسیریاب‌ها برای هر یک از Interface های خود دارای یک آدرس IP جداگانه می‌باشند و عمل Routing را بین شبکه‌هایی با آدرس‌های مختلف انجام می‌دهند. برای این‌کار یکی از آدرس‌های موجود در آن شبکه‌ای که Interface مربوطه، به آن متصل شده است را انتخاب کرده و به آن Interface اختصاص می‌دهیم. توجه داشته باشید

که Rang آدرس‌های IP بکاربرده شده در Interface ها نباید همپوشانی داشته باشد، چون در این صورت در عمل هیچگاه اجازه‌ی برقراری ارتباط بین چنین interfaceهایی، داده نخواهد شد. توسط دستور IP address که در داخل Interface اجرا می‌شود می‌توان برای هر یک از Interface های مسیریاب یک آدرس IP اختصاصی در نظر گرفت. بصورت ذیل:

Router(config-if) # ip address IP-address subnet-mask

به عنوان مثال داریم:

Router(config)# interface Ethernet 0
Router(config-if) # ip address 192.168.1.1 255.255.255.0
Router(config-if) # no shutdown
Router(config-if) # Exit

۷-۳-۳-۶- دستور **show Interface** :

یکی از مهمترین دستورات مسیریاب است که اطلاعاتی مهم در رابطه با Interface های مسیریاب، وضیعت آن‌ها و موارد دیگر را نمایش می‌دهد.

Router> show interface [type [slot#/] port#]

۷-۳-۳-۷- دستور show IP Interface :

با این دستور می‌توان پیکربندی مربوط به آدرس‌های Interface را مشاهده کرد.

Router> show ip interface [type [slot#/] port#]

۷-۳-٤- مدیریت فایل‌های پیکربندی

هر زمان که شما در پیکربندی**Router** تغییراتی ایجاد می‌کنید، باید تغییرات را در حافظه ذخیره کنید. زیرا اگر این کار را انجام ندهید تمامی تنظیمات شما با خاموش شدن و یا بارگذاری مجدد از دست می‌روند. فایل‌های پیکربندی دو نوع می‌باشند:

- Runnig Configuration
- Srartup Configuration

دستورات مورد استفاده در مد privileged برای کارکردن با فایل‌های پیکربندی به شرح ذیل می‌باشند:

Configure terminal: برای اصلاح دستی فایل running configuration از ترمینال می‌باشد.

Show running-config : فایل running configuration را نمایش می‌دهد.

Show startup-config : فایل startup configuration رانمایش می‌دهد.

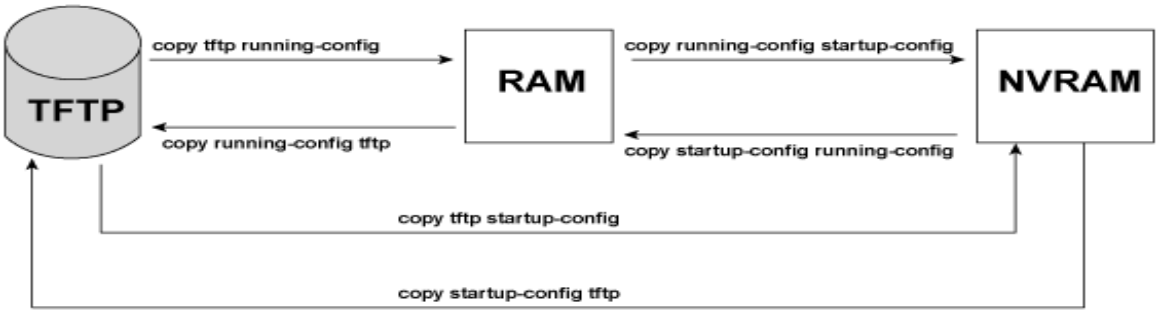
Copy running-config stsrtup-config : برای کپی کردن فایل running configuration در فایل startup configuration می‌باشد.

Copy startup-config running-config : برای کپی کردن فایل startup configuration در فایل running configuration می‌باشد.

erase srartup config : برای پاک کردن startup configuration از حافظه NVRAM می‌باشد. اگر مسیریاب در این لحظه reload شود هیچ مقدار اولیه‌ای برای پیکربندی وجود ندارد.

copy tftp running-config: برای بارگذاری یک فایل پیکربندی ذخیره شده از TFTP server به running می‌باشد.

Copy running-config tftp : برای ذخیره کردن فایل running configuration در TFTP server می‌باشد.



شکل ۷-۳ مکان‌های کپی انواع پیکربندی‌ها، دستورات کپی و نتایج آن‌ها

در دستور **copy** همواره، هنگامی که فایلی به **NVRAM** یا به **FTP server** کپی می‌شود، جایگزین فایل موجود می‌شود. به عبارت دیگر، طوری عمل می‌کند که فایل مقصد پاک می‌شود و فایل جدید به طور کامل روی فایل قبلی، جایگزین می‌شود.

وقتی دستور **copy** یک فایل پیکربندی را به **RAM** کپی می‌کند، فایل پیکربندی در **RAM** جایگزین نمی‌شود. هر کپی به **RAM** درست مثل این است که دستوراتی را درفایل پیکربندی مبدأ، تایپ می‌کنید تا

در فایل پیکربندی لیست شود. به عبارت دیگر طوری کار می‌کند که گویی فایل پیکربندی **RAM** و فایل‌های جدید کپی شده، ادغام می‌شوند. اگر **running config** را تغییر دهید و سپس تصمیم بگیرید به چیزی که در فایل **startup-config** است برگردید، تنها راه این است که دستور **reload** را استفاده کنید تا مسیریاب **reload** یا **reboot** شود.

۷-۳-۵- حافظه‌ها و واسط‌های Router

- **RAM**: گاهی DRAM[۱] نامیده می‌شود. RAM در مسیریاب به همان منظور که در هر کامپیوتری استفاده می‌شود، استفاده می‌گردد (برای کارهای ذخیره‌سازی). فایل پیکربندی در حال اجرا یا فعال در این حافظه ذخیره می‌شود.
- **ROM**: این نوع حافظه (حافظه فقط خواندنی) یک bootable IOS image را ذخیره می‌کند که معمولاً در عملیات معمولی استفاده نمی‌شود. ROM شامل کدی است که تا زمانی که مسیریاب بفهمد کجا full IOS image را پیدا کند، برای بوت کردن مسیریاب استفاده می‌شود و یا به‌عنوان back up bootable image در مواردی که مشکلاتی به وجود می‌آید، مورد استفاده قرار می‌گیرد.
- **Flash memory**: یا یک EEPROM یا یک PCMCIA، functional IOS image را به طور کامل ذخیره می‌کند و مکان پیش‌فرض است که مسیریاب IOS خود را هنگام بوت می‌گیرد. Flash memory همچنین می‌تواند برای ذخیره‌ی هر فایل دیگری شامل فایل‌های پیکربندی نیز استفاده شود.
- **NVRAM**: RAM غیر فرار[۲] مقدار اولیه یا startup فایل پیکربندی را ذخیره می‌کند.

همه‌ی این انواع حافظه، به جز RAM، حافظه‌ی پایدار هستند. هیچ هارددیسک یا دیسک ذخیره‌سازی‌ای در مسیریاب‌های سیسکو وجود ندارد. شکل ۷- ۴، استفاده‌ی حافظه در مسیریاب‌های سیسکو را خلاصه می‌کند.

---

[۱] Dynamic Random – Access Memory

[۲] Nonvolatile

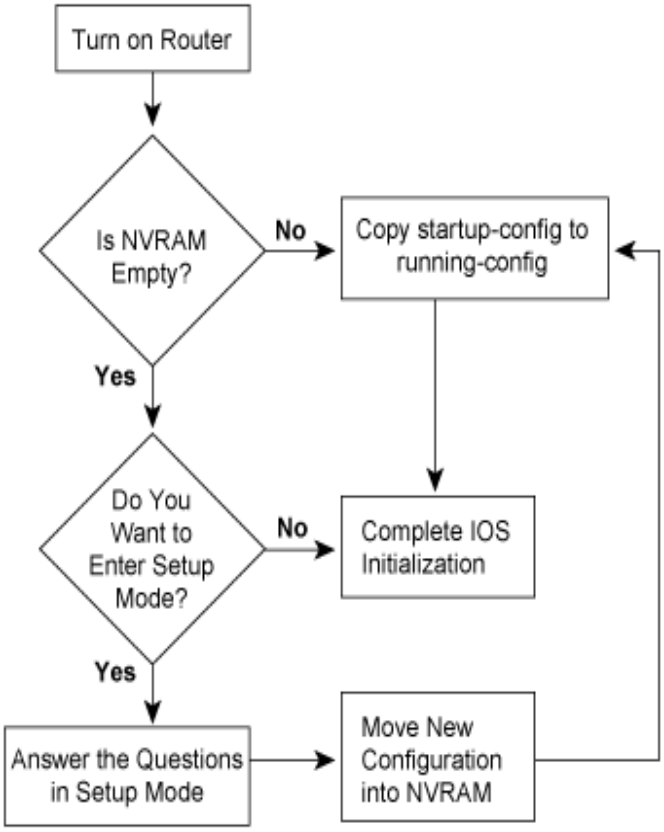
شکل ۷-٤ انواع حافظه مسیریاب سیسکو

۷-۳-٦- مقداردهی اولیه‌ی پیکربندی (مد Setup)

مد **Setup**، راهبر مسیریاب را برای پیکربندی اساسی مسیریاب با استفاده از سؤالاتی که او را به تعیین پارامترهای اصلی پیکربندی وامی‌دارد، هدایت می‌کند. مسیریاب سیسکو به جای استفاده از مد **setup**، می‌تواند با استفاده از **CLI** در مد پیکربندی، پیکربندی شود. در حقیقت، اکثر پرسنل شبکه اصلاً از **setup** استفاده نمی‌کنند اما کاربران جدید گاهی مایلند ازمد **setup** استفاده کنند تا با مد پیکربندی **CLI** بیشتر آشنا شوند.

شکل و مثال زیر، پروسه‌ای که مد **setup** استفاده می‌کند را توضیح می‌دهد. مد **Setup**، وقتی مسیریاب بوت می‌شود و هیچ پیکربندی‌ای در **NVRAM** وجود ندارد، بارها استفاده می‌شود. می‌توان با استفاده از دستور **setup** ازمد **privileged** به مد **setup** وارد شد. به صورت ذیل:

Router# setup



شکل ۷-۵ اولین تنظیمات مسیریاب و مد setup

مثال زیر، صفحه‌ای را نشان می‌دهد که مسیریاب بدون وجود هیچ پیکربندی‌ای در **NVRAM**، بوت شده است و از مد **setup** استفاده می‌کند.

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any promp .
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you to
configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no
First ,would you like to see the current interface summery?[yes]:
Any interface listed with ok? Value "NO" does not have a valid configuration

```
Interface              IP-Address    OK?  Method   Status        Protocol
Ethernet0              unassigned     NO   unset      up          down
Serial0                unassigned     NO   unset    down          down
Serial1                unassigned     NO   unset    down          down

Configuring global parameters:
Enter host name [Router]: R1
    The enable secret is a password used to protect access to
    privileged EXEC and configuration modes. This password, after
      entered, becomes encrypted in the configuration.
Enter enable secret: cisco
   The enable password is used when you do not specify an
   enable secret password, with some older software versions, and
        some boot images.
Enter enable password: fred
   The virtual terminal password is used to protect
    access to the router over a network interface.
Enter virtual terminal password: barney
Configure SNMP Network Management ? [yes]: no
Configure bridging? [no]:
Configure DECnet ? [no]:
Configure Appletalk ? [no]:
Configure IPX? [no]:
Configure IP ? [yes]:
Configure IGRP routing ? [yes]:
Your IGRP autonomous system number [1]:
Configuring interface parameters:

Do you want to configure ethernet0 interface ? [yes]:
Configure IP on this interface ? [yes]:
IP address for this interface : 172.16.1.1
Subnet mask  on this interface [255.255.0.0]: 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits ; mask is /24

Do you want to configure Serial0 interface ? [yes]:
Configure IP on this interface ? [yes] :
Configure IP unnumbered on this interface ? [no]
IP address for this interface : 172.16.12.1
Subnet mask  on this interface [255.255.0.0] : 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits ; mask is /24

Do you want to configure Serial1 interface ? [yes]:
Configure IP on this interface ? [yes] :
Configure IP unnumbered on this interface ? [no] :
IP address for this interface : 172.16.13.1
Subnet mask  on this interface [255.255.0.0] : 255.255.255.0
Class B network is 172.16.0.0, 24 subnet bits ; mask is /24

The following configuration command script was created:
```

```
hostname R1
enable secret 5 $1$PNaE$Hk5/rzmOAV.vzhfcfDl/o.
enable password fred
line vty 0 4
password barney
no snmp-server
!
no bridge 1
no decent routing
no appletalk routing
no ipx routing
ip routing
!
interface Ethernet0
ip address 172.16.1.1 255.255.0.0
no mop enable
!
interface Serial0
ip address 172.16.12 255.255.0.0
no mop enable
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
router igrp 1
redistribute connectd
network 172.16.0.0
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2] : 2
Building configuration…
[ok] use the enable mode 'configure' command to modify this configuration.
Press RETURN to get started!
```

Setup مانند مثال پیش رفتار می‌کند چه با بوت شدن با **NVRAM** خالی، به آن دست یابید چه از دستور **setup** در مد **privileged** استفاده کنید. ابتدا، مسیریاب می‌پرسد: "آیا می‌خواهید وارد محاوره‌ی پیکربندی اولیه شوید؟". پاسخ **y** یا **yes** شما را در مد **setup** قرار می‌دهد. وقتی کار با **setup** تمام می‌شود، در مرحله بعد سه گزینه وجود دارد که انتخاب یک گزینه مشخص می‌کند در قدم بعد چه کاری باید انجام شود. گزینه‌ی ۲ به مسیریاب می‌گوید که فایل پیکربندی را در **NVRAM** ذخیره کرده و خارج شود. در مثال 1-1، این گزینه استفاده شده است. مسیریاب، پیکربندی را هم در **NVRAM** و هم در

RAM قرار می‌دهد. این تنها عملیات در **IOS** است که همه‌ی فایل‌های پیکربندی، که بر اساس عملکرد کاربر محتوای یکسان دارند، تغییر می‌کنند. گزینه‌های ۰ و ۱ به مسیریاب می‌گوید که از پیکربندی‌ای که شما وارد کرده‌اید، صرف‌نظر کند و همچنین از **command prompt** خارج شود (گزینه ۰) یا دوباره با **setup**، شروع شود (گزینه ۱). همچنین می‌توان قبل از پاسخ‌دهی به همه‌ی سؤالات، از پروسه‌ی **setup** صرف‌نظر کرد و با فشار **cntl-c** وارد **CLI prompt** شد.

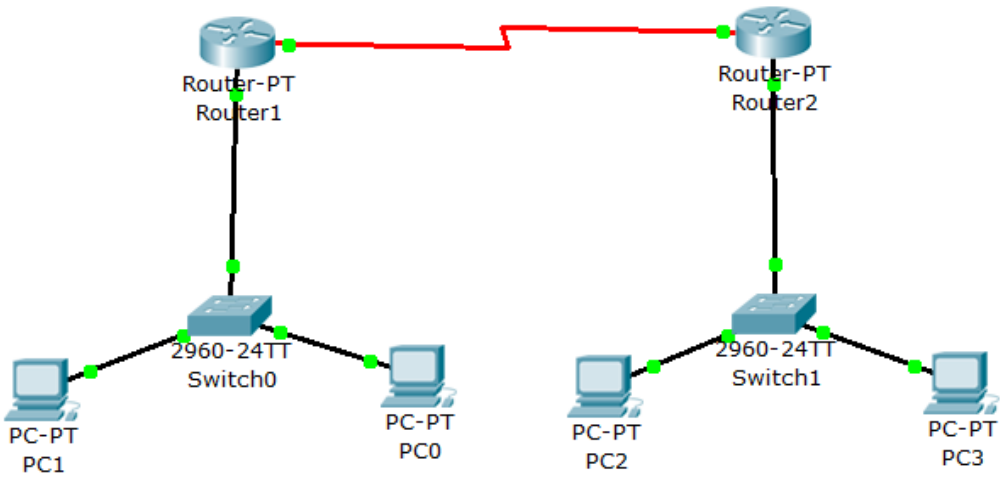
۷-٤- مراجع

1. Melissa Craft, Elliot Lewis, **Building a Cisco Network for Windows 2000**, By Syngress, Syngress Media, Inc., 2000.
2. Wendell Odom, **CCNA INTRO**, Cisco Press, 2005. (for 640-821 exam)
3. Wendell Odom, **CCNA ICND**, Cisco Press, 2005. (for 640-811 exam)

دستور کار

نکته: برای وارد کردن دستورات تنظیم PCها و Routerها، حتما از حالت خط فرمان استفاده کنید و از فرم‌های گرافیکی تسهیل کننده‌ی ورود داده استفاده نشود زیرا در آزمون نهایی، فقط از حالت خط فرمان سوال خواهد آمد.

۱. در نرم‌افزار Packet Tracer، پیکربندی زیر را که مشتمل بر دو شبکه‌ی LAN مرتبط با هم از طریق دو مسیریاب است، ایجاد کنید. در هنگام اتصال Interfaceهای مسیریاب‌ها، از FastEthernet0/0 برای اتصال به شبکه داخلی و Serial 2/0 برای اتصال دو مسیریاب به هم استفاده کنید. توجه داشته باشید که ارجاعات آزمایشات بعدی براساس نام تجهیزات تنظیم شده در شکل زیر می‌باشد:



۲. الف) ابتدا بر PC0 و PC1 آدرس IP مناسب به گونه‌ای تنظیم کنید که دو سیستم از لحاظ منطقی در یک شبکه باشند. آدرس‌های انتخابی را برگه گزارش کار یادداشت نمایید.

ب) با انتخاب شماره شبکه‌ی متفاوت از شبکه‌ی سمت چپ، برای PC2 و PC3 نیز آدرس IP مناسب تخصیص دهید. آدرس‌های انتخابی را برگه گزارش کار یادداشت نمایید.

ت) صحت ارتباط بین کامپیوترهای دو شبکه را از طریق دستور Ping بررسی کنید.

ث) چه تفاوتی بین RTT در Ping مشاهده شده در نرم‌افزار شبیه‌ساز، با آنچه در دنیای واقع در شبکه‌های LAN رویت می‌شود وجود دارد؟ به نظر شما چرا؟

۳. با استفاده از آنچه در پیش‌آگاهی آمده است، اینترفیس FastEthernet 0/0 را در هر دو مسیریاب Router1 و Router2 تنظیم نمایید، به نحوی که با کامپیوترهای موجود در شبکه‌های متصل‌شان در یک شبکه باشند و از خط فرمان هر دو مسیریاب، یکی از کامپیوترهای هم شبکه‌ای را Ping نمایید. دستور Ping در این حالت، چه تفاوتی با حالتی دارد که آن را از کامپیوتر انجام دهیم؟

۴. با اتخاذ آدرس‌های IP، 172.16.0.1/16 برای اینترفیس Serial 2/0 در Router1 و 172.16.0.2/16 برای اینترفیس Serial 2/0 در Router2، و تنظیم Clock بر آن Interface که در محیط نرم‌افزار در زمان نگه‌داشتن ماوس علامت ساعت بر آن پدیدار می‌شود (Serial DCE)، دو مسیریاب را به هم متصل نمایید. با دستور Ping از صحت برقراری ارتباط، اطمینان حاصل کنید.

۵. آیا اکنون که ارتباط دو به دوی تمام تجهیزات در دو شبکه‌ی LAN و نیز ارتباط بین دو مسیریاب برقرار شده است، می‌توان از PC1، PC3 را Ping نمود و پاسخ Reply دریافت کرد؟ حدس می‌زنید چرا؟

۶. با کمک دستور زیر، مسیریابی را به صورت ایستا (یعنی بدون تغییر در مسیر ارسال) برای مسیریاب‌ها تنظیم نمایید به گونه‌ای که اجازه دهند، بسته از شبکه‌ی داخلی متصل به آن‌ها خارج شود و به شبکه‌ی دیگر برود.

ip route *Destination-network Destination-netmask gateway*

اکنون از PC1، PC3 را Ping نمایید. پاسخ باید Reply باشد، RTT را در پاسخ Reply بنویسید. اگر Reply نبود با کمک حالت گرافیکی شبیه‌سازی یا Simulation در نرم‌افزار، Ping را انجام دهید و علت را دریابید. در هر صورت دستور مسیریابی تنظیم شده را یادداشت کنید.

۷. اکنون که ارتباط PCهای دو شبکه‌ی LAN بر بستر WAN، برقرار شده است، دستور tracert را برای طی مسیری که بسته از PC1 به PC3 می‌پیماید، اجرا و خروجی آن را در برگه گزارش کار یادداشت نمایید.

آزمایش هفتم

شبکه محلی مجازی (VLAN)

۸-۱- مقدمه

کامپیوترها در شبکه‌های LAN با بیش از دو کامپیوتر، توسط یکی از دستگاه‌های هاب[1] یا سوییچ[2] به هم متصل می‌شوند. برخلاف هاب که تمام پورت‌های آن با هم تشکیل یک شبکه‌ی همه‌پخشی می‌دهند و هر پورت خاصیت Half-Duplex در ارسال دارد و اگر دو کامپیوتر متصل به دو پورت آن به صورت همزمان اقدام به ارسال کنند، تصادف پیش می‌آید، در شبکه‌هایی که کامپیوترها با سوییچ به هم متصل هستند، دارای ارتباطات Full-Duplex هستیم و تصادفی در زمان ارسال همزمان روی نمی‌دهد. در عوض سوییچ، فریم ورودی از یک پورت را ابتدا به داخل بافر خود کپی کرده و چک خطای آن را براساس CRC موجود در دنباله[3] انجام می‌دهد و سپس بر اساس جدولی که در داخل خود متناظر با آدرس‌های MAC و شماره پورت‌ها ایجاد کرده است، ارسال به پورت خروجی مناسب را انجام می‌دهد.

اصولا در شبکه‌های LAN جاری استفاده از هاب بسیار کم است و به دلیل مزایای متعددی که سوییچ‌ها در اختیار قرار می‌دهند. از سوییچ استفاده می‌شود. در این راستا تنظیم و خصوصیات ویژه‌ای در رابطه با شبکه‌های LAN و مدیریت آن‌ها مطرح می‌شود که VLANها یکی از آن موارد هستند.

---

[1] Hub
[2] Switch
[3] Trailer

۸-۲- هدف

آشنایی با مفهوم VLAN و نحوه‌ی ایجاد و تنظیم آن

۸-۳- پیش‌آگاهی

محدوده‌ای که اگر دو کامپیوتر در آن، به صورت همزمان اقدام به ارسال کنند، تصادف پیش آید، **محدوده‌ی تصادف** یا **Collision Domain** نام دارد. تمام پورت‌های یک هاب، تشکیل یک محدوده‌ی تصادف می‌دهند، در حالی که هر پورت یک سوییچ به تنهایی خود یک محدوده‌ی تصادف است. زیرا اگر دو کامپیوتر در دو پورت یک سوییچ اقدام به ارسال همزمان کنند، تصادفی روی نخواهد داد. محدوده‌ی تصادف سبب کاهش کارایی شبکه می‌شود زیرا ترافیک حجیم غیرضروری به همه‌ی ماشین‌های متصل به هاب ارسال می‌شود، چه بخواهند و چه نخواهند. احتمال تصادف و ارسال مجدد نیز بالا می‌رود.

البته سوییچ‌ها نیز در مقابل یک نوع خاص ترافیک مقاومت نمی‌کنند و اگر فریمی با آدرس مقصد FF:FF: FF:FF:FF:FF، که بیانگر آدرس گیرنده همه است، از یک پورت دریافت کنند،آن را از همه‌ی پورت‌های خود به بیرون ارسال می‌نمایند یا به اصطلاح همه‌پخشی می‌کنند. به فریم‌های دارای آدرس مقصد FF:FF: FF:FF:FF:FF، فریم‌های همه‌پخشی گفته می‌شود. بدین ترتیب سوییچ‌ها در مقابل یک فریم ورودی چند واکنش نشان می‌دهند:

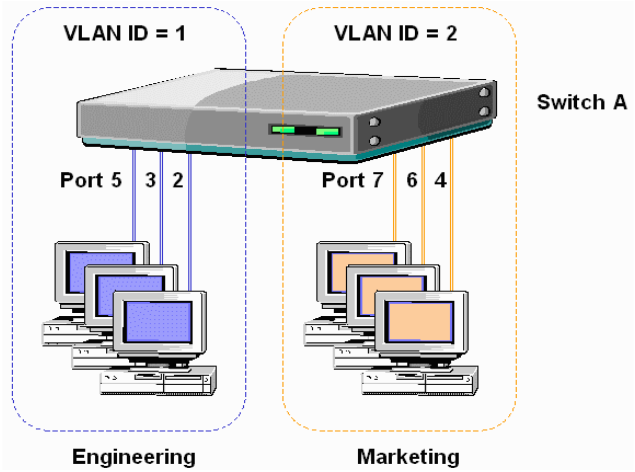
- اگر آدرس مقصد آن به یک کامپیوتر متصل به شبکه اشاره داشته باشد، آن را به پورت خروجی متصل به آن ماشین ارسال می‌کنند.
- اگر آدرس مقصد آن :FF:FF: FF:FF:FF:FF باشد، آن را به همه‌ی پورت خروجی متصل به آن ماشین ارسال می‌کنند.
- اگر آدرس مقصد آن دارای الگوی چندپخشی[1] (گروهی) باشد، آن را به یک سری پورت‌های خاص که به اعضای گروه متصل هستند ارسال می‌کنند.
- اگر آدرس مقصد آن به یک کامپیوتر غیر متصل به شبکه اشاره داشته باشد، فریم مورد نظر را صرفنظر[2] می‌کنند.

[1] Multicast
[2] Discard

تمام پورت‌های یک سوییچ، در یک **محدوده‌ی همه‌پخشی** یا Broacast Domain قرار می‌گیرند. به عبارت دیگر، محدوده‌ای که یک فریم همه‌پخشی به تمام کامپیوترهای آن می‌رسد، محدوده‌ی همه‌پخشی نام دارد. بدین ترتیب سوییچ‌ها که خود از دست محدوده‌ی تصادف رسته‌اند، در صورت افزایش تعداد، دچار مشکلات دیگر مانند فریم‌های همه‌پخشی هستند. یعنی اگر تصور کنیم ۱۰ عدد سوییچ ۲۴ پورتی توسط یک سوییچ به هم متصل شده‌اند، قابلیت اتصال ۲۴۴ کامپیوتر را با هم فراهم کرده‌ایم. کاربردهای زیادی در شبکه‌های محلی مبتنی بر استفاده از فریم‌های همه‌پخشی هستند. بنابراین فریم‌های همه‌پخشی در شبکه‌های LAN با تعداد زیاد ماشین، خود مشکلی دیگر به حساب می‌آید.

۸-٤- چیستی و اهمیت VLAN

فرض کنید یک سوییچ ۴۸ پورتی خریداری کرده باشیم و بخواهیم دو شبکه‌ی LAN مجزا را توسط آن مدیریت کنیم. چه کاری می‌توان در این زمینه انجام داد؟ شاید تعویض آن به دو سوییچ ۲۴ پورتی یک راه‌حل خوب به نظر برسد. اما به دلایل مختلف ممکن است این کار همیشه امکان‌پذیر نباشد. راهکاری وجود دارد که می‌توان به صورت نرم‌افزاری (یعنی با IOS سیسکو) پورت‌های سوییچ را به دو مجموعه‌ی کاملا مجزا تقسیم کرد. این راهکار امکان داشتن دو یا بیشتر LAN مجازی[1] در یک سوییچ فیزیکی را فراهم می‌سازد. در شکل ۸-۱، دو بخش مجزای یک شرکت در یک شبکه‌ی محلی، به نام بخش‌های بازاریابی و مهندسی توسط VLAN از هم تفکیک شده‌اند و درست مانند آن است که دو سوییچ مجزای غیر مرتبط برای آن‌ها اختصاص داده باشیم. پورت‌های شماره‌ی ۲، ۳ و ۵ در VLAN با شناسه‌ی ۱ و شماره پورت‌های ۴،۷ و ۸ در VLAN با شناسه‌ی ۲ قرار گرفته اند.



شکل ۸-۱ نمونه‌ای از استفاده از VLAN برای تفکیک پورت‌های سوییچ

[1] Virtual LAN

بنابراین، به جای اینکه همه‌ی پورت‌های یک سوئیچ در یک قلمروی همه‌پخشی باشند، سوئیچ به وسیله‌ی پیکربندی، آن‌ها را به چند قلمروی همه‌پخشی تقسیم می‌کند. البته انتساب پورت فیزیکی سوییچ به شماره‌ای به نام شماره VLAN، می‌تواند در چندین سوییچ به هم مرتبط نیز گسترش یابد و به عنوان مثال در چند سوییچ متصل به هم یک VLAN با شماره‌ی ۱ داشته باشیم. به طور پیش‌فرض تمام پورت‌های یک سوییچ در ابتدا در یک VLAN به نام Default VLAN قرار دارند، مگر اینکه راهبر شبکه، خود در تنظیمات سوییچ تغییر ایجاد کند.

انگیزه‌های زیادی برای استفاده ازVLAN وجود دارد، مانند:

- گروه‌بندی کاربرها بر اساس بخش یا گروه‌هایی که با هم کار می‌کنند به جای اینکه بر اساس مکان فیزیکی آن‌ها را مجزا کنیم
- کاهش باراضافی[1] فریم‌های همه‌پخشی سوییچ‌ها در شبکه‌های LAN با تعداد زیادی کامپیوتر با محدود کردن اندازه قلمروی همه‌پخشی
- اعمال امنیت بیشتر با قراردادن دستگاه‌های حساس روی یک VLAN جداگانه
- برای جدا کردن ترافیک خاصی از جریان اصلی ترافیک. برای مثال، قرار دادن IP telephone ها روی یک VLAN جدا از User PCها

۸-۵- ایجاد VLAN

به‌طور معمول، سوئیچ‌ها، VLANها را به این شکل تعریف می‌کنند: اگر پورت‌ها در یک VLAN هستند، می‌توانید یک پیکربندی ساده مثل "interface 0/1 is in VLAN 1" و "interface 0/2 is in VLAN 33" بنویسید. یکی از روش‌های رایج ایجادVLAN که VLANهای مبتنی بر پورت[2] نام دارد، می‌تواند خیلی ساده و بدون نیاز به دانستن MAC آدرس هر دستگاه انجام شود. البته لازم است که مستندسازی متناظر در شبکه‌ی فیزیکی انجام گیرد تا اطمینان حاصل شود دستگاه‌ها، به پورت درستی از سوئیچ برای قرار دادن آن‌ها در یک VLAN خاص، کابل‌بندی شده‌اند.

یک روش غیرمعمول برای ایجاد VLAN، گروه‌بندی دستگاه‌ها به VLAN بر اساس آدرس MAC است. مهندس شبکه آدرس MAC همه‌ی دستگاه‌ها را روی سوئیچ‌های مختلف پیکربندی می‌کند به این شکل که هر آدرس MAC در چه VLANای است. وقتی یک دستگاه به پورت دیگری از سوئیچ منتقل شود و

[1] Overload
[2] Port-based VLAN

فریمی را ارسال کند، دستگاه در همان VLAN باقی می‌ماند. این ویژگی باعث می‌شود تا دستگاه‌ها راحت‌تر جابه‌جا شوند. این کار سبب افزایش حجم پیکربندی‌های مسئول شبکه می‌شود زیرا پیکربندی MAC آدرس همه‌ی دستگاه‌ها می‌تواند حجم زیادی داشته باشد، بنابراین این گزینه کمتر استفاده می‌شود. آنچه در این آزمایش پیاده‌سازی خواهد شد، VLAN مبتنی بر پورت است.

۸-٦- Trunking به وسیله‌ی ISL و 802.1q

وقتی VLAN در شبکه‌هایی که چند سوئیچ متصل به هم دارند استفاده می‌شود، باید بین سوئیچ‌ها VLAN Trunking انجام شود تا شماره ی یک VLAN در تمام شبکه‌ها به هم مرتبط شود. هنگام ارسال یک فریم به سوئیچ دیگر، لازم است راهی برای تشخیص VLANای که فریم از آن ارسال شده است، وجود داشته باشد. به وسیله‌ی VLAN Trunking، سوئیچ‌ها هر فریمی که بینشان ارسال می‌شود را برچسب می‌زنند تا بفهمند فریم به کدام VLAN تعلق دارد. به زبان ساده، Trunk رابطی است بین دو سوییچ که اضافه بر برقراری ارتباط، VLANهای متناظر را نیز به هم می‌پیوندد. دو شیوه‌ی Trunking رایج در سوییچ‌ها، استفاده از پروتکل ISL[1] و IEEE 1q. است. که اولی مختص به تجهیزات شرکت سیسکو است و دومی برای انواع سوییچ‌های شرکت‌های مختلف کاربرد دارد. بنابراین پورت‌های سوییچ در دو حالت عمل می‌کنند یا حالت دسترسی متعارف یا حالت دسترسی از نوع ترانک. حالت اول را Access Mode و حالت دوم را Trunk Mode گوییم.

در مثال زیر که بخشی از پیکربندی VLANهای با شماره‌های ۲ و ۳ است، **fastethernet1/1 و fastethernet2/1 در VLAN2 و interface fastethernet3/1** را در VLAN3 قرار داده شده است. همچنین اتصال Switch و Router از نوع Trunk تنظیم شده است.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name vlan2
Switch(config-vlan)#exit
Switch(config)#interface fastethernet1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastethernet2/1
Switch(config-if)#switchport mode access
```

[1] Inter-Switch Link Protocol

```
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#interface fastethernet3/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to upSwitch(config-if)#exit
Switch(config)#
```

۸-۷- دسترسی به سوییچ از طریق Telnet

برای اینکه بتوان سوییچ را از راه دور تنظیم کرد، بایستی یک آدرس IP به آن نسبت داد. سوییچ به صورت پیش‌فرض دارای آدرس IP نیست. زیرا عملکرد آن در لایه‌ی ۲ از مدل OSI است و در این لایه تنها آدرس MAC است که اهمیت دارد. اما اگر به عنوان یک دستگاه قابل مدیریت در شبکه به سوییچ نگاه شود، بایستی بتوان بر آن آدرس IP تنظیم نمود تا قابلیت دسترسی داشته باشد.

۸-۸- تنظیم نام‌کاربری و رمز عبور

سوییچ‌ها و مسیریاب‌ها همانند سایر تجهیزات شبکه دارای اهمیت اساسی هستند وباید از دسترسی‌های غیرمجاز حفاظت شوند. بدین منظور می‌توان در سطوح مختلف بر آن‌ها نام کاربری و رمز عبور تنظیم نمود. با توجه به آزمایش پیشین سه راه دسترسی به یک سوییچ یا مسیریاب در شبکه استفاده از روش‌های Console، Telnet و Aux است. روش دسترسی با Console تنها در اولین تنظیم سوییچ یا مسیریاب به صورت مستقیم از نزدیک رایج است. بعدها راهبران شبکه از راه دور و با دستور telnet به چنین تجهیزاتی متصل می‌شوند. برای حفظ امکان کنترل و دسترسی از راه دور سوییچ‌ها و مسیریاب‌ها در حالتی که ارتباط

آن‌ها با شبکه قطع شده است، از پورتی کمکی[1] که دارای مودم است و قادر است از طریق خط تلفن ارتباط را برقرار سازد،کمک گرفته می‌شود. به این ترتیب باید بتوان بر هرسه‌ی این پورت‌ها رمز عبور و نام کاربری تنظیم کرد. از طرفی برای هر سوییچ یا مسیریاب در زمان استفاده، دو سطح دسترسی معمول (User Mode) و ممتاز (Priviledge Mode) وجود دارد. در سطح دسترسی کاربر معمول، تنها قادر به رویت تنظیمات سطحی و ساده هستیم و امکان تغییر در پیکربندی دستگاه نیز وجود ندارد در حالی که در سطح دسترسی ممتاز امکان اعمال تغییرات، به صورت کامل فراهم است. برای ورود به حالت ممتاز از معمولی از دستور enable استفاده می‌شود.

برای هر یک از سه روش دسترسی، می‌توان رمز عبور تعریف نمود. در جدول زیر، رمزهای عبور برای کنسول، کمکی و Telnet، جداگانه تعریف شده است. لازم به ذکر است که رمزهای عبوری که درجدول نشان داده شده است، پیش‌فرض نیستند.

جدول ۸-۱ پیکربندی رمزعبور CLI

Access From	Password Type	Configuration
Console	**Console password**	**line console 0** **password** hamed **login**
Auxiliary	**Auxiliary password**	**line aux 0** **password** ahmad **login**
Telnet	**vty password**	**line vty 0 4** **password** student **login**

با توجه به اینکه هیچ رمزعبور از پیش تنظیم شده‌ای وجود ندارد. بنابراین باید رمزهای عبور دسترسی به Telnet و کمکی را ابتدا از کنسول، پیکربندی کرد. همه‌ی سوییچ‌ها و مسیریاب‌های سیسکو دارای پورت کنسول هستند، اما اغلب آن‌ها پورت کمکی را دارند. پورت کنسول برای دسترسی محلی راهبر از یک ترمینال ASCII یا یک کامپیوتر تعبیه شده است(به عنوان مثال، نرم‌افزار Hyper Terminal در سیستم‌عامل ویندوز XP).

پورت کمکی که در بعضی مدل‌های دستگاه‌های سیسکو وجود ندارد، اغلب برای پشتیبان ارتباط[2] استفاده می‌شود. در ستون آخر جدول فوق، اولین دستور در هر پیکربندی سبب تعیین محل اعمال تنظیمات می‌شود. دستور **password**، متن رمز عبوری را که کاربر باید آن را تایپ کند تا اجازه‌ی دسترسی یابد، نشان می‌دهد. سپس دستور **login** به مسیریاب یا سوییچ می‌گوید که درخواست password را در ورود به

[1] Auxiliary
[2] Dial backup

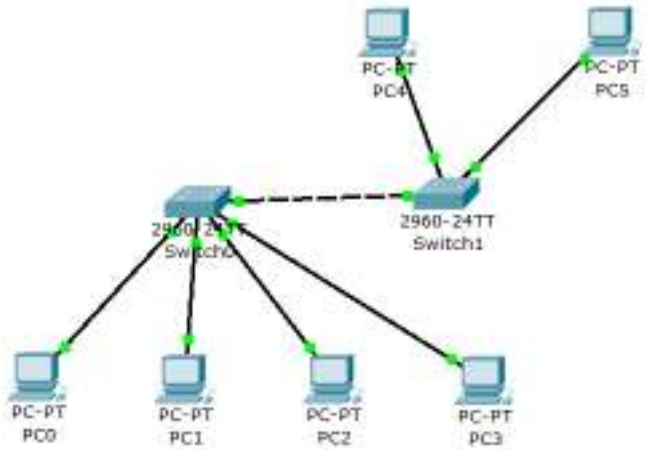
دستگاه نمایش بدهد. گاهی مهندسین شبکه، هر سه رمز عبور را با یک مقدار تنظیم می‌کنند تا همگی آنها اجازه رفتن به مد کاربر را بدهند. vty به ارث برده شده از لینوکس و به معنی virtual Terminal است. یعنی اینکه چند نفر می‌توانند همزمان به یک دستگاه سیسکو وارد شوند. بنابراین در جدول فوق vty 0 4 نشان‌دهنده‌ی پنج Session همزمان کار با آن دستگاه است.

۸-۹- تکلیف جلسه آتی

دستور Vlan database را بررسی کنید، چه کاربردی دارد و بگویید چگونه استفاده می‌شود؟

۸-۱۰- دستورکار

۱. شبکه‌ی زیر را ایجاد کنید و به کامپیوترها، آدرس IP مناسب به نحوی اختصاص دهید که بتوانند با همدیگر ارتباط داشته باشند. صحت عملکرد را برای نمونه بین دو کامپیوتر با دستور ping بررسی کنید. آدرس‌های تنظیم شده را در برگه گزارش کار یادداشت کنید.



۲. با دستور hostname در حالت پیکربندی، اسم سوییچ سمت چپ را به left و سمت راست را به right تغییر دهید.

۳. در سوییچ سمت چپ، برای هر سه حالت دسترسی ذکر شده در بخش ۸-۸، رمزهای عبور را همانگونه که در جدول آمده است تنظیم کنید.

الف) برای کدامیک از حالات، امکان تنظیم رمز عبور وجود ندارد؟ چرا؟

ب) پس از تنظیم رموز عبور، با دستورات exit متوالی یا Ctl+z از سوییچ خارج شوید. در ورود مجدد به سوییچ، کدامیک از رموز عبور کار خواهند کرد؟ چرا؟

ج) با دستور show running-config، تغییر ایجاد شده در پیکربندی را مشاهده کنید.

۴. در سوییچ سمت چپ، به حالت پیکربندی بروید و با دستورات زیر، گونه‌ای دیگر از رمزعبور را تنظیم نمایید.

left(config)#enable secret test

الف) با خروج از مسیریاب و ورود مجدد به حالت پیکربندی، ذکر کنید که این رمز عبور در ورود به کدام حالت به کار می‌آید؟

ب) با استفاده از دستور show running-config، تفاوت نحوه‌ی ذخیره‌ی رمز عبور این تمرین با تمرین پیش را بیان کنید.

۵. بر اساس آنچه در بخش ۸-۶ آموخته‌اید، دو کامپیوتر PC0 و PC2 را در Default VLAN و دو کامپیوتر PC1 و PC3 را در VLANجدیدی که با نام VLAN 2 ایجاد می‌کنید قرار دهید.

الف) با دستور sh r تنظیمات جدید را مشاهده کنید.

ب) خروجی دستور ping برای دو کامپیوتر در یک VLAN و دو کامپیوتر در دو VLAN متفاوت را به مربی نشان دهید.

ج) بر سوییچ سمت راست، VLAN2 را تنظیم نمایید و کامپیوتر PC5 را در آن قرار دهید و یکی از کامپیوترهای Dfault VLAN و یکی از کامپیوترهای VLAN2 در سوییچ سمت چپ را ping کنید و نتیجه را یادداشت کنید.

۶. با کمک محتوی پیش آگاهی، ارتباط مشترک دو سوییچ را در حالت Trunkتنظیم کنید و بخش ج از تمرین قبل را تکرار کنید و نتیجه را تفسیر نمایید.

۷. اگر بخواهیم از پشت یکی از PCها مثلا PC0، هر دو سوییچ را مدیریت کنیم، لازم است که ابتدا با دادن آدرس IP به یکی از VLANها در سوییچ، آن را قابل دسترسی از راه دور کنیم. با کمک دستورات جدول زیر، به سوییچ‌ها، آدرس‌های IP مناسب در محدوده‌ی آدرس کامپیوترها نسبت دهید و از PC0 به هر دو سوییچ دسترسی پیدا کنید و خروجی دستور sh r را که از خط فرمان PC0 در هر دو سوییچ اجرا کرده‌اید به مربی نشان دهید.

Command	Description
interface vlan 1	Global command. Moves the user to interface configuration mode for a VLAN interface.
ip address *address subnet-mask*	Interface configuration mode command that sets the IP address for in-band switch management.
ip default-gateway *address*	Global command that sets the default gateway so that the management interface can be reached from a remote network.

دستورات صحیح انتساب آدرس IP به یکی از سوییچ‌ها را پس از انجام درست آزمایش، بنویسید.

راهنمایی:

پس از تنظیم IP Address بر سوییچ‌ها، بایستی بتوان آن‌ها را از کامپیوتر موجود در همان VLAN آدرس داده شده، ping نمود. در صورت بروز مشکل در ping، از دستور sh r برای رویت راهکار استفاده کنید.

۸. خروجی دستور show VLAN در سوییچ سمت چپ را در برگه گزارش کار بنویسید.

آزمایش هشتم

مسیریابی و کنترل دسترسی

۹-۱- مقدمه

ارتباط بین کامپیوترهای در دو شبکه‌ی LAN مختلف از طریق مسیریابی برقرار می‌شود. نوعی از مسیریابی ایستا را در آزمایش ششم انجام دادیم. اکنون نوبت به شناخت بیشتر و دقیق‌تر و فراگیری تنظیمات مسیریابی برای پروتکل‌های رایج آن است. همچنین یکی از مهمترین نکات مرتبط با شبکه در زمینه‌ی کنترل دسترسی کامپیوترها، با کمک آدرس IP بیان خواهد شد. چنین امکانی در شبکه‌های LAN که کامپیوترها از طریق سوییچ به هم متصل هستند به سادگی فراهم نیست.

۹-۲- هدف

فراگیری مفهوم و نحوه‌ی تنظیم پروتکل مسیریابی RIP و ACL در مسیریاب‌های سیسکو

۹-۳- پیش‌آگاهی

اکثر محدوده‌ی آدرس‌های IP همانند شماره‌های تلفن، هزینه بر هستند و دارای متولی مشخص واگذاری هستند، اما برخی از محدوده‌ها برای استفاده‌های داخلی (همانند شماره تلفن داخلی یک سازمان که در بیرون از آن مفهومی ندارد) به کار می‌روند و نیازی به خرید ندارند و در اینترنت واقعی نیز، بسته با آدرس‌های چنین، مسیریابی نمی‌شوند. اما در شبیه‌ساز جاری از چنین محدوده‌هایی استفاده خواهد شد. دو مورد از محدوده آدرس‌های داخلی 192.168.x.x/24 و 172.16.x.x/16 هستند که می‌توان به جای x هر عددی را گذاشت.

در بستن یک شبکه‌ی WAN بایستی interfaceهای دو به دو مرتبط (یعنی دارای ارتباط Point to Point) بایستی دارای یک محدوده‌ی آدرس IP باشند تا همدیگر را ببینند. از طرفی چون وظیفه‌ی مسیریاب، برقراری ارتباط بین شبکه‌های مختلف است، مجاز نیستیم که دو interface یک مسیریاب را از یک محدوده‌ی آدرس انتخاب کنیم و انتظار داشته باشیم مسیریابی بین این دو صورت پذیرد، زیرا هر دو در یک شبکه واقعند!

به‌طور کلی پروتکل‌های مسیریابی به دو دسته تقسیم می‌شوند:

۱. ایستا

این نوع مسیریابی توسط راهبر شبکه تنظیم می‌شود و در این حالت، مسیر تنظیم شده برای عبور بسته‌ها، پس تنظیم تغییر نخواهد کرد. چنین رویکردی معمولا در حالتی که پیکربندی شبکه ساده باشد، مسیر از قبل مشخص باشد یا گزینه‌های متنوعی نداشته باشیم مورد استفاده قرار می‌گیرد.

۲. پویا

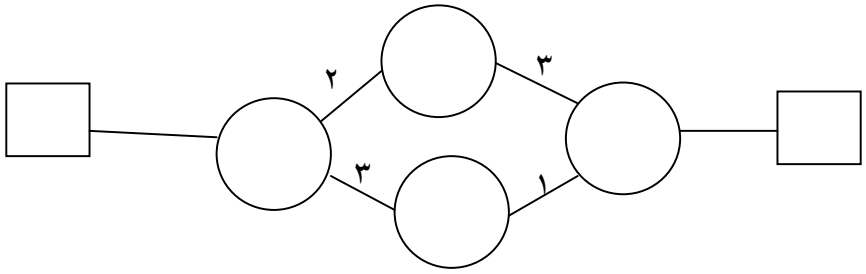
در این حالت، مسیرعبور بسته‌ها بر اساس توپولوژی شبکه و وضعیت مسیریاب‌ها و ترافیک آن‌ها قابل تغییر است، و مسیریابی در هر لحظه بر اساس جدولی که مسیریاب در حافظه ایجاد کرده است، صورت می‌گیرد. نحوه ایجاد این جدول به یکی از دو صورت زیر است:

i. **الگوریتم‌های بردار فاصله یا Distance Vector:** در این حالت مسیریاب جدول را فقط بر اساس اطلاعات همسایه‌های مستقیما متصل ایجاد می‌کند. در گراف شبکه در این صورت، مسیریاب‌ها، گره‌ها[1] و یال‌های بین مسیریاب‌ها، لینک‌های فیزیکی بین آن‌ها هستند. برای ارزیابی مسیر، باید به لینک‌ها عددی نسبت داده شود که منعکس کننده‌ی فاصله یا تأخیر خط باشد. دو نوع معیار

[1] Nodes

ارزیابی یا Metric داریم: معیار ارزیابی ساده که Hop Count یا شمارش گام نیز نامیده می‌شود و به هر لینک عدد یک را منتسب می‌کند، در این حالت تعداد گام‌ها تعیین کننده‌ی مسیر نهایی است و کوتاه‌ترین مسیر، مسیری است که تعداد گام‌های کمتری داشته باشد. در این آزمایش، چنین گزینه‌ای پیکربندی خواهد شد. رویکرد دیگر انتساب عدد به لینک‌ها، بر اساس پارامترهای واقعی‌تر از جمله میزان تأخیر خط است. از رایج‌ترین پروتکل‌های بردار فاصله، RIP[1] است. به عنوان مثال جدول زیر برای شبکه‌ای که در ادامه‌ی آن آمده است، در هر مسیریاب تشکیل و پر می‌شود:

Destination	Next Hop	Metric
A		
B		
C		
D		



و طی یک سلسله محاسبات و رد و بدل شدن بسته‌های کنترلی بین مسیریاب‌ها، در نهایت مسیر پایین که کوتاه‌تر است به عنوان مسیر برگزیده برای ارسال بسته‌ها انتخاب می‌شود.
با توجه به اینکه بررسی دقیق نحوه‌ی عملکرد پروتکل در درس شبکه ۲، صورت می‌گیرد، از ذکر آن در این مستند خودداری می‌شود.

b. **الگوریتم‌های وضعیت لینک یا Link State:** در این حالت، مسیریاب در هر لحظه ساختمان‌داده‌ی گراف کل شبکه را در خود نگهداری می‌کند، بنابراین می‌تواند برای سنجش فاصله‌ی دو نقطه، یک محاسبه براساس الگوریتمی مانند الگوریتم Dijikstra انجام دهد.در این حالت نیز به لینک‌ها عددی منتسب می‌شود متناظر با پارامترهای واقعی خط از جمله تأخیر آن. از رایج‌ترین پروتکل‌های حالت لینک، OSPF[2] است.

[1] Routing Information Protocol
[2] Open Shortest Path First

به هنگام سازی جدول در یک مسیریاب براساس ارتباطات همه‌ی ندهای دیگر شبکه صورت می‌گیرد و بار محاسباتی بیشتری نسبت به حالت بردار فاصله بر CPU یک مسیریاب تحمیل می شود.

۹-٤- پیکربندی مسیریابی بردارفاصله

در حالتی که از مسیریابی پویا مبتنی بر بردار فاصله با معیار فاصله‌ی شمارش گام استفاده می‌کنیم باید با بعد از ورود به حالت پیکربندی و تعیین نوع پروتکل همانند زیر

```
#conf t
#router rip
```

با توجه به شماره شبکه‌ی هر interface مسیریاب، تنظیم دستور زیر را نوشت:

```
#network شماره شبکه
```

به عنوان مثال اگر یکی از کارت‌های شبکه‌ی مسیریاب دارای آدرس IP از محدوده‌ی 192.168.1.0/24 باشد، دستور زیر را وارد می‌کنیم.

```
#network 192.168.1.0
```

پس از آن‌که به ازای تمام کارت شبکه‌های متصل به مسیریاب، روند را تکرار کردیم، باید اندکی صبر کرد تا تغییرات در شبکه منعکس شود، سپس می‌توان حاصل را آزمود.

۹-۵- لیست کنترل دسترسی ACL[1]

ACL همانطور که در ترجمه لغوی به معنای لیست کنترل دسترسی در تجهیزات سیسکو می‌باشد، زیاد هم از معنای واقعی خود دور نیست و برای کنترل ترافیک بر مسیریاب‌ها استفاده می‌شود. یعنی با در نظر گرفتن آدرس IP، کنترل‌هایی جهت عبور یا عدم عبور بسته از یک interface یک مسیریاب به داخل یا خارج آن اعمال می‌کنند. در تجهیزات سیسکو دو مرحله برای ایجاد یک Access List داریم. اول می‌بایستACL مربوطه را نوشته و دوم آن را به یک واسط اعمال کنیم. بدیهی است در صورت عدم اعمال ACL به یک interface، ACL مذکور بی‌استفاده خواهد ماند. Access Listها یا IP Access Listهای به دو نوع تقسیم می‌شوند:

[1] Access Control List

- Standard: در بسته‌های عبوری، تنها آدرس IP مبدأ[1] کنترل شده و بر اساس قاعده‌ی تعریف شده، به آن اجازه‌ی عبور یا لغو[2] داده می‌شود.
- Extended: برحسب آدرس IP مبدأ و مقصد و نیز شماره‌ی پورت، یعنی نوع کاربرد بسته، می‌تواند محدودیت ایجاد کند.

معمولاً برای نام‌گذاری Access List ها از اعداد استفاده می‌شود. که از شماره ۱ تا ۹۹ برایStandard و ۱۰۰ تا ۱۹۹ برایExtended استفاده می‌شود. البته اضافه بر آن، اعداد ۱۳۰۰ تا ۱۹۹۹برای Standard و ۲۰۰۰ تا ۲۶۹۹ برای Extended نیز رزرو شده اند.

قالب کلی یک Standard Access list که در حالت پیکربندی در مسیریاب نوشته می شود، بدین صورت است:

access-list access-list-number {permit|deny} {host|source source-wildcard|any}

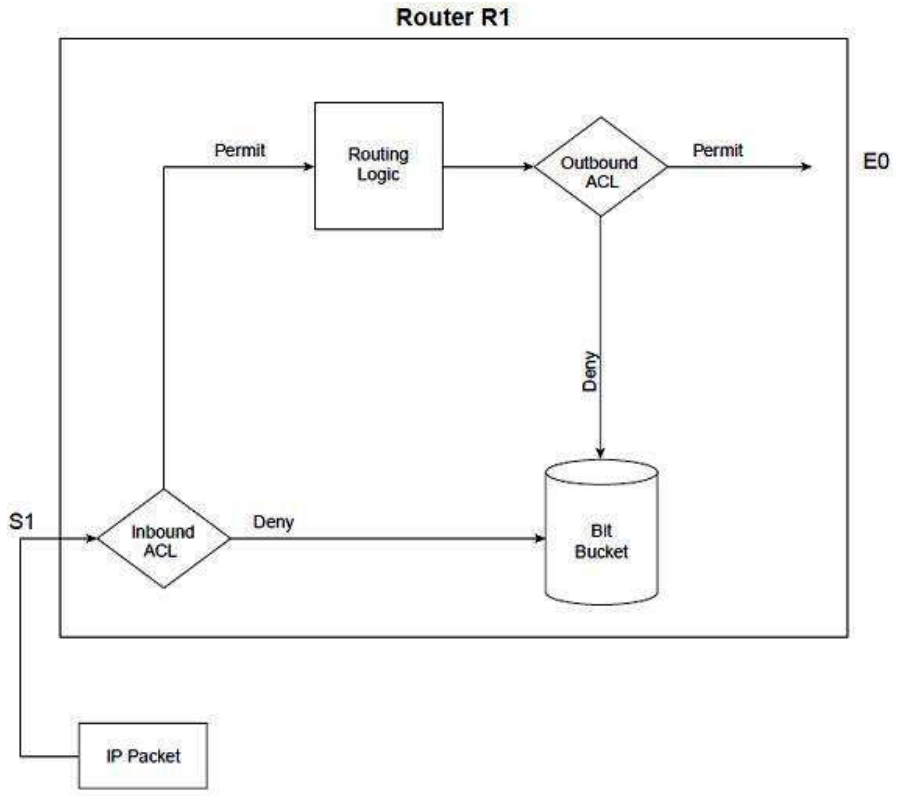
یعنی در ابتدا می‌بایست عبارت access-list را تایپ نموده سپس یک شماره به آن اختصاص می‌دهیم، سپس وظیفه آن که نابودی یا اجازه عبور یک Packet است را مشخص می‌کنیم، در انتها هم آدرس IP مبدا را می‌نویسیم. به طور خلاصه wildcard mask شیوه‌ای از مشخص کردن شماره زیر شبکه است که معکوس subnet mask است. به‌طور مثال ip و wildcard زیر، محدوده‌ی صفر تا ۲۵۵ را نشان می‌دهد:

۱۹۲.۱۶۸.۱۰.۰ ۰.۰.۰.۲۵۵

عدد ۲۵۵ در wildcard فوق نشان‌دهنده‌ی آن است که شماره ماشین در شبکه هرچه باشد سیاست به آن اعمال می‌گردد. به عبارت دیگر بایت‌های صفر در wildcard mask، بخش‌هایی از آدرس شبکه ذکر شده را مشخص می‌کنند که مایلیم با آدرس مبدأ بسته تطابق داده شود. یعنی اگر ۰.۰.۰.۰ باشد، یعنی همه‌ی آدرس مبدأ باید با آنچه آمده تطابق کند. پس ازاینکه تصمیم گرفتیم که چه ترافیکی باید فیلتر شود، می‌توان مشخص کرد که این کار بر کدام مسیریاب انجام گیرد.

بسته را می‌توان در ورود به یک interface از یک مسیریاب یا در خروج از آن بررسی کرد. چنین مفاهیمی inbound و outbound نامیده می‌شوند. شکل زیر بیان گویایی از حالت‌های امکان اعمال ACL در مسیریاب است که در آن بسته در مسیریاب R1 از interface سریال وارد و از interface اترنت خارج می‌شود.

[1] SOURCE IP address
[2] Discard



شکل ۹-۱ اعمال ACL در ورود به یک Interface یا در خروج از آن

پس از یافتن مسیریاب مناسب در شبکه برای اعمال سیاست کنترلی، بایستی interface مناسب از آن را تعیین کنیم. هرگونه اشتباه در این روند به عبور بسته‌های غیرمجاز یا مسدود شدن بسته‌های مجاز و در نتیجه مشکلات پیاده‌سازی منجر خواهد شد. نمودار فوق حاوی نکات مهمی است که در زیر به آن‌ها اشاره شده است:

- بسته‌ها ممکن است در ورود به یک interface و پیش از تصمیم مسیریابی فیلتر شوند.
- بسته‌ها را می‌توان پیش از خروج از interface و پس از اتخاذ تصمیم مسیریابی فیلتر کرد.
- deny اصطلاحی است در سیستم‌عامل سیسکو برای اشاره به فیلتر شدن یک بسته.
- permit اصطلاحی است در سیستم‌عامل سیسکو برای اشاره به اجازه‌ی عبور یک بسته.
- منطق فیلتر کردن در Access List پیکربندی می‌شود
- پیش فرض ACL آن است که بسته‌هایی که در قاعده صدق می‌کنند، سیاست تدوین شده در رابطه با آن‌ها اعمال شود اما آن‌ها که در قاعده صدق نمی‌کنند باید کلا فیلتر شوند. بنابراین در

آخر هر مجموع ACL باید دستور permit any را وارد نمود وگرنه سایر بسته‌ها همه فیلتر خواهند شد.

بنابر آنچه بیان شد در منطق ACLهادر هنگام عمل، دو گام صورت می‌پذیرد:

- تطابق یا matching
- عمل یا action که خود می‌تواند یکی از دو مورد زیر باشد:
  - Deny
  - Permit

دستورات مرتبط برای تنظیم در پیکربندی عمومی در جدول زیر آمده است، منظور حالتی است که ACL تعریف شده اما اعمال نشده است.

Standard IP Access List Configuration Commands

Command	Configuration Mode and Description
access-list *access-list-number* {deny | permit} *source* [*source-wildcard*] [log]	Global command for standard numbered access lists. Use a number between 1 and 99 or 1300 and 1999, inclusive.
access-list *access-list-number* remark *text*	Defines a remark that helps you remember what the ACL is supposed to do.

دستور برای انتساب یک ACL خاص به یک interface:

Table 12-3 *Standard IP Access List Configuration Commands (Continued)*

Command	Configuration Mode and Description
ip access-group {*number* | *name* [in | out]}	Interface subcommand to enable access lists.
access-class *number* | *name* [in | out]	Line subcommand to enable either standard or extended access lists.

دستورات رویت و بررسی ACLها تعریف و اعمال شده نیز در جدول زیر آمده‌اند.

Table 12-4 *Standard IP Access List EXEC Commands*

Command	Description
show ip interface [*type number*]	Includes a reference to the access lists enabled on the interface.
show access-lists [*access-list-number* | *access-list-name*]	Shows details of configured access lists for all protocols.
show ip access-list [*access-list-number* | *access-list-name*]	Shows IP access lists.

برای واضح‌تر شدن موضوع، مثال زیر را مشاهده نمایید.

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

access-list 1 remark stop all traffic whose source IP is Bob
access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
```

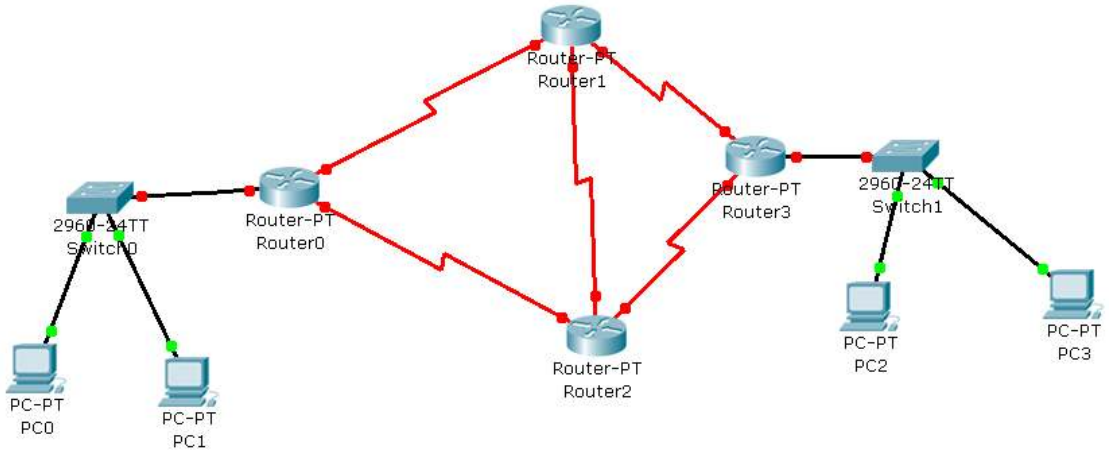
البته می‌توان به جای دستور آخر، دستور زیر را که از لحاظ نگارشی نیز ساده‌تر است نوشت:

access-list 1 permit any

گرچه کار کردن با Extended Access Listها بسیار سودمند است اما به جهت نیاز به مفاهیم پیش‌نیاز زیاد، از ذکر آن در این آزمایش اجتناب می‌شود و خواننده پیشنهاد می‌شود در صورت تمایل به سادگی آموزش کار و استفاده آن را از اینترنت تهیه نماید.

۹-٦- دستور کار

۱. به تمام interfaceهای ماشین‌ها و مسیریاب‌های شبکه‌ی زیر را ابتدا بر روی برگه‌ی گزارش کار، آدرس دهید و پس از تأیید مربی، آن را پیاده‌سازی کنید و تست‌های زیر را انجام دهید و نتیجه را در برگه‌ی گزارش کار یادداشت کنید.



راهنمایی ۱: پیشنهاد می‌شود محدوده‌ی آدرس LAN سمت چپ را 192.168.1.0/24 و محدوده‌ی آدرس LAN سمت راست را 192.168.2.0/24 و محدوده‌ی آدرس interfaceهای مسیریاب‌ها را 172.x.0.0/16 بدهید که x برای هر زوج interface تفاوت داشته باشد.

راهنمایی ۲: اگر مسیریاب ۱ و ۲ دارای دو کارت شبکه باشند، می‌توانید پس از خاموش کردن به آن‌ها یک کارت شبکه‌ی سریال اضافه کنید.

۲. الف) از PC2، PC1 را ping کنید و دو سطر از پاسخ را در کاربرگ گزارش کار بنویسید.

ب) با دستور tracert، مسیری را که بسته از PC2 به PC1 طی می‌کند بیابید و بنویسید.

ج) با دستور sh r وضعیت پیکربندی یکی از مسیریاب‌ها را بعد از پیکربندی پروتکل مسیریابی، مشاهده کنید.

د) دستور show ip route را بزنید و با کمک help خط فرمان سیسکو و آنچه تاکنون در گزارش کار آموخته‌اید و در آزمایش انجام داده‌اید، جزییات خروجی دستور را تفسیر کنید و به صورت خلاصه در برگه گزارش کار بنویسید.

۳. یک Server به LAN سمت چپ اضافه کنید و با ACL، دستوراتی بنویسید که اجازه‌ی ارتباط PC2 با Server را ندهد اما PC3 بتواند چنین ارتباطی داشته باشد.

الف) به نظر شما دستور مربوطه باید بر کدام interface از کدام مسیریاب تنظیم شود؟

ب) دستورات مربوطه را در گزارش‌کار یادداشت کنید.

۴. الف) برای جلوگیری از ارتباط PC2 و PC3 چه مکانیزمی را پیشنهاد می‌کنید؟

ب) برای جلوگیری از ارتباط PC1 و PC3 چه مکانیزمی را پیشنهاد می‌کنید؟

ج) هر دو مکانیزم را پیاده‌سازی کنید و به مدرس اطلاع دهید تا صحت عملکرد را تست نماید.

د) چه نتیجه‌ای از مقایسه‌ی مورد الف و ب می‌توان گرفت؟

و)دستورات مرتبط با رویت Access Listها را بیازمایید و نتیجه را مشاهده کنید.

آزمایش نهم

Group Policy

۱۰-۱- مقدمه

در این جلسه با مفاهیمی آشنا خواهید شد که در سیستم‌عامل ویندوز تعبیه شده و امکانات مفید متعددی در اختیار کاربر (راهبر شبکه یا کاربر حرفه‌ای) برای اعمال سیاست‌های مختلف در استفاده از منابع، قرار می‌دهد.

به عنوان مثال، مواردی مانند اینکه کاربران نتوانند برخی پارامترهای سیستمی تنظیمات کارت شبکه یا ساعت سیستم یا بسیاری موارد دیگر را تغییر دهند، به سادگی در Group Policy قابل تنظیم است. همچنین انواع تنظیمات مورد نیاز راهبران سیستم‌ها و شبکه‌های کامپیوتری نیز با Group Policy قابل اجراست، حتی مواردی ساده مانند جلوگیری از تغییر عکس پس‌زمینه در Desktop ویندوز. در این آزمایش علاوه بر آشنایی با Group Policy و نحوه کار با آن، از برخی نکات کاربردی مفید دیگر نیز مطلع خواهید شد.

۱۰-۲- هدف

آشنایی با Group Policy و نحوه‌ی کار با آن

۱۰-۳- پیش‌آگاهی

با توجه به عدم امکان جستجو در محیط Group Policy و عدم امکان حذف و تشخیص کامل روابط بین اجزای آن در نگاه اول برای مبتدیان، بهتر است با نگرشی ساده و در عین‌حال کامل به Group Policy پرداخت تا بیشترین بازدهی را برای فراگیران داشته باشد.

۱۰-۳-۱- Group Policy چیست؟

Group Policies مجموعه‌ای از تنظیمات مرتبط با پیکربندی[1] است که راهبر شبکه در مورد چگونگی استفاده از برنامه‌ها، منابع و سیستم‌عامل توسط کاربر و کامپیوتر، اعمال می‌کند. این امکان در سیستم‌عامل ویندوز فراهم شده است و به عبارت دیگر وظیفه‌ی آن کنترل کاربران است که چه کارهایی بتوانند انجام دهند و چه کارهایی نتوانند انجام دهند. به خصوص در سازمان‌ها، ادارات، مدارس، دانشگاه‌ها و ... از آن برای محدود کردن یا اعمال سیاست‌های استفاده از محیط کامپیوتری، استفاده می‌شود. این سیاست‌ها در سطوح مختلف ازجمله یک کامپیوتر، Domain، سایت و یک گروه از کاربران قابل اعمال هستند. از موارد استفاده این سیاست‌ها ایجاد امنیت بیشتر و همچنین بهبود محیط کاربر می‌باشد.

البته برخی از دانشجویان با تجربه ممکن است با رجیستری ویندوز نیز کار کرده باشند که امکانات متنوع و بسیار دقیقی برای کار با سیستم عامل ویندوز و تنظیم آن در اختیار قرار می‌دهد، و این سوال ممکن است به ذهن ایشان خطور نماید که تفاوت بین Group Policy و Registry در چیست و آیا هر دو دارای یک توانایی هستند؟ در پاسخ باید اشاره شود که گرچه قابلیت‌های رجیستری بسیار است و می‌توان کارهای مربوط به Group Policy را نیز به نوعی با آن انجام داد، اما ریسک کار با آن به خصوص برای کاربران غیرحرفه‌ای زیاد است و عواقب تنظیمات اشتباه در رجیستری خطرناک‌تر از Group Policy است. برخی تغییرات مانند حذف یک کلید در رجیستری امکان بازگشت ندارد در حالی که تغییرات Group Policy قابل بازگشت هستند.

۱۰-۳-۲- انواع Group policy

جزییات دقیق مرتبط با Group Policy را در دستورکار خواهید یافت اما به صورت کلی، در پنج حیطه می‌توان سیاست تعریف و اعمال کرد:

[1] Configuration Setting

۱- Scripts

این امکان را به Administrator می‌دهد که با اعمال سیاست‌هایی اجرایی، Scriptها وفایل‌های دسته‌ای[1] خاص را در زمان‌های معین اجرا کند. مثلا در زمان ورود کاربر به سیستم، عکسی در پیش‌زمینه‌ی کامپیوتر به مناسبتی خاص نمایش داده شود، یا پیش از خاموش شدن کامپیوتر، پیامی به کاربر برای یادآوری داده شود یا ....

۲- Security Settings

این‌سیاست‌ها به‌صورت محدودکردن دسترسی کاربرها به فایل و پوشه‌ها و همچنین کنترل مربوط به Registry و... می‌باشد.

۳- Administrative templates

این سیاست‌ها شامل‌سیاست‌های مبتنی بر رجیستری[2] مانندبرنامه‌های کاربردی و اجزای‌سیستم عامل می‌شود و در آن می‌توان انواع تنظیمات مانند تنظیمات مربوط به جزییات Control Panel، شبکه، چاپگر و ... را انجام داد.

٤- RIS[3]

مربوط به گزینه‌های مرتبط با نصب و کنترل برنامه بر چندین کامپیوتر، از طریق Server است. بدین ترتیب که می‌توان سیستم‌عامل ویندوز را به طور همزمان بدون نیاز به اینکه به تک تک کامپیوترها مراجعه کنیم، بر همه‌ی آن‌ها نصب نماییم.

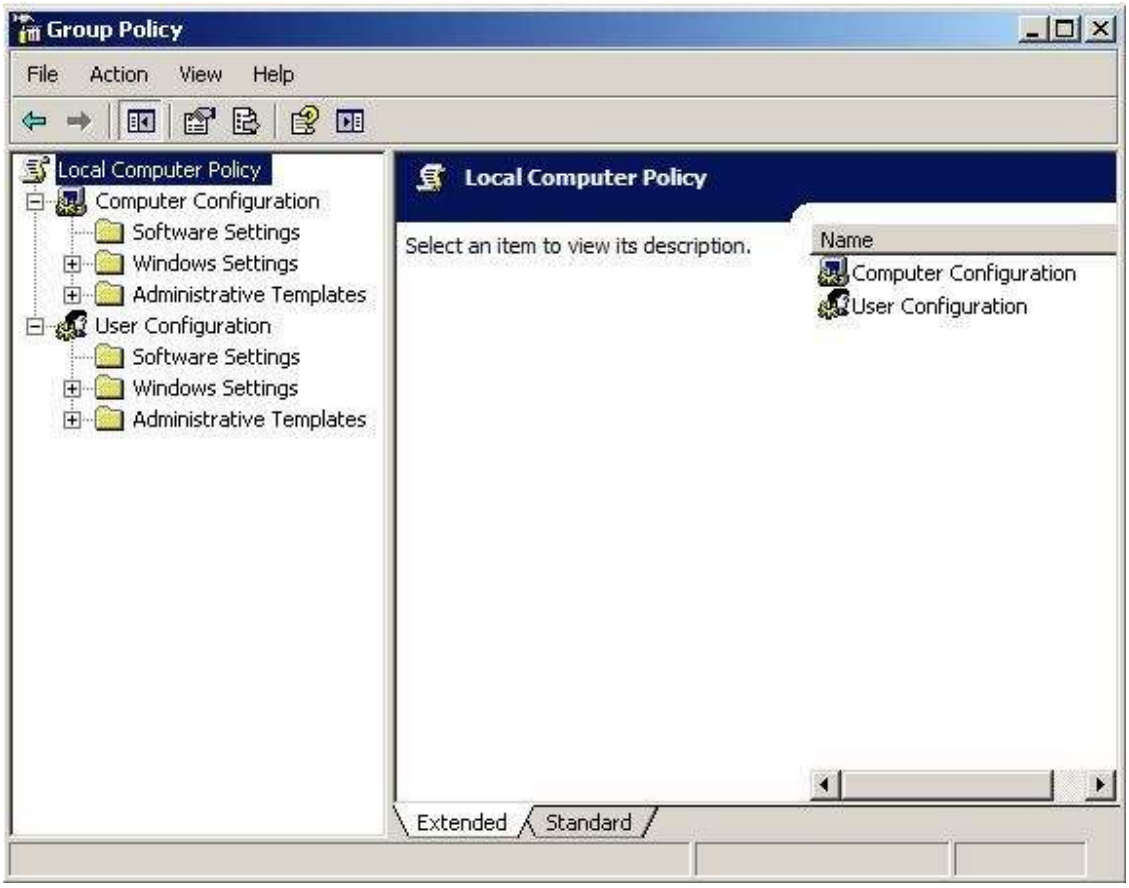
۵- Software Settings

برروی برنامه‌های کاربردی که کاربرها می‌توانند به آنها دسترسی داشته باشند و آنها را نصب و اجرا کنند اعمال می‌شوند. به عنوان مثال، مدیریت متمرکز نصب، به‌هنگام‌سازی و حذف برنامه‌های مختلف از قبیل محصولات Microsoft Office.

۱۰-۳-۳- آشنایی با محیط Group Policy

ورود به محیط ویرایش Group Policy با اجرای دستور gpedit.msc در Run انجام می‌پذیرد و حق دسترسی کامل به آن، به قوی‌ترین کاربر در سیستم یعنی Administrator (راهبر) اختصاص دارد. نمای Group Policy شبیه به شکل زیر است:

[1] Batch Files
[2] Registry- Based
[3] Remote Installation Service



شکل ۱۱۰- نمای Group Policy و اجزای آن

در پنجره‌ی سمت چپ، دو رده‌ی اصلی برای اعمال سیاست‌ها، در زیر عنوان Local computer policy، وجود دارد:

- Computer Configuration

راهبران می‌توانند با این گزینه سیاست‌هایی که به کامپیوتر اعمال می‌شود را فارغ از اینکه اکنون چه کاربری در حال استفاده از آن است، تنظیم کنند.

- User Configuration

راهبران می‌توانند به خصوص در شبکه‌هایی که از نوع Domain هستند، این تنظیمات را به کاربر یا کاربرانی اعمال کنند، فارغ از اینکه در حال استفاده از کدام کامپیوتر هستند.

همچنین نمای Extended که در گوشه‌ی پایین بخش سمت راست پنجره در کنار نمای Standard قرار دارد، این امکان را فراهم می‌کند که برای بسیاری از گزینه‌هایی که با توضیح همراه است، بتوان توضیحات مربوطه را همزمان با استفاده، مشاهده نمود.

هر کدام از این دو انتخاب در سه بخش کلی سازماندهی شده است، به نام‌های:

۱- Software Settings

۲- Windows Settings

۳- Administrative Templates

که همانطور که اشاره شد، به ازای کامپیوتر یا به ازای کاربر قابل تعریف است.

Software Settings به صورت پیش‌فرض خالی است، اما گزینه‌های Windows Setting که به نوعی نام آن‌ها بیانگر عملکرد آن‌ها نیز هست، به سادگی قابل درک هستند در حالی که برای گزینه‌های Administrative Templates شرح مبسوط ارائه شده است.

۱۰-٤- تکلیف

یکی از دو پرسش زیر را به دلخواه پاسخ دهید:

۱. یک مورد کاربرد برای Scripts (Logon/Logoff) در Windows Settings در User Configuration یا Computer Configuration بیابید و تشریح کنید (مورد باید عملی و کاربردی و قابل انجام باشد و قابل درک).

۲. فرض کنید که در یک شبکه‌ی Domain می‌خواهید با کمک Group Policy تنظیماتی در Domain Controller لحاظ کنید که تمام کاربران پس از وارد کردن نام کاربری خود و ورود به کامپیوتر تحت Domain، یک تصویر خاص را Background رویت کنند. روند را به دقت تشریح کنید.

۱۰-۵- دستورکار

توجه:
با توجه به اینکه تغییرات در Group Policy ممکن است سبب پیشامدهای ناخواسته در سیستم‌عامل گردد، در اعمال آن‌ها دقت کنید و پس از مشاهده‌ی اثر تغییرات، آن را به حالت قبل بازگردانید.

۱. در Group Policy به مسیر زیر بروید

Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

گزینه‌ی Enforce Password History بیانگر تعیین تاریخچه برای استفاده از رمز عبور تکراری است، یعنی اگر مقدار آن ۳ باشد و کاربری رمز عبور خود را تغییر دهد یا مجبور به تغییر آن شود، نخواهد توانست ۳ رمز عبور پیشین خود را مجددا استفاده نماید و باید رمز عبور جدیدی غیر از آن‌ها برگزیند. .
حال شما نیز مشابه به توضیح فوق به سوالات پایین پاسخ دهید.
الف) سه گزینه‌ی زیر را هرکدام در یک سطر شرح دهید و حداکثر و حداقل مقدار مجاز برای هرکدام را بنویسید:

- Maximum Password Age
- Minimum Password Age
- Minimum Password Length

راهنمایی: در صورت بروز ابهام در رابطه با کاربرد یا مقدار هر یک، بر آن کلیک دوگانه کنید و از سربرگ Explain This Setting، جزییات آن را بخوانید و اگر سربرگ مذکور در سیستم‌عامل ویندوز شما وجود نداشت، با زدن کلید F1 گزینه‌ی مربوطه را از Help بیابید و شرح آن را ببینید.

ب) با استفاده از سربرگ Explain This Setting یا Help، پس از کلیک دوگانه بر گزینه‌ی Password Must Meet Complexity Requirements، خصوصیات پیچیدگی رمزعبور در سیستم‌عامل ویندوز را بنویسید.

۲. در Group Policy به مسیر زیر بروید

Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

Account lockout threshold را با مقدار ۳، گزینه Account lockout duration را با مقدار ۲ دقیقه و گزینه Reset account lockout counter after را با مقدار ۱ تنظیم کنید.

سپس Logoff نمایید و سه بار پشت سرهم رمز عبور را اشتباه وارد کنید.

الف) پس از بار سوم اشتباه وارد کردن رمز عبور، چند دقیقه سیستم قفل خواهد شد؟

ب) اگر مجددا روند را از نو تکرار کنید، یعنی پس از یک Login موفق، Logoff کنید و دو بار رمز عبور را اشتباه وارد نموده و سپس یک دقیقه صبر کنید، چند بار دیگر رمز عبور را می‌توان اشتباه وارد کرد، تا سیستم به حالت قفل برود؟

ج) با توجه به نتایج قسمت الف و ب، کاربرد هر یک از مواردی را که مقداردهی کردید، بنویسید.

راهنمایی: همچنین می‌توانید از Help یا سربرگ Explain This Setting نیز کمک بگیرید.

۳. به Start سپس Run بروید و عبارت gpedit.msc را تایپ نمایید، سپس OK را کلیک کنید. در محیط باز شده، از Computer Configuration، Windows Settings و بعد Security Settings و سپس از Local Policies گزینه‌ی Audit Policy را انتخاب نمایید و در پنجره‌ی سمت راست گزینه‌ی Audit logon events را کلیک دوگانه کنید.

حال از پنجره‌ی باز شده، هر دو مورد Success و Failure را علامت بزنید. سپس سیستم را Logoff کنید و در ورود مجدد به سیستم، ابتدا یک نام کاربری و رمزعبور ناشناخته وارد کنید تا پیام خطا ظاهر شود و سپس نام کاربری و رمزعبور مجاز برای ورود به سیستم را وارد کنید.

الف) به Event Viewer که در Administrative Tools در Control Panel قرار دارد بروید و با کلیک بر Security، رویدادهای مرتبط را بیابید و Event ID و شرح رویداد تلاش ناموفق برای ورود را بیابید و در برگه‌ی گزارش کار بنویسید.

توجه:

چنانچه به دلیل نرم‌افزار خاص نصب شده در سایت، پس از Login مجدد، تمام تنظیمات به حالت اول برگشته بود، به جای انجام Logoff از Switch User استفاده نمایید.

ب) در Group Policy در همان مسیر Audit logon events گزینه‌ی Audit account management را انتخاب نمایید و هر دو مورد Success و Failure را برای آن علامت بزنید و سپس، براساس روند زیر، یک کاربر در سیستم ایجاد نمایید:

به این مسیر بروید:

Start -> Setting -> Control Panel -> Administrative Tools -> Computer Management

از قسمت System Tools، Local Users and Groups و سپس Usersرا انتخاب نمایید و با کلیک راست در فضای خالی سمت راست پنجره و انتخاب New User کاربر جدیدی با مشخصات زیر ایجاد کنید:

User: user
Password: 123

به نظر شما رویداد متناظر با عملکرد شما اکنون در کجا ثبت شده است؟ چند رویداد به ازای تعریف این یک کاربر، در سیستم ایجاد شده است؟

ج) کاربرد Audit object access را شرح دهید.

۴. در Group Policy به مسیر زیر بروید:

Local Computer Policy -> Computer Configuration -> Windows Settings -> Local Policies -> User right assignment

سه مورد دلخواه را که می‌توانید عملکرد و استفاده‌ی آن را درک کنید به صورت خلاصه بنویسید.

۵. در Group Policy به مسیر زیر بروید

Local Computer Policy -> Computer Configuration -> Windows Settings -> Local Policies -> security options

گزینه‌های مربوط به موارد زیر را بیابید و فقط عنوان انگلیسی معادل آن‌ها را بنویسید(تغییری ایجاد نکنید):

a. تغییر نام Administrator
b. حذف نیاز به استفاده از Ctrl+Alt+Del در شروع به کار سیستم
c. کاربری که Log on نکرده است، اجازه داشته باشد که سیستم را خاموش کند یا خیر

۶. به خط فرمان بروید و دستور **gpupdate** را بنویسید و علاوه بر یادداشت خروجی آن، ذکر کنیدکه به چه کار می‌آید. آیا دیگر نیازی هست که برای اعمال تغییرات در Group Policy سیستم را Restart یا Logoff کرد؟

۷. موارد زیر را در Administrative Templates بیابید تست کنید و آدرس آن را یادداشت کنید:

الف) جلوگیری از تغییر عکس پس‌زمینه (Wall Paper) در ویندوز

ب) جلوگیری از دسترسی به Add or Remove Programs

ج) جلوگیری از پاک کردن تاریخچه دسترسی به وب‌سایت‌ها (Browsing History) در Internet Explorer

توجه: قسمت الف و ب را انجام دهید و صحت انجام آن را تست کنید و به مربی نشان دهید.

آزمایش دهم

کابل کشی ساختیافته

۱۱-۱- مقدمه

پس از فراگیری مفاهیم نرم‌افزاری در رابطه با راهبری شبکه، آخرین مبحثی که بسیار برای راهبران شبکه، به خصوص شبکه محلی مفید است، اتصالات فیزیکی و کابل کشی است. این موضوع خود به تنهایی، مفصل و مشروح است و نمی‌توان در یک آزمایش کوتاه مدت تمام جنبه‌های آن را آزمود. در این مستند سعی بر آن بوده است تا به شروع کار در چنین زمینه‌ایی اشاره شود و دانشجو بتواند خود برای کسب اطلاعات بیشتر اقدام نماید. توجه کنید که این آزمایش به هیچ‌وجه کل مبانی را بیان نکرده و با محدودیت زمانی تهیه شده و مطالب بیشتر را در بخش مراجع می‌توان یافت.

لازم به ذکر است در این آزمایش از جزوه‌ی همکار ارجمند جناب آقای مهندس مهران علمداری که برای موسسه آموزش عالی زرندیه آماده کرده‌اند نیز در قسمت استاندارد های رنگ کابل شبکه استفاده شده است. همچنین از برخی پیشنویس‌های دوست گرامی جناب آقای مهدی‌شیخ‌زاده دانشجوی زبان دانشگاه ایرانشهر نیز استفاده شده است.

۱۱-۲- هدف

آشنایی با مفاهیم پایه‌ی کابل‌کشی ساختیافته و ایجاد یک کابل Cross Over

۱۱-۳- پیش‌آگاهی

تا زمانی که استانداردهایی برای کابل‌کشی تدوین و عرضه نشده بود، عملیات مربوط به آن بدون هیچ طرح و نقشه‌ایی صورت می‌گرفت، این امر تا وقتی شبکه کوچک باشد با مشکلات زیادی همراه نیست، اما به محض افزایش تعداد کامپیوترها به شدت آزار دهنده می‌شود به نحوی که مطابق با آمارهای اعلام شده، حدود هفتاد درصد از قطعی‌ها در شبکه به کابل‌کشی و ایرادات آن مربوط می‌شود.

ANSI نهادی آمریکایی است که در تدوین بسیاری استانداردهای کامپیوتری نقش داشته است که برخی از آن‌ها جهانی شده‌اند و برخی استانداردهای دیگر هم از موسسات بین‌المللی استاندارد مانند ISO تبعیت کرده‌اند.

با فراگیر شدن شبکه‌های کامپیوتری و نیاز به قواعد یکنواخت برای کابل‌کشی و سیم‌بندی آن‌ها، نهاد ANSI، استانداردی به نام TIA/EIA 568 برای استانداردسازی کابل‌کشی ارائه داد، که به دلایل زیر مورد اقبال عمومی قرار گرفت:

- فراهم کردن راهنما برای طراحی و اجرای کابل‌کشی ساخت‌یافته بر اساس معیارهای فنی و کارایی
- مرجعی برای طراحی و اجرای کابل‌کشی ساخت‌یافته برای محیط‌های تجاری
- تحت پوشش دادن و قبول شرکت‌های متعدد برای استفاده از آن

چنین استانداردی، حداقل نیازمندی‌ها برای کابل‌کشی در یک محیط اداری، مسافت و چیدمان[1] توصیه شده، رابط‌ها و اتصال[2]، طول عمر سیستم‌های کابل‌کشی (که معمولا بیش از ۱۰ سال نیست)، نوع تجهیزات به عنوان مثال برای اتصالات یک طبقه ساختمان[3] یا بین طبقات[4] یا بین ساختمان‌ها و تعاریف متعدد مرتبط با کابل‌کشی ساختیافته را در بر می‌گیرد.

[1] Topology
[2] Connector and Pin Assignment
[3] Horizontal Cabling
[4] Backbone Cabling

لازم به ذکر است که کابل‌کشی و سیستم‌های مرتبط با آن، امری است که می‌تواند با پیچیدگی‌های فراوان همراه باشد. همچنین لازم نیست که برای خودتان قواعدی تدوین کنید و یا روی مواردی مانند مثلا نوع کابل برای اتصال دوربین مداربسته به سیستم فکر کنید، زیرا که همه‌ی این‌ها در استاندارد پاسخ داده شده است.

۱۱-۳-۱- برخی تقسیم‌بندی‌ها

در حالت کلی، سه ناحیه برای کابل‌کشی تعریف می‌شود:

- **ناحیه اولیه یا اصلی:**

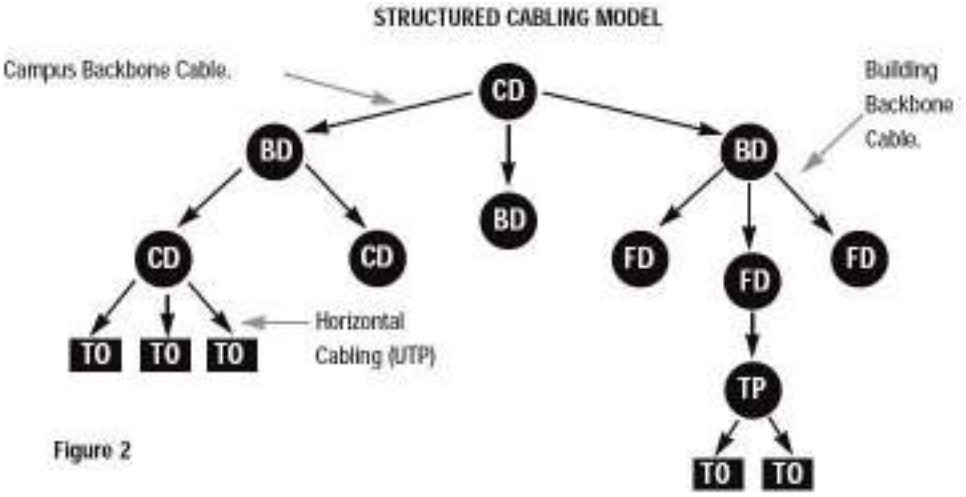
منظور اتصال دو ساختمان[1] است که معمولا برای این امر از فیبرنوری استفاده می‌شود و تنظیمات پهنای‌باند و اتصالات[2]، اهمیت کلیدی دارد.

- **ناحیه ثانویه:**

اتصال سوییچ‌های متصل کننده‌ی ساختمان‌ها، به سوییچ‌ها یا هاب‌های هر طبقه از ساختمان مربوطه‌شان. برخی موارد برای این امر فیبرنوری استفاد می‌شود و برخی موارد از کابل UTP Cat6

- **ناحیه سوم:**

اتصال سوییچ‌ها یا هاب‌های هر طبقه به کامپیوترهای همان طبقه. معمولا در این حالت از کابل UTP Cat5e استفاده می‌شود.



شکل ۱۱۱- نواحی اصلی کابل‌کشی

[1] Campus Cabling
[2] Interfaces

یک قاعده کلی وجود دارد که می‌گوید هرچه به کامپیوتر نزدیک‌تر می‌شوید، کابل مسی بیشتر استفاده می‌شود. همچنین این نحوه‌ی ناحیه‌بندی با توصیه‌های شرکت سیسکو برای ایجاد شبکه به صورت سلسله‌مراتبی که در کلاس درس نیز مطرح شد، همخوانی دارد. شکل زیر بیانگر ناحیه‌های بالاست:

در حالت دقیق‌تر و به خصوص برای پیاده‌سازی واقعی، ۶ محدوده[1] برای کابل‌کشی تعریف می‌شود، که می‌توان از آن‌ها به عنوان عناصر کابل‌کشی نیز نام برد، زیرا هر یک را می‌توان به صورت جدا انجام داد. البته در برخی مراجع نیز از ۷ محدوده نام برده شده، اما اصول کار برهمین مبنایی است که ذکر می‌شود:

۱. Work Area

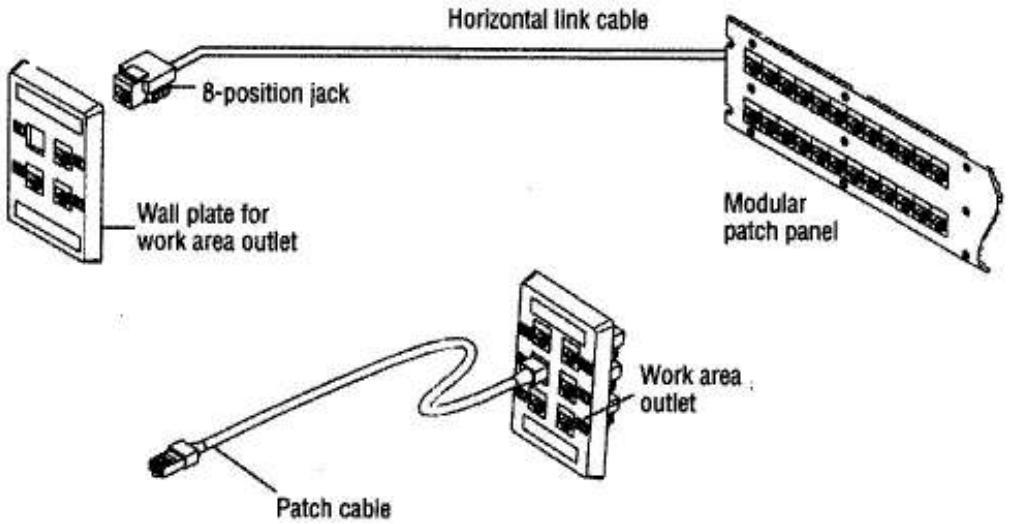
منظور فضایی است که به ازای آن حداقل باید یک پریز شبکه[2] وجود داشته باشد. مثلا در ایران به ازای هر ۸ متر مربع در ساختمان باید یک پریز لحاظ نمایید ولی در کشورهای وسیع‌تر مانند آمریکا هر ۱۰ متر و در کشورهای با فضای فشرده‌تر مانند ژاپن هر ۶ متر یک Work Area به حساب می‌آید.

در این فضا با کابلی که شما یک نمونه آن را در آزمایش امروز آماده خواهید کرد، کامپیوتر را به پریز وصل می‌کنیم. به این کابل Patch Cable گفته می‌شود.

۲. Horizontal Cabling

کابل‌هایی که از جعبه‌ی استقرار سوییچ یا هاب (که به صورت کلی اینجا به نام Telecommunication Closet نامیده می‌شود) به پریز شبکه وصل می‌شود. توجه کنید که کابل معمولا به صورت مستقیم به سوییچ وصل نمی‌شود بلکه صفحه‌ایی با نام Patch Panel جهت جلوگیری از هرز شدن پورت سوییچ و تسهیل جابجایی و تغییرات آتی، بین این دو واقع می‌شود. درضمن خود سوییچ نیز در محفظه‌ایی مناسب به نام Rack گذارده می‌شود که هم منبع تغذیه و هم خنک کننده و ... در آن وجود دارد و درب نیز دارد که سوییچ را از دسترسی فیزیکی افراد غیرمجاز محافظت می‌کند. در شکل زیر کابل Horizontal Link Cable نباید بیش از ۹۰ متر باشد و کابل Patch Cable نیز نباید بیش از ۵ متر باشد. همچنین نوع کابل نیز Straight است که در ادامه توضیح داده خواهد شد.

[1] Area
[2] Telecommunication Outlet



شکل ۲۱۱- استفاده از Patch Panel وPatch Cable برای افزایش انعطاف فوق‌العاده در کابل‌کشی

۳. Telecommunication Closet یا Wiring Closet

مکانی که کابل‌های یک طبقه به آن ختم می‌شود (یعنی هاب‌ها و سوییچ‌ها در آن قرار می‌گیرند.)

۴. Equipment Room

در حالات پیچیده‌تر برای هر طبقه، اتاقی تخصیص داده می‌شود که علاوه بر سوییچ و هاب، کامپیوترهای کارگزار[1] نیز در آن قرار دارند و تجهیزات خاص خنک کننده، ضد حریق، کنترل تردد حفاظت شده نیز ممکن است در آن لحاظ شده باشد.

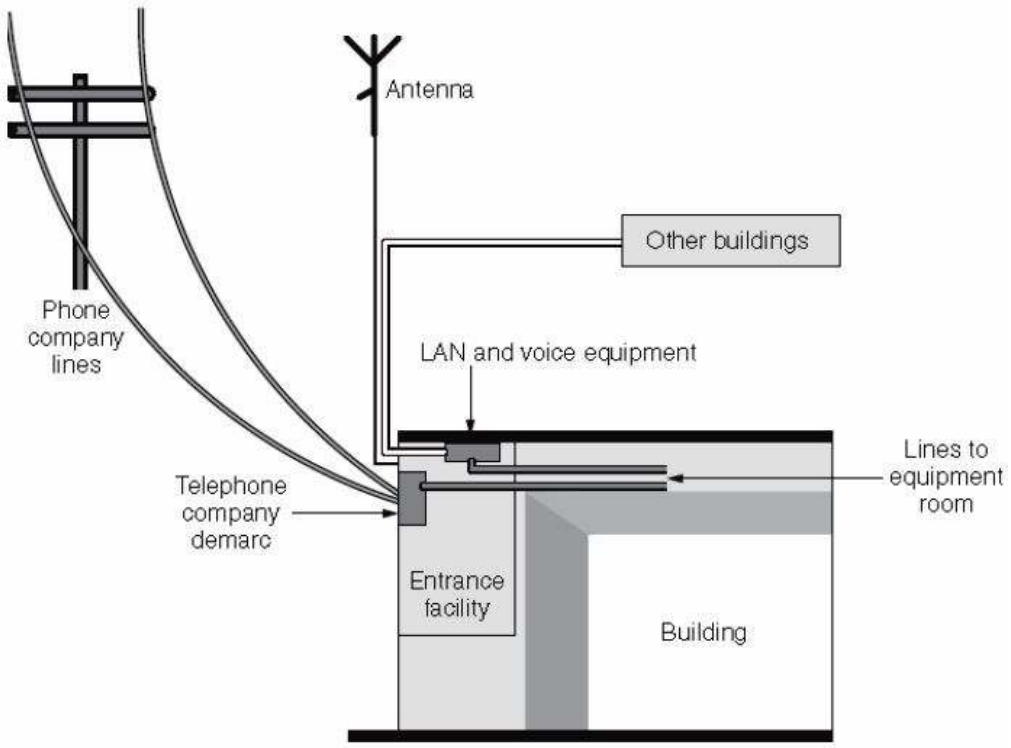
۵. Building Backbone Cabling

هم‌بندی ستاره‌ایی[2] برای ارتباط بین Telecommunication Closetهای طبقات، Equipment Room و Building entrance facilities که در مورد ۶ تشریح می‌شود. این اتاق یا مجموعه اتاق‌ها در اصل مرکز IT سازمان را تشکیل می‌دهند و در صورت بزرگ و وسیع بودن، با نام Data Center هم نام برده می‌شود.

۶. Building entrance facilities

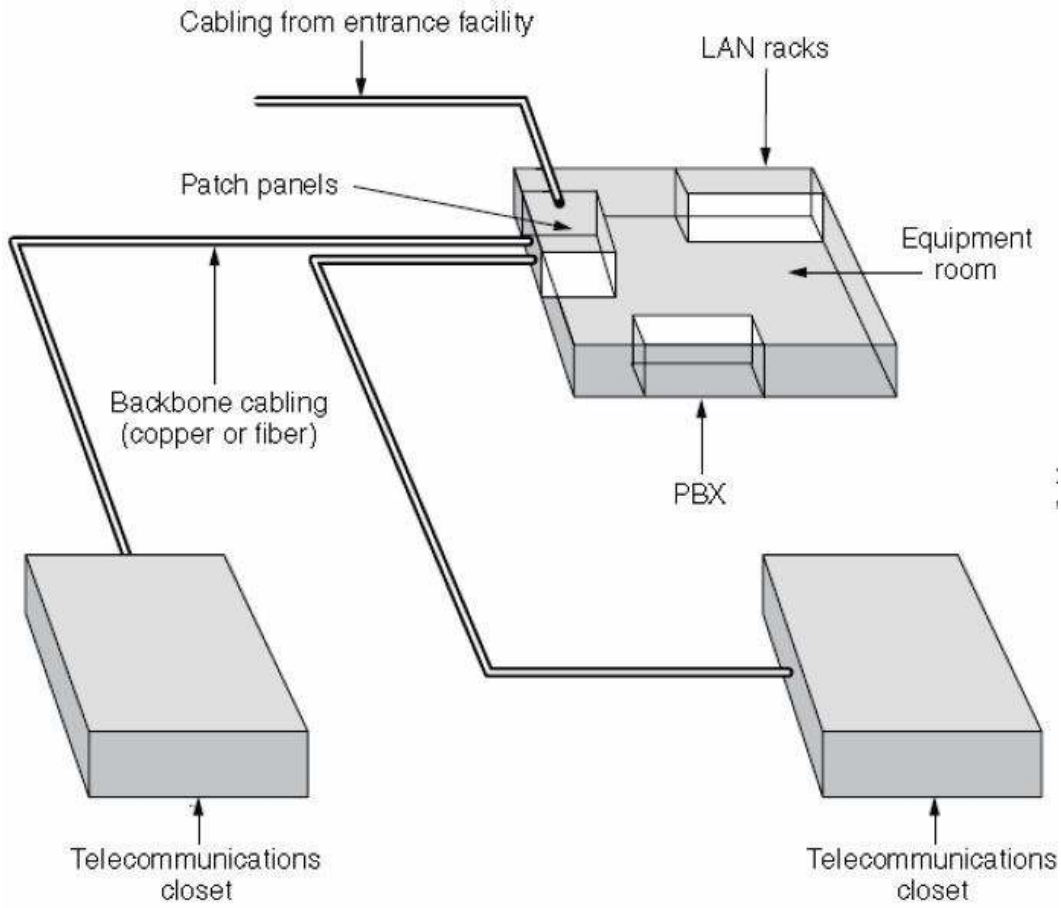
کابل‌ها و تجهیزات مورد استفاده برای اتصال شبکه داخلی ساختمان با بیرون به هر منظور، از قبیل دسترسی به اینترنت (شکل زیر). در برخی مراجع از این ناحیه به Demarc هم یاد شده است، یعنی جایی که کابل‌های سرویس‌دهنده خارجی به کابل‌های مشتری اتصال می‌یابند.

[1] Servers
[2] Star Topology



شکل ۳۱۱- نما و موقعیت Entrance Facility

هر یک از موارد فوق به تشریح مفصل نیاز دارد و تجهیزات توصیه شده و قواعد خاص خود را دارد که به علت کوتاهی مجال، به آن پرداخته نخواهد شد و تنها به ذکر یک شکل که بخشی از ارتباطات را به صورت واضح‌تر نشان می‌دهد اکتفا می‌شود.

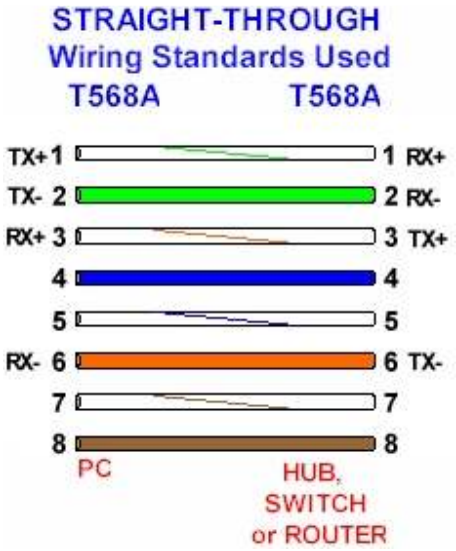


شکل ۱۱ 4-نمای ارتباط محدوده‌های مختلف شبکه

۱۱-۳-۱-۱- استانداردهای رنگ کابل شبکه

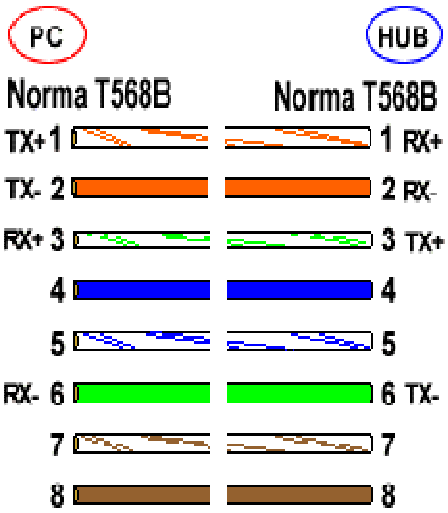
دو نوع استاندارد برای ترتیب رنگ های کابل شبکه وجود دارد:

۱. استاندارد T568 A – در این استاندارد، ترتیب رنگ ها به صورت زیر است:



Pin	رنگ
۱	سفید سبز
۲	سبز
۳	سفید نارنجی
٤	آبی
٥	سفید آبی
٦	نارنجی
۷	سفید قهوه‌ای
۸	قهوه ای

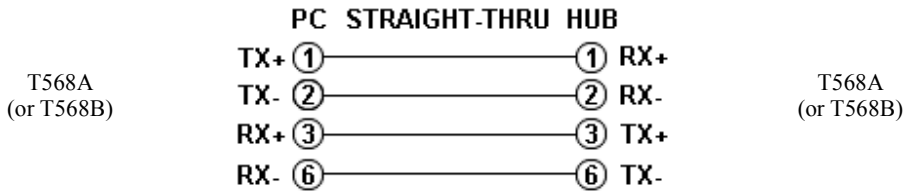
۲. استاندارد T568B – در این استاندارد، ترتیب رنگ ها به صورت زیر است(جانب راست):



Pin	رنگ
۱	سفید نارنجی
۲	نارنجی
۳	سفید سبز
٤	آبی
٥	سفید آبی
٦	سبز
۷	سفید قهوه‌ای
۸	قهوه ای

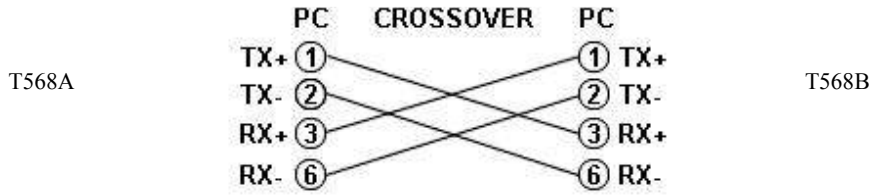
۱۱-۳-۲- اتصال به صورت Straight Through

در مواردی که بخواهیم یک کامپیوتر را به Hub، Router و یا Switch متصل کنیم، از اتصال مستقیم یا straight استفاده می کنیم. در این نوع اتصال، همه pin ها به صورت یک به یک به هم متصل می شوند و می توان از هر یک از استاندارد های T568 A و T568 B در هر دو طرف کابل، استفاده کرد.



۱۱-۳-۲-۱- اتصال به صورت Cross Over

در مواردی که بخواهیم یک کامپیوتر را به یک کامپیوتر دیگر متصل کنیم، از اتصال ضربدری یا cross استفاده می کنیم. در اتصال cross، زوج ارسال (send) از یک طرف کابل، به زوج دریافت (receive) سمت دیگر متصل می شود.



همچنان که در شکل ادامه نیز دیده می‌شود، در این حالت pin های ۱ و ۲ (send) از یک طرف کابل به pin های ۳ و ۶ (receive) طرف دیگر (و باالعکس) متصل می‌شوند.

T568A

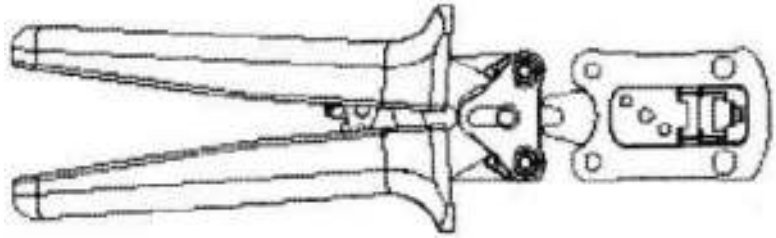
Pin	رنگ
۱	سفید سبز
۲	سبز
۳	سفید نارنجی
٤	آبی
٥	سفید آبی
٦	نارنجی
۷	سفید قهوه ای
۸	قهوه ای

T568B

Pin	رنگ
۱	سفید نارنجی
۲	نارنجی
۳	سفید سبز
٤	آبی
٥	سفید آبی
٦	سبز
۷	سفید قهوه‌ای
۸	قهوه ای

۱۱-۳-۳- آموزش ایجاد کابل

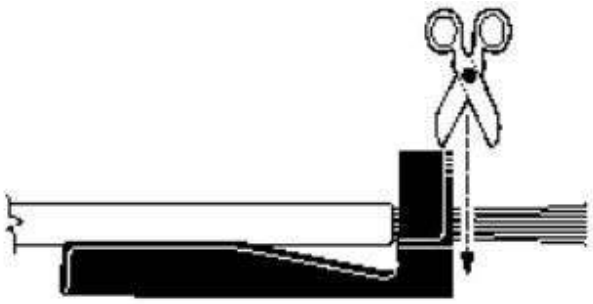
در ادامه سعی خواهد شد تا به صورت تصویری، فرایند آماده سازی کابل و اتصال آن به Connector شرح داده شود. دستگاه‌های مختلفی برای این کار می‌توان استفاده کرد که رایج‌ترین آن‌ها انبر شبکه است که نمای آن در زیر آمده است:



شکل ۵۱۱- نمای انبر شبکه یا Panduit RJ-45 Crimp Tool

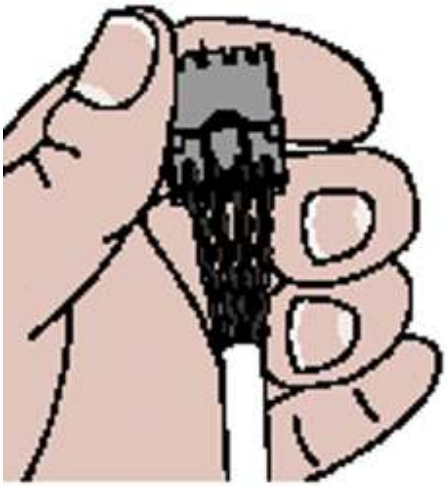
ابتدا پیچ زوج‌سیم‌ها را باز کنید و از چیده شدن آن‌ها به ترتیب صحیح اطمینان حاصل کنید، سپس آنقدر آن‌ها را محکم بکشیدتا صاف و یکنواخت در کنار هم قرار گیرند. این امر به خصوص برای کابل‌هایی که ساخت کارخانه‌های معتبر نیستند باید بیشتر انجام گیرد.

حال باید روکش بیرونی کابل که تمام زوج سیم‌ها را احاصه کرده است به انداز حدود سانتی‌متر بردارید، توجه کنید که نباید هیچ‌یک از رشته سیم‌ها زخمی شود. سپس باید سرزوج سیم‌ها را در یک امتداد قطع نمایید تا برای قرار گرفتن در Connector آماده شوند.

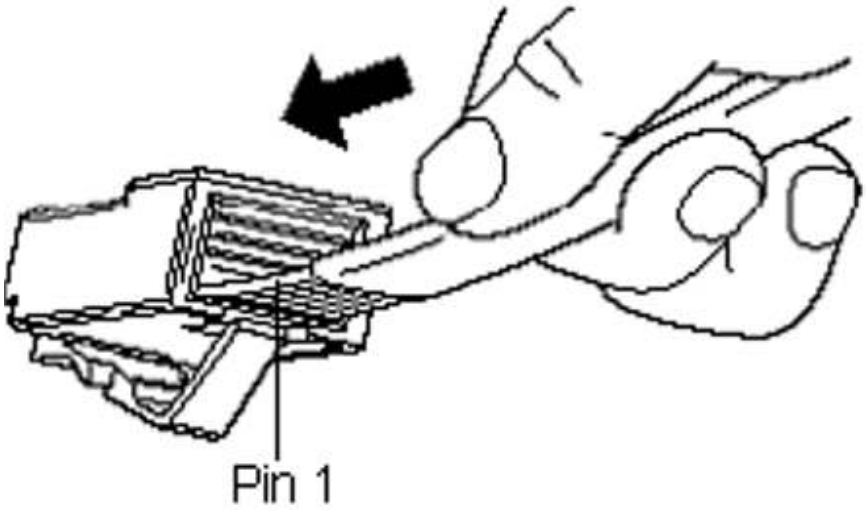


شکل ۶۱۱-هموار نمودن سرسیم‌ها برای قرار دادن در Connector

کابل را باید به درستی جای دهید، برای این کار شماره ترتیب Pinها را باید از چپ به راست در نظرگرفت، طوری که وقتی پشت Connector به سمت شماست، پین سمت چپ شماره یک داشته باشد (همانند دو عکس ادامه).



شکل ۷۱۱- قرار دادن سر سیم‌ها به طور کامل در Connector



شکل ۸۱۱- تعیین شماره ترتیب سیم‌ها برای حالات 568A و 568B

پس از ایجاد کابل باید با دستگاه Tester آن را چک نمود که این مورد نیز در آزمایشگاه به صورت عملی انجام خواهد شد و جزییات مفصلی دارد که از حوصله این متن خارج است. دستگاه‌های Tester اسم‌ها و شکل‌ها و قابلیت‌های متنوع دارند که Fluke620 یا LinkRunner را می‌توان از آن جمله نام برد.

۱۱-٤- مراجع

1. **Cabling: The Complete Guide to Network Wiring**, D. Barnett, D. Groth, J. McBee, Sybex Pub, 2004.
2. **Structured Cabling Supplement**, Cisco Network Academy, 2005.
3. **Building Ethernet Systems,** Wolfgang Schreiner, University of Applied Sciences in Hagenberg, Available at: http://cblinux.fh-hagenberg.at/~schreine/ss2002/net2/slides/ether7/slides-main.pdf

۱۱-۵- دستورکار

توجه:

- حتما پس از پایان آزمایش، خورده کابل‌ها و آشغال‌های ایجاد شده را جمع کنید و در زباله‌دان بریزد. در صورتی که پس از پایان آزمایش، در زیر یا روی هر میزی، تمیز نباشد و زواید ناشی از آزمایش مشاهده شود، نمره صفر لحاظ می‌گردد.
- نظر به اینکه تجهیزات به تعداد دانشجویان است و ممکن است تجهیزات اضافی وجود نداشته باشد، در انجام صحیح آزمایش کوشا باشید.
- به هر دانشجو باید یک کابل UTP از نوع Cat5e و دو Connector از نوع RJ45 داده می‌شود.

۱. با توجه به آموخته‌های پیش‌آگاهی، یک کابل Cross Over برای اتصال دو PC بسازید.

آزمایش یازدهم

شنود و تحلیل بسته‌ها در شبکه

۱۲-۱- مقدمه

شناخت و درک نسبت به عملکرد واقعی شبکه و قالب حقیقی داده بر خط، مکمل شناخت نظری از پروتکل‌ها و مدل لایه‌ای نظری آموزش داده شده در کلاس درس است. دانشجو با رویت و بررسی جزییات سرآیند پروتکل‌های واقعی فعال در شبکه‌ی مورد استفاده، علاوه بر فراگیری سریعتر مفاهیم، آن‌ها را برای زمان بیشتری در خاطر خواهد داشت و در حل مسایل مرتبط نیز قدرت تحلیل بالاتری پیدا می‌کند. یک ضرب‌المثل چینی مؤید این مطلب است که می‌گوید: "آنچه را به من بگویی از یاد می برم و آنچه را به من نشان دهی به خاطر می‌سپارم، اما اگر من را در فرایندی مشارکت دهی، آن را درک می‌کنم[1]". در این آزمایش، رویت پروتکل‌ها و سرآیند آن‌ها و درک نحوه و ترتیب تبادل پیام بین ماشین‌ها در شبکه واقعی، از طریق یک نرم‌افزار رایج کد باز مناسب شنود و تحلیل بسته[2] به نام Wireshark، انجام خواهد شد.

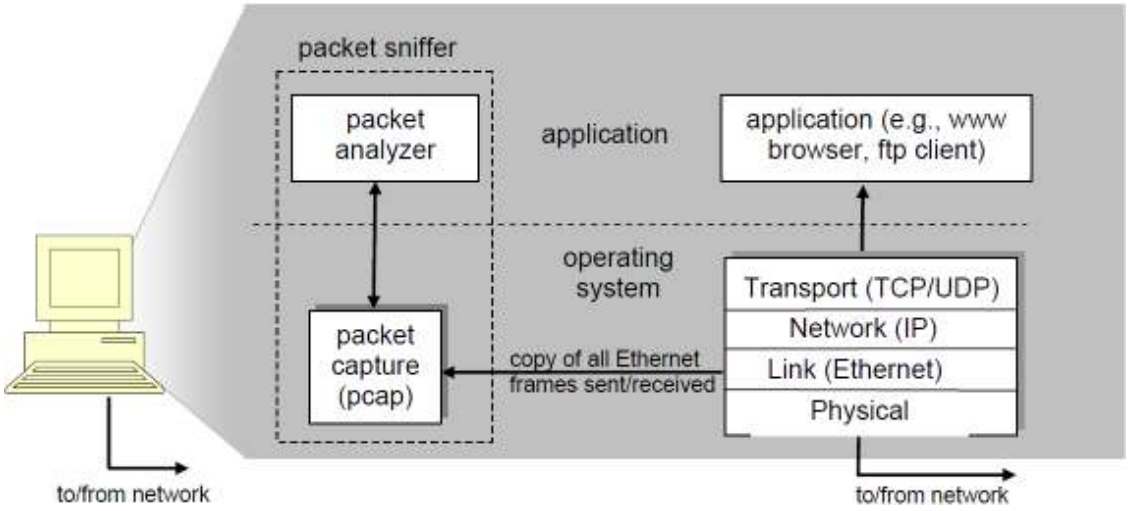
[1] "Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb
[2] Packet Sniffer and Analyzer

۱۲-۲- هدف

تحلیل و شناسایی پروتکل‌ها در عمل، با نرم‌افزار شنود و تحلیل بسته‌ی Wireshark

۱۲-۳- پیش‌آگاهی

ابزارهای پایه برای مشاهده‌ی پیام‌های تبادلی بین موجودیت‌های تبادل کننده‌ی آن‌ها برمبنای یک پروتکل خاص، نرم‌افزارهای شنود بسته (Packet Sniffer) نام دارند. چنین نرم‌افزاری، بسته‌های ارسالی یا دریافتی کامپیوتر را شنود می‌کند و قابلیت ذخیره‌سازی و نمایش فیلدهای مختلف پروتکل‌های درون آن‌ها را دارد. نرم‌افزارهای شنود، ماهیت غیرفعال دارند، یعنی می‌توانند بسته‌های تبادلی توسط برنامه‌ها را دریافت و شنود کنند اما خود اقدام به ارسال بسته نمی‌کنند. آدرس مقصد بسته‌های دریافتی نیز به هیچ وجه نرم‌افزار شنود نیست. پس در واقع می‌توان گفت نرم‌افزار شنود، یک کپی از بسته‌ی تبادلی را دریافت می‌کند. شکل زیر ساختار یک نرم‌افزار شنود بسته را نشان می‌دهد.



شکل ۱۲-۱ ساختار نرم‌افزار شنود بسته (Packet Sniffer)

در سمت راست شکل فوق، برنامه‌ها و پروتکل‌های لایه‌ی کاربرد قرار دارند. مانند نرم‌افزارهای مرورگر از قبیل Internet Explorer یا پروتکل‌های رایج اینترنت از قبیل HTTP[1]، FTP که بر رایانه شما در حال اجرا هستند. نرم‌افزار شنود، به برنامه‌های جاری در رایانه شما اضافه می‌شود و دو بخش دارد. بخش اول مجموعه توابع کتابخانه‌ای گرفتن بسته[2] است که یک کپی از تمام فریم‌های لایه‌ی پیوند داده را که از کارت

[1] Hyper Text Transfer Protocol، پروتکلی که مرورگری مانند Internet Explorer، با آن زبان از Web Server که میزبانی وب‌سایت را انجام می‌دهد، درخواست صفحه‌ی وب می‌کند.

[2] Packet Capture Library

شبکه‌ی جاری ارسال می‌شود یا توسط آن دریافت می‌شود، ضبط می‌کند(بخش سمت چپ پایین تصویر). از مطالب درس شبکه ۱ و آشنایی با مدل‌های لایه‌ای OSI به خاطر داریم که در بخش داده‌ی فریم‌های لایه‌ی پیوند داده، علاوه بر داده‌ی اصلی کاربر، سرآیند لایه‌های بالاتر از قبیل IP، TCP، UDP، FTP، HTTP و ... محصور[1] شده‌اند. البته می‌دانیم در لایه‌ی پیوند داده نیز تنوعی از پروتکل‌ها موجودند اما با توجه به اینکه لایه‌ی پیوند داده در اغلب شبکه‌های جهان، Ethernet است و ما نیز در آزمایشگاه با چنین پروتکلی در لایه‌ی ۲ از مدل OSI در ارتباط هستیم، در شکل فوق نیز لایه‌ی ۲ را Ethernet فرض کرده‌ایم.

جزء دوم یک نرم‌افزار شنود بسته، تحلیل‌گر بسته[2] است، که محتوی تمامی فیلدهای پروتکل‌های درون پیام را نشان می‌دهد. چنین امری نیاز به شناخت ساختار تمام پیام‌های تبادلی همه‌ی پروتکل‌ها دارد. به عنوان مثال تصور کنید که در یک ارتباط رویت صفحات وب توسط مرورگر در رایانه‌مان، مایل هستیم جزییات سرآیند پروتکل HTTP که متولی انتقال صفحات وب بین کارگزار وب و نرم‌افزار مرورگر است را رویت نماییم. نرم‌افزار شنود قالب فریم‌های Ethernet را می‌شناسد، بنابراین پس از حذف سرآیند و دنباله‌ی لایه‌ی ۲، دیتاگرام IP را از آن استخراج می‌نماید. با توجه به اینکه نرم‌افزار شنود، از سرآیند IP نیز شناخت کامل دارد، می‌تواند پس از حذف سرآیند لایه‌ی ۳، سگمنت TCP را درک کرده و سرآیند آن را با تمام جزییات نمایش دهد و با توجه به اینکه قالب بسته‌ها در دنیای واقعی، مبتنی بر پشته‌ی پروتکلی TCP/IP است، پس از عبور از سرآیند TCP به سرآیند لایه‌ی کاربرد خواهیم رسید که همان HTTP خواهد بود. اکنون به صورت دقیق می‌توان مثلا فهمید که پنج بایت اول درخواست در قالب HTTP چه بوده؟ آیا صفحه‌ای از کارگزار وب طلب شده است (دستور GET) یا سندی به کارگزار وب Upload شده است (POST) یا درخواست رویت بخش اول یک صفحه‌ی وب از کارگزار وب صورت گرفته است (HEAD)؟ این‌ها هریک دستوراتی از پروتکل HTTP هستند.

نرم‌افزار مورد استفاده برای شنود بسته در این آزمایش، Wireshark است که در آدرس اینترنتی http://www.wireshark.org موجود است. این نرم‌افزار که وظیفه‌ی شنود و تحلیل بسته را همزمان انجام می‌دهد یک نرم‌افزار رایگان است که در سطوح مختلف پشته‌ی پروتکلی TCP/IP قابل استفاده است و بر سیستم‌عامل‌های Windows، Linux/Unix و Mac قابل اجراست. مستندات جامعی مشتمل بر راهنمای کاربر، مربوط به نرم‌افزار Wireshark تدوین شده و در آدرس

[1] Encapsulated
[2] Packet Analyzer

http://www.wireshark.org/docs/wsug_html_chunked در دسترس است. همچنین فهرست سوالات رایج متداول در زمینه‌ی نرم‌افزار (FAQ) در آدرس http://www.wireshark.org/faq.html موجود است. عملکرد غنی و قابلیت‌های بالای نرم‌افزار در تحلیل صدها پروتکل و رابط کاربرپسند آن، امکان شروع و یادگیری سریع با آن را فراهم کرده است. از این نرم‌افزار می‌توان در شبکه‌های Ethernet، Token-Ring، FDDI، PPP، شبکه‌های بی‌سیم مبتنی بر استاندارد IEEE 802.11 و حتی ارتباطات مبتنی بر پروتکل ATM استفاده کرد.

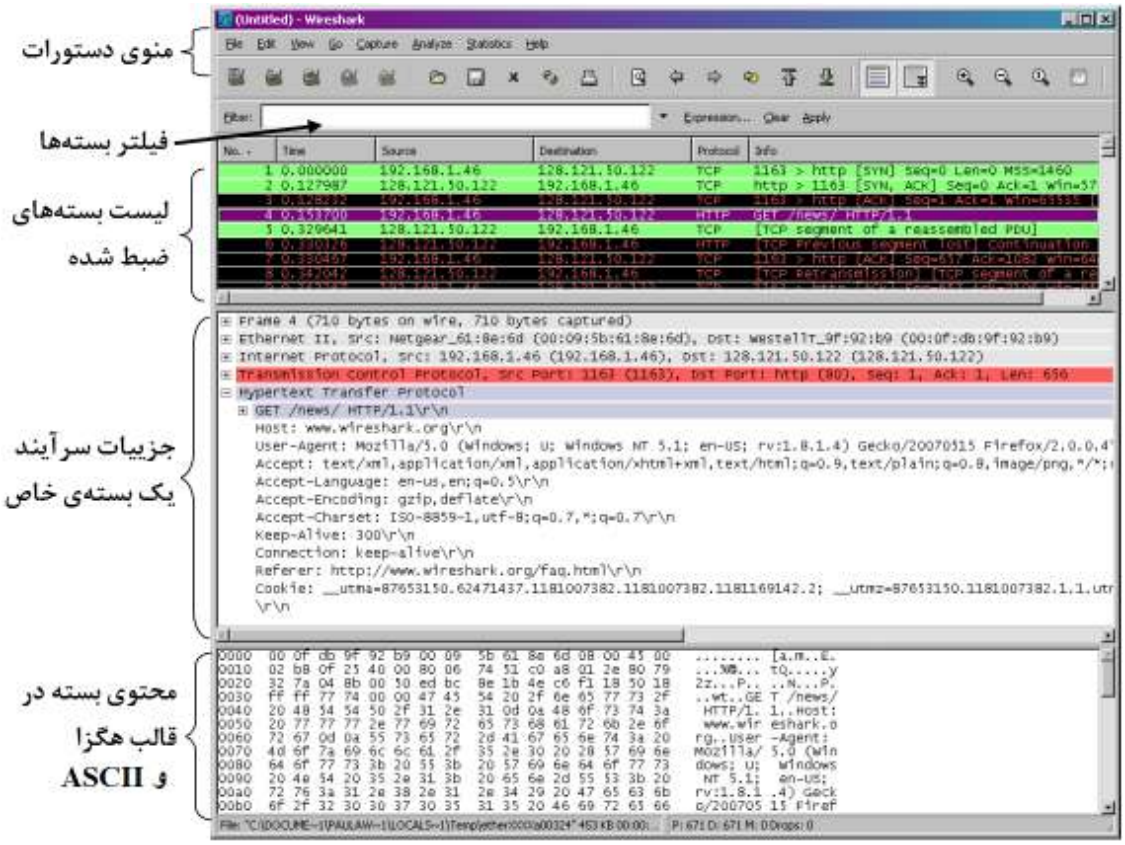
لایه‌ی زیرین نرم‌افزار Wireshark که امکان برداشتن بسته‌ها از خط را فراهم می‌کند، lipcap یا WinPCap است که توابع کتابخانه‌ای گرفتن بسته را در خود دارد و معمولا در حین نصب نرم‌افزار Wireshark، آن نیز نصب خواهد شد. پیشنهاد می‌شود اضافه برگرفتن نرم‌افزار Wireshark از آدرس http://www.wireshark.org/download.html، لیست سوالات رایج و راهنمای آن را نیز دانلود کنید. به خصوص اگر در نصب نرم‌افزار به مشکلی برخوردید یا ابهامی داشتید که خارج از محدوده‌ی این آزمایش بود.

۱۲-۳-۱- اجرای Wireshark

رابط گرافیکی Wireshark مانند شکل ۱۲-۲ است. البته پیش از شروع به کار، داده‌ای در پنجره‌ی مربوطه نمایش داده نخواهد شد. نرم‌افزار Wireshark دارای پنج قسمت اصلی است:

- **منوی دستورات** که دارای کلیدها و منوهای رایج مورد استفاده است. دو جزء اصلی در آن، منوی File و Capture هستند. گزینه‌های File در عین اهمیت، بدیهی هستند اما از گزینه‌ی Capture، می‌توانید برای انتخاب کارت شبکه‌ی فعال مورد نظر، Interfaces را انتخاب کنید و شروع شنود نیز در همین گزینه است.
- **لیست بسته‌های ضبط شده** که شرحی یک سطری از مهمترین اطلاعات هر بسته‌ی ضبط شده مشتمل بر شماره‌ی آن در نرم‌افزار Wireshark، زمان ضبط، آدرس مبدأ و مقصد، نوع پروتکل و ویژگی‌های خاص پروتکل در بسته، است. می‌توان بسته‌ها را با کلیک بر ستون مناسب، بر اساس هرکدام از این خصیصه‌ها مرتب کرد. فیلد نوع پروتکل، نام پروتکل بالاترین لایه‌ی تولید کننده‌ی بسته را نشان می‌دهد.
- **جزییات سرآیند یک بسته‌ی خاص** جزییات بسته‌ی انتخابی (Highlight شده) در لیست پروتکل‌ها را نشان می‌دهد. این جزییات، محتوی اطلاعاتی در رابطه با فریم Ethernet، و دیتاگرام

IP محصور شده در آن است. سطح تجرید و میزان جزییات هرکدام از لایه‌های IP یا Ethernet را می‌توان با کلیک بر علامت + در سمت چپ آن‌ها باز یا بسته کرد. اگر چنین بسته‌هایی را پروتکل لایه‌ی بالاتر TCP یا UDP مسبب شده باشند، می‌توان جزییات هر یک را نیز رویت کرد. برای پروتکل‌های لایه‌ی بالاتر نیز به همین ترتیب می‌توان عمل کرد.



شکل ۱۲-۲ رابط گرافیکی کاربر نرم‌افزار Wireshark

- **محتوی بسته در قالب هگزا و ASCII** نمایشگر کل محتوی فریم ضبط شده است که در قالب ASCII و Hexadecimal نشان داده می‌شوند.
- سمت بالای عکس فوق مشتمل بر فیلتر پالایش نمایش بسته‌ها با عنوان **فیلتر بسته‌ها** است که می‌توان در آن نام یک پروتکل یا کلمه‌ای درج کرد، تا تنها اطلاعات مرتبط نمایش داده شود. به عنوان مثال در آزمایش‌های آتی، ما از این فیلد برای نمایش تنها بسته‌های مرتبط با پروتکل HTTP استفاده خواهیم کرد.

۱۲-٤- دستورکار

توجه ۱: پیش از هرچیز کامپیوتر خود را به اینترنت متصل نمایید و در صورتی که دسترسی ندارید، از مربی راهنمایی بگیرید.

۱. مراحل زیر را به ترتیب انجام دهید:

a. Internet Explorer را باز کنید و به www.google.com بروید.

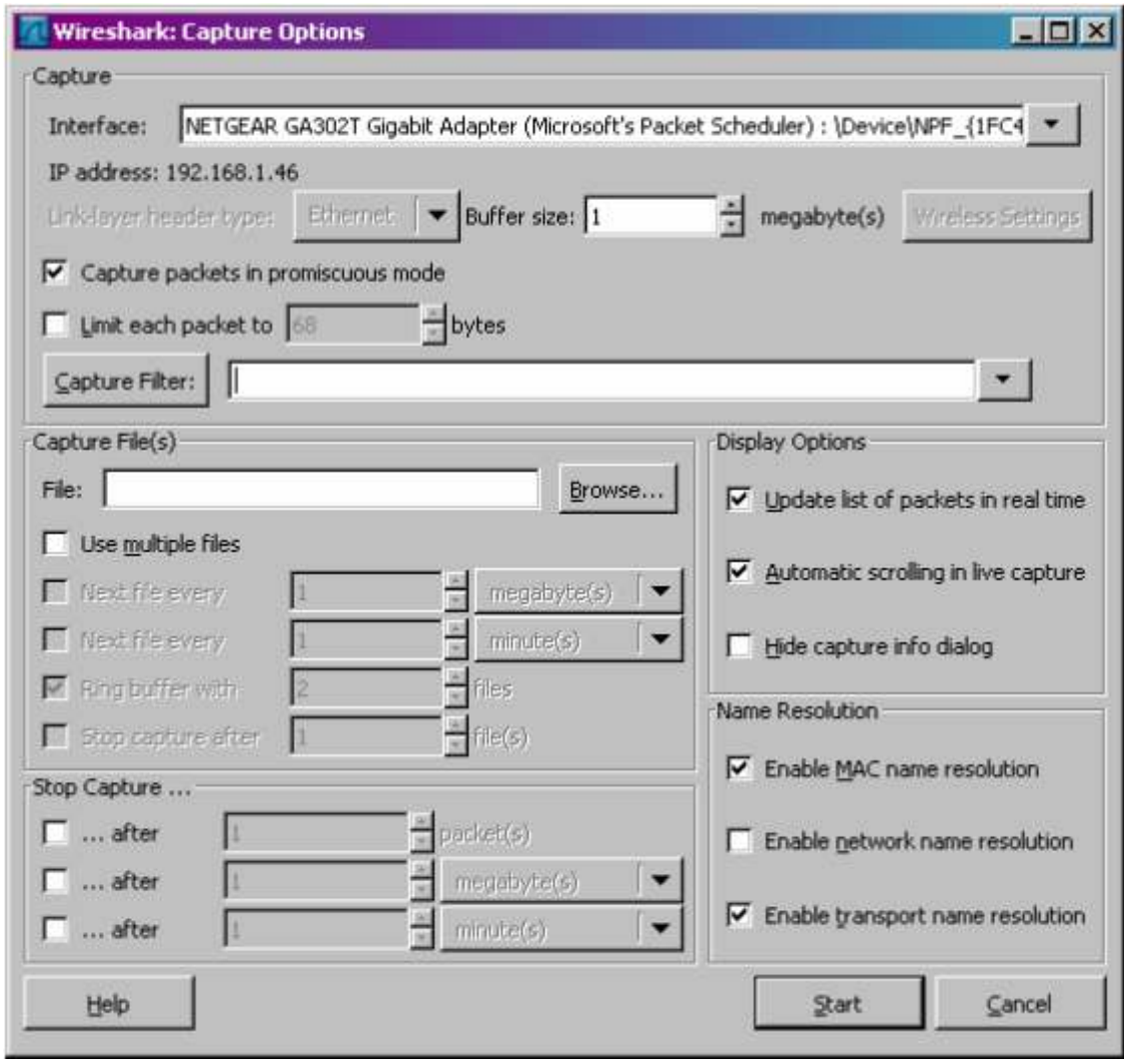
b. نرم‌افزار Wireshark را بازکنید. شکلی مشابه به شکل ۱۲-۲ اما خالی از داده رویت خواهید کرد، چرا که شنود در نرم‌افزار، هنوز آغاز نشده است. برای شروع ضبط بسته‌ها، منوی Capture و سپس گزینه‌ی Options را انتخاب کنید تا پنجره‌ای مشابه به شکل ۱۲-۳ ببینید.

c. پیش از هر چیز مطمئن شوید که گزینه‌ی Hide capture info dialog از همین پنجره در قسمت Display Options، تیک نخورده باشد. کارت‌های شبکه‌های کامپیوتر شما تحت نام Interface در بخش بالای پنجره‌ی جاری، با گزینه‌ی پایین‌کشیدنی[1]، قابل انتخاب هستند. مطمئن شوید که کارت شبکه‌ی فیزیکی جاری و نه کارت شبکه‌ی مجازی یا غیرفعال، انتخاب شده باشد. حال کلید Start را از پایین پنجره کلیک کنید.

d. پس از شروع به شنود بسته‌ها، پنجره‌ی شنود را رویت خواهید کرد که تعداد بسته‌های ضبط شده را نمایش می‌دهد (شکل ۱۲-۴). در حالی که پنجره در حالت اجراست، آدرس زیر را بزنید: http://itvirtuallab.com/documents/test.htm و صبر کنید تا پنجره را در مرورگر خود ببنید. برای اینکه صفحه‌ی مورد نظر در مرورگر شما نمایش داده شود، مرورگر شما با کامپیوتری که HTTP Server است و میزبانی اینترنتی وب‌سایت ITVirtualLab را انجام می‌دهد تماس می‌گیرد و با آن به تبادل پیام‌هایی می‌پردازد که صفحه‌ی وب مذکور را به کامپیوترتان منتقل کند و محتوی آن را نمایش دهد. پس از نمایش صفحه‌ی test.htm از وب‌سایت مذکور، عملیات ضبط را با فشردن کلید Stop متوقف کنید تا صفحه‌ی اصلی Wireshark که مشابه به شکل ۱۲-۲ است را ببینید. گرچه شما فقط یک صفحه‌ی وب درخواست کردید، اما تعداد زیادی پروتکل متعاقبا اجرا شده است. آنچه برای ما لازم است، دسترسی به سرآیند HTTP مربوط به درخواستی است که دادیم. در بخش فیلتر، با حروف

[1] Pull down menu

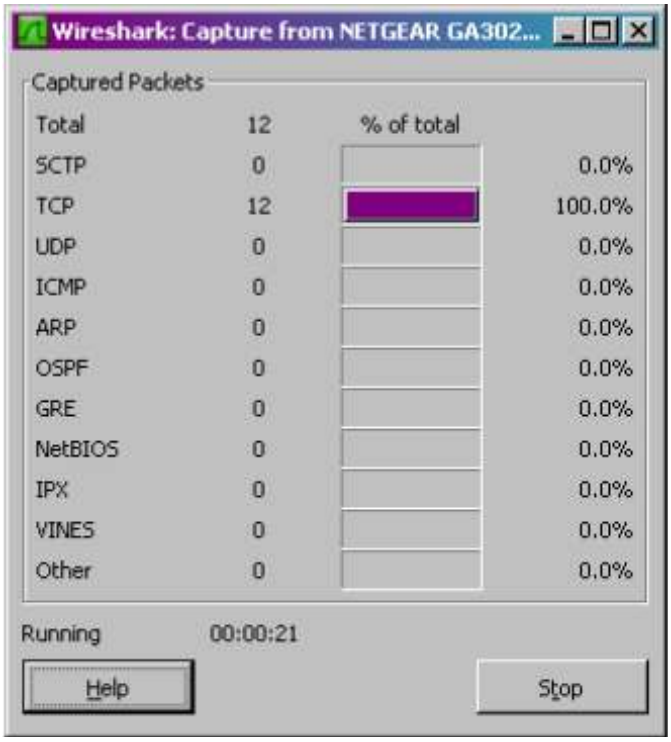
کوچک، http را تایپ کنید و گزینه‌ی Apply را در سمت راست آن بزنید تا فقط بسته‌های http رویت شوند. اولین پیام http که از نوع http GET است را انتخاب کنید. به این ترتیب تمام سرآیندهای محصورکننده‌ی آن را نیز رویت خواهید کرد (Ethernet، IP و TCP).



شکل ۱۲-۳ پنجره‌ی Option برای انتخاب گزینه‌های ضبط بسته‌ها در Wireshark

e. با کمک علامت + و بستن سایر سرآیندها و باز کردن سرآیند Http و دقت در قالب درخواست http GET به زبان ساده بیان کنید که یک مرورگر در زمان درخواست یک صفحه‌ی وب از Web Server (همان http Server است)، چه اطلاعاتی در اختیار آن قرار می‌دهد تا صفحه‌ی وب را در مناسب‌ترین قالب دریافت کند؟

۲. پس از برداشتن فیلتر http، اسم ده پروتکلی را که در ستون پروتکل در لیست بسته‌های ضبط شده مشاهده می‌کنید، بنویسید.



شکل ۱۲-٤ پنجره‌ی خلاصه آمار بسته‌های ضبط شده در هنگام اجرای شنود

۳. از زمان ارسال HTTP GET تا دریافت پاسخ HTTP OK چه مدتی طول می‌کشد؟ (به صورت پیش‌فرض، مقدار موجود در ستون Time بر حسب ثانیه است) برای نمایش فیلد زمان برحسب زمان کنونی، از گزینه‌ی view، Time Display Format را انتخاب کنید.

۴. آدرس اینترنتی وب‌سایت http://itvirtuallab.com را از سرآیند درخواست HTTP استخراج کنید و بنویسید. آیا می‌توانیم آن را از طریق پروتکل یا پروتکل‌های دیگری که اکنون بسته‌اش ضبط شده، بیابیم؟ نام آن پروتکل چیست؟ آن را بیابید.

۵. شماره کد معادل با پیام برگشتی HTTP OK، یعنی مقدار فیلد Response Code را بنویسید.

۶. تاریخ آخرین تغییر فایل بازیابی شده توسط مرورگر شما از Server، را به صورت دقیق بنویسید.

۷. چه تعداد بایت به مرورگر شما بازگردانده شده است؟

۸. از سرآیند Ethernet در همان فریم محتوی بسته‌ی HTTP آدرس MAC مبدا و مقصد را بیابید و در برگه گزارش‌کار یادداشت کنید. آدرس MAC مقصد مربوط به چه کامپیوتری است؟ آیا متعلق به کامپیوتر، http://itvirtuallab.com است؟ چرا؟

۹. اگر صفحه‌ای از وب‌سایت http://itvirtuallab.com در خواست کنیم که وجود نداشته باشد، چه کدی معادل با آن در پاسخ برخواهد گشت؟ تست کنید و بنویسید.

۱۰. تست کنید که

الف) در هنگام دانلود یک فایل حجیم (بیش از ۳۰۰ کیلوبایت) توسط مرورگر شما، از وب سایت http://itvirtuallab.com، چند درخواست HTTP GET از مرورگر شما صادر می‌شود. (مثلا یکی از فایل‌های یکی از دروس را دانلود کنید)

ب) چند سگمنت TCP برای انتقال داده‌ی حجیم در آزمایش شما لازم شده است؟

راهنمایی: در سرآیند HTTP OK، سرآیند TCP با عنوانی شامل Reassembled TCP Segment را بررسی کنید.