Design and Implementation of Network Infrastructures

Lecturer: Javad Forghani

Email: jforghani@live.com

طراحی و پیاده‌سازی زیرساخت‌های شبکه

۱. آشنایی با تعاریف و مفاهیم اولیه شبکه‌های کامپیوتری
۲. معرفی مدل‌های لایه‌بندی‌شده‌ی توسعه‌ی شبکه‌های کامپیوتری (TCP/IP, OSI)
۳. آشنایی با دستگاه و تجهیزات شبکه
۴. سیستم‌بندی ساخت‌یافته‌ی شبکه‌های کامپیوتری(حذف)
۵. آشنایی با دستگاه‌های Cisco
۶. آشنایی با پیکربندی اولیه‌ی سوئیچ‌های Cisco*
۷. آشنایی با پیکربندی اولیه‌ی روترهای Cisco*
۸. معرفی پروتکل‌ها
۹. مسیریابی Static
۱۰. مسیریابی Dynamic
۱۱. پیکربندی و عیب‌یابی پروتکل RIP*
۱۲. پیکربندی پروتکل EIGRP*
۱۳. پیکربندی پروتکل OSPF*
۱۴. معرفی شبکه‌های مجازی VLAN
۱۵. پیکربندی VLAN روی سوئیچ‌ها*
۱۶. پیکربندی HDLC*
۱۷. پیکربندی PPP*
۱۸. پیکربندی Frame Reply*
۱۹. پیکربندی DHCP*
۲۰. پیکربندی Talent*
موارد‌ی که علامت دارند، عملی هستند. *

کتب مرجع

۱. مهندسی اینترنت احسان ملکیان
۲. شبکه‌های کامپیوتری اندر اس. تننباوم
۳. CCNA و CCNP مسعود حسینقلی‌پور
۴. شبکه (درس و تست) انتشارات پوران پژوهش

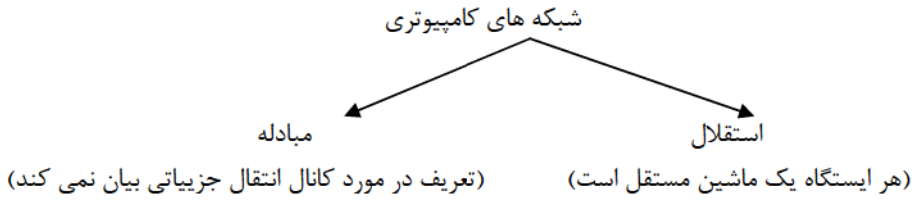
نرم افزار شبیه‌سازی: Cisco Packet Tracer

آشنایی با تعاریف و مفاهیم اولیه شبکه های کامپیوتری

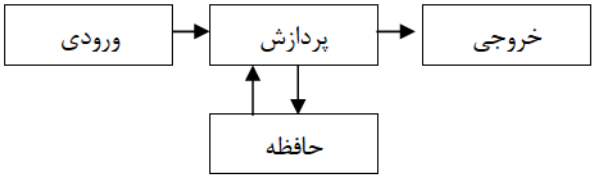
تعریف شبکه های کامپیوتری

شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای مستقل هستند که به‌نحوی با یک‌دیگر، داده و اطلاعات را مبادله می‌نمایند.

شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای **مستقل** جهت **مبادله‌ی** داده و اطلاعات



ماشین فون نویمن



کاربردهای شبکه های کامپیوتری

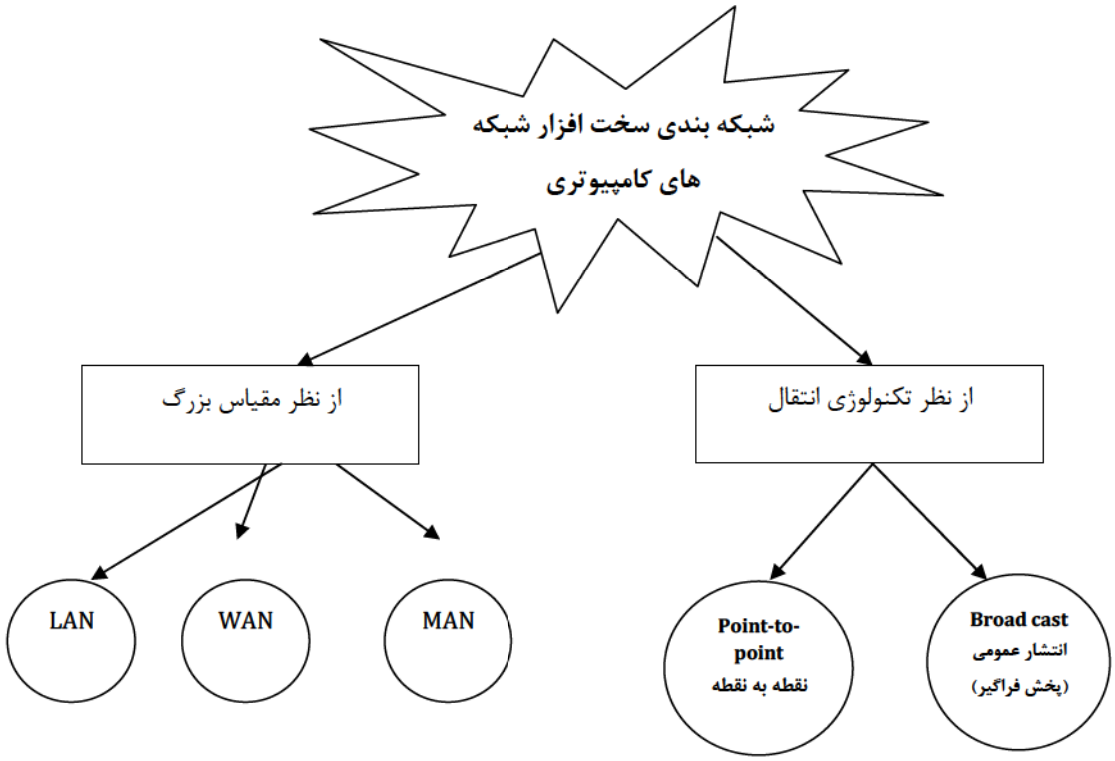
۱. اشتراک منابع : استفاده از یک پرینتر در شبکه
۲. حذف محدودیت‌های جغرافیایی : استفاده از شبکه های youtube و upload کردن یک فایل
۳. کاهش هزینه : نتیجه دو مورد بالا کاهش هزینه را به دنبال دارد.(مثلا به جای اینکه چند پرینتر استفاده کنیم، از یک پرینتر استفاده میکنیم و آن‌را شبکه میکنیم)
۴. بالا رفتن قابلیت اعتماد سیستم‌ها : استفاده از منابع برای چندین بار- دانلود یک موضوع و بعد از حذف شدن آن توانایی دانلود مجدد
۵. افزایش کارایی سیستم : نتیجه اشتراک منابع است

خدمات معمول در شبکه

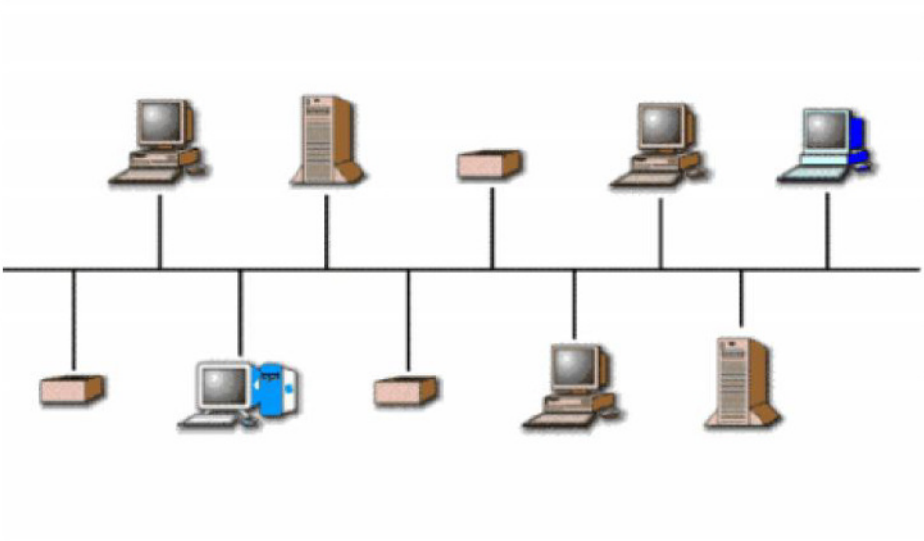
۱. دسترسی به اطلاعات بانک‌های راه دور (اشتراک منابع)
۲. پست الکترونیکی (آپلود و دانلود) پروتکل مربوط به آن Fttp است.
۳. انتقال فایل
۴. ورود به سیستم از راه دور
۵. گروه‌های خبری (RSS)
۶. جستجوی اطلاعات (مثل موتور های جستجوی گوگل)
۷. تجارت الکترونیک

۸. بانکداری الکترونیک
۹. سرگرمی
۱۰. روزنامه های الکترونیکی
۱۱. آموزش از راه دور
۱۲. کنفرانس از راه دور
۱۳. درمان از راه دور
۱۴. تلفن از طریق شبکه
۱۵. رادیوی شبکه‌ای
و . . .

دسته بندی سخت افزار شبکه های کامپیوتری



شبکه های پخش فراگیر



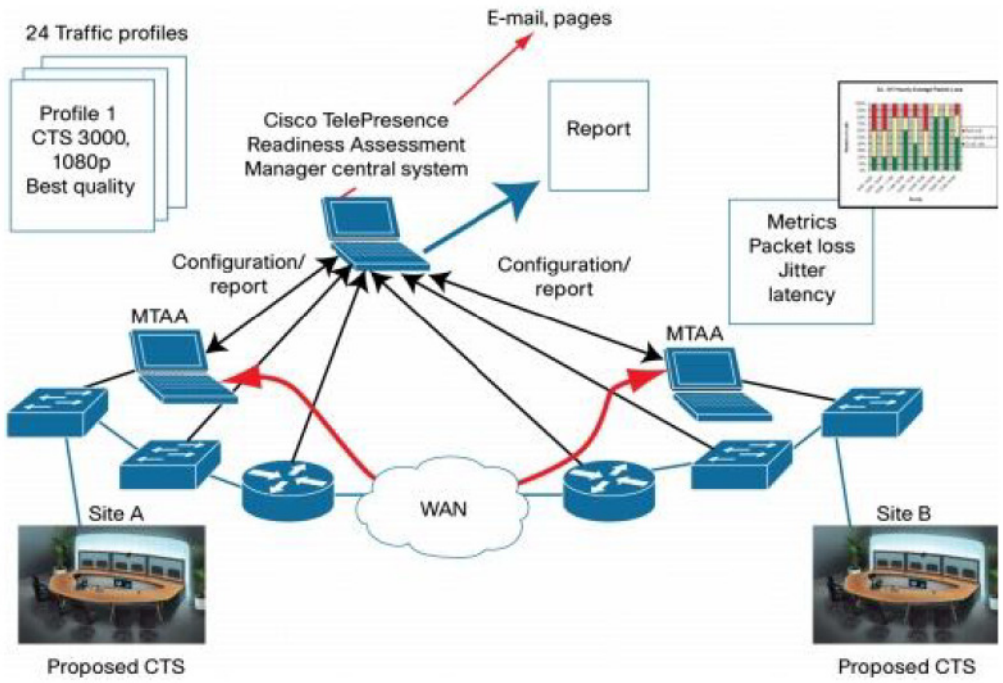
شکل ۱: شبکه پخش فراگیر

معایب:

۱. مدیریت کانال اشتراک پیچیده است
۲. کارایی پایین
۳. امنیت کم

شبکه نقطه به نقطه

دارای یک کانال فیزیکی مستقیم (فقط و فقط یکی) بین هر دو ایستگاه



شبکه های LAN

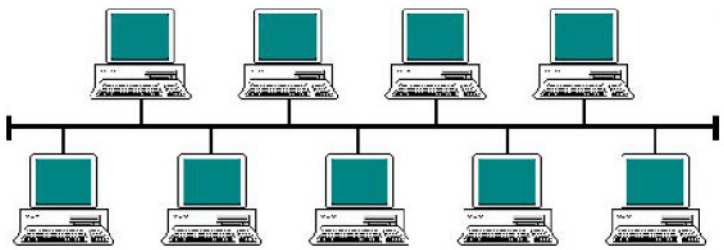
ویژگی ها در فواصل جغرافیایی محدود پیاده می شوند و تعداد ایستگاه های آن کم است و طول کانال (مسیر ارتباطی)کم است.

مزیت های شبکه LAN

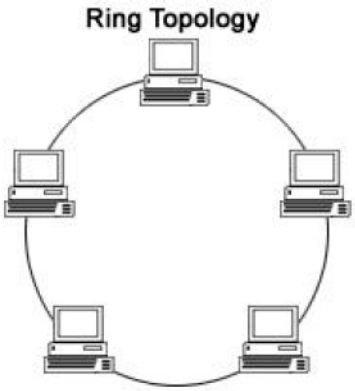
۱. افت سیگنال کم است
۲. نرخ خطای پایین (وقتی افت سیگنال کم باشد، طبیعتاً خطا کمتر است)
۳. نرخ ارسال بالا(؟ بیت پر سکند)
۴. تاخیر انتشار ناچیز
۵. مدیریت آسان
۶. هزینه پایین

انواع شبکه های LAN(Local Area Network)

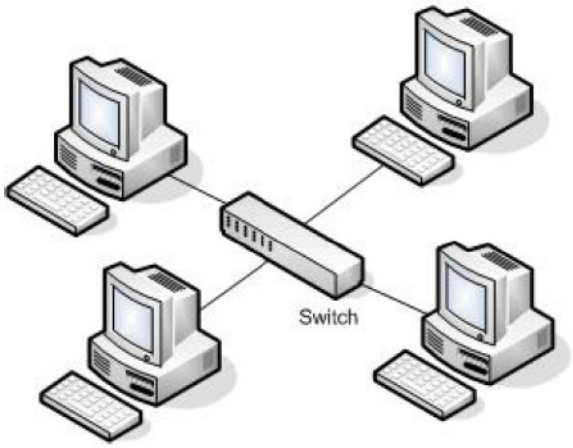
۱. توپولوژی BUS (خطی)



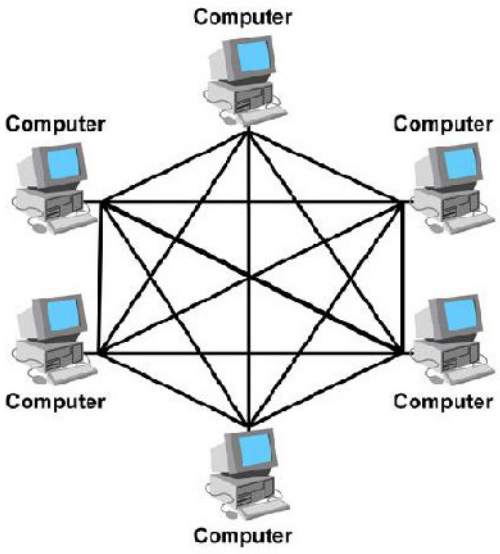
۲. توپولوژی Ring (حلقه)



۳. توپولوژی STAR (ستاره)



۴. توپولوژی MESH (گراف)



شبکه های MAN (METROPOLITAN AREA NETWORK)

برای مناطق نسبتاً وسیع در حد یک شهر و برای اتصال چند شبکه محلی به هم استفاده می شود. تکنولوژی و توپولوژِی این نوع از شبکه ها، مشابه شبکه های LAN است و به دلیل طول زیاد کانال از فیبر نوری در آن استفاده می شود.

شبکه های WAN (WIDE AREA NETWORK)

ویژگی ها:

۱. پیاده سازی در گستره جغرافیایی یک کشور یا جهان.
۲. اتصال شبکه هایLAN و MAN به هم.
۳. دارای ساختار ناهمگون یعنی شبکه های نتصب شده و پدید آورنده WAN دارای تنوع در توپولوژِ سخت افزار و نرم افزار هستند

زیرساخت ارتباطی شبکه‌های WAN

نمودار ۱: زیرساخت ارتباطی شبکه‌های WAN

شبکه های بی‌سیم (Wireless)

موارد استفاده

۱. ایجاد شبکه هایی با ایستگاه های متحرک
۲. استفاده در مکان هایی که کابل کشی به صرفه نیست

مزایا

۱. ساده بودن نصب و راه اندازی

معایب

احتمال نرخ ارسال پایین

۱. نرخ خطای نسبتاً بالا
۲. امنیت کم

روش های ارسال و دریافت بین دو کامپیوتر

سوییچینگ مداری

نیاز به برقراری ارتباط، عدم برقراری ارتباط کامپیوتر های دیگر با دو کامپیوتر در حال ارتباط(هنگام مشغول بودن خط) زمان بر

سوییچینگ پیام

دارای اتصال دائمی، دیجیتال، وجود یک مرکز سوییچ پیام که پیام را به طور کامل دریافت کند و داده های مورد نیاز را به آن بیافزاید، از دست نرفتن پیام هنگام مشغول بودن خط به دلیل وجود مرکز سوییچ

سوییچینگ بسته و سلول

مشابه سوییچینگ پیام با این تفاوت که پیام را به بسته هایی تقسیم میکند آنگاه هر بسته به مرکز سوییچ پیام ارسال می شود.

تعاریف انواع ارتباط

ارتباط یک طرفه (SIMPLEX)

یکطرف همیشه فرستنده و یکطرف همیشه گیرنده است.

ارتباط دوطرفه ی غیرهمزمان(Half Duplex)

هر دو ماشین می توانند فرستنده یا گیرنده باشند ولی نه بطور همزمان .

ارتباط دوطرفه ی همزمان(Full Duplex)

هر دو طرف می توانند به طور همزمان فرستنده و گیرنده باشند مانند خطوط ماکرو ویو .

جلسه دوم

۱۳۹۲/۰۷/۱۲

معرفی مدل های لایه بندی شده ی توسعه ی شبکه های کامپیوتری (TCP/IP, OSI)

مدل ۷ لایه‌ی OSI

مدل ۷ لایه‌ی OSI بر اساس پیشنهادی سازمان بین‌المللی استانداردها (ISO) به‌عنوان اولین استاندارد بین‌المللیِ شبکه‌های چندلایه پیشنهاد داده شد.

انتخاب لایه‌ها برای این مدل، بر این اساس بوده است که وظایف مختلف در در شبکه‌های کامپیوتری از همه تفکیک شوند و این وظایف برای هر لایه با در نظر گرفتنِ پروتکل‌های استاندارد، انتخاب شوند. مرزهای هر لایه باید، طوری انتخاب شود که کم‌ترین انتقال اطلاعات از آن‌ها لازم باشد.

نمایی از مدل اولیه‌ی OSI در شکل زیر قابل مشاهده است:

Application(لایه‌ی کاربردی)
Presentation (نمایش(ارائه))
Session (جلسه)
Transport(انتقال)
Network(شبکه)
Data link(پیوند داده)
Physical (فیزیکی)

جدول ۱: مدل OSI

تعریف لایه‌ی فیزیکی

به مجموعه‌ای از تجهیزات و ابزار و ماژول‌های (روال‌های) سخت‌افزاری که انتقال بیت‌ها را به‌صورت سیگنال‌های الکتریکی و ارسال آن‌ها بر روی کانال را بر عهده داشته باشند، تحت عنوان لایه‌ی فیزیکی شناخته می‌شوند.

- واحد اطلاعاتی در این لایه، بیت است.

مؤلفه های لایه ی فیزیکی عبارتند از

۱. ظرفیت کانال
۲. نرخ ارسال بیت‌ها
۳. موارد مکانیکی، الکتریکی و الکترومغناطیسی مانند نوع کابل، نوع رابط کابل (Connector)،
۴. نوع فرکانس
۵. نحوه‌ی تبدیل فرکانس (Modulation)
۶. تأخیر فاز در خطوط انتقال
۷. باند فرکانسی و ...

تعریف لایه ی پیوند داده

تجهیزات، سخت‌افزار و دستوراتی که کارکرد رساندن داده‌ها به مقصد به‌صورت بدون خطا و مطمئن را مکانیزم کشف و کنترل خطا انجام می‌دهند، در لایه پیوند داده قرار می‌گیرند.

وظایف لایه ی پیوند داده

وظایف این لایه عبارتند از :

۱. شکستن اطلاعات ارسالی از لایه‌ی بالاتر به واحدهای استاندارد و کوچک‌تر و تعیین ابتدا و انتهای واحدها با فاصله‌گذاری از طریق نشانه هایی که Delimiter نامیده می‌شوند.
۲. کشف خطا از طریق اضافه کردنِ بیت‌های کنترل خطا
۳. کنترل ارسال و دریافت از طریق هماهنگی بین مبدأ و مقصد
۴. مدیریت اعلام رسیدن یا نرسیدن داده‌ها به فرستنده
۵. تنظم قراردادهایی برای جلوگیری از تصادم سیگنال‌ها
۶. کنترل سخت‌افزار لایه‌ی فیزیکی

❖ واحد اطلاعاتی در این لایه Frame است

تعریف لایه ی شبکه

تجهیزات و برنامه‌هایی که سازماندهی اطلاعات، به‌صورت بسته (Packet) را بر عهده دارند، تحت لایه‌ی شبکه، قرار می‌گیرند.

وظایف لایه ی شبکه

۱. تعیین مسیر بسته‌ها
۲. کاستن از ترافیک تجهیزات (مسیریاب‌ها یا Switchها)
۳. اختصاص آدرس‌های منحصربه‌فرد و استاندارد به بسته‌ها

❖ واحد اطلاعاتی در این لایه، بسته یا Packet می‌باشد.

تعریف لایه ی انتقال

تجهیزات و برنامه‌هایی که زمان‌بندیِ ارتباط و اطمینان از آمادگی دریافت داده‌ها را بر عهده دارند، جزء لایه‌ی انتقال می‌باشند. موارد موجود در این لایه همچنین، اطمینان از عدم از بین رفتن بسته‌ها و حفظ ترتیب آن‌ها را نیز حاصل می‌نماید.

وظایف لایه ی انتقال

۱. شماره‌گذاری بسته‌ها
۲. آدرس‌دهی فرایندهای مختلف در حال اجرا روی یک ماشین
۳. تقسیم پیام‌های دریافتی از لایه‌های بالاتر به بسته‌های اطلاعاتی کوچک‌تر
۴. بازسازی بسته‌های اطلاعاتی و تشکیل یک پیام کامل
۵. نام‌گذاری ایستگاه‌های موجود در شبکه

تعریف لایه ی جلسه

مدیریت و برقراری ارتباط بین کاربران شبکه در سطوح بالا را بر عهده دارد.

وظایف لایه ی جلسه

۱. برقراری گفتگو و مدیریت آن
۲. شناسایی طرفین گفتگو
۳. تعیین اعتبار پیام‌ها
۴. اعلام اتمام گفتگو
۵. مدیریت حساب‌های مشتریان

تعریف لایه ی نمایش (ارائه)

وظیفه‌ی اجزا و اعضایی که در لایه‌ی نمایش دسته‌بندی می‌شوند آن است که برای کامپیوترهایی با ساختار متفاوت، وضعیتی مشخص و استاندارد فراهم نمایند که در عین داشتن ساختار متفاوت از پیام‌ها، بتوانند با هم ارتباط برقرار کنند.

وظایف لایه ی نمایش (ارائه)

۱. فشرده سازی فایل
۲. رمزگزاری و رمزگشایی
۳. تبدیل کدها در استانداردهای مختلف

تعریف لایه ی کاربرد

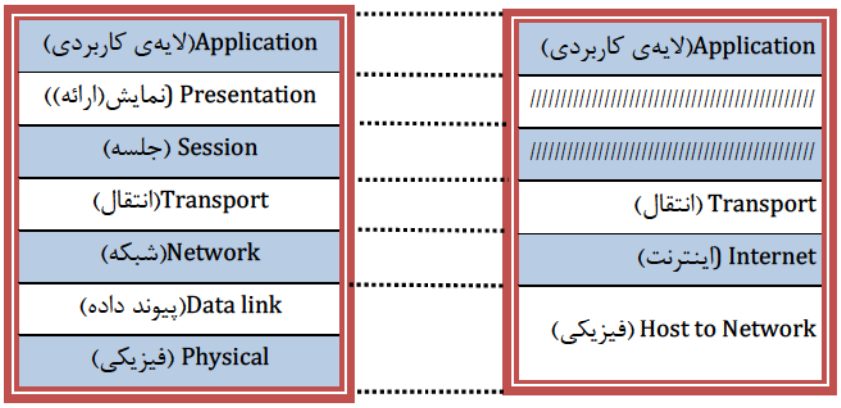
آن‌چه ارتباط کاربران نهایی با شبکه را برقرار می‌کند در لایه‌ی کاربرد قرار می‌گیرد. نرم‌افزارهای این لایه، موارد زیر را به انجام می‌رسانند.

وظایف لایه ی کاربرد

۱. مدیریت ایمن
۲. انتقال فایل
۳. انتقال صفحات وب
۴. دسترسی به بانک‌های اطلاعاتی راه دور

مدل چهار لایه ی TCP/IP

مدل TCP/IP ارتباط یکپارچه‌ی شبکه‌های مختلف را در عمل فراهم می‌آورد. این‌کار از طریق تأمین حداقل‌هایی‌ست که ارتباط دو کامپیوتر را تا زمانی‌که روشن باشند، فراهم می‌آورد یا برقرار می‌سازد حتی اگر تعدادی از ماشین‌های واسط بین آن‌ها از مدار خارج شوند. علاوه بر آن این مدل گرچه همه‌ی استانداردهای OSI را پوشش می‌دهد اما از عهده‌ی اجرایِ مطمئنِ طیف وسیعی از کاربردهای متنوع (از مکالمه‌ی واقعی تا انتقال فایل) برمی‌آید.
نمایی از مدل‌های چهار لایه‌ی TCP/IP در مقایسه با OSI در ادامه مشاهده می‌شود.



۱. لایه‌ی اول از مدل TCP/IP به نام‌های دیگری مانند Network Interface، میزبان شبکه، دسترسی به شبکه و رابط شبکه نیز نامیده می‌شود.
این لایه تعریف استانداردهای سخت‌افزار، تولید نرم‌افزارهای راه‌انداز و پروتکل‌های[۱] شبکه را بر عهده دارد، پروتکل‌هایی که در این لایه تعریف می‌شوند، مبتنی بر ارسال رشته‌بیت یا مبتنی بر ارسال بایت‌ها می‌باشد.

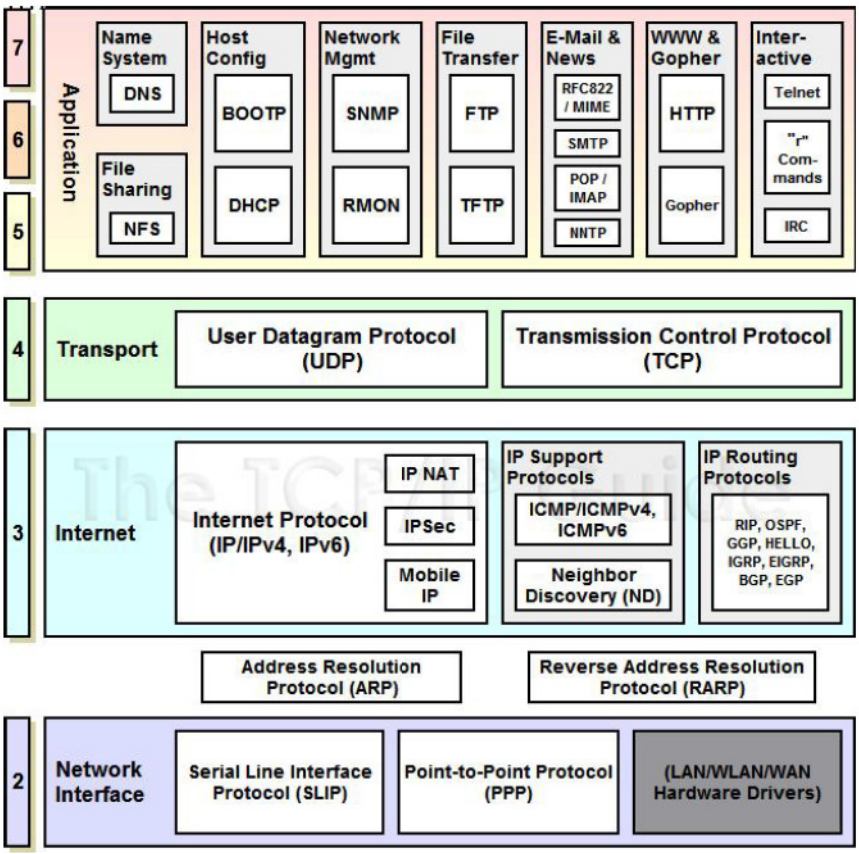
۲. لایه‌ی دوم از مدل TCP/IP با عناوین Network، شبکه، اینترنت و ارتباطات اینترنت نیز شناخته می‌شود. در این لایه، بسته‌هایی با نام بسته‌های IP تعریف و ایجاد می‌شود و هدایت این بسته‌ها روی شبکه، از مبدأ تا مقصد انجام می‌شود، همچنین ارسال چندپخشی (Multicast) که به معنای ارسال یک یا چند بسته‌ی اطلاعاتی به چندین مقصد می‌باشد، از توانایی‌های این لایه است.

۳. لایه‌ی سوم از مدل TCP/IP با نام‌های Host-to-Host، End-to-End، انتقال، لایه‌ی ارتباط میزبان به میزبان و ارتباط عناصر انتهایی نیز معروف است. این لایه، برقراری ارتباط مطمئن از طریق سرویس‌ها را با ماشین‌های انتهایی یا میزبان‌ها انجام می‌دهد. همچنین، دارای برنامه‌های کاربردی و توابع سیستمی‌ای است که ارسال یا دریافتِ داده‌ها را امکان‌پذیر می‌کنند.

۴. لایه‌ی چهارم از مدل TCP/IP لایه‌ی کاربرد یا همان لایه‌ی سرویس‌های کاربرد است که مشابه لایه‌ی متناظر خود در مدل OSI وظایف زیر را بر عهده دارد:
   ۱. شبیه‌سازی پایانه‌ها
   ۲. انتقال فایل‌ها
   ۳. مدیریت ایمیل
   ۴. انتقال صفحات وب

و ...
جزئیات لایه‌های TCP/IP با ذکر پروتکل‌های هر لایه و به‌صورت مقایسه‌ای با لایه‌های OSI در شکل زیر مقایسه می‌شود.

۱ - به مجموعه ای از قوانین و دستورالعمل ها برای رسیدن به هدف خاصی گفته می شود.



شکل ۲: جزئیات لایه های TCP/IP با ذکر پروتکل های هر لایه و به صورت مقایسه ای با لایه های OSI

جلسه سوم ۱۳۹۲/۰۷/۱۹

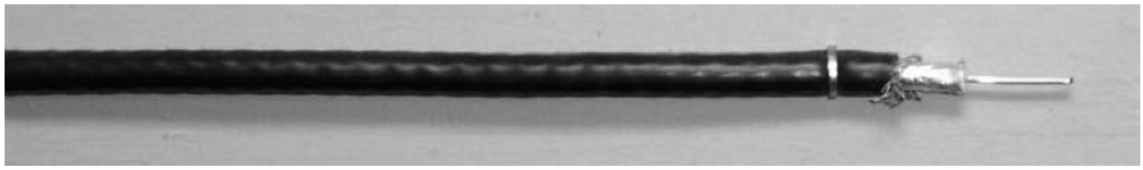
آشنایی با دستگاه ها و تجهیزات شبکه

رسانه (Media) و اتصال (Connector) در شبکه

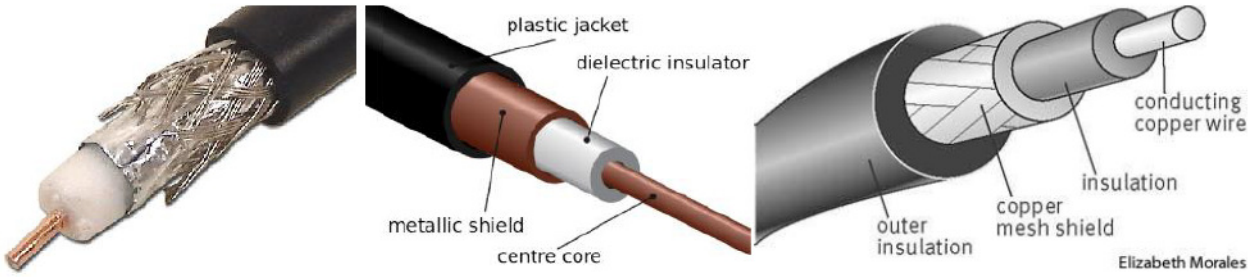
کابل‌کشی امکانی برای انتقال داده‌ها برای بین میزبان‌ها Hosts درون یک LAN است. در یک LAN کامپیوترها می‌توانند با انواع متفاوتی از کابل‌ها به هم متصل شوند که در ادامه به آن می‌پردازیم:

کابل کواکسیال (Coaxial)

این کابل از نظر ظاهری، شبیه به کابل‌های انتقال سیگنال تلویزیونی است که یک رشته‌ی مسی در وسط این کابل وجود دارد و در اطراف آن، لایه‌ای جهت محافظت و پوشش از فُویل قرار دارد که اصطلاحاً به آن Shield می‌گویند. در لایه‌ی آخر از این کابل نیز، یک پوشش پلاستیکی موجود است. به خاطر وجود لایه‌های محافظتی، کابل کواکسیال نسبت به تداخل خارجیِ نویز، مقاوم است.



شکل ۳: کابل Coax

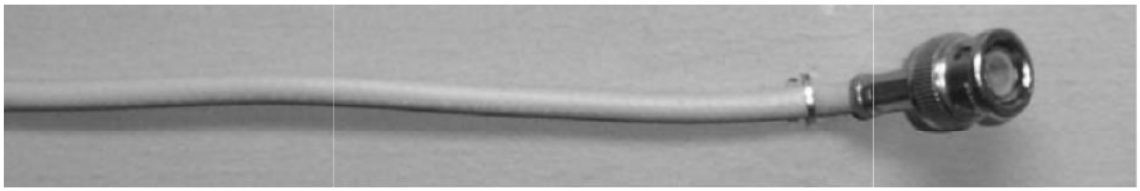


انواع کابل کواکسیال

دو نوع از کابل کواکسیال موجود است که به قرار زیر می‌باشند:

۱- Thinnet

استاندارد کابل‌کشی برای این نوع از کابل کواکسیال، RG-58 است و این نوع کابل در حدود یک‌چهارمِ اینچ ضخامت دارد. برای مسافت‌های کوتاه استفاده می‌شود و انعطاف‌پذیری کافی برای اتصال یک Work Station (ایستگاه کاری) را دارد. کابل Thinnet به‌صورت مستقیم به کارت شبکه وصل می‌شود. اتصالی یا کانکتوری که روی کارت شبکه، این کابل را می‌پذیرد، BNC (British Naval Connector) نام دارد. حداکثر طولی که می‌توان برای این کابل استفاده کرد، ۱۸۵ متر می‌باشد.



شکل ۴: BNC Connector

۲- Thicknet

با استاندارد RG-8 شناخته می‌شود و از آن نام آن مشخص است که از نوع اول، ضخیم‌تر است. ضخامت آن در حدود یک‌دوم اینچ می‌باشد. حداکثر فاصله‌ای که می‌توان از این کابل استفاه کرد، ۵۰۰ متر می‌باشد.

معمولاً یک دستگاه فرستنده، گیرنده و به‌طور مستقیم به کابل Thicknet از طریق کانکتوری که Vampire tap نامیده می‌شود، متصل می‌گردد. اتصال دستگاه گیرنده و فرستنده به کارت شبکه، به کمک یک کابل و کانکتور AUI (Adaptor Unit Interface) امکان‌پذیر است.

نرخ انتقال برای هر دو کابل Thinnet و Thicknet، 10 Mbps است.

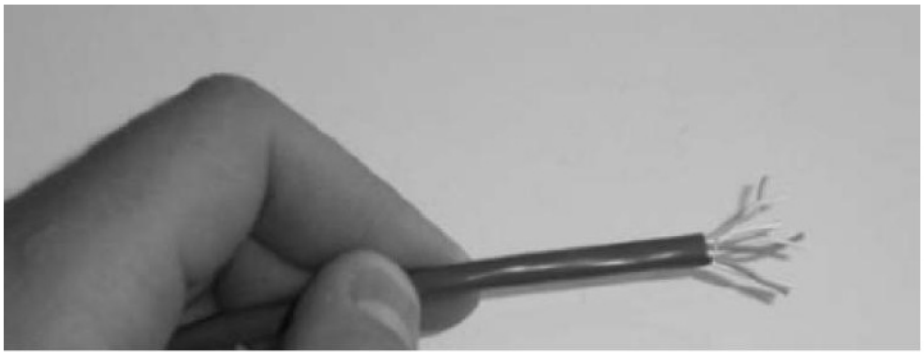
کابل زوج سیم (Twisted Pair Cable)

این کابل نام خود را از داشتنِ چهار زوج از سیم‌ها که به هم پیچیده شده‌اند، می‌گیرد. پیچیدن زوج‌سیم‌ها به‌هم باعث می‌شود که تداخلِ نویز و دستگاه‌های محیط بر آن کاهش یابد. دو نوع از کابل زوج‌سیم موجود است که در ادامه به آن می‌پردازیم.

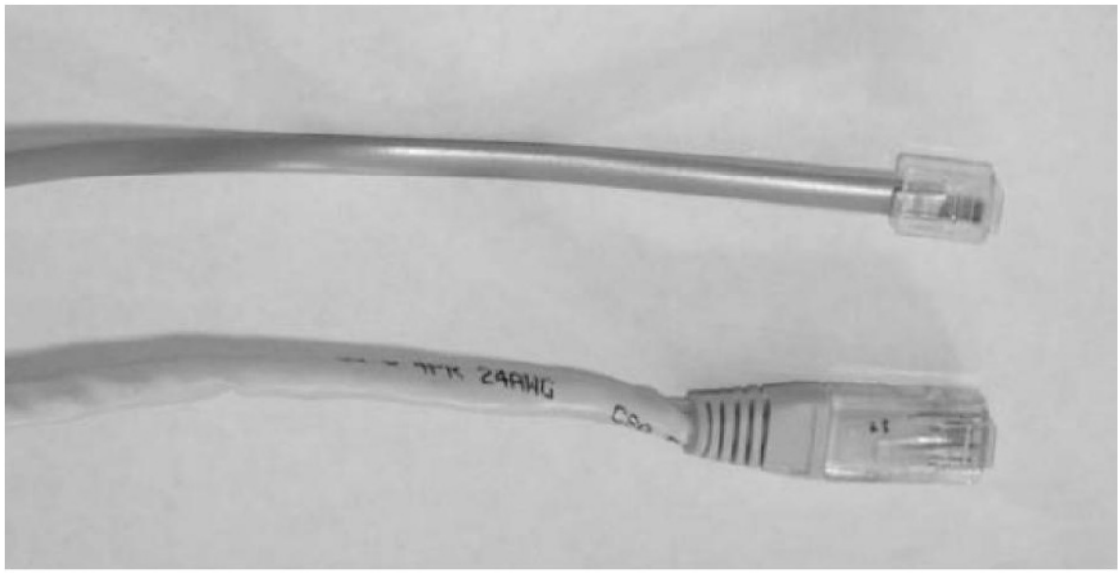
UTP (Unshielded Twisted Pair)

این کابل از نظر ظاهری مشابه کابل تلفن است و حداکثر فاصله‌ای که می‌تواند پوشش دهد ۱۰۰ متر می‌باشد. دارای یک کانکتور کوچک پلاستیکی با نام RJ-45 است. این کانکتور هم مشابه کانکتور سیم‌های تلفن است، با این تفاوت که، به‌جای ۴ سیم، دارای ۸ سیم می‌باشد.

مزایای کابل UTP آن است که راحت‌تر از کابل Coaxial نصب می‌شود، دارای انعطاف‌پذیری بیش‌تر و سایز کوچک‌تر است.
از معایب کابل UTP آن است که دارای حساسیت بیش‌تری نسبت به نویز و محیط اطراف می‌باشد (مثلاً نسبت به کابل Coaxial) بنابراین قابل استفاده از محیط‌هایی که دارای دستگاه‌های بزرگ الکترونیکی یا الکتریکی هستند، نمی‌باشد.



شکل ۵: کابل UTP



شکل ۶: کانکتورهای RJ11 و RJ45

Categoryهای کابل UTP در جدول زیر مشاهده می‌شود.

CAT	نوع	نرخ انتقال
1	صدا	4 Mbps
2	داده	10 Mbps
3	داده	16 Mbps
4	داده	100 Mbps

5	داده	1 Gbps
6	داده	10 Gbps

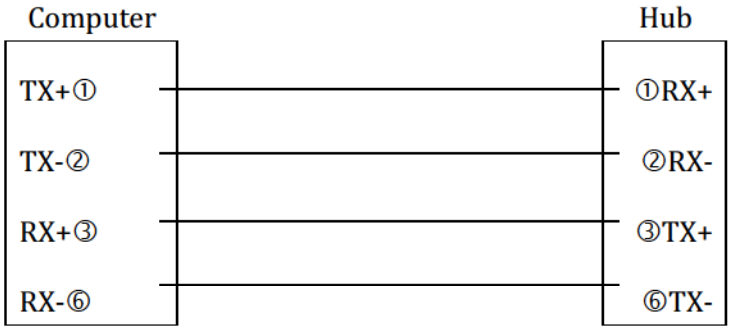
جدول ۲: اتصال مستقیم کابل UTP

کابل کشی CAT5 UTP

برای ارسال و دریافت اطلاعات در شبکه، معمولاً فقط از چهار سیم استفاده می‌کنند که سیم‌های شماره‌ی ۱، ۲، ۳ و ۶ می‌باشند.

سیم‌های ۱و ۲، جهت ارسال و سیم‌های ۳ و ۶ جهت دریافت به‌کار می‌روند. در ضمن، پین (Pin) ارسال روی کامپیوتر به پینِ دریافت روی دستگاه Hub (هاب) از طریق سیم‌های ۱و ۲ متصل می‌شوند. ذکر این نکته از آن جهت مهم است که بدانیم دیتای ارسال‌شده از کامپیوتر، توسط هاب دریافت می‌شود و برعکس دیتای ارسال‌شده توسط هاب به‌وسیله‌ی کامپیوتر دریافت می‌گردد. به‌طور مشابه، پینِ ارسال روی هاب از طریق سیم‌های ۳ و ۶، به پین‌های دریافت، روی کامپیوتر مرتبط می‌گردند.

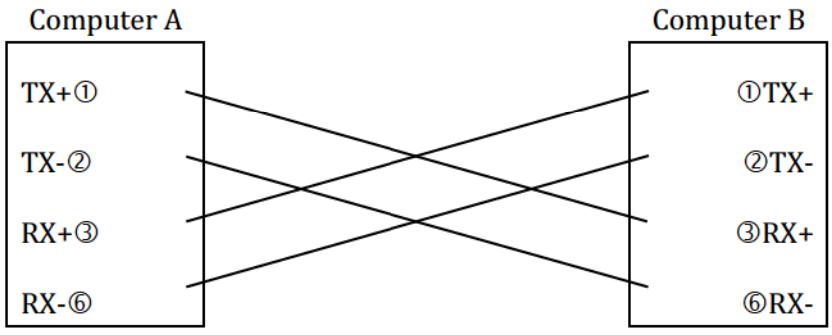
شکل زیر نشان می‌دهد که اتصالِ مشابه پین‌ها به‌هم، علتِ نام‌گذاریِ این نوع از ارتباط بین یک کامپیوتر و یک دستگاه مانند هاب است.



TX پینِ ارسال و RX پینِ دریافت است.

اتصال غیر مستقیم(Cross Over) کابل UTP

اگر بخواهیم دو کامپیوتر را به هم وصل کنیم، اتصال مستقیم باعث می‌شود که پین‌های دریافت به دریافت و پین‌های ارسال به ارسال متصل گردند، در این‌صورت هیچ ارتباطی برقرار نمی‌شود، پس هنگام متصل ساختنِ دو کامپیوتر به‌هم، باید به ترتیب سیم‌های شماره‌ی ۱ و ۲، به‌ترتیب به سیم‌های ۳ و ۶ از کامپیوتر دیگر، وصل شود. مانند شکل زیر:



مزایای کابل UTP

انعطاف پذیری

کوچک بودن کانکتور

در مقایسه با کابل کوآکسیال از انعطاف پذیری کمتری در نصب بر خوردار است

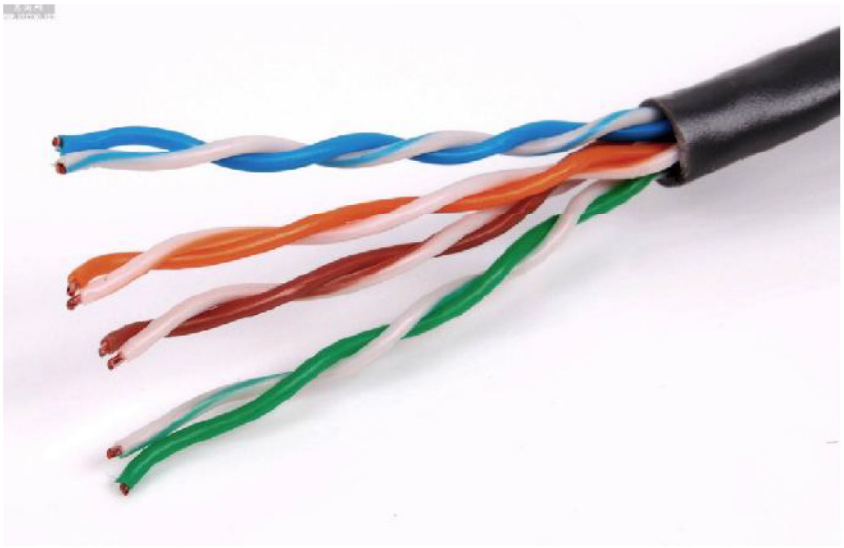
معایب کابل UTP

به علت حساسیت بیشتر(باز هم درمقایسه با کوآکسیال) مقاومت کمتری در مقابل تداخل محیطی و نویز دارد.

مشخصات کابل UTP در شکل و دو جدول زیر مشاهده می شود.

1	White-orange
2	Orange
3	white-green
4	Blue
5	white-blue
6	Green
7	White-brown
8	Brown

جدول ۳: شناسایی سیم های UTP بر اساس رنگ



شکل ۷:

Connector#1	Connector#2
White-orange	**White-orange**
Orange	**Orange**
white-green	**white-green**
Blue	**Blue**
white-blue	**white-blue**
Green	**Green**
White-brown	**White-brown**
Brown	**Brown**

جدول ۴ : اتصال مستقیم

Connector#1	Connector#2
White-orange1	**white-green3**
Orange2	**Green6**
white-green3	**White-orange1**
Blue	**Blue**
white-blue	**white-blue**
Green6	**Orange2**
White-brown	**White-brown**
Brown	**Brown**

جدول ۵: اتصال غیرمستقیم

(Shielded Twisted Pair) STP

بسیار شبیه به کابل UTP است، با این تفاوت که یک لایه‌ی محافظ دارد و به همین علت ضخیم تر و گران تر می باشد.که کیفیتِ انتقال داده را در آن افزایش می‌دهد. ضخامت و قیمت آن نسبت به UTP بیش‌تر است.

شکل ۸: جفت کابل بالایی CAT 3 UTP، جفت کابل پایینی CAT 5e STP

حداکثر فاصله قابل پوشش توسط هر دو کابل زوج سیم ۱۰۰ متر می باشد.

کابل فیبر نوری

دیتارا با استفاده ازپالس‌های نوری انتقال می دهد، در آن یک استوانه‌ی نازک شیشه‌ای در وسط این کابل وجود دارد و دارای دو نوع می-باشد:

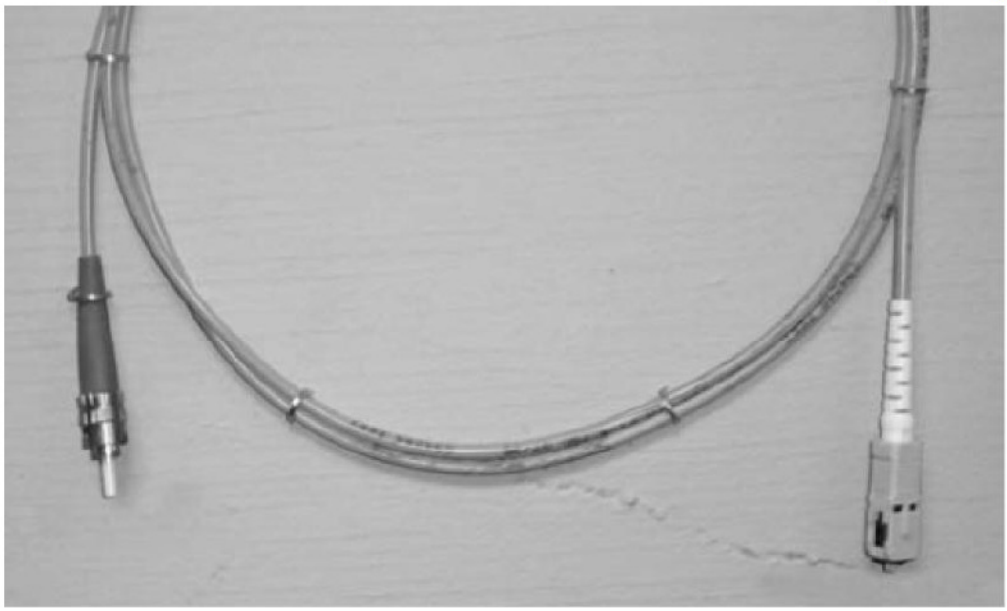
Single-mode Fiber (تک‌سطحی): که فقط برای ارسال است.

Multi-Mode Fiber (چندسطحی): که برای ارسال و دریافت همزمان است.

ماکسیمم فاصله قابل پوشش توسط فیبر نوری ۲۰۰۰ متر و توانایی پوشش ۱۰۰۰ ایستگاه کاری و دارای حداقل **1Gbps** نرخ انتقال می باشد.

دو نوع کانکتور دارد:

۱. (Straight) ST
۲. (Subscriber) SC



شکل ۹: نمایی از فیبر نوری، سمت راست:SC ، سمت چپ: ST

✓ این قسمت در جلسه ششم ارائه گردید

تجهیزت انتقال ترافیک شبکه

هاب(Hub)

دستگاهی است که در شبکه های LAN با توپولوژی استار تمام اجزای ماشین های شبکه را به هم متصل می کند. در استفاده از Hub هر دستگاه یا ماشین مستقیماً و از طریق یک کابل مجزا به Hub متصل می شود. هر واحد انتقالی از داده ها که به یک پورت Hub برسد به همه پورت های دیگر آن انتقال می یابد بنابر این Hub دستگاهی است که ترافیک شبکه را بیهوده افزایش می دهد چرا که ممکن است تمامی دستگاه ها و ماشین های متصل به Hub خواستار داده ارسالی نباشند ولی Hub مکانیسمی برای تشخیص مقصد از غیر آن ندارد.

شکل ۱۰: نمایی از یک **Hub**

شکل ۱۱: نمایی از یک **Hub** در شبکه

تکرار کننده(Repeater)

سیگنال درون شبکه و تحت یک مدیا(مثلاً سیم) دچار افت می شود برای ارسال واحدهای انتقالی از دیتا به فواصلی که بیش از حد تحمل مدیا باشد از دستگاه **repeater** استفاده می کنند. این دستگاه دارای عملکرد تقویت کنندگی است به این معنا که سیگنال دریافتی را تقویت می کند و به مقاصد بعدی ارسال می کند.

شکل ۱۲: نمایی از یک **Repeater**

سوئیچ(Switch) 

مشکل افزایش بیهوده ترافیک که توسط دستگاهی مانند **Hub** به شبکه تحمیل می شد توسط سوئیچ برطرف می شود. سوئیچ ترافیک دریافتی را فقط به پورت مقصد منتقل می کند. سوئیچ ها در لایه های مختلفی از مدل **OSI** پیاده سازی می شوند. مثلاً سوئیچ لایه یک موجود است که با مولفه های فیزیکی کار می کند این نوع از کارکرد برای این نوع سوئیچ مساله ای بدیهی است چراکه لایه فیزیکال شامل مولفه های فیزیکی می باشد. از انواع دیگر سوئیچ می توان به سوئیچ لایه دو و سوئیچ لایه سه نیز اشاره کرد. سوئیچ لایه سه دارای قابلیت مسیر یابی است به این معنا که با مولفه **IP Address** کار می کند و به همین خاطر برای برقراری ارتباط چندین **Subnet** درون این شبکه به کار می رود.امروزه سوئیچ ها به دلیل دارا بودن پورت هایی با سرعت بالا می توانند مسیر یابی داخل شبکه ای را با کارایی خوبی انجام دهند.

شکل ۱۳: نمایی از یک **Switch**

روتر(Router) 

مهمترین ابزاریست که توانمندی مسیر یابی بین شبکه ای متفاوت را فراهم می سازد. در واقع پروسه انتقال پکت ها از یک شبکه به شبکه دیگر با استفاده از روتر و تجهیزات لایه سه صورت می گیرد و به این عملیات مسیریابی یا **Routing** می گوییم. روتر ها برای اینکه بتوانند به صورت صحیح وظیفه مسیریابی را انجام دهند باید پیکر بندی شوند، پیکربندی عبارتست از ایجاد یک جدول مسیریابی بر روی یک روتر که در آن اطلاعات آدرس و مسیر همه شبکه هایی که ارتباط با آنها وجود دارد، ذکر شده است. روتر بر اساس این جدول تصمیمات مسیر یابی را اتخاذ می کند دو گونه از پیکر بندی جدول مسیریابی وجود دارد که عبارتند از :

۱. Static
۲. Dynamic

برای پیکر بندی جدول مسیریابی به صورت استاتیک مدیر شبکه باید از اطلاعات مربوط به شبکه های موجود و آدرس های آنها مطلع باشد و به صورت دستی مسیر هاو شبکه ها را در جدول مسیریابی روتر تعریف نماید. روتری که به این صورت پیکر بندی شده باشد اصطلاحاً مسیریابی ایستا(**Static Routing**) انجام میدهد. در پیکر بندی روتر به صورت **Dynamic** یک روتر جدول مسیریابی اش را با سایر روتر های شبکه مبادله می کند با این کار که به طور خودکار انجام می شود مسیرهای جدید اضافه می گردند و جدول مسیابی روتر ها به روزرسانی میشود اگر ازاین روش برای پیکربندی استفاده شود می گوییم روتر مسیریابی پویا(**Dynamic Routing**) انجام می دهد.

شکل ۱۴: نمایی از یکRouter مدل Cisco 2500

جلسه چهارم

آدرس های شبکه

در شبکه از آدرس های منحصر به فرد استفاده می شود. این آدرس ها اگر قالب ۳۲ بیتی داشته باشند، تحت استاندارد IPV4 و اگر قالب ۱۲۸ بیتی داشته باشند تحت استاندارد IPV6 دسته بندی می شوند. در این صورت هر ابزار شبکه مانند ماشین های میزبان مسیر یاب ها چاپگر های شبکه و غیره، با یک آدرس شناسایی می شوند که به طور خلاصه به آن "IP" می گویند.

در حالت ۳۲ بیتی IP به ۴ بایت تقسیم می شود که هر بایت اصطلاحاً یک Octet نام دارد.Octet ها با یک نقطه از هم جدا می شوند.IP در واقع یک عدد ۳۲ بیتی دو دویی است اما برای راحتی Octet ها را به صورت ده دهی نمایش می دهند.

مثال)IP مقابل را در مبنای دو دویی بنویسید؟ "34.21.225.1"

00100010.00010101.11100001.00000001

کلاس های IP

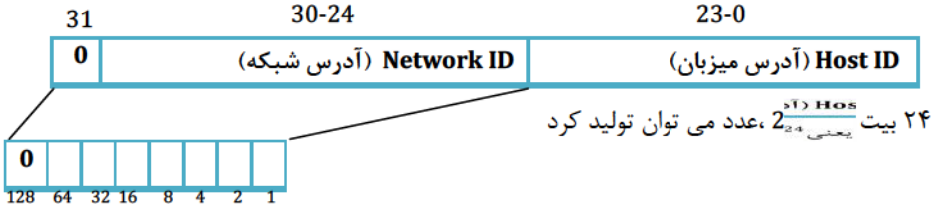
فضای ۳۲ بیتی IP حدود 4,300,000,000 آدرس در اختیار می گذارد که برای اختصاص آن باید سلسله مراتبی وجود داشته باشد.

سلسله مراتب آدرس دهی بر اساس IP به صورت زیر است.

"آدرس میزبان/آدرس زیر شبکه/آدرس شبکه"

آدرس کلاس A

قالب آن به صورت زیر است.



۲۴ بیت یعنی 2^{24} عدد می توان تولید کرد

در کلاس A، Octet پر ارزش در محدوده ۰ تا ۱۲۷ تغییر می کند. در عمل مشخصه شبکه نمی تواند اعداد ۰ یا ۱۲۷ انتخاب شود، بدان خاطر که انتخاب مقادیر تماماً ۰ یا تماماً ۱ برای بیت های مربوط به آدرس شبکه مجاز نمی باشد.

مثال) 74.103.14.138

بنابر این تعداد شبکه هایی که در جهان می توانند از کلاس A استفاده کنند ۱۲۶ تا خواهد شد که Network ID آنها اعداد ۱ تا ۱۲۶ را می توانند اختیار کنند.

- رفتار آدرس دهی در کلاس A: تعداد کمی از شبکه های بزرگ. در هر شبکه حدود ۱۷,۰۰۰,۰۰۰ میزبان وجود دارد.

آدرس های کلاس B

قالب آن بصورت زیر است.

در آدرس های کلاس B تعداد Network ID هایی که می تواند تعریف شود می تواند $2^{14} - 2$ باشد اعداد تماماً ۰ یا تماماً ۱ برای Network ID پذیرفته نیست.

1	0	000000	00000000

128.0._._ پذیرفته نیست

1	0	111111	11111111

191.255._._ پذیرفته نیست

در آدرس های کلاس B تعداد Host ID هایی که می تواند تعریف شود می تواند$2^{16} - 2$ باشد اعداد تماماً ۰ یا تماماً ۱ برای Host ID پذیرفته نیست.

Octet پر ارزش از ۱۲۸ تا ۱۹۱ می تواند تغییر کند.

- رفتار کلاس B تعداد متوسطی از شبکه$(2^{14} - 2)$ و میزبان $(2^{16} - 2)$

مثال) 134.64.143.24

کلاسB است چون 134 بین 128 و 191 می باشد.

آدرس کلاس C

قالب آن به صورت زیر است.

31	30	29	28-8	7-0
1	1	0	Network ID (آدرس شبکه)	Host ID (آدرس میزبان)

در آدرس های کلاس C تعداد Network ID هایی که می تواند تعریف شود می تواند $2^{21} - 2$ باشد. همچنین برای تشخیص آدرس های کلاس C می گوییم Octet پر ارزش باید مابین اعداد 192 تا 223 باشد. اعداد تماماً ۰ یا تماماً ۱ برای Network ID پذیرفته نیست.

1	1	0	00000	00000000	00000000	

192.0.0._ پذیرفته نیست

1	1	0	11111	11111111	11111111	

223.255.255._ پذیرفته نیست

در آدرس های کلاس C تعداد Host ID هایی که می تواند تعریف شود می تواند $2^{8} - 2$ باشد اعداد تماماً ۰ یا تماماً ۱ برای Host ID پذیرفته نیست.

مثال) 199.164.78.132

چون مابین 199 و 223 است.

- رفتار کلاس C تعداد زیادی از شبکه کوچک $(2^{21} - 2)$ با تعداد میزبان کم $(2^{8} - 2)$

آدرس کلاس D

قالب آن بصورت زیر است

31	30	29	28	27-0
1	1	1	0	Multi Cast Address (آدرس چند مقصدی)

از آدرس های این کلاس برای ارسال همزمان دیتا به چندین ماشین میزبان استفاده می کنند.چنین عملیاتی را چندپخشی می نامند. برای تشخیص ادرس های کلاس D باید بررسی کرد که Octet پر ارزش بین اعداد 224 و 239 باشد.

مثال) 230.50.124.90

آدرس کلاس E

قالب آن بصورت زیر است

31	30	29	28	27	26-0
1	1	1	1	0	Unused Address Space (آدرس بدون استفاده)

این آدرس ها کاربرد ندارند و برای استفاده در آینده باقی گذاشته شده بودند، گاهی به صورت آزمایشی از این آدرس ها استفاده شد ولی جهانی نشدند. Octet پر ارزش کلاس E بین اعداد 240 تا 247 است.

آدرس های خاص

۱. 255.255.255.255

برای ارسال پیام های فراگیر به تمامی ماشین های میزبان بر روی شبکه محلی استفاده می شود.

۲. Net ID.255 یا Net ID.255.255 یا Net ID.255.255.255

برای ارسال پیام های فراگیر به تمامی ماشین های یک شبکه راه دور استفاده می شود.آدرس شبکه مورد نظر در قسمت Net ID تعیین می شود و تمامی بیت های قسمت Host ID یک قرار داده می شوند.

۳. 127._._._

به عنوان آدرس بازگشت (Loop Back) شناخته می شود.مثلاً اگر بسته ای به آدرس 127.0.0.1 ارسال شود بسته برای فرستنده باز خواهد گشت.کاربرد آن برای اشکال زدایی نرم افزاری است و استفاده از یک سیستم هم به عنوان سرور هم کلاینت.

آدرس های زیر شبکه

همانطور که گفته شد با در نظر گرفتن یک IP می توان فهمید که از چه کلاسی است اما اگر این IP ، IP ماشین مقصد باشد به جز تشخیص کلاس برای فرستنده مسائل دیگری مطرح است، مسائلی مانند اینکه ماشین مقصد در شبکه ای واقع است که دارای زیر مجموعه هایی است یا خیر، اگر چنین باشد می گوییم شبکه مقصد به زیرشبکه هایی(Sub Networks) تقسیم شده است.همچنین باید دانست که ماشین مقصد در همان زیر شبکه ای واقع است که ماشین مبدأ. برای آنکه بتوان زیرشبکه های یک شبکه را تفکیک کرد به غیر از قسمت آدرس شبکه بایستی در قسمت Host ID ، به گونه ای زیرشبکه ها نیز مشخص گردد این کار از طریق مفهومی با نام الگوی زیرشبکه(Subnet Mask) انجام می شود. فرض کنید یک آدرس IP به صورت 131.55.213.73 اختصاص داده شده است می توان فهمید که این آدرس از کلاس B است با صفر قرار دادن قسمت Host ID مشخصه شبکه به دست می آید یعنی 131.55.0.0 . همچنین با صفر قرار دادن Net ID، مشخصه میزبان به دست می آید یعنی 0.0.213.73 .

حال فرض کنیم شبکه 131.55.0.0 می خواهد حد اکثر دارای 254 زیرشبکه باشد در اینصورت باید بایت پر ارزش از Host ID را به عنوان مشخصی مربوط به زیرشبکه تعریف کند در اینصورت قالب IP را برای مثال فوق بصورت زیر می توان نشان داد:

31	30	29-16	15-0	
1	0	Network ID (آدرس شبکه)	15-8	7-0
			Subnet ID(آدرس زیرشبکه)	Host ID(آدرس میزبان)

در این مثال هر ماشینی که بخواهد IP فوق را به عنوان آدرس ماشین مقصد استفاده کند باید تشخیص دهد که این IP در شبکه محلی خودش واقع است یا در خارج شبکه محلی قرار دارد و بنا بر این برای دسترسی به آن باید از فرایند مسیر یابی سود جست. Subnet mask

به عنوان یک مقایسه گر ابزاری است که در این جهت استفاده می شود **Subnet mask** با صفر قرار دادن **Host ID** و یک قرار دادن همه بیت های دیگر به دست می آید یعنی برای مثال قبل می شود

دودویی = 11111111.11111111.11111111.00000000

دهدهی = 255.255.255.0

جلسه پنجم.....

تحلیل IP

هرگاه ماشینی بخواهد یک آدرس IP را تحلیل کند الگوی Subnet Maskرا با آدرس IP خودش AND می کند. با این کار Host ID صفر می شود.سپس مجدداً Subnet Maskرا با آدرس IP مقصد AND می کنند. با این کار Host ID ماشین مقصد هم صفر می شود سپس نتیجه دو مرحله را با هم X-OR می نمایند اگر نتیجه X-OR تماماً صفر بود هر دو ماشین روی یک زیرشبکه هستند و در غیر این صورت بسته باید به مسیر یاب ارسال شود.

مثال)

آدرس مبدأ: 131.55.213.73

آدرس مقصد: 131.55.108.75

Subnet Mask: 255.255.255.0

جواب)

تبدیل آدرس مبدأ به دودویی:

Computer#1:10000011.00110111.11010101.01001001

تبدیل Subnet Mask به دودویی:

11111111.11111111.11111111.00000000

10000011.00110111.11010101.00000000

تبدیل آدرس مقصد به دودویی:

Computer#2:10000011.00110111.01101100.01001011

تبدیل Subnet Mask به دودویی:

11111111.11111111.11111111.00000000

10000011.00110111.01101100.00000000

00000000.00000000.10111001.00000000

- بدلیل اینکه تماماً صفر نشده است یعنی دو کامپیوتر از یک شبکه نیستند.

- IP
- Subnet Mask
- IP AND Subnet Mask
- (X OR)

مثال)

آدرس مبدأ: 131.55.213.73

آدرس مقصد: 131.55.213.84

Subnet Mask: 255.255.255.0

جواب)

تبدیل آدرس مبدأ به دودویی:

Computer#1:10000011.00110111.11010101.01001001

تبدیل Subnet Mask به دودویی:

11111111.11111111.11111111.00000000

10000011.00110111.11010101.00000000

تبدیل آدرس مقصد به دودویی:

Computer#2:10000011.00110111.11010101.01010100

تبدیل Subnet Mask به دودویی:

11111111.11111111.11111111.00000000

10000011.00110111.11010101.00000000

00000000.00000000.00000000.00000000

- بدلیل اینکه تماماً صفر شده است یعنی دو کامپیوتر از یک شبکه هستند.

زیر شبکه بندی(Subnetting)

همانطور که درمطالب قبلی گفته شد یک شبکه ممکن است تعدادی زیر شبکه داشته باشد.مثلاً یک شبکه در کلاس B بصورت:

255.255.255.0:10Network ID | Network ID | Subnet ID | Host ID

(یک Octet | یک Octet | یک Octet | یک Octet)

آدرس بندی می شود.

یا یک شبکه در کلاس A به صورت های:

255.255.255.0:0Network ID | Network ID | Subnet ID | Host ID

255.255.0.0: 0Network ID | Network ID | Subnet ID | Host ID

(یک Octet | یک Octet | یک Octet | یک Octet)

تقسیم بندی می شود.

به چنین تقسیم بندی ای که در آن یک یا دو Octet به طور کامل به Subnet ID اختصاص می یابد اصطلاحاً زیر شبکه بندی Classfull می گویند که در الگوی Subnet Mask برای این نوع زیرشبکه بندی فقط اعداد 0 و 255 مشاهده می شود.

اگر اختصاص بیت ها به Subnet ID به صورت Octet های کامل نباشد می گوییم زیرشبکه بندی به صورت Classless است.

مثال)

10Network ID | Network ID | Subnet ID | Host ID | Host ID

(یک Octet | یک Octet | نصف Octet | نصف Octet | یک Octet)

Subnet Mask: 11111111.11111111.11110000.00000000

255. 255. 240. 0

مثال)

اگر در یک زیرشبکه بندی از نوع Classless و با داشتن شبکه ای از کلاس A فقط ۶ بیت از Octet سوم (از سمت راست) به Subnet ID اختصاص یابد، Subnet Mask را بیابید.

10Network ID | Subnet ID | Host ID | Host ID | Host ID

۶ بیت ۲ بیت

Subnet Mask: 11111111.11111100.00000000.00000000

255. 252. 0. 0

مثال)

اگر در یک زیرشبکه بندی از نوع Classless و با داشتن شبکه ای از کلاس C فقط ۳ بیت پر ارزش از Octet اول (از سمت راست) به Subnet ID اختصاص یابد، Subnet Mask را بیابید.

110Network ID | Network ID | Network ID | Host ID

مشترکاً توسط Host و Subnet

110Network ID | Network ID | Network ID | Subnet ID | Host ID

۳ بیت ۵ بیت

Subnet Mask: 11111111.11111111.11111111.11100000

255. 252. 255. 224

واضح است که زیرشبکه بندی در واقعیت بر عکس مثال های فوق دلخواه نیست بلکه بستگی به تعداد زیرشبکه ها و تعداد میزبان ها در هر زیرشبکه دارد الگوریتم زیر مراحل زیرشبکه بندی را به ترتیب شرح می دهد.

۱- تعداد زیرشبکه ها و تعداد ماشین های میزبان روی هر زیرشبکه باید مشخص گردد. به تعداد زیرشبکه ها و ماشین های میزبان می باید عدد ۲ را افزود چرا که زیر شبکه یا ماشینی که تمام بیت های ID آن صفر یا تمام بیت های آن یک باشد قابل تعریف نیست.سپس باید تعیین کرد که هر کدام از اعداد زیر شبکه و ماشین ها به چند بیت جهت تبدیل دودویی نیاز دارند.

۲- Subnet Maskرا باید به گونه ای تنظیم کرد که در سمت راست به تعداد بیتی که برای آدرس دهی ماشین های میزبان نیاز است 0 قرار گیرد و مابقی بیت ها نیز 1 شود.

۳- Subnet Mask می باید از الگوی دودویی به فرم دهدهی نقطه دار تبدیل شود.

۴- زیرشبکه ها و ماشین های میزبان روی هر زیرشبکه آدرس دهی شود.

مثال)

شبکه 131.55.0.0 را در نظر بگیرید. این شبکه از کلاس B می باشد آن را به گونه ای زیرشبکه بندی کنید که دارای ۲۵ زیرشبکه باشد و هر زیرشبکه حداکثر تا ۱۰۰۰ میزبان را پوشش دهد.ذکر الگوی Subnet Mask ، ID هر زیرشبکه و اولین و آخرین آدرس معتبر در هر زیرشبکه الزامی است.

جواب)

عدد زیر شبکه ها:25 + 2 = 27

تعداد بیت ها برای زیر شبکه ها:5 (11011)

5 بیت

Network ID	Network ID	Subnet ID	Host ID	Host ID
		5 بیت	3 بیت	

11111111.11111111.11111000.00000000

255. 255. 248. 0

131.55.0.0

زیرشبکه اول:10000011.00110111.00001000.000000000

131.55.8.0

IP#1:10000011.00110111.00001000.00000001
131.55.8.1

IP#n:10000011.00110111.00001111.11111110
131.55.15.254

زیرشبکه دوم:10000011.00110111.00010000.000000000

131.55.16.0

IP#1:10000011.00110111.00010000.00000001
131.55.16.1

IP#n:10000011.00110111.00010111.11111110
131.55.23.254

زیرشبکه سوم:10000011.00110111.00011000.000000000

131.55.24.0

IP#1:10000011.00110111.00011000.00000001
131.55.24.1

IP#n:10000011.00110111.00011111.11111110
131.55.31.254

جلسه ششم

تمرین)ID ی یک زیرشبکه 191.60.23.0 می باشد.

پنج زیرشبکه برای این شبکه طراحی کنید(Subnet Mask) را پیدا کنید و ID های زیرشبکه و اولین و آخرین IPهای قابل قبول در هر شبکه را ذکر کنید.

عدد زیر شبکه ها:$5 + 2 = 7$

تعداد بیت ها برای زیر شبکه ها:3 (111)

۳ بیت

10111111.00111100.00010111.00000000
191.60.23.0

11111111.11111111.11111111.11100000
255.255.255.224

زیرشبکه اول(ID#1):10111111. 00111100. 00010111.001000000

IP#1: 10111111. 00111100. 00010111.00100001
191.60.23.33

IP#n: 10111111. 00111100. 00010111.00111110
191.60.23.62

191.60.23.32

تازیرشبکه پنجم ادامه داده شود...

❖ درواقع ID داده شده در مثال مربوط به یک زیرشبکه است که خود به صورت سلسله مراتبی به زیرشبکه های دیگری تقسیم گردد.

تمرین)ID ی یک شبکه 54.0.0.0 می باشد.

سه زیرشبکه برای این شبکه طراحی کنید(Subnet Mask) را پیدا کنید و ID های زیرشبکه و اولین و آخرین IPهای قابل قبول در هر شبکه را ذکر کنید.

عدد زیر شبکه ها:$3 + 2 = 5$

تعداد بیت ها برای زیر شبکه ها:5 (101)

۳ بیت

00110110.00000000.00000000.00000000
54.0.0.0

Subnet Kask: 11111111.11100000.00000000.00000000
255.224.0.0

زیرشبکه اول(ID#1):00110110. 00100000. 00000000.000000000

IP#1: 00110110. 00100000.00000000.00000001
54.32.0.1

IP#n: 00110110. 00111111. 11111111.11111110
54.63.255.254

54.32.0.0

تازیرشبکه سوم ادامه داده شود...

جلسه هفتم

IP های Private :

IP های Private ، IP هایی هستند که در اینترنت رویت نمی شوند، در مقابل IP های Valid یا Public دسترسی و قابلیت رویت پذیری را درون اینترنت دارند و برای استفاده از آن ها باید جهت خریداریشان هزینه پرداخت کرد. جدول زیر گستره IP های Private را در سه کلاس A، B و C نمایش می دهد.

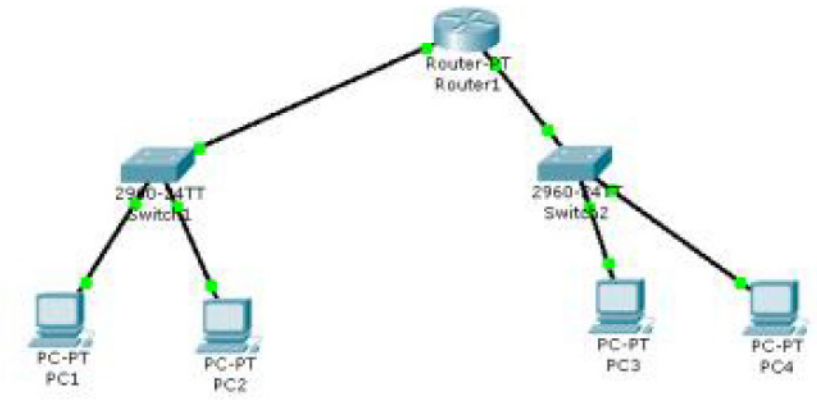
A Class	10.0.0.0→10.255.255.255
B Class	172.16.0.0→172.31.255.255
C Class	192.168.0.0→192.168.255.255

جدول ۶: جدول IP های Private

آشنایی با دستگاه‌های Cisco

مثال) مروری بر آدرس دهی و مسیر یابی

شبکه ای را با دو زیرشبکه که به کمک یک روتر زیرشبکه ها را به هم متصل می سازد، در نظر بگیرید شمایی از این شبکه در شکل زیر مشاهده می شود.



شکل ۱۵: شمایی از یک شبکه با دو زیرشبکه که با یک روتر به هم متصل شده اند

جواب)

ابتدا یک روتر از نوع عمومی[1] انتخاب کرده و در صفحه نرم افرار قرار می دهیم سپس جهت قرار دادن چهار کامپیوتر[2] در دو زیرشبکه که توانایی ارسال و دریافت مناسب اطلاعات را داشته باشند چهار کامپیوتر از نوار ابزار پایین برنامه انتخاب و به طرز مناسبی در صفحه قرار می دهیم. لازم به ذکر است می توان برای این کامپیوتر ها شماره نیز قرار داد که با کلیک کردن بر روی آیکون کامپیوتر مورد نظر می توان نام آن را تغییر داد. باید توجه داشت که روتر[3] یک مسیریاب بوده و نمی توان تعداد زیادی کامپیوتر یا دیگر ماشین ها را به وسیله یک روتر به

1-Generic
2-PC
1-Router

هم ارتباط داد برای این کار باید ما از یک سوییچ[1] استفاده کرد. در مثال فوق برای این منظور از یک سوییچ لایه دوم(2960-24TT) برای یکی از زیرشبکه ها و یک سوییچ مشابه برای زیرشبکه دیگر قرار می دهیم برای سوییچ ها نیز همانند کامپیو تر ها می توان به همان طریق شماره گذاری کرد. هر کدام از این سوییچ ها دارای ۲۴ عدد پورت Fast Ethernet و دو عدد پورت Gigabit Ethernet می باشد که با نگه داشتن ماوس بر روی آیکون سوییچ قابل مشاهده می باشد همچنین می توان جهت افزایش تعداد پورت ها، سوییچ ها را چندلایه نموده و تعداد بیشتری پورت در اختیار داشت . حال می توان از قسمت Connection Type بر روی گزینه کلیک کرده و هر بار یک ارتباط بین یک کامپیوتر با سوییچ برقرار کرد. بعد از مرتبط کردن تمام کامپیوتر ها با سوییچ ها از همان طریق ارتباط بین سوییچ ها و روتر را نیز برقرار می کنیم. در مرحله بعد باید برای هر کامپیوتر IP اختصاص دهیم برای این منظور بر روی آیکون PC کلیک کرده از پنجره باز شده بر روی گزینه Desktop کلیک می کنیم و سپس در این قسمت وارد بخش IP Configuration شده و در قسمت مخصوص به IP Address باید یک IP اختصاص دهیم که در اینجا 192.168.1.2[2] قرار می دهیم.

در اینجا با توجه به اینکه 192 و 168 ثابت می باشد می توانیم دو Octet دیگر را برای زیرشبکه و هاست استفاده کنیم. حال با توجه به اینکه این IP از کلاس C می باشد و ClassFull عمل می کنیم Subnet Mask به صورت 255.255.255.0 می باشد. که در این قسمت با ورود به این قسمت به صورت خودکار ثبت می شود. این عمل را برای تمام PC های این زیرشبکه به ترتیب با هاست های مختلف انجام می دهیم . برای اختصاص دادن IP به PC های موجود در زیرشبکه دیگر باید شماره زیرشبکه تغییر کند و در آن زیرشبکه به ترتیب هاست ها را برای هر PC تغییر دهیم به طور مثال برای اولین PC در این زیرشبکه از IPای 192.168.2.2 استفاده می کنیم. و Subnet Mask نیز مانند قبل انجام می گردد. حال باید روتر را نیز Config کنیم به این صورت که بر روی آیکون روتر کلیک می کنیم از پنجره باز شده بر روی قسمت Config کلیک کرده در قسمت Interface بر روی FastEthernet0/0 کلیک می کنیم برای فهمیدن این قسمت با نگه داشتن ماوس بر روی کانکشن سمت روتر fa0/0 ظاهر می شود. در این قسمت MAC Address به صورت یونیک بوده و در قسمت مربوطه ثبت شده است، قسمت بعدی مربوط به IP Address می باشد که در اینجا IP باید هم رنج و هم شبکه با IP های زیرشبکه ای باشد که به این Interface متصل شده است مثلاً در این مثال با توجه به یک IP ای که در ابتدای رنج خالی گذاشتیم IPای 192.168.1.1 را انتخاب می کنیم. Subnet Mask نیز به صورت خودکار با کلیک در قسمت مربوطه ثبت می شود و در نهایت Port Status را On می کنیم و خارج می شویم. حالا همین کار را برای Interface زیرشبکه دیگر انجام می دهیم اینبار بر روی FastEthernet1/0 کلیک می کنیم و مانند قبی عمل می کنیم.

در اینجا زمانی که بخواهیم اطلاعاتی را از یک PC در یک زیرشبکه به یک PC در یک زیرشبکه دیگر که توسط یک روتر به هم متصل هستند ارسال کنیم باید این اطلاعات را به یک مسیریاب پیش فرض[3] ارسال کنیم زیرا ما IPای تمام PC ها را نمی توانیم حفظ کنیم پس این کار را روتر برای ما انجام میدهد برای این منظور باید IPای برای روتر در نظر بگیریم که وقتی اطلاعات را برای آن IP ارسال می کنیم مانند این است که اطلاعات برای روتر ارسال می شود که به این IP مسیریاب پیش فرض یا Default Gateway گفته می شود که IPای که به این مسیریاب پیش فرض باید اختصاص دهیم همان IP پورتیست از روتر که شبکه به آن متصل است. برای این منظور مجدداً بر روی آیکون PC ها کلیک کرده و بر روی قسمت Desktop کلیک کرده به بخش IP Configuration رفته و در قسمت Default Gateway همان IPای FastEthernet را اختصاص می دهیم یعنی 192.168.1.1 و برای زیرشبکه دیگر 192.168.2.1 را اختصاص می دهیم . این IP ها را

2-Switch

۲ -علت استفاده از این IP این است که می خواهیم شبکه ای ایجاد کنیم که در اینترنت نیست و این IP ها به IP های Private می گوییم. این IP ها دارای رنجی مشخص می باشند که قبلاً توضیح داده شده است. که شبکه هایی که در اینترنت نیستند بتوانند از این رنج IP استفاده کنند. IP های دیگر که در اینترنت نیز وجود داند به IP های Public معروفند که به آن ها IP های Valid نیز می گویند (IP Valid).

4-Default Gateway

برای تمام PC ها در زیرشبکه مربوطه در بخش Default Gateway ثبت می کنیم. حالا برای تست شبکه یا از طریق نوار ابزار سمت راست بر روی آیکون پاکت نامه کلیک می کنیم و بر روی PCی مبدا و مقصد کلیک می کنیم در صورت صحیح بودن مسیر پیغام Successful ظاهر می شود، یا از طریق Ping کردن به این صورت که بر روی PC مبدا کلیک کرده و در قسمت Command Prompt دستور Ping را به صورت "Ping 192.168.1.3" تایپ می کنیم در صورت صحیح بودن مسیر پیغام "Reply From 192.168.1.3 ..." را خواهیم دید و مشاهده پیغام "Time Out" به معنی عدم ارتباط صحیح می باشد، استفاده می کنیم.

نکات مهم:

زمانی که بر روی آیکون روتر کلیک می کنیم در پنجره باز شده قسمتی به نام CLI[1] وجود دارد که اعمالی که در قسمت Config به صورت دستی انجان دادیم می توانیم در این قسمت به صورت دستوری انجان دهیم. زمانی که به این قسمت وارد می شویم یک Command Prompt به صورت > وجود دارد که این حالت بیانگر قرار گرفتن در سطح کاربر می باشد در حالی که برای انجام دادن Config می بایست در سطح Admin قرار بگیریم برای این منظور از دستور "Enable" استفاده می کنیم. با نوشتن کلمه enable و زدن دکمه Enter علامت از حالت ">" به حالت "#" در می آید و این یعنی ما در وضعیت Admin قرار گرفته ایم. از جمله دستورات مهم در این بخش نمایش جدول مسیریابی[2] می باشد به این صورت که دستور "show ip rout" را در این قسمت تایپ کرده و Enter می زنیم. لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول مسیریابی می باشد. توضیح دو خط انتهایی آن که با حرف C شروع شده اند و در مثال قبل به صورت زیر می باشد:

C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet1/0

در خط اول "192.168.1.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه اول می باشد که به صورت مستقیم و از طریق FastEthernet0/0 وصل می باشد.

در خط دوم "192.168.2.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه دوم می باشد که به صورت مستقیم و از طریق FastEthernet1/0 وصل می باشد.

در اینجا IPهایی که FastEthernet0/0 و FastEthernet1/0 گرفته اند به عنوان Defult Gateway برای این دو شبکه در نظر گرفته می شود.

نکته: معنی اعداد مقابل FastEthernet

0/0 به معنی پورت یا Interface یا واسط FastEthernet شماره 0 از Slot شماره 0 روتر.

1/0 به معنی پورت یا Interface یا واسط FastEthernet شماره 1 از Slot شماره 0 روتر.

1-Command Line Interface
2-Routing Table

اجزا و قالب بندی شبکه فوق در جدول زیر مشاهده می شود.

	Device	IP Address	Subnet Mask	Gateway
Subnet#1	PC 1	192.168.1.2	255.255.255.0	**192.168.1.1**
	PC 2	192.168.1.3	255.255.255.0	**192.168.1.1**
Subnet#2	PC 3	192.168.2.2	255.255.255.0	**192.168.2.1**
	PC 4	192.168.2.3	255.255.255.0	**192.168.2.1**
Router	Fast Ethernet0/0	192.168.1.1	255.255.255.0	----------
	Fast Ethernet1/0	192.168.2.1	255.255.255.0	----------

جدول ۷: اجزاء و قالب بندی شبکه برای مثال بالا

❖ در جدول فوق برخی از موارد نیاز به توضیح دارند.

۱- Defult Getway : IP مسیر یاب پیش فرض است که برای یک زیر شبکه همان آدرس IP ای خواهد بود که به پورت روتر، متصل به همان زیرشبکه اختصاص یافته است.

۲- Fast Ethernet: نام و نوع پورت روتر را معلوم می سازد.انواع محتلفی از پورت ها روی روتر هستند که ویژگی هایشان با هم متفاوت است. یکی از این ویژگی ها نرخ ارسال و دریافت می باشد. دیگر پورت های معروف روی روتر موارد Serial و Gigabit Ethernet می باشند. ضمناً این پورت ها اصطلاحاً به Inter Face یا واسط روتر معروفند. اعدادی که در جلوی نام آن ها ذکر می شوند به صوذت زیر تفسیر می گردند.

شماره اسلات ⟵ X/Y ⟵ شماره پورت

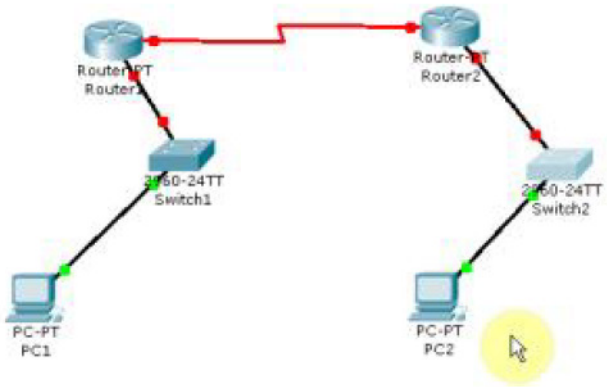
اگر به جدول مسیریابی(Routing Table) روتر این شبکه نگاه کنید رکورد های زیر را خواهیم یافت.

نشانگر	شبکه	دسترسی	نوع واسط
C	192.168.1.0	Directly	**Fast Ethernet0/0**
C	192.168.2.0	Directly	**Fast Ethernet1/0**

جدول ۸: رکوردهای مربوط به جدول مسیریابی روتر در این شبکه

مثال ۲)

شبکه ای را با دو زیرشبکه که به کمک ۲ روتر زیرشبکه ها را به هم متصل می سازد، در نظر بگیرید شمایی از این شبکه در شکل زیر مشاهده می شود.



شکل ۱۶: شمایی از یک شبکه با دو زیرشبکه که با ۲ روتر به هم متصل شده اند

جواب:

در این مثال به دلیل وجود دو روتر مسالهٔ تبادل اطلاعات و اینکه این روتر ها باید از شبکه های یکدیگر شناخت داشته باشند اهمیت پیدا می کند. در چنین مواردی باید از Static Routing یا Dynamic Routing استفاده کنیم زیرا ممکن است شبکه ها به جای دو زیرشبکه، دو شبکه مجزا با دو رنج IP متفاوت باشند.

در این مثال نیز جهت انجام تنظیمات تا قبل از دو روتر دقیقاً مانند مثال قبل عمل می کنیم نکته مهم ارتباط دو روتر با هم و شناساندن دو شبکه به روتر هاست.

در اینجا نوع اتصال دو روتر همانطور که در شکل بالا مشاهده می کنید با بقیه اتصال ها متفاوت است زیرا دو روتر به صورت پیش فرض به جای پورت FastEthernet با پورت Serial به هم متصل می گردند.

در این مثال ما برای اینکه دو شبکه مجزا داشته باشیم قرار داد می کنیم:

Network ID شبکه اول از رنج ۱ تا ۷ با Host ID های متفاوت

Network ID شبکه دوم از رنج ۸ تا ۱۵ با Host ID های متفاوت

در انتها یک Network ID با شماره ۱۶ برای ارتباط بین دو روتر درنظر می گیریم.

حال برای ست کردن ارتباط بین روترها ابتدا با نگه داشتن ماوس بر روی کانکشن بین دو روتر شماره Serial نمایش داده می شود که در اینجا se2/0 برای هر دو روتر نشان داده می شود. پس بر روی روتر اول(سمت چپ) کلیک کرده در بخش Config بر روی منوی Serial2/0 کلیک می کنیم. باید توجه داشت که ارتباط بین دو روتر را باید همانند یک زیرشبکه با یک رنج IP جداگانه در نظر گرفت، در این مثال .حالا برای قسمت IP Address با توجه به اینکه برای Network ID ها رنج ۱ تا ۱۵ را درنظر گرفتیم برای این IP رنج ۱۶ را در نظر می گیریم زیرا IP این قسمت باید خارج از رنج IP ی دو شبکه باشد باشد و نمی توان از رنج IPای شبکه هایشان استفاده کرد زیرا این دو روتر از طریق Gateway های خودشان به هم متصل شده و یک مسیر فراهم می کنند برای رسیدن به آن شبکه پس رنج IP باید خارج از رنج دو شبکه باشد پس مسیری که مابین دو روتر قرار دارد شبیه به یک زیرشبکه عمل می کند و باید برای خود یک رنج IP جداگانه داشته باشد. پس:

IP Address : 192.168.16.1
Subnet Mask: 255.255.255.0

می شود سپس Port Status را On کرده و Clock Rate[1] را انتخاب می کنیم.

بعد از پایان تنظیمات روتر اول، باید به همین ترتیب تنظیمات روتر دوم(سمت راست) را نیز انجام دهیم. پس:

IP Address : 192.168.16.2
Subnet Mask: 255.255.255.0

نکته: علت "۲" شدن Host IDی IP Address مربوط به روتر دوم این است که شماره ۱ را برای سمت روتر دیگر استفاده کردیم.

نکته: جهت مشاهده جدول مسیریابی در این مثال بر روی آیکون روتر کلیک کرده به CLI رفته Enter می کنیم. اگر در این بخش در مقابل کلمهٔ روتر چیزی مشاهده کردیم بدین معناست که ما در سطوح بالاتری قرار گرفته ایم و برای رفتن به یک سطح پایین تر دستور "exit" را تایپ کرده و Enter را می زنیم با این کار به سطح پایین تر رفته و این کار را تا زمان رسیدن به سطح روتر ادامه می دهیم. حالا در این سطح دستور و در مقابل Router# دستور "show ip rout" را تایپ کرده Enter را می زنیم. با اجرای این دستور لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول مسیریابی می باشد. توضیح دو خط انتهایی آن که با حرف C شروع شده اند و در مثال قبل به صورت زیر می باشد:

---

۱ – یعنی نرخ تبادل داده ای که بین دو روتر رد و بدل می شود. برای تنظیم مناسب این بخش لازم است که عدد ماکسیمم Clock Rate دو روتر را مشاهده کرده و از میان این دو عدد کمترین مقدار را به عنوان Clock Rate انتخاب می کنیم.

C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.16.0/24 is directly connected, Serial2/0

در اینجا شبکهٔ 192.168.1.0 و شبکه 192.168.16.0 شناخته شده است ولی هنوز شبکهٔ 192.168.8.0 شناخته نشده است پس کار در اینجا به پایان نرسیده است و باید به دلیل اینکه Static Routing قرار است انجام پذیرد باید و Routing Table می بایست توسط Admin شبکه کامل شده و اطلاعات شبکه های دیگر در جدول مسیریابی هر روتر ذخیره گردد. این کار را هم از طریق منوی Config می توانیم انجام دهیم و هم از طریق دستورات مربوطه در بخش CLI .

(از طریق منوی Config) می خواهیم شبکه 192.168.8.0 را معرفی کنیم پس در حالی که در منوی روتر سمت چپ(192.168.1.0) هستیم به قسمت Config رفته در زیر بخشRouting بر روی Static کلیک کرده و بخش های مربوطه را به این صورت تکمیل می کنیم:

Network: 192.168.8.0
Mask: 255.255.255.0
Next Hop[1]: 192.168.16.2

سپس بر روی Add کلیک می کنیم. مجدداً به بخش CLI رفته و به سطح روتر می رویم، دستور "show ip rout" را تایپ کرده Enter می زنیم. این بار با اجرای این دستور لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول جدید مسیریابی می باشد.

توضیح سه خط انتهایی آن که با حرف C و S شروع شده اند و در مثال قبل به صورت زیر می باشد:

C 192.168.1.0/24 is directly connected, FastEthernet0/0
S 192.168.8.0/24 [1/0] Via 192.168.16.2
C 192.168.16.0/24 is directly connected, Serial2/0

در خط اول "192.168.1.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه/شبکه اول می باشد که به صورت مستقیم و از طریق FastEthernet0/0 وصل می باشد.

در خط دوم "192.168.8.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه/شبکه دوم می باشد که از طریق IPای 192.168.16.2وصل می باشد.

در خط سوم "192.168.16.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه سوم(مسیری که توسط کانکشن Serial بین دو روتر بوجود آمده) می باشد که به صورت مستقیم و از طریق Serial2/0 وصل می باشد.

اگر به جدول مسیریابی(Routing Table) روتر این شبکه نگاه کنید رکورد های زیر را خواهیم یافت.

نشانگر	شبکه	دسترسی	نوع واسط
C	192.168.1.0	Directly	**Fast Ethernet0/0**
S	192.168.8.0	Via 192.168.16.2	----------
C	192.168.16.0	Directly	**Serial2/0**

جدول ۹: رکوردهای مربوط به جدول مسیریابی روتر در این شبکه

۱ ـ Gateway ایست که با پورت سریال معین کرده ایم. در اینجا IP Address ای که برای سمت مقابل پورت Serial در روتر مقابل تعریف کردیم یعنی 192.168.16.2

برای تنظیم روتر دوم(سمت راست) و از طریق دستوری می خواهیم شبکه 192.168.1.0 را معرفی کنیم پس در حالی که در منوی روتر سمت راست(192.168.8.0) هستیم به قسمت CLI می رویم. باید توجه داشت که برای تنظیم روتر از طریق دستوری باید در سطح Config قرار بگیریم، اگر در سطوح بالاتر قرار داشتیم با تکرا دستور "exit" به سطح Config می رسیم ولی اگر در سطح پایین تر قرار داشتیم برای رفتن به سطح Config، از دستور "config t" استفاده می کنیم و حالا در سطح Config این دستور را تایپ می کنیم :

Router(Config)#ip rout 192.168.1.0 255.255.255.0 Via 192.168.16.1

سپس Enter می زنیم و پس از رفتن به سطح روتر دستور مشاهده جدول مسیریابی را اجرا می کنیم.

این بار با اجرای این دستور لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول جدید مسیریابی می باشد. توضیح سه خط انتهایی آن که با حرف C و S شروع شده اند و در مثال قبل به صورت زیر می باشد:

```
S    192.168.1.0/24  [1/0]  Via 192.168.16.1
C    192.168.8.0/24 is directly connected, FastEthernet0/0
C    192.168.16.0/24 is directly connected, Serial2/0
```

در خط اول "192.168.1.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه/شبکه اول(مقابل) می باشد که از طریق IPای 192.168.16.1وصل می باشد.

در خط دوم "192.168.8.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه/شبکه دوم(شبکه روتر جاری) می باشد که به صورت مستقیم و از طریق FastEthernet0/0 وصل می باشد.

در خط سوم "192.168.16.0" که در انتهای این IP عدد 0 وجود دارد بیانگر مشخصه زیرشبکه سوم(مسیری که توسط کانکشن Serial بین دو روتر بوجود آمده) می باشد که به صورت مستقیم و از طریق Serial2/0 وصل می باشد.

حالا تمام ارتباط ها بین شبکه ها برقرار بوده و این همان Static Routing می باشد و Routing Tableها از طریق Admin شبکه معرفی شد و می توانیم از این شبک ها تست بگیریم.

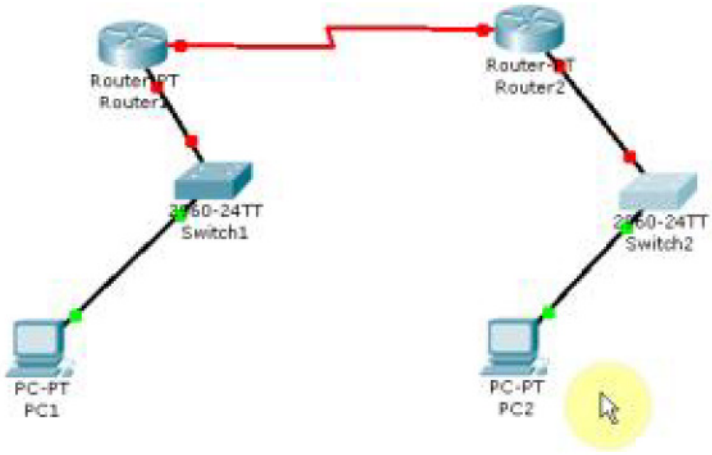
اگر به جدول مسیریابی(Routing Table) روتر این شبکه نگاه کنید رکورد های زیر را خواهیم یافت.

نشانگر	شبکه	دسترسی	نوع واسط
S	192.168.1.0	Via192.168.16.1	----------
C	192.168.8.0	Directly	**Fast Ethernet0/0**
C	192.168.16.0	Directly	**Serial2/0**

جدول ۱۰: رکوردهای مربوط به جدول مسیریابی روتر در این شبکه

مسیریابی ایستا (Stating Routing)

در این مثال مطابق شرحی که قبلاً برای مسیر یابی استاتیک ذکر کردیم دو شبکه متفاوت را با استفاده از دو روتر (یکی برای هر کدام) به هم متصل می سازیم شمایی از این شبکه ها و اتصال بین آنها در شکل زیر قابل مشاهده است.



شکل ۱۷: شکل مربوط به مثال فوق

در ارتباط با شکل فوق تنظیمات جدول زیر می تواند بر قرار گردد.

Device	InterFace	IP Address	Subnet Mask	Default Gateway
PC 1		192.168.1.2	255.255.255.0	**192.168.1.1**
PC 2		192.168.8.2	255.255.255.0	**192.168.8.1**
Router#1	Serial2/0	192.168.16.1	255.255.255.0	----------
	Fast Ethernet0/0	192.168.1.1	255.255.255.0	----------
Router#2	Serial2/0	192.168.16.2	255.255.255.0	----------
	Fast Ethernet0/0	192.168.8.1	255.255.255.0	----------

جدول ۱۱: اجزاء و قالب بندی شبکه برای مثال بالا

در توضیح جدول فوق داریم:

Serial InterFace : پورتی است از روتر که از آن برای اتصال به روتر دیگر استفاده می شود IP آدرسی که به این پورت ها اختصاص می یابد برای هر دو روتر از یک Subnet ID است(مثلاً در شبکه فوق 16 می باشد) در ضمن برای پورت های Serial می باید Clock Rate (نرخ انتقال در زمان تعیین کرد به این صورت که حداکثر Clock Rate دو روتر را پیدا می کنیم و از این دو، آن را که کمتر باشد انتخاب می نماییم و برای هر دو روتر در نظر می گیریم)

مسیریابی پویا(Dynamic Routing)

در این مثال سعی می کنیم تا همان شبکه مثال قبل را با استفاده از مسیر یابی پویا به صورتی که قبلاً شرح داده شد به کمک یکی از پروتکل های مربوطه توسعه دهیم. پروتکلی که استفاده خواهیم کرد پروتوکل RIP است که به معنای Routing Information Protocol می باشد. این پروتکل دارای دو نسخه است که هر دو نسخه از الگوریتم مسیریابی Distance Vector سود می برند.

RIP Ver 1

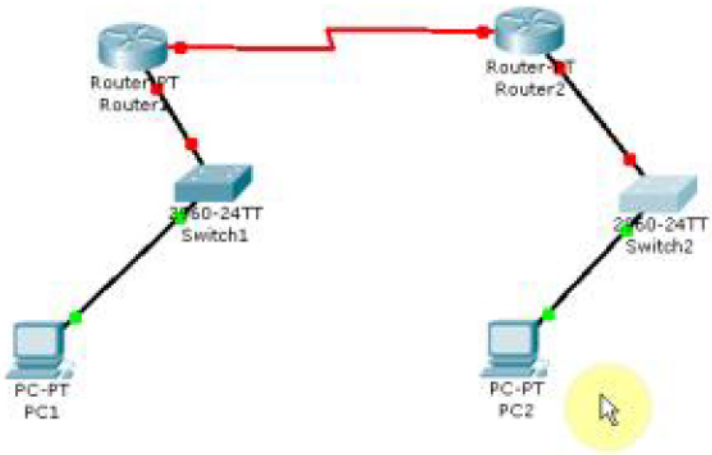
این نسخه جهت به روز رسانی جدول مسیریابی بین روتر های شبکه از پیام های **Broadcast** استفاده می کند. و هر ۳۰ ثانیه یکبار کل جدول مسیریابی را از طریق **InterFace** های فعال منتشر می سازد این پروتکل به صورت **ClassFull** عمل می کند.

RIP Ver 2

این نسخه پیام ها را به صورت **Multi Tasking** رد و بدل می سازد. اما قابلیت کار به صورت **Broadcasting** را نیز دارد. یک پروتکل **ClassLess** است. همچنین قابلیت **Authentication** یا احراز هویت را پشتیبانی می کند که این توانمندی باعث می شود روتر ها قبل از رد و بدل کردن جدول های مسیریابی، یکدیگر را احراز هویت نمایند.

مثال)

در این مثال دو شبکه متفاوت را با استفاده از دو روتر (یکی برای هر کدام) به هم متصل می سازیم شمایی از این شبکه ها و اتصال بین آنها در شکل زیر قابل مشاهده است.



شکل ۱۸: دو شبکه مجزا متشکل از دو سوییچ و دو روتر و تعدادی کامپیوتر

جواب:

برای حل این مثال تمام تنظیمات همانند مسیریابی استاتیک انجام می گیرد با این تفاوت که تنها در هنگام معرفی شبکه ها به یکدیگر مانند روش استاتیک به صورت دستی و توسط ادمین شبکه انجام نمی پذیرد بلکه اینبار با معرفی شبکه های متصل به هر روتر به روتر جاری کار ارتباط بین دو روتر توسط خود روتر و به صورت پویا و به شکلی که در بالا توضیح داده شد انجام می گیرد.

برای این منظور و به صورت موردی در این مثال تنظیمات را انجام می دهیم:

بر روی روتر سمت چپ کلیک کرده در بخش **Config** و در قسمت **Routing** بر روی **RIP** کلیک کرده و در قسمت **Network** مشخصه های شبکه های متصل به این روتر را نوشته و **Add** می کنیم و همین کار را برای روتر سمت راست نیز تکرار می کنیم.

روتر سمت چپ:

Network	192.168.1.0	→	Add
Network	192.168.16.0	→	Add

روتر سمت راست:

Network 192.168.8.0 → Add

Network 192.168.16.0 → Add

لازم به ذکر است این کار را به صورت دستوری نیز می توانیم انجام دهیم به این صورت که بر روی روتر سمت راست کلیک کرده و در بخش CLI و در سطح Config Routre مشخصه های شبکه های متصل به این روتر را با دستور "Network" می نویسیم همین کار را برای روتر سمت راست نیز انجام می دهیم به این صورت :

روتر سمت چپ:

```
Router(Config Router)#network 192.168.1.0    Enter
Router(Config Router)#network 192.168.16.0   Enter
```

روتر سمت راست:

```
Router(Config Router)#network 192.168.8.0    Enter
Router(Config Router)#network 192.168.16.0   Enter
```

پس از رفتن به سطح روتر دستور مشاهده جدول مسیریابی را اجرا می کنیم.

روتر سمت چپ:

با اجرای این دستور لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول مسیریابی می باشد. سه خط انتهایی آن که با حروف C و R شروع شده اند و در مثال قبل به صورت زیر می باشد:

```
C   192.168.1.0/24 is directly connected, FastEthernet0/0
R   192.168.8.0/24 [120/1] via 192.168.16.2, 00:00:25, Serial2/0
C   192.168.16.0/24 is directly connected, Serial2/0
```

روتر سمت راست:

با اجرای این دستور لیستی در زیر دستور نمایش داده می شود که نمایانگر جدول مسیریابی می باشد. سه خط انتهایی آن که با حرف C و R شروع شده اند و در مثال قبل به صورت زیر می باشد:

```
R   192.168.1.0/24 [120/1] via 192.168.16.1, 00:00:19, Serial2/0
C   192.168.8.0/24 is directly connected, FastEthernet0/0
C   192.168.16.0/24 is directly connected, Serial2/0
```

حالا تمام ارتباط ها بین شبکه ها برقرار بوده و این همان Dynamic Routing می باشد و Routing Tableها به صورت پویا توسط خود روتر به یکدیگر همانگونه که گفته شد معرفی می گردند و می توانیم از این شبک ها تست بگیریم.

جلسه نهم

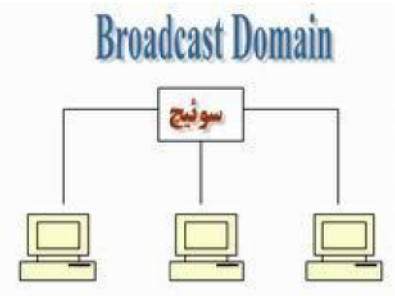
مطالب ارائه شده در زیر صرفاً توضیحات تکمیلی بوده و جهت روشن تر شدن و قابل درک تر شدن موضوع می باشد و به عنوان جزوه در کلاس ارائه نشده است.از اینجا...

معرفی شبکه های مجازی VLAN

VLAN (Virtual Local Area Networks) ، یکی از جدیدترین و جالبترین تکنولوژی های شبکه است که اخیراً مورد توجه بیشتری قرار گرفته است. رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گران قیمت بدون از دست دادن کارآیی و امنیت ، اهمیت و ضرورت توجه بیشتر به VLAN را مضاعف نموده است .

وضعیت شبکه های فعلی

تقریباً در اکثر شبکه های امروزی از یک (و یا چندین) سوئیچ که تمامی گره های شبکه به آن متصل می گردند ، استفاده می شود . سوئیچ ها روشی مطمئن و سریع به منظور مبادله اطلاعات بین گره ها در یک شبکه را فراهم می نمایند. با این که سوئیچ ها برای انواع شبکه ها، گزینه ای مناسب می باشند ولی همزمان با رشد شبکه و افزایش تعداد ایستگاه ها و سرویس دهندگان، شاهد بروز مسائل خاصی خواهیم بود. سوئیچ ها دستگاه های لایه دوم (مدل مرجع OSI[1]) می باشند که یک شبکه Flat را ایجاد می نمایند .



شکل ۱۹: یک شبکه flat با استفاده از سوییچ لایه دوم

همانگونه که در شکل فوق مشاهده می نمائید، به یک سوئیچ، سه ایستگاه متصل شده است. ایستگاه های فوق قادر به ارتباط با یکدیگر بوده و هر یک به عنوان عضوی از یک Broadcast domain مشابه می باشند. بدین ترتیب، در صورتی که ایستگاهی یک پیام broadcast را ارسال نماید، سایر ایستگاههای متصل شده به سوئیچ نیز آن را دریافت خواهند داشت.

در یک شبکه کوچک، وجود پیام های Broadcast نمی تواند مشکل و یا مسئله قابل توجهی را ایجاد نماید، ولی در صورت رشد شبکه، وجود پیام های braodcast می تواند به یک مشکل اساسی و مهم تبدیل گردد. در چنین مواردی و در اغلب مواقع، سیلابی از اطلاعات بی ارزش بر روی شبکه در حال جابجائی بوده و عملاً از پهنای باند شبکه استفاده مطلوب نخواهد شد. تمامی ایستگاه های متصل شده به یک سوئیچ، پیام های Braodcast را دریافت می نمایند. چراکه تمامی آنان بخشی از یک Broadcast doamin مشابه می باشند.

در صورت افزایش تعداد سوئیچ ها و ایستگاه ها در یک شبکه، مشکل اشاره شده ملموس تر خواهد بود. همواره احتمال وجود پیام های Braodcast در یک شبکه وجود خواهد داشت.

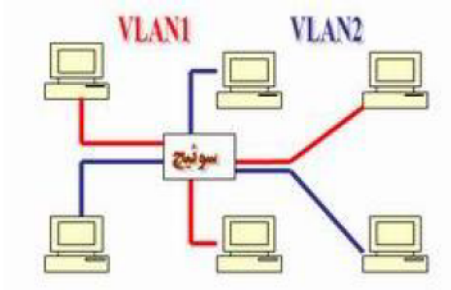
یکی دیگر از مسائل مهم، موضوع امنیت است. در شبکه هائی که با استفاده از سوئیچ ایجاد می گردند هر یک از کاربران شبکه قادر به مشاهده تمامی دستگاههای موجود در شبکه خواهند بود. در شبکه ای بزرگ که دارای سرویس دهندگان فایل، بانک های اطلاعاتی و سایر اطلاعات حساس و حیاتی است این موضوع می تواند امکان مشاهده تمامی دستگاههای موجود در شبکه را برای هر شخص فراهم نماید.

1- Open Systems Interconnection

بدین ترتیب منابع فوق در معرض تهدید و حملات بیشتری قرار خواهند گرفت. به منظور حفاظت اینچنین سیستم هایی می بایست محدودیت دستیابی را در سطح شبکه و با ایجاد سگمنت های متعدد و یا استقرار یک فایروال در جلوی هر یک از سیستم های حیاتی انجام داد.

معرفی VLAN

تمامی مسائل اشاره شده در بخش قبل را و تعداد بیشتری را که به آنان اشاره نشده است را می توان با ایجاد یک VLAN به فراموشی سپرد. به منظور ایجاد VLAN، به یک سوئیچ لایه دوم که این تکنولوژی را حمایت نماید نیاز می باشد. تعداد زیادی از افرادیکه جدیداً با دنیای شبکه آشنا شده اند، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفاً می بایست به منظور فعال نمودن VLAN، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند (برداشتی کاملاً اشتباه !). با توجه به این که در شبکه های VLAN، میلیون ها محاسبات ریاضی انجام می شود، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است، استفاده گردد (دقت در زمان تهیه یک سوئیچ)، در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده وجود نخواهد داشت. هر VLAN که بر روی سوئیچ ایجاد می گردد، به منزله یک شبکه مجزا می باشد. بدین ترتیب برای هر VLAN موجود یک broadcast domain جداگانه ایجاد می گردد. پیام های broadcast، به صورت پیش فرض از روی تمامی پورت هایی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند. ویژگی فوق، یکی از مهمترین دلایل متداول شدن VALN در شبکه های بزرگ امروزی است (تمایز بین سگمنت های شبکه). شکل زیر یک نمونه شبکه با دو VLAN را نشان می دهد :



شکل ۲۰: یک نمونه شبکه با دو VLAN(هر VLAN به منزله یک شبکه جداگانه)

در شکل فوق، یک شبکه کوچک با شش ایستگاه را که به یک سوئیچ (با قابلیت حمایت از VLAN) متصل شده اند مشاهده می نمائیم. با استفاده از پتانسیل VLAN سوئیچ، دو VLAN ایجاد شده است که به هر یک سه ایستگاه متصل شده است (VLAN1 و VLAN2). زمانی که ایستگاه شماره یک متعلق به VLAN1 ، یک پیام Braodcast را ارسال می نماید (نظیر : FF:FF:FF:FF:FF:FF)، سوئیچ موجود آن را صرفاً برای ایستگاه های شماره دو وسه فوروارد می نماید . در چنین مواردی سایر ایستگاههای متعلق به VLAN2، آگاهی لازم در خصوص پیام های broadcast ارسالی بر روی VLAN1 را پیدا نکرده و درگیر این موضوع نخواهند شد.

در حقیقت، سوئیچی که قادر به حمایت از VLAN می باشد، امکان پیاده سازی چندین شبکه مجزا را فراهم می نماید(مشابه داشتن دو سوئیچ جداگانه و اتصال سه ایستگاه به هر یک از آنان در مقابل استفاده از VLAN). بدین ترتیب شاهد کاهش چشمگیر هزینه های برپاسازی یک شبکه خواهیم بود.

فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمائیم. بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاه های مورد نظر به هر یک از آنان دوازده شبکه مجزا که امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم. یکی دیگر از روش های تامین خواسته فوق استفاده از VLAN است. بدین منظور می توان از یک و یا چندین سوئیچ که VLAN را

حمایت می نمایند، استفاده و دوازده VLAN را ایجاد نمود. بدیهی است هزینه برپاسازی چنین شبکه هایی به مراتب کمتر از حالتی است که از دوازده سوئیچ جداگانه ، استفاده شده باشد.

در زمان ایجاد VALN، می بایست تمامی ایستگاهها را به سوئیچ متصل و در ادامه ایستگاه های مرتبط با هر VLAN را مشخص نمود. هر سوئیچ در صورت حمایت از VLAN قادر به پشتیبانی از تعداد مشخصی VLAN است. مثلاً یک سوئیچ ممکن است ۶۴ و یا ۲۶۶ VLAN را حمایت نماید.

تا اینجا...

در این بخش به انواع قابلیت های کارگزاری شده در Switchها می پردازیم.

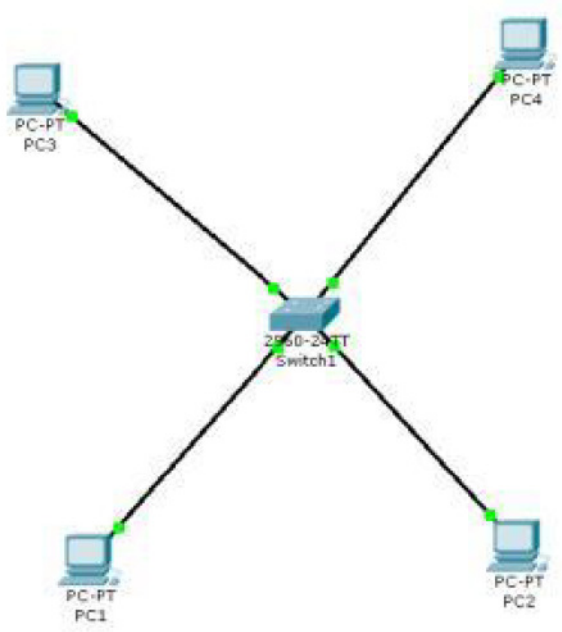
پیکربندی VLAN

VLAN برگرفته از عبارت(Virtual LAN) می باشد که یکی از توانمندی های مربوط به Switch است که امکان می دهد کامپیوترهای متصل به یک Switch یا چندین Switch، منطقاً در گروه های مجزاّ قرار گیرند. با این کار، ترافیک این گروه ها از هم جدا می شوند، به عبارت دیگر، هر گروه یا هر VLAN تبدیل به یک حوزهٔ Broadcast مجزاّ خواهد شد. در ادامه، چند مثال از مبحث VLANبازگو خواهد شد.

پیکربندی VLAN بر روی یک Switch

مثال)

می خواهیم شبکه ای(LAN) مانند شکل زیر ایجاد کنیم و با استفاده از تکنولوژی VLAN این شبکه را به صورت مجازی به دو شبکه مجزا تقسیم کنیم به گونه ای که هر بخش امکان دسترسی به بخش دیگر را نداشته باشد.



شکل ۲۱: شبکه ای شامل دو شبکه مجازی

جواب)

همانگونه که در قبل آموختیم یک سوییچ لایه دوم انتخاب کرده و ۴ عدد کامپیوتر را به این سوییچ متصل می کنیم. سپس همانند زیر به این کامپیوتر ها با توجه به عدم حضور روتر IP اختصاص می دهیم:

PC1 { IP Address: 192.168.1.1
Subnet Mask:255.255.255.0

PC2 { IP Address: 192.168.1.2
Subnet Mask:255.255.255.0

PC3 { IP Address: 192.168.1.3
Subnet Mask:255.255.255.0

PC4 { IP Address: 192.168.1.4
Subnet Mask:255.255.255.0

حالا شبکه ای ایجاد شده است که تمامی سیستم ها به دلیل وجود سوییچ با یکدیگر ارتباط دارند. حال برای اینکه بخواهیم شبکه را به دو بخش به دلیل مسائلی که قبلاً اشاره شد تقسیم کنیم و اصطلاحاً شبکه های مجازی(VLAN) ایجاد کنیم به روش زیر عمل می کنیم.

بر روی سوییچ کلیک کرده و به قسمت CLI می رویم به سطح ادمین رفته(با دستور Enable) و در اینجا با وارد کردن دستور "Show VLAN" اطلاعاتی نمایش داده می شود که نمایانگر وجود یک VLAN با نام Default بوده و تمام پورت های این سوییچ در این VLAN قرار دارد و تمامی پورت های آن در این شبکه قرار دارد.

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
 --More--
```

جهت اضافه نمودن VLAN ها به این شبکه به صورت دستوری به این صورت عمل می کنیم.

```
Switch#
Switch#Config t
Switch(Config)#VLAN 2
Switch(Config-VLAN)#
```

در اینجا VLAN ساخته شده و وارد سطح تنظیمات VLAN می شود برای خروج و ایجاد VLAN بعدی:

```
Switch(Config-VLAN)#Exit
Switch(Config)#VLAN 3
Switch(Config-VLAN)#
```

با این کار VLAN دوم نیز ساخته شده است. حال مجدداً برای دیدن VLAN ها :

```
Switch(Config-VLAN)#Exit
Switch(Config)# Exit
Switch#Show VLAN
```

با اجرای این دستور لیست زیر نمایش داده می شود:

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
2    VLAN0002                          active
3    VLAN0003                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
 --More--
```

در اینجا مشاهده می گردد که دو VLAN جدید به لیست ما اضافه شده است اما هنوز هیچ پورتی در این VLAN ها قرار ندارد برای اضافه کردن این پورت ها باید به سطح Config پورت مربوطه رفته و پورت ها را به VLAN مورد نظر اضافه کنیم برای این منظور:

Fa0/1 → VLAN 2

```
Switch#Config t
```
ورود به سطح config

```
Switch(config)#interface fastEthernet 0/1
```
ورود به سطح پورت مربوطه

```
Switch(config-if)# switchport access vlan 2
```
افزودن به VLAN مورد نظر

```
Switch(config-if)#Exit
```
بازگشت به سطح Config

Fa0/2 → VLAN 2

```
Switch(config)#interface fastEthernet 0/2
```
ورود به سطح پورت مربوطه

```
Switch(config-if)# switchport access vlan 2
```
افزودن به VLAN مورد نظر

```
Switch(config-if)#Exit
```
بازگشت به سطح Config

Fa0/3 → VLAN 3

```
Switch(config)#interface fastEthernet 0/3
```
ورود به سطح پورت مربوطه

```
Switch(config-if)# switchport access vlan 3
```
افزودن به VLAN مورد نظر

```
Switch(config-if)#Exit
```
بازگشت به سطح Config

Fa0/4 → VLAN 3

```
Switch(config)#interface fastEthernet 0/4
```
ورود به سطح پورت مربوطه

```
Switch(config-if)# switchport access vlan 3
```
افزودن به VLAN مورد نظر

```
Switch(config-if)#Exit
```
بازگشت به سطح Config

```
Switch(config)# Exit
```
بازگشت به سطح Switch

```
Switch#Show VLAN
```
اجرای دستور مقابل جهت مشاهده لیست VLAN ها

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
2    VLAN0002                          active    Fa0/1, Fa0/2
3    VLAN0003                          active    Fa0/3, Fa0/4
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

اکنون Fa0/1 و Fa0/2 در VLAN 2 و Fa0/3 و Fa0/4 در VLAN 3 قرار گرفته اند و دو شبکه مجازی هر کدام با دو سیستم به وجود آورده ایم به صورتی که هر شبکه مجازی به صورت مجزا عمل می کند.

Device		ID	VLAN- Speciation
PC#1		192.168.1.1	#2
PC#2		192.168.1.2	#3
PC#3		192.168.1.3	#2
PC#4		192.168.1.4	#3
Switch	Interface FA 0/1	-	#2 (Access)
	Interface FA 0/2	-	Access
	Interface FA 0/3	-	Access
	Interface FA 0/4	-	Access

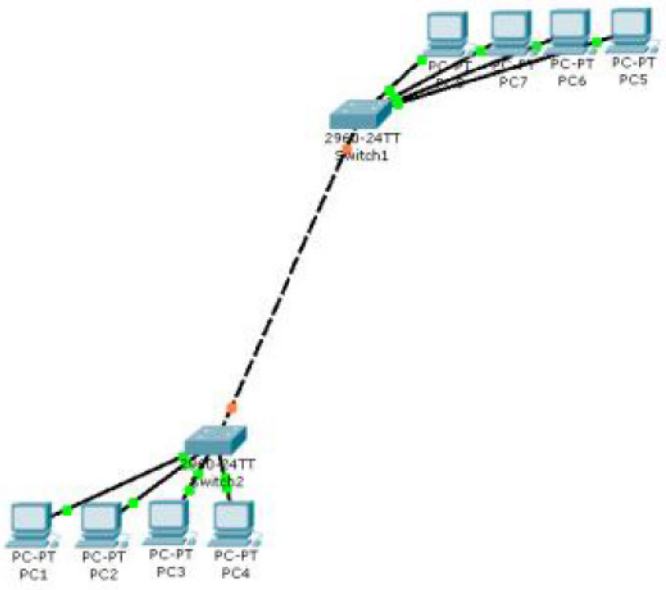
شکل ۲۲: اطلاعاتِ این مثال در جدول فوق قابل مشاهده است

در توضیح جدول فوق، باید گفت که دو گروه مجزّا، به‌صورت VLAN#2 و VLAN#3 مشاهده می‌شوند. این‌ها همان LANهای مجازی هستند، که به VLANهای سوئیچ افزوده شده‌اند. علت آن‌که شماره از ۲ آغاز می‌شود این است که هر سوئیچ، یک VLAN پیش‌فرض با نام Default و شمارهٔ ۱ دارد که در ابتدا همهٔ Interfaceهای سوئیچ در آن قرار دارند.

پیکربندی VLAN بر روی چندین Switch

مثال)

می خواهیم شبکه ای(LAN) مانند شکل زیر با تعداد ۸ عدد کامپیوتر و این بار با ۲ عدد سوییچ ایجاد کنیم و با استفاده از تکنولوژی VLAN این شبکه را به صورت مجازی به دو شبکه مجزا تقسیم کنیم به گونه ای که هر بخش امکان دسترسی به بخش دیگر را نداشته باشد.



شکل ۲۲: نمایی از این مثال در شکل فوق مشاهده می گردد

جواب)

همانگونه که از قبل آموختیم این بار ۲ سوییچ لایه دوم انتخاب کرده و ۸ عدد کامپیوتر را همانند شکل بالا به این سوییچ ها متصل می کنیم. می خواهیم کامپیوتر های PC01 و PC02 و PC05 و PC06 را در یک شبکه قرار دهیم پس برای این منظور در IPای این PCها برای بخش Subnet عدد 1 را در نظر می گیریم و کامپیوتر های PC03 و PC04 و PC07 و PC08 را در شبکه ای دیگر قرار دهیم پس برای این منظور در IPای این PCها برای بخش Subnet عدد 2 را در نظر می گیریم سپس همانند زیر به این کامپیوتر ها با توجه به عدم حضور روتر IP اختصاص می دهیم:

PC1
IP Address: 192.168.1.1
Subnet Mask:255.255.255.0

PC2
IP Address: 192.168.1.2
Subnet Mask:255.255.255.0

PC3
IP Address: 192.168.2.1
Subnet Mask:255.255.255.0

PC4
IP Address: 192.168.2.2
Subnet Mask:255.255.255.0

PC5
IP Address: 192.168.1.3
Subnet Mask:255.255.255.0

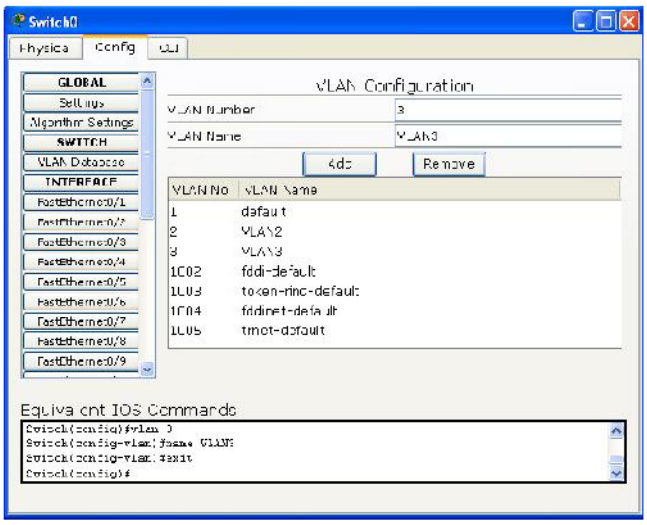
PC6
IP Address: 192.168.1.4
Subnet Mask:255.255.255.0

PC7
IP Address: 192.168.2.3
Subnet Mask:255.255.255.0

PC8
IP Address: 192.168.2.4
Subnet Mask:255.255.255.0

نکته: باید توجه داشت که سیستم هایی که می خواهیم در یک VLAN قرار داشته باشند باید دارای رنج IP یکسانی باشند در غیر این صورت باید درون آن VLAN یک روتر داشته باشیم.

پس از تنظیم IP برای کامپیوتر ها باید تنظیمات را بر روی سوییچ ها انجام دهیم. این بار برای آشنایی بیشتر به جای حالت دستوری از قسمت CLI با حالت تنظیم ویزاردی بر روی سوییچ اول کلیک کرده به محیط Config می رویم و در قسمت SWITCH در بخش VLAN Database کافیست شماره VLAN مورد نظر-در این مثال 2 -را نوشته و بر روی دکمه Add کلیک کنیم خواهیم دید که قسمت نام VLAN به صورت خودکار "VLAN 2" شده و در باکس زیر مشخصات این VLAN اضافه می گردد همین کار را برای VLAN بعدی-در این مثال 3 - نیز انجام می دهیم و در نهایت شماره و نام هر دو VLAN در باکس زیر نمایش داده می شود.



شکل ۲۳: نمایش VLANهای ایجاد شده در سوییچ

حالا برای قرار دادن کامپیوترها در این VLANها باید در قسمت INTERFACE در همین محیط FastEthernetهای متصل به این سوییچ یعنی Fa0/1 و Fa0/2 و Fa0/3 و Fa0/4 را درون VLAN های مربوطه قرار دهیم برای این منظور بر روی هر FastEthernet کلیک می کنیم و شماره VLAN مربوطه را انتخاب می کنیم، به صورت زیر:

FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 2
FastEthernet0/3→VLAN 3
FastEthernet0/4→VLAN 3

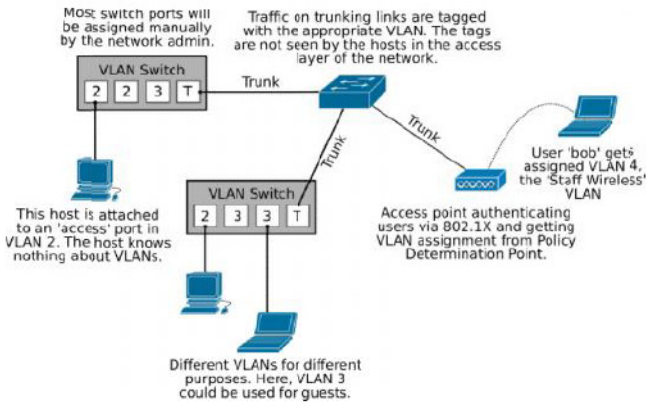
همین کار را برای سوییچ بعدی نیز انجام می دهیم و پس از معرفی VLANها به سوییچ برای قرار دادن کامپیوترها در این VLANها باید در قسمت INTERFACE در همین محیط FastEthernetهای متصل به این سوییچ یعنی Fa0/5 و Fa0/6 و Fa0/7 و Fa0/8 را نیز درون VLAN های مربوطه قرار دهیم برای این منظور همانند قبل بر روی هر FastEthernet کلیک می کنیم و شماره VLAN مربوطه را انتخاب می کنیم، به صورت زیر:

FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 2
FastEthernet0/3→VLAN 3
FastEthernet0/4→VLAN 3

اکنون با تنظیم موارد بالا هنوز امکان انتقال اطلاعات بین شبکه ها وجود ندارد زیرا هنوز تنظیمات لازم بر روی پورت های بین سوییچ ها انجام نشده است. برای تنظیم این پورت ابتدا به توضیح مختصری در باره Trunking می پردازیم.از اینجا...

Trunking

ترانکینگ تکنولوژیی است که به اطلاعاتِ از VLANهای مختلف اجازه حمل شدن تنها از طریق یک لینک میان سوئیچها را خواهد داد. این بدین معناست که زمانی که VLAN در شبکه هایی که با چندین سوییچ به هم متصل شده اند استفاده شود، برای بخش های بین سوییچ ها بایستی که از VLAN Trunking استفاده کنیم یا به عبارت ساده تر وقتی روی سوییچ ها VLAN تعریف می کنیم، سوییچ ها را از طریق ترانک به هم وصل می کنیم.



شکل ۲۴: نمای واگذاری VLan و Trunking

تا اینجا...

حال به مثال قبل باز می گردیم و پورت ترانک را برای هر دو سوییچ تعریف می کنیم که در این مثال Fa0/5 برای هر دو سوییچ رابطِ بین سوییچ هاست پس در محیط Config سوییچ بر روی FastEthernet 0/5 کلیک کرده و نوع ارتباط را از حالت Access به Trunk تغییر میدهیم همین کار را برای سوییچ دیگر نیز انجام می دهیم.

(ضمناً تنظیم این پورت نیز به صورت دستوری به صورت "Switch(config-if)#switchport mode trunk" می باشد.)

برای تنظیم سوییچ دیگر به صورت دستوری بر روی سوییچ کلیک کرده و در قسمت CLI به سطح Config می رویم و دستورات زیر را اجرا می کنیم.

```
Switch>enable
Switch#config t
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode trunk
```

Device		ID	VLAN- Speciation
PC#1		192.168.1.1	#2
PC#2		192.168.1.2	#2
PC#3		192.168.2.1	#3
PC#4		192.168.2.2	#3
PC#5		192.168.1.3	#2
PC#6		192.168.1.4	#2
PC#7		192.168.2.3	#3
PC#8		192.168.2.4	#3
Switch#1	Interface FA 0/1	-	#2 (Access-PC#1)
	Interface FA 0/2	-	#2 (Access-PC#2)
	Interface FA 0/3	-	#3 (Access-PC#3)
	Interface FA 0/4	-	#3 (Access-PC#4)
	Interface FA 0/5		Trunk (Switch#2)
Switch#2	Interface FA 0/1	-	#2 (Access-PC#5)
	Interface FA 0/2	-	#2 (Access-PC#6)
	Interface FA 0/3	-	#3 (Access-PC#7)
	Interface FA 0/4	-	#3 (Access-PC#8)
	Interface FA 0/5		Trunk (Switch#1)

جدول ۱۲: اطلاعات مثال اخیر در این جدول مشاهده می شود

در جدول فوق، بعضی از مفاهیم نیاز به توضیح دارد:

انواع سطح کارکردی Switch

Portهای یک Switch در دو حالت، یکی Access Mode و دیگری Trunk Mode می توانند کار کنند که در ادامه به شرح بیشتر آنها می پردازیم.

Access Mode

این حالت فقط قادر به عبور و پردازش اطلاعات درون VLAN است و فقط یک VLAN را پشتیبانی می کند.

Trunk Mode

این حالت قادر به عبور دادن بیش از یک VLAN می باشد، بنابراین در اتصال دو Switch به هم، Portها را باید از نوع Trunk انتخاب کرد.

در اتصالات Trunk، از دو روش برای Encapsulation یا همان برگرفتن اطلاعات VLAN استفاده می شود. این دو روش، یکی IEEE 802.1Q است که توسط همهٔ تولیدکنندگان تجهیزات مختلف، پشتیبانی می شود. روش دیگر ISL[1] است که اختصاصی برای شرکت Cisco است.

پروتکل VTP یا VLAN Trunking Protocol

همان طور که از نامش مشخص است، VTP پروتکل VLAN Trunking است. یعنی مخصوص VLAN ها آن هم برای حالت Trunking است. و تنها از ترانک برای انتشار می تواند استفاده کند. یعنی تنها مخصوص انتقال بین "سوییچ ها" است.

با استفاده از پروتکل VTP می توانیم اطلاعات VLAN را روی یک سوییچ ست کنیم بعد با استفاده از VTP سایر سوییچ ها را از وجود این VLAN و پیکربندی اش آگاه کنیم. نتیجه این می شود که بقیه سوییچ ها نیز این VLAN را خواهند شناخت.

به طور کلی پروتکل VTP سوییچ ها را در سه حالت دسته بندی می کند و هر سوییچ تنها در یکی از این سه حالت قرار می گیرد که باز تنظیم این حالت به عهده ادمین شبکه است. حالت های Server ، کلاینت و Transparent (شفاف) .

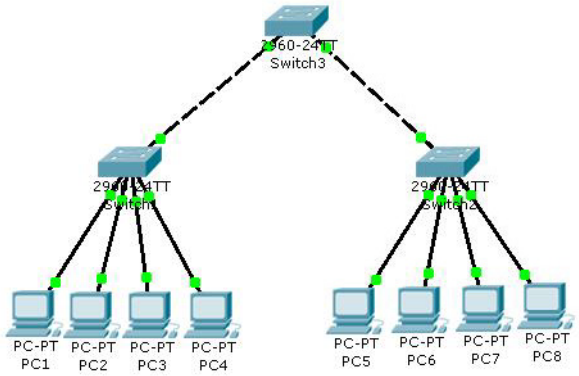
هر ادمین یک یا چند تا از سوییچ ها را در حالت VTP Server و باقی را برای حالت VTP Client ست می کند. به این ترتیب تنها روی سوییچ های VTP Server می توانیم پیکربندی های دلخواه را تنظیم یا تغییر دهیم و سپس از طریق پروتکل VTP این تنظیمات را به دیگر سوییچ های VTP Server و VTP Client مخابره کنیم. هر کدام از سوییچ های VTP Server و کلاینت هم که این پیام را دریافت کردند آنها هم متقابلاً آن پیام را برای ترانک های خارجی شان می فرستند.

پیکربندی VLAN با استفاده از پروتکل VTP

مثال)

می خواهیم شبکه ای(LAN) مانند شکل زیر با تعداد ۸ عدد کامپیوتر و این بار با ۳ عدد سوییچ ایجاد کنیم و با استفاده از تکنولوژی VTP این شبکه را به صورت مجازی به دو شبکه مجزا تقسیم کنیم به گونه ای که هر بخش امکان دسترسی به بخش دیگر را نداشته باشد. در ضمن در اینجا یکی از سوییچ ها(Switch 3) به عنوان Server و دو سوییچ دیگر به عنوان Client در نظر گرفته می شوند بنا به دلایلی که در بالا اشاره شد و تنها تنظیمات و یا تغییرات بر روی سوییچ سرور اعمال می گردد و این تنظیمات و تغییرات به دیگر سوییچ ها اعلام می گردد.

1-Inter Switch Link



شکل ۲۵: نمایی از این مثال در شکل فوق مشاهده می گردد

جواب)

همانند شکل بالا ۸ عدد کامپیوتر را به دو سوییچ وصل کرده و سوییچ ها را به یک سوییچ دربالا متصل می کنیم.

ابتدا برای معرفی سوییچ 3 به عنوان VTP Server، بر روی این سوییچ کلیک می کنیم و در محیط CLI به سطح Config رفته و به این صورت دستورات زیر را اجرا می کنیم:

```
Switch>enable
Switch#config t
Switch(config)#vtp mode server
```

بعد از اجرای این دستورات سیستم به صورت زیر اعلام می کند که این سوییچ به صورت پیش فرض به عنوان سرور موجود بوده است.

```
Device mode already VTP SERVER
```

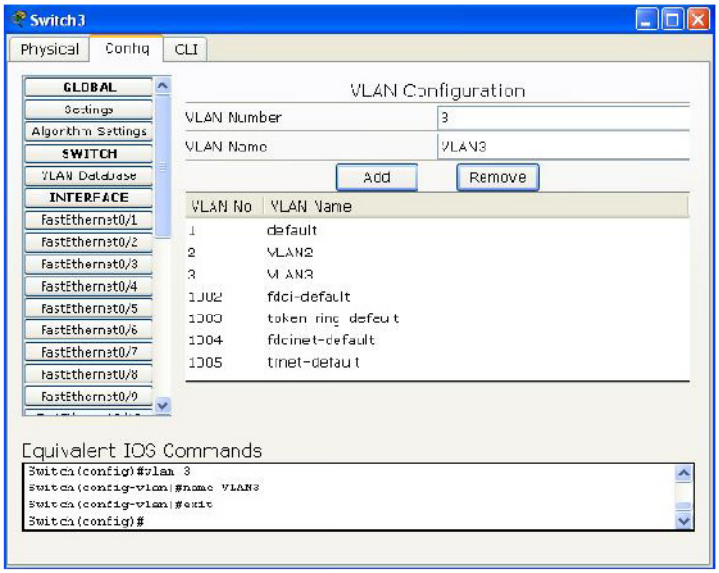
سپس باید برای این سوییچ یک حوزه سرویس دهی مشخص کنیم مثلا حوزه ای با نام tabarsi طبق دستور زیر:

```
Switch(config)#vtp domain tabarsi
```

و سیستم تغییر نام ایجاد شده را به این صورت ننمایش می دهد:

```
Changing VTP domain name from NULL to tabarsi
```

سپس به محیط Config سوییچ می رویم و در آنجا مانند قبل دو VLAN مورد نظر را معرفی می کنیم.



شکل ۲۶:نمایش VLANهای ایجاد شده در سوییچ سرور

سپس برای تنظیم پورت های این سوییچ یعنی Fa0/1 و Fa0/2 به دلیل اینکه این پورت ها به سوییچ های دیگری متصل شده اند باید از نوع Trunk باشند، در بخش INTERFACE بر روی FastEthernet0/1 و FastEthernet02 کلیک می کنیم و برای هر دو نوع ارتباط را از حالت Access به Trunk تغییر میدهیم.

حالا باید سویچ های دیگر را به عنوان Client در حوزه Server مربوطه معرفی کنیم. برای این منظور دستورات زیر را اجرا می کنیم:

```
Switch>enable
Switch#config t
Switch(config)#vtp mode client
```

بعد از اجرای این دستورات سیستم به صورت زیر اعلام می کند که این سوییچ به عنوان یک Client تنظیم گردید.

```
Setting device to VTP CLIENT mode
```

سپس باید برای این سوییچ یک حوزه سرویس گیری مشخص کنیم مثلا حوزه ای با نام tabarsi طبق دستور زیر:

```
Switch(config)#vtp domain tabarsi
```

و سیستم تغییر نام ایجاد شده را به این صورت ننمایش می دهد:

```
Domain name already set to tabarsi
```

با Client واقع شدن این سوییچ به صورت خودکار پورت Fa0/5 نیز از حالت Access به حالت Trunk تغییر می کند.

همین کار را برای سوییچ 2 نیز انجام می دهیم.

کامپیوتر ها را نیز به صورت زیر IP می دهیم:

PC1
- IP Address: 192.168.1.1
- Subnet Mask:255.255.255.0

PC2
- IP Address: 192.168.1.2
- Subnet Mask:255.255.255.0

PC3
- IP Address: 192.168.1.3
- Subnet Mask:255.255.255.0

PC4
- IP Address: 192.168.1.4
- Subnet Mask:255.255.255.0

PC5
- IP Address: 192.168.1.5
- Subnet Mask:255.255.255.0

PC6
- IP Address: 192.168.1.6
- Subnet Mask:255.255.255.0

PC7
- IP Address: 192.168.1.7
- Subnet Mask:255.255.255.0

PC8
- IP Address: 192.168.1.8
- Subnet Mask:255.255.255.0

حالا باید کامپیوتر ها را در VLANهای مورد نظر قرار دهیم که این کار را به صورتی که در مثال های قبل توضیح دادیم انجام می دهیم. بر روی سوییچ کلیک می کنیم در محیط Config در قسمت INTERFACE بر روی FastEthernetهای متصل به سوییچ جاری کلیک کرده و به صورت زیر Fa ها را به VLAN ها اختصاص می دهیم

Switch1:
FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 2
FastEthernet0/3→VLAN 3
FastEthernet0/4→VLAN 3
Switch2:
FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 2
FastEthernet0/3→VLAN 3
FastEthernet0/4→VLAN 3

Device		ID	VLAN- Speciation
PC#1		192.168.1.1	#2
PC#2		192.168.1.2	#2
PC#3		192.168.1.3	#3
PC#4		192.168.1.4	#3
PC#5		192.168.1.5	#2
PC#6		192.168.1.6	#2
PC#7		192.168.1.7	#3
PC#8		192.168.1.8	#3
Switch#1	Interface FA 0/1	-	#2 (Access-PC#1)
	Interface FA 0/2	-	#2 (Access-PC#2)
	Interface FA 0/3	-	#3 (Access-PC#3)
	Interface FA 0/4	-	#3 (Access-PC#4)
	Interface FA 0/5		Trunk (Switch#3)
Switch#2	Interface FA 0/1	-	#2 (Access-PC#5)
	Interface FA 0/2	-	#2 (Access-PC#6)
	Interface FA 0/3	-	#3 (Access-PC#7)
	Interface FA 0/4	-	#3 (Access-PC#8)
	Interface FA 0/5		Trunk (Switch#3)
Switch#3	Interface FA 0/1	-	Trunk (S1)
	Interface FA 0/2	-	Trunk (S2)

جدول ۹: اطلاعات مثال اخیر در این جدول مشاهده می گردد

دربارهٔ پروتکل VTP

در مثال‌های قبل، پیکربندی VLAN به‌صورت دستی انجام می‌شد، اما در این مثال، پروتکل VTP، ما را از وارد کردن VLANها به‌صورت جداگانه در هر Switch، بی‌نیاز می‌سازد. زیرا، این پروتکل روی یک Switch در حالتِ VTP Server تعریف می‌شود (در مثال فوق Switch#3) و آن‌گاه اطلاعات VLANها را به‌صورت اتوماتیک به Switchهای دیگرِ شبکه، که در حالتِ VTP Client هستند ارسال می‌دارد.

جلسه دهم

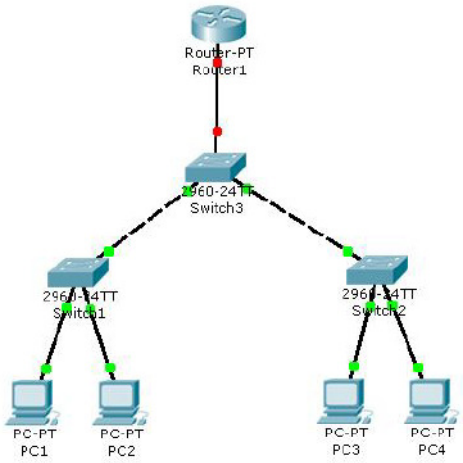
توضیحات مطالب نوشته شده در صفحات بالا مربوط به جلسه نهم در جلسه دهم ارائه شد.

می خواهیم شبکه ای ایجاد کنیم متشکل از چندین کامپیوتر و تعدادی سوییچ و برای این شبکه، شبکه های مجازی ای ایجاد کنیم تا بتوانیم علاوه بر بالا بردن سطح امنیت شبکه از ایجاد ترافیک های ناخاسته در بخش های دیگر شبکه جلوگیری کنیم و ... ضمناً می خواهیم در صورت نیاز امکان انتقال اطلاعات به تمام بخش های شبکه نیز وجود داشته باشد. برای این کار کافیست درون شبکه خود یک روتر اضافه کنیم و کار مسیر یابی و انتقال اطلاعات میان شبکه های مجازی را به این روتر بسپاریم.

در این مثال یک روتر ارتباط بین دو **VLAN** را بر قرار میکند نمایی از شبکه این مثال را در شکل زیر مشاهدخ می کنید

مثال)

می خواهیم شبکه ای با ۴ کامپیوتر، ۳ سوییچ و یک روتر مانند شکل زیر ایجاد کنیم تا موارد ذکر شده در بالا محقق گردد.



شکل ۲۷: شبکه ای با پروتکل **VTP** و استفاده از **Router** جهت مسیر یابی

جواب)

در این مثال تمامی تنظیمات تا قبل از اضافه کردن و تنظیمات مربوط به روتر همانند مثال قبل و موارد آموخته شده است .

۱- IP های کامپیوتر ها را به صورت زیر سِت می کنیم:

PC1
- IP Address: 192.168.1.1
- Subnet Mask:255.255.255.0

PC2
- IP Address: 192.168.2.2
- Subnet Mask:255.255.255.0

PC3
- IP Address: 192.168.1.3
- Subnet Mask:255.255.255.0

PC4
- IP Address: 192.168.2.4
- Subnet Mask:255.255.255.0

۲- Switch3 به عنوان Server اتخاب می شود و تنظیمات مربوطه همانند قبل انجام می گردد.لازم به ذکر است در این مرحله تنها به دلیل اضافه شدن روتر، پورت Fa0/3 سوییچ نیز فعال شده و باید نوع ارتباط بین سوییچ و روتر را نیز مشخص کرده که از نوع Trunk انتخاب می کنیم.

۳- Switch1 و Switch2 به عنوان Client اتخاب می شوند و تنظیمات مربوطه همانند قبل انجام می گردد. در این مرحله با شناخته شدن VLAN های ساخته شده در سرور و معرفی شده به کلاینتها پورت ها را به صورت زیر به VLAN ها اختصاص می دهیم:

Switch1:
FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 3
FastEthernet0/3→Trunk
Switch2:
FastEthernet0/1→VLAN 2
FastEthernet0/2→VLAN 3
FastEthernet0/3→Trunk

۴- انجام تنظیمات روتر مطابق توضیحات زیر.

در اینجا ما یک VLAN با Subnet ID رنج 1 داریم و یک VLAN با Subnet ID رنج 2 داریم و می خواهیم این دو VLAN توسط یک روتر به هم دسترسی داشته باشند با توجه به اینکه در این مثال ما روتر خود را به سوییچ سرور متصل کرده ایم و تنها یک InerFace با شماره FastEthernet0/0 در اختیار داریم می بایست این یک InterFaceی را که در اختیار داریم به Sub InterFace هایی(در اینجا دو Sub InterFace) تقسیم کنیم و هر کدام را به یک VLAN اختصاص دهیم. برای این منظور بر روی روتر کلیک می کنیم و در محیط CLI به سطح Config رفته و دستورات زیر را اجرا می کنیم:

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1Q 2
```

حالا باید یک IP Address به این بخش از Sub Interface اختصاص دهیم تا این IP Address را به عنوان Default Gateway به کامپیوتر های VLAN مربوطه اعلام کنیم.

```
Router(config-subif)#ip address 192.168.1.100 255.255.255.0
```

بعد از تنظیم Sub InterFace اول برای تنظیم Sub InterFace بعدی به روش زیر عمل می کنیم:

```
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#encapsulation dot1Q 3
```

در اینجا نیز همانند قبلی باید یک IP Address به این بخش دیگر از Sub Interface اختصاص دهیم تا این IP Address را به عنوان Default Gateway به کامپیوتر های VLAN مربوطه اعلام کنیم.

```
Router(config-subif)#ip address 192.168.2.100 255.255.255.0
Router(config-subif)#
```

در نهایت تیک On وضعیت پورت[1] روتر را می زنیم و خارج می شویم.

1-Port Status

اطلاعات مثال فوق در جدول زیر مشاهده می شود.

Device		VLAN-Spec	IP
Pc#1		2	**192.168.1.1**
Pc#2		3	**192.168.2.2**
Pc#3		2	**192.168.1.3**
Pc#4		3	**192.168.2.4**
Switch#1	Fa0/1 Fa0/2 Fa0/3	PC#1 PC#2 Trunk	---
Switch#2	Fa0/1 Fa0/2 Fa0/3	PC#3 PC#4 Trunk	---
Switch#3	Fa0/1 Fa0/2 Fa0/3	Trunk Trunk Trunk	---
Router#1	Fa0/0.1 Fa0/0.2		**192.168.1.100** **192.168.2.100**

در جدول فوق نحوه تقسیم کردن یک InterFace روتر به دو InterFace کوچکتر(Sub InterFace) نیاز به توضیح دارد.
این عملیات به صورت تبدیل یک پورت فیزیکی به دو عدد پورت منطقی انجام می گیرد تا عمل Routing بین VLAN 2 و VLAN3 انجام گردد. هنگام تقسیم یکپورت فیزیکی به دو پورت منطقی باید نوع رد و بدل شدن اطلاعات VLANها را(Encapsulation) در حالت DOT1Q تعیین کرد.

پروتکل DHCP

پروتکلی است که به معنی Dynamic Host Configuration Protocol می باشد و عملیات اختصاص IP را به صورت اتوماتیک انجام می دهد. برای این کار باید یک DHCP Server در شبکه وجود داشته باشد. هنگامی که کاپیوتری قصد گرفتن تنظیمات IP Address را از یکDHCP Server را دارد پیغامی را با نام DHCP Discover در شبکه Broadcast می نماید. DHCP Server به این پیغام با پیغام دیگری به نام DHCP Offer پاسخ می گوید که در آن تنظیمات IP را شامل IP Address و Subnet Mask و DefaultGateway و DNS Server IP قرار می دهد. هنگامی که Client این پیغام را دریافت می کند در مرحله بعد به آن با پیغامی به نام DHCP Request پاسخ می دهد که مضمون این پیغام پذیرش تنظیمات IP است. دز نهایت DHCP Server با دریافت پیغام پذیرش از سوی Client تنظیمات IP مربوط به آن Client را در Database خود ذخیره می کند و با فرستادن پیغامDHCP ACK به ارتباط خاتمه می دهد با این روند در واقع Client تنظیمات IP را از سرور اجاره کرده است(Lease). مادامی که Client ریبوت نشده باشد می تواند تنظیمات را در اختیار داشته باشد و به این زمان Lease Time می گویند.

از اینجا...

DHCP یا (Dynamic Host Configuration Protocol) یکی از سرویسهای بسیار مهم و پرکاربرد در شبکه است.

پروتکل پیکربندی پویای میزبان (DHCP) به شما اجازه می دهد آدرسهای IP را بصورت پویا به کامپیوترها و وسایل جانبی روی شبکه اختصاص دهید. آدرس های IP از مخزنی از آدرس های تهیه شده و به کامپیوترها اختصاص داده می شوند. اختصاص آدرس IP بصورت دائم و مو قت خواهد بود. وقتی این مسئله را در نظر بگیرید که باید به هر کامپیوتر مشتری ، آدرس IP ماسک زیر شبکه و آدرس دروازه اختصاص دهید در می یابید که احتمال خطا در اختصاص آدرس ها بسیار بالاست. DHCP یک محیط پویا ایجاد می کند که آدرس های IP را به

کامپیوترها و وسایل جانبی روی شبکه اختصاص می دهد. با این روش با دردسرهای اختصاص آدرس IP بصورت دستی روبه رو نمی شوید و اختصاص آدرس های IP به کامپیوترها با دقت بالایی انجام می گیرد.

سرور DHCP وظیفه دارد آدرس IP ، ماسک زیر شبکه، دروازه پیش ساخته، آدرس سرور DNS و آدرس سرور WINS را به مشتری DHCP ارائه دهد. مشتری DHCP هر کامپیوتر یا وسیله ای روی شبکه است که برای کسب پویای آدرس IP پیکربندی شده است. هنگامی که یک مشتری DHCP برای اولین بار راه اندازی می شود بدنبال آدرس IP می گردد. مشتری یک پیغام DHCP DISCOVER را نشان می دهند که قرارداد IP فرستاده شده به همه سرورهای DHCP را درخواست می کند. پیام نمایش داده شده نام میزبان مشتری و آدرس سخت افزار MAC مشتری را ارائه می کند.

در مرحله بعد یک سرور DHCP که روی زیر شبکه قرار دارد توسط پیام DHCP OFFER آدرس IP پیشنهادی به همراه ماسک زیر شبکه و قرارداد IP را ارائه می کند. این پیام آدرس IP سرور DHCP را نیز شامل می شود.

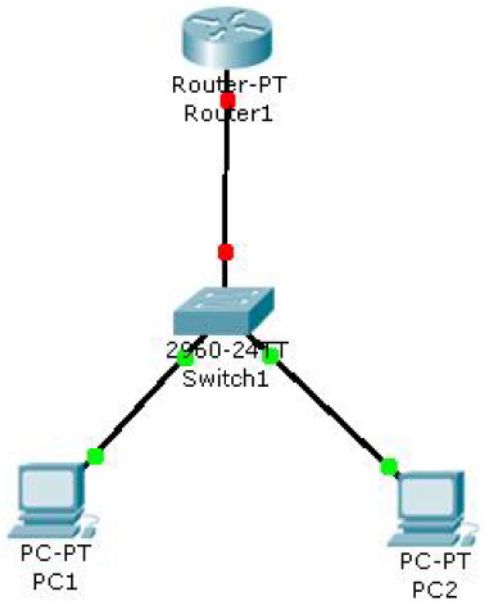
هنگامی که مشتری اولین پیام DHCP OFFER را دریافت می کند یک پیام DHCP REQUEST به همه سرورهای DHCP شبکه می فرستند و پذیرش پیشنهاد ارائه شده را اعلام می کند. این پیام آدرس IP سرور DHCP ای را در بر می گیرد که مشتری با آن موافقت نموده است. بقیه سرورهای DHCP منتظر می مانند تا هنگامی که مشتری دیگری درخواست آدرس IP داشت به آن درخواست پاسخ دهند. درنهایت سرور DHCPکه با پیشنهادش موافقت شده یک پیام تایید برای مشتری می فرستد.

تبدیل یک روتر به یک DHCP Server

مثال)

می خواهیم شبکه ای با ۲ کامپیوتر، ۱ سوییچ و ۱ روتر مانند شکل زیر ایجاد کنیم و به کامپیوتر ها به صورت اتوماتیک IP اختصاص داده شود.

نمایی از این مثال را در شکل زیر مشاهده می کنید.



شکل ۲۸: شبکه ای با پروتکل DHCP

جواب)

برای تنظیم روتر در این مثال بر روی روتر کلیک می کنیم و با توجه به اینکه این روتر از طریق FastEthernet0/0 به شبکه متصل شده است در محیط Config در بخش INTERFACE بر روی FastEthernet0/0 کلیک می کنیم و وضعیت پورت را On می کنیم و بعد یک IP Address به آن اختصاص می دهیم:

Address IP : 192.168.1.100
Subnet Mask : 255.255.255.0

سپس وارد محیط CLI می شویم و در سطح Config باید DHCP را معرفی کنیم پس دستورات زیر را اجرا می کنیم:

```
Router(config-if)#
Router(config-if)#exit
Router(config)#ip dhcp pool tabarsi
```

معرفی رنج IPهایی که از این استخر IPهای DHCP می خواهیم استفاده کنیم. لازم به ذکر است که این رنج IP باید همان ID شبکه ای که باشد که به InterFace روتر متصل شده است.

```
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
```

با توجه به اینکه همان InterFaceای که تعیین کرده بودیم این IPها را اختصاص می دهد:

```
Router(dhcp-config)#default-router 192.168.1.100
```

تعیین یک DNS Server[1]:

```
Router(dhcp-config)#dns-server 4.2.2.1
```

بازگشت به سطح Config

```
Router(dhcp-config)#exit
```

می توان برخی از IP ها را اختصاص نداد و این IP ها را مستثنی کرد و رنج IP مورد نظر را به صورت زیر مشخص می کنیم

```
Router(config)#ip dhcp excluded-address 192.168.1.50 192.168.1.68
Router(config)#
```

حالا DHCP Server ما تنظیم شده است.

پس از انجام تنظیمات DHCP Server بر روی روتر بر روی کامپیوتر ها کلیک می کنیم و IP Configuration را از حالت Static به حالت DHCP تغییر می دهیم در این لحظه سیستم از سرور DHCP درخواست IP می کند (Requesting IP Address) سپس این درخواست مورد تأیید قرار می گیرد (DHCP Request Successful) و تمامی تنظیمات برای IP Address ، Subnet Mask ، Default Gateway و DNS Server به همه کامپیوتر ها ارسال می گردد.

اطلاعات مثال فوق در جدول زیر قابل مشاهده است.

Device		IP Address
Router	Inter Face Fa 0/3	192.168.1.1
PC#1		توسط DHCP
PC#2		توسط DHCP

۱ - سرورهایی که برای ترجمه آدرس به IP در فضای اینترنت کار می کنند