دولت جمهوری اسلامی افغانستان
ادارۀ تعلیمات تخنیکی و مسلکی
معاونیت امور اکادمیک
ریاست نصاب و تربیه معلم

روتینگ و سویچینگ ۲

رشته: کمپیوتر ساینس - دیپارتمنت: شبکه

صنف ۱۴ - سمستر دوم

سال: ۱۳۹۹ هجری شمسی

شناسنامه کتاب

نام کتاب: روتینگ و سویچینگ -۲ (Routing & Switching)

رشته: کمپیوتر ساینس

تدوین کننده: پوهنیار صبغت الله اسلمزی

همکار تدوین کننده: سمیه عثمان

کمیته نظارت:

- ندیمه سحر رئیس ادارۀ تعلیمات تخنیکی و مسلکی
- عبدالحمید اکبر معاون امور اکادمیک ادارۀ تعلیمات تخنیکی و مسلکی
- حبیب الله فلاح رئیس نصاب و تربیه معلم
- عبدالمتین شریفی آمر انکشاف نصاب تعلیمی، ریاست نصاب و تربیه معلم
- روح الله هوتک آمر طبع و نشر کتب درسی، ریاست نصاب و تربیه معلم
- احمد بشیر هیله‌من مسؤل انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- محمد زمان پویا کارشناس انکشاف نصاب، پروژه انکشاف مهارت‌های افغانستان
- علی خیبر یعقوبی سرپرست مدیریت عمومی تألیف کتب درسی، ریاست نصاب و تربیه معلم

کمیته تصحیح:

- دوکتور احمد فرید اسداللهی
- دوکتور نظر محمد بهروز
- محمد امان هوشمند مدیرعمومی بورد تصحیح کتب درسی و آثار علمی

دیزاین: صمد صبا و سیدکاظم کاظمی

سال چاپ: ۱۳۹۹ هجری شمسی

تیراژ: ۱۰۰۰

چاپ: اول

ویب سایت: www.tveta.gov.af

ایمیل: info@tveta.gov.af

سرود ملی

دا وطـــن افغانســـتان دی — دا عــزت د هــر افغــان دی

کــور د ســولې کــور د تــورې — هــر بچـی یــې قهرمــان دی

دا وطــن د ټولــو کــور دی — د بلوخـــــو، د ازبکـــــو

د پښـــتون او هـــزاره وو — د ترکمنـــــو، د تاجکـــــو

ورسره عــرب، ګوجــر دي — پامیریـــان، نورســـتانیان

براهــوي دي، قزلبــاش دي — هــم ایمــاق، هــم پشــه‌یان

دا هیــواد بــه تــل ځلیــږي — لکــه لمــر پــر شــنه آســمان

پــه ســینه کــې د آســیا بــه — لکـــه زړه وی جاویـــدان

نــوم د حــق مــو دی رهبــر — وایـو الله‌اکبر وایـو الله‌اکبر

پیام ادارهٔ تعلیمات تخنیکی و مسلکی

استادان نهایت گرامی و محصلان ارجمند!

تربیت نیروی بشری ماهر، متخصص و کارآمد از عوامل کلیدی و انکارناپذیر در توسعهٔ اقتصادی و اجتماعی هر کشور محسوب می‌گردد و هر نوع سرمایه‌گذاری بزرگ در بخش‌های مختلف اقتصادی نیازمند به پلان‌گذاری و سرمایه‌گذاری در بخش نیروی بشری و توسعهٔ منابع این نیرو می‌باشد. بر مبنای این اصل و بر اساس فرمان شماره ۱۱ مقام عالی ریاست جمهوری اسلامی افغانستان به تاریخ ۱۳۹۷/۲/۱ ادارهٔ تعلیمات تخنیکی و مسلکی از بدنهٔ وزارت معارف مجزا و فصل جدیدی در بخش عرضه خدمات آموزشی در کشور گشوده شد.

اداره تعلیمات تخنیکی و مسلکی به‌عنوان متولی و مجری آموزش‌های تخنیکی و مسلکی در کشور محسوب می‌شود که در چارچوب استراتژی ۵ ساله خویش دارای چهار اولویت مهم که عبارت‌اند از افزایش دسترسی عادلانه و مساویانه فراگیران آموزش‌های تخنیکی و مسلکی در سطح کشور، بهبود کیفیت در ارائه خدمات آموزشی، یادگیری مادام‌العمر و پیوسته و ارائه آموزش نظری و عملی مهارت‌ها به‌طور شفاف، کم‌هزینه و مؤثر که بتواند نیاز بازار کار و محصلان را در سطح محلی، ملی و بین‌المللی برآورده کند، می‌باشد.

این اداره که فراگیرترین نظام تعلیمی کشور در بخش تعلیمات تخنیکی و مسلکی است، تلاش می‌کند تا در حیطهٔ وظایف و صلاحیت خود زمینهٔ دستیابی به هدف‌های تعیین‌شده را ممکن سازد و جهت رفع نیاز بازار کار، فعالیت‌های خویش را توسعه دهد.

نظام اجتماعی و طرز زندگی در افغانستان مطابق به احکام دین مقدس اسلام و رعایت تمامی قوانین مشروع و معقول انسانی عیار است. ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان نیز با ایجاد زمینه‌های لازم برای تعلیم و تربیت جوانان و نوجوانان مستعد و علاقه‌مند به حرفه‌آموزی، ارتقای مهارت‌های شغلی در سطوح مختلف مهارتی، تربیت کادرهای مسلکی و حرفوی و ظرفیت‌سازی تخصصی از طریق انکشاف و ایجاد مکاتب و انستیتوت‌های تخنیکی و مسلکی در سطح کشور با رویکرد ارزش‌های اسلامی و اخلاقی فعالیت می‌نماید.

فلهذا جهت نیل به اهداف عالی این اداره که همانا تربیهٔ افراد ماهر و توسعهٔ نیروی بشری در کشور می‌باشد؛ داشتن نصاب تعلیمی بر وفق نیاز بازار کار امر حتمی و ضروری بوده و کتاب درسی یکی از ارکان مهم فرایند آموزش‌های تخنیکی و مسلکی محسوب می‌شود، پس باید همگام با تحولات و پیشرفت‌های علمی نوین و مطابق نیازمندی‌های جامعه و بازار کار تألیف و تدوین گردد و دارای چنان ظرافتی باشد که بتواند آموزه‌های دینی و اخلاقی را توأم با دست‌آوردهای علوم جدید با روش‌های نوین به محصلان انتقال دهد. کتابی را که اکنون در اختیاردارید، بر اساس همین ویژگی‌ها تهیه و تدوین گردیده است.

بدین‌وسیله، صمیمانه آرزومندیم که آموزگاران خوب، متعهد و دلسوز کشور با خلوص نیت، رسالت اسلامی و ملی خویش را ادا نموده و نوجوانان و جوانان کشور را به‌سوی قله‌های رفیع دانش و مهارت‌های مسلکی رهنمایی نمایند و از محصلان گرامی نیز می‌خواهیم که از این کتاب به‌درستی استفاده نموده، در حفظ و نگهداشت آن سعی بلیغ به خرج دهند. همچنان از مؤلفان، استادان، محصلان و اولیای محترم محصلان تقاضا می‌شود نظریات و پیشنهادات خود را در مورد این کتاب از نظر محتوا، ویرایش، چاپ، اشتباهات املایی، انشایی و تایپی عنوانی ادارهٔ تعلیمات تخنیکی و مسلکی کتباً ارسال نموده، امتنان بخشند.

در پایان لازم می‌دانیم در جنب امتنان از مؤلفان، تدوین‌کنندگان، مترجمان، مصححان و تدقیق کنندگان نصاب تعلیمات تخنیکی و مسلکی از تمامی نهادهای ملی و بین‌المللی که در تهیه، تدوین، طبع و توزیع کتب درسی زحمت‌کشیده و همکاری نموده‌اند، قدردانی و تشکر نمایم.

ندیمه سحر

رئیس ادارهٔ تعلیمات تخنیکی و مسلکی جمهوری اسلامی افغانستان

فهرست

عنوان صفحه

مقدمه

در این کتاب خواننده می‌تواند به مفاهیم routing یا مسیریاب (router)هایی که در شرکت‌های متفاوت تولید شده است، آشنا شود و آن‌ها را جهت یافتن شبکه‌های داخلی که به‌صورت غیر مستقیم وصل شده است تنظیم کند. شبکه‌های محلی که دور از هم واقع گردیده باهم در ارتباط باشد مثل پروتوکول‌های IGRP, EIGRP, OSPF و RIP بحث شده است که خوانندۀ کتاب می‌تواند در مورد این پروتوکول‌ها معلومات کافی داشته باشد و نیز بتواند که این پروتوکول‌ها را عملاً بین مسیریاب‌ها تطبیق نماید. و در قسمت سویئچنیگ VLANها و پروتوکول‌ها مورد بحث قرار داده شده، زمانی‌که چندین کمپیوتر را به یک سویچ متصل می‌کنیم، آن‌ها به راحتی می‌توانند باهم ارتباط داشته باشند و از منابع شبکه استفاده کنند، اما تعداد زیاد کمپیوترها می‌تواند حجم کاری سویچ را افزایش دهند، یعنی این‌که تمام سویچ‌ها در یک منطقۀ کاری باهم در ارتباط هستند و امنیت در این نوع شبکه‌ها بسیار پایین می‌آید، اما می‌توان با تقسیم یک منطقه به چندین منطقه امنیت را افزایش داد و ترافیک شبکه را به راحتی کنترول کرد و مثال‌های عملی نیز شامل کتاب شده است که می‌توان با استفاده از مثال داده‌شده بخش عملی را خوب‌تر یاد گرفت. که در قسمت بخش‌های دیگر این کتاب پروتوکول‌هایی مانند Fram realy و ستندرهای آن مثل Cisco, Ansi,Q.933، و به‌خاطر کنترول ترافیک شبکه و تعیین مجوزهای دسترسی برای ترافیک‌ها Access List تشریح شده است، و همین قسم NAT ترجمۀ آدرس‌های Invalid بـه آدرس‌های Valid می‌باشد در قسمت آخر شبکۀ گسترده (wan) که یک شبکۀ کمپیوتری است که ناحیۀ جغرافیایی نسبتاً وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قارهای دیگر) این شبکه‌ها معمولاً از امکانات انتقال خدمات‌دهندگان عمومی، مانند شرکت‌های مخابرات استفاده می‌کند. به عبارت کمتر رسمی، این شبکه‌ها از مسیریاب‌ها و لینک‌های ارتباطی عمومی استفاده می‌کنند، تشریح گردیده است. برعلاوه در این کتاب در هر فصل فعالیت‌ها و کارهای عملی در نظر گرفته شده است که انجام‌دادن فعالیت‌ها به خوانندۀ کتاب بیشر کمک می‌کند تا موضوعات را بهتر فراگیرد.

هدف کلی کتاب

آشنایی با نصب و اعیارسازی پروتوکول های چون (IGRP, EIGRP, OSPF)، تنظیمات VLAN
ACL, VTP, NAT، ارتباطات شبکه WAN و شبکه Frame Relay.

فصل اول

مسیریابی IGRP

هدف کلی: آشنایی در مورد پروتوکول مسیریابی IGRP. و عملکرد آن.

اهداف آموزشی: در پایان این فصل از محصلان انتظار می‌رود که:

۱. پروتوکول مسیریابی IGRP و عملکرد آن را تشریح نمایند.
۲. تنظیم پروتوکول مسیریابی IGRP روی یک شبکه را بدانند.
۳. طریقهٔ تطبیق و تنظیم IGRP را توضیح نمایند.

در این فصل کوشش بر آن شده که خواننده به مفاهیم routing یا مسیریاب (router) های که از شرکت‌های متفاوت تولید شده است، آشنا شود و آن‌ها را جهت یافتن شبکه‌های داخلی که به‌صورت غیر مستقیم وصل شده است، تنظیم کند که چندین شبکهٔ محلی که دور از هم واقع گردیده باهم در ارتباط باشند تا منابع به‌صورت مشترک قابل دسترس باشد. که این کار باعث به‌وجودآمدن یک شبکهٔ بزرگ‌تر می‌گردد که می‌تواند تمام منابع جهت ایجاد سهولت و کارایی بالا برای یک شرکت به‌صورت مشترک قابل دسترس باشد.

در این فصل ما با موضوعات ذیل آشنا می‌شویم:

۱. مسیریابی (Routing) و انواع مسیریابی؛
۲. مقایسهٔ Static Rouing با Dynamic Routing؛
۳. نحوهٔ عیارسازی و انجام‌دادن ((Static routing؛
۴. پروتوکول مسیریابی IGRP و عملکرد آن؛
۵. فعال‌کردن راه‌اندازی پروتوکول مسیریابی IGRP روی روترها؛
۶. معرفی و بررسی جدول مسیریابی در پروتوکول IGRP.

۱.۱ معرفی مسیریابی

مسیریابی پروسهٔ انتخاب مسیر برای دسترسی به شبکه‌های غیر محلی می‌باشد. بنابراین روتر با شناخت از شبکه‌ها و مسیرهای رسیدن به هر کدام، نگهداری این اطلاعات در یک جدول به‌عنوان یک مسیریاب نقش ایفا می‌کند. مسیریابی معمولاً با Bridging مقایسه می‌شود. اولین تفاوت آن این است که Bridging مربوط به Data Link Layer می‌باشد. درصورتی‌که میسریابی مربوط به Network Layer است. این تفاوت باعث می‌شود که در پروسس انتقال اطلاعات از اطلاعات متفاوتی استفاده شود.

۱.۲ وظیفهٔ مسیریابی

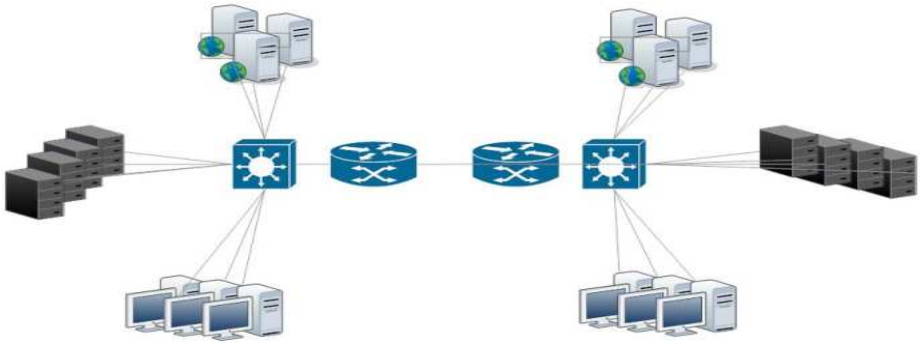
مسیریابی وظیفهٔ انجام دو کار عمده را دارد، تعیین کوتاترین مسیر و انتقال گروه‌های اطلاعاتی (Packets) از طریق شبکه می‌باشد. وظیفهٔ مسیریابی این است که اطلاعات را از یک دستگاه در شبکه دریافت کرده و آن را به دستگاه دیگری که در شبکهٔ دیگر قرار دارد، ارسال کند. در واقع به عمل روتینگ، عمل مسیریابی نیز می‌گویند.

۱.۳ تعیین مسیریابی

متریک، یک استندرد برای محاسبه است. مثل طول مسیر که در الگوریتم‌های مسیریابی استفاده می‌شود. برای مسیریابی این الگوریتم‌ها جدول‌های مسیریابی (Routing Table) دارند و اطلاعات مسیر با توجه به الگوریتم تغییر می‌کنند. این جدول‌ها، اطلاعات متنوعی دارند؛ مثلاً next hop به یک روتر می‌گوید که یک روتر به مقصد مشخص می‌تواند از طریق یک Router مشخص که همان hop بعدی است رسید. وقتی‌که

یک Router یک Packet را می‌گیرد، آدرس مقصد را چک می‌کند و سعی می‌کند رابطه‌یی بین آن و hop بعدی را برقرار کند.

مثل جدول ذیل:



شکل (۱-۱)ساختار سادۀ یک شبکه

Routerها به خاطر اتصال شبکه‌ها با هم رابطه برقرار می‌کنند و از طریق رد و بدل کردن پیغام جدول‌های Routing را می‌سازند. پیغام Routing update، معمولاً تمام یا قسمتی از جدول Routing را در بر دارد با بررسی جدول بقیه Routerها، هر Router، می‌تواند در یک دقیقه از شبکه برای خود ترسیم کند. نوع دیگری از پیغام‌ها، اعلام عمومی Link – State است. که به بقیه Router ها در مورد وضعیت رابطه‌های فرستنده اطلاعات می‌دهد.

۱.۴ معرفی Static Routing و Dynamic Routing

روتر شبکه‌های وصل‌شده (محلی) را به کمک انترفیس‌های فعال خود می‌شناسد و شبکه‌های غیر محلی را توسط دو روش می‌شناسد:

- Static Routing
- Dyanmic Routing

۱.۵ Static Routing

در این روش شبکه‌های غیر محلی و راه دسترسی به هر کدام از آن‌ها به‌صورت دستی به روتر معرفی می‌شود. در واقع شما به‌عنوان مدیر شبکه با شناخت از هر روتر و مسیرهای رسیدن به هر کدام و به‌صورت کلی با شناخت از ساختار کل شبکه، خودتان مسیردهی به هر کدام از شبکه‌های غیر محلی را انجام می‌دهید.

با معرفی دستی مسیرهای روتر، دیگر نیازی ندارد که خود مسیرها را به‌صورت اتوماتیک شناسایی کند ویا تغییرات وارده در شبکه چون حذف یا اضافه‌شدن یک Network به شبکه را از روترهای دیگر بگیرد. همان‌طوری‌که می‌دانید در حالتی که روتر فقط شبکه‌های متصل به خود را بشناسد، فقط شبکه‌های وصل در Routing Table نمایش داد می‌شود. برای دسترسی به شبکه‌های غیر محلی به روش Static مدیر شبکه

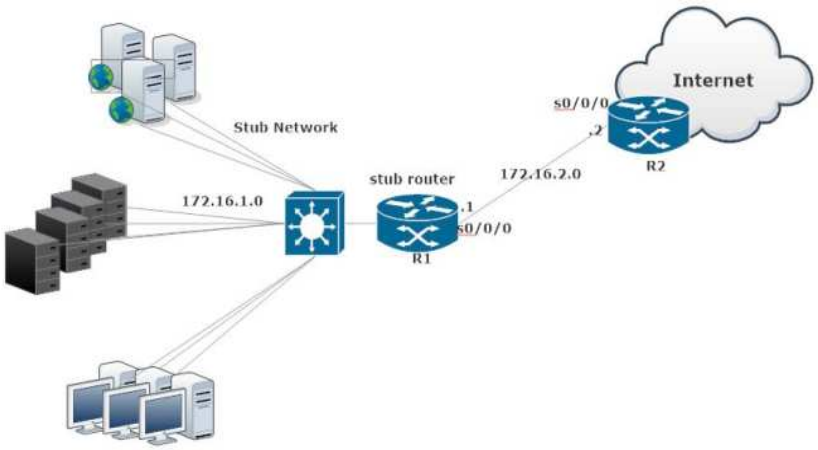
خود باید که تمام مسیرها را در Routing Table اضافه نماید. در واقع مدیر شبکه باید هر یک از شبکه‌ها و مسیر رسیدن به هر کدام از آن‌ها را بداند و خود به‌صورت دستی این مسیرها را به روتر معرفی کند.

بنابراین درصورتی‌که Network اضافه ویا حذف شود، خود ما باید که روی هر روتر این تغییرات را وارد نماییم این بدین معنا است که روترها به‌صورت اتوماتیک از تغییرات اعمال‌شده در شبکه، مطلع نمی‌باشند. بنابراین با توجه به تنظیم دستی هر روتر، مدیریت در شبکه‌های بزرگ سخت‌تر می‌شود.

درنتیجه استفاده از این روش‌ها در شبکه‌های کوچکتر که مدیریت آن به‌صورت دستی امکان‌پذیر باشد، ترجیح داده می‌شود.

۱.۶ مسیریابی Static

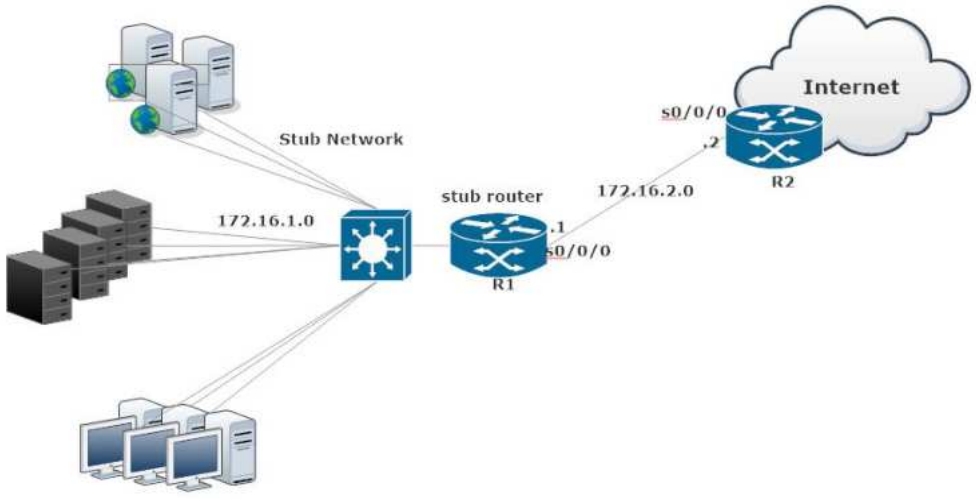
تا به اینجا یاد گرفتید که به کمک Static Route می‌توانیم به‌صورت دستی تمامی شبکه‌های غیر محلی را به روتر معرفی کنیم و دانستیم که استفاده از این روش در شبکه‌های بزرگ چگونه مشکل‌ساز می‌باشد. در واقع کاربرد اصلی این روش برقراری ارتباط یک Stub Network با شبکه‌های خارجی چون انترنت می‌باشد که در شکل ذیل نشان داده شده است:



شکل (۱-۲) Static Route

Stub Network شبکه‌یی است که فقط یک راه خروجی (Gateway) برای رسیدن به شبکه‌های دیگر چون انترنت دارد. به‌گونهٔ مثال فرض کنید شبکهٔ محلی یک شرکت قرار است به انترنت وصل شود. برای این منظور ترافیک موجود در این شبکه می‌بایست به کمک یک Route به خارج از شبکه منتقل شود. با توجه به این مثال فرض کنید که از Stationهای موجود در شبکه درخواستی برای سایت www.facebook.com داشته باشد، اما مقصد این درخواست در شبکهٔ محلی ۱۷۲.۱۶.۱.۰ موجود نمی‌باشد. بنابراین این درخواست باید از این شبکه خارج شود.

بنابراین کافی است که تمامی ترافیک موجود در Stub Network را به انترفیس ۱۷۲.۱۶.۲.۱ هدایت کنیم و چون این انترفیس با انترفیس S0 از روتر A در یک رنج IP می‌باشند، بنابراین ترافیک به سمت انترفیس ۱۷۲.۱۶.۲.۲ از روتر A هدایت می‌شود.



شکل (۱-۳) Stub Network

پس کافی است که روی روتر A، Static Route راه‌اندازی کنیم. درصورتی‌که روتر A بسته‌یی را دریافت کرد که مقصدش شبکهٔ ۱۷۲.۱۶.۱.۰ بود آن را به انترفیس S0/0/0 هدایت می‌کند. چون یک مسیر به این شبکه از طریق این انترفیس دارد. برای فعال‌کردن Static Route کافی است به روتر A به‌صورت دستی بگوییم که مسیر به شبکهٔ ۱۷۲.۱۶.۱.۰ از طریق انترفیس ۱۷۲.۱۶.۲.۱ وجود دارد. اما روی روتر B چه تنظیمات باید انجام دهیم؟ پاسخ به این سؤال Default Route می‌باشد که در ادامه با آن آشنامی‌شوید.

۱.۷ Dynamic Routing

در این روش، شناخت به کمک الگوریتم‌های مسیریابی که در فصل‌های بعدی با آن‌ها آشنا می‌شویید صورت می‌گیرد. در واقع در روش دوم مسیریابی به‌صورت اتوماتیک انجام می‌گیرد به این ترتیب که روتر اطلاعات شبکه را از روترهای دیگر گرفته و بعد از تبادلات لازم و تغییرات بعضی از فیلدها، آن را در Routing Table نگهداری می‌کند و همچنین درصورتی‌که تغییری در شبکه رخ دهد، این تغییرات منجر به تغییر Routing Table می‌شود. درنتیجه هر نوع از مسیریابی، مشخصات خاص خویش را دارد که در جدول ذیل به‌شکل مقایسوی نشان داده شده است:

جدول (۱-۱) مقایسهٔ static routing با dynamic routing

Static Routing	Dynamic Routing
مشخص بودن نتورک‌هایی که به‌صورت غیر مستقیم وصل می‌باشند	دانستن شبکه‌های غیر مسقیم برای مدیر شبکه لازم نیست
همزمان نظر به سایز شبکه بیشتر می‌شود	وابسته به سایز شبکه نیست
توسط مدیر شبکه تمام تغییرات باید آورده شود	به‌شکل خودکار تغییر وارد می‌شود
قابل استفاده در شبکه‌های کوچک که بین 10 الی 15 روتر به کار رفته باشد	قابل استفاده در شبکه‌های کوچک و بزرگ
امنیت بیشتر دارد	امنیت کمتر دارد
منابع بیشر ضرورت ندارد	CPU، حافظه و هم bandwith بیشتر ضرورت دارد

۱.۸ Default Route

تا به اینجا با ستاتیک روت و نحوهٔ کار آن آشنا شدید. در مثال پیش دیدید که چگونه با فعال‌کردن ستاتیک روت روی روتر A یک مسیر به شبکهٔ Stub فعال کردیم. در واقع روتر A به کمک این مسیر به شبکهٔ ۱۷۲.۱۶.۱.۰ دسترسی پیدا می‌کند. اما سؤال اینجا مطرح می‌شود که روتر B چگونه شبکه‌های دیگر را بشناسد؟ همان‌طور که مشاهده می‌کنید، شبکهٔ ۱۷۲.۱۶.۱.۰ یک شبکهٔ Stub می‌باشد و روتر B نقش یک دروازه برای دسترسی به شبکه‌های دیگر را برای شبکهٔ Stub باز می‌کند. اما این روتر باید تمامی شبکه‌های غیر محلی را بشناسد. اما مشکل اینجاست که ما نمی‌توانیم شبکه‌های غیر محلی را یک‌یک به این روتر معرفی کنیم. پس برای این منظور کافی است، Packet که آدرس مقصد جای دیگری به غیر از شبکهٔ محلی است، مسیر دهی شده و از این شبکه خارج شود تا توسط روترهای دیگر مسیردهی شده و به مقصد برسد. در واقع Default route با فعال یک مسیر به تمامی شبکه‌های غیر محلی، راه حل این مشکل است.

برخلاف ستاتیک روت Dynamic Routing Protocol ها دارای عملکرد غیر دستی می‌باشد که ما به‌صورت دستی شبکه‌های غیر محلی را به روتر معرفی نمی‌کنیم. این شناخت از طریق روترهای مجاور صورت می‌گیرد.

هر کدام از این پروتوکول ها دارای الگوریتم مخصوص به خود هستند و به کمک اطلاعات به‌دست‌آورده نسبت به انتخاب مسیر تصمیم‌گیری می‌کنند.

۱.۹ پروتوکول IGRP

Interior Gateway Protocol توسط شرکت سیسکو در دهۀ ۱۹۸۰ طراحی و ارائه شد. این پروتوکول از جمله پروتوکول‌های dynamic distance vector به شمار می‌آید. به‌طور پیش‌فرض هر ۹۰ ثانیه یک update packet را به‌صورت Broadcast ارسال می‌کند. اگر در عرض ۲۷۰ ثانیه جوابی از یک مسیریاب دریافت نکند، آن را غیر قابل دسترس (inaccessible) معرفی می‌کند و اگر پس از ۶۳۰ ثانیه پاسخی دریافت نکرد، آن مسیر را از routing table حذف می‌نماید.

قبل از دهۀ ۸۰، پروتوکول RIP از مشهورترین و پرکاربردترین پروتوکول‌ها بود. اما RIP فقط برای شبکه‌های کوچک مفید بود (شبکه‌هایی که حد اکثر طول مسیر در آن‌ها hop۱۶ بود) در ضمن فاصلۀ مسیریاب‌ها را فقط با شمردن تعداد hop های بین آن‌ها تعیین کرد که در محیط‌های پیچیده و شبکه‌های گسترده بازدهی کار را پایین می‌آورد. به این دلایل پس از ابداع IGRP، این پروتوکول به سرعت جایگزین RIP شد.

این پروتوکول از دسته پروتوکول‌های IGPs است و سازندۀ آن شرکت سیسکو است. از نظر قدرت نسبت به پروتوکول Rip خیلی کارآمدتر است.

۱.۱۰ Unegual Load Balancing

پروتوکول IGRP مانند RIP می‌تواند ترافیک را بین چند مسیر بیلانس نماید اما تفاوتی که این پروتوکول با RIP دارد این است که می‌تواند ترافیک را بین چند مسیر با متریک‌های مختلف بیلانس کند IGRP به‌صورت Default تا چهار مسیر را برای Unegual Load Balancing انتخاب می‌کند.

۱.۱۱ بررسی متریک در IGRP

برای محاسبۀ Metric این پروتوکول باید کمی بیشتر کار کرد، یعنی مانند پروتوکول Rip نیست که Metric از طریق تعداد روترها تشخیص داده شود. بلکه در این پروتوکول از پنج فکتور اصلی برای محاسبۀ Metric استفاده می‌کنند.

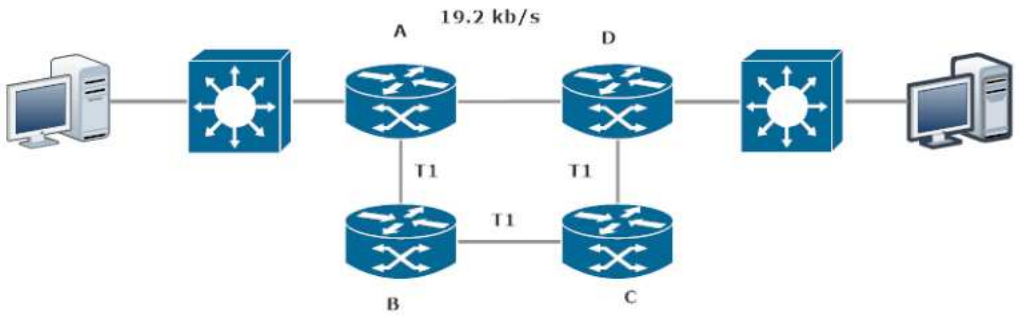
IGRP برخلاف RIP دارای متریک Composite می‌باشد. متغیرهایی‌که در تعیین متریک نقش دارند قرار ذیل‌اند:

- Bandwidth
- Delay
- Load
- MTU
- Relibility

به‌صورت پیش‌فرض دو متغیر Bandwidth و Delay در تعیین متریک نقش دارند، که در ادامۀ این درس به هر کدام این متریک‌ها آشنا خواهم شد. همان‌طوری‌که RIP دارای محدودیت ۱۵ گام در متریک

می‌باشد. این بدان معنا است که RIP، متریک بیشتر از ۱۵ را بی‌نهایت در نظر می‌گیرد. لذا RIP با محدودیت وسعت شبکه مواجه می‌باشد.

اما در IGRP برخلاف RIP این مقدار ۲۵۵ می‌باشد. بنابراین IGRP محدودیت RIP را در Maximumm hop count بهبود بخشید. سوالی که اینجا مطرح می‌شود اینست که چرا IGRP چندین متغیر را برای تعیین متریک در نظر می‌گیرد و مزیت این انتخاب نسبت به RIP که فقط یک متغیر در تعیین متریک شرکت می‌کند در چیست؟ به‌شکل زیر توجه کنید:



شکل (۱-۴) Hop Count

فرض کنید پروتوکول مسیریابی RIP روی تک تک روترها نصب می‌شود، از آنجایی که متریک در RIP تعداد گام (hop count) می‌باشد، بنابراین مسیر Administrative Distannce به‌عنوان بهترین مسیر انتخاب می‌شود. در واقع مسیری که Bandwidth کمتر دارد به مسیری به BandwidthT۱ ترجیح داده می‌شود IGRP با درنظرگرفتن این مشکل متریک را اصلاح می‌کند در IGRP, Bandwith یکی از فاکتورهای تعیین متریک می‌باشد.

۱.۱۲ Bandwidth در IGRP

درصورتی‌که IGRP به‌عنوان پروتوکول مسیریابی انتخاب شود، با فرض ثابت‌بودن متغیرهای دیگر روی تمامی مسیرها، مسیری‌که bandwidth بیشتر دارد به‌عنوان بهترین مسیر انتخاب می‌شود. بنابراین درصورتی‌که روتر، APacket را دریافت کرد که مقصد آن PC-۲ باشد، آن را از مسیر ABCD که Bandwidth بیشتر دار هدایت می‌کند.

۱.۱۲.۱ الف) Delay

مقایسه از زمانی است که یک packet درطول مسیر حرکت می‌کند و مقدار است بین ۰ تا ۲۵۵ بنابراین با فرض ثابت‌ماندن فاکتورهای دیگر در تعیین متریک، مسیری که Dealy کمتری دارد به‌عنوان بهترین مسیر انتخاب می‌شود.

در مورد Delay هم گفتیم که بستگی به پورت‌های استفاده‌شده دارد. پورت‌های GigabiteEthernet، نسبت به پورت‌های FastEthernet از زمان پاسخ‌گویی کمتری برخوردار بودند. اگر در یک شبکه، Bandwidth یکی باشد، به زمان Delay نگاه می‌کنند که هر چه این زمان پایین‌تر باشد، بهتر است.

۱.۱۲.۲ ب) Load

حجم ترافیک بر اساس bit/second که از یک مسیر می‌تواند منتقل شود. این پارامتر به‌صورت پیش‌فرض در تعیین متریک IGRP نقشی ندارد و در غیر این‌صورت این عدد بین ۰ تا ۲۵۵ می‌تواند تغییرکند. مسیری که load آن ۲۵۵ است load آن ۱۰۰ درصد می‌باشد با فرض ثابت‌ماندن فاکتورهای دیگر در تعیین متریک مسیری که load کمتری دارد به‌عنوان بهترین مسیر انتخاب می‌شود.

۱.۱۲.۳ ج) Reliability

مقیاسی برای پایداری و مطمئن بودن یک مسیرمی باشد. فاکتورهایی چون دفعات down شدن یک مسیر ویا از Packet lost روی این پارامتر تأثیر می‌گذارد. یا اطمینان‌پذیری که بدین معنا است که اگر یک خط همیشه Up باشد و مشکلی نداشته باشد، این خط از Reliability بالاتری برخوردار است و از این خط به‌عنوان بهترین مسیر استفاده می‌شود، به‌شرطی‌که بقیه فکتورها ثابت باشد. این را هم اضافه کنیم که اگر یک خط Down شود و بعداً Up شود، Reliability آن به نسبت خط‌های دیگر کاهش می‌یابد.

این پارامتر به‌صورت پیش‌فرض در تعیین متریک IGRP نقشی ندارد و در آن‌صورت این مقدار بین ۰ تا ۲۵۵ می‌تواند تغییر کند. بنابراین با فرض ثابت‌ماندن فاکتورهای دیگر در تعیین متریک مسیری که Reliability بیشتری داشته باشد به‌عنوان مسیر انتخاب می‌شود.

۱.۱۲.۴ د) MTU:

Maximum Transmission Unit حد اکثر اندازه‌یی که برای یک پکت در نظر گرفته می‌شود، بدون این‌که Fragment شود به‌صورت پیش‌فرض این پارامتر در تعیین متریک نقشی ندارد. ویا به حد اکثر اندازۀ یک بسته بر روی یک خط است که هر چه آن خط بتواند بسته‌یی با اندازۀ بیشتر را انتقال دهد، آن خط به‌عنوان بهترین مسیر استفاده می‌شود؛ اما در کل به ندرت استفاده می‌شود.

متریک با پهنای باند (Bandwidth) رابطۀ معکوس ویا Delay رابطۀ مستقیم دارد. درصورتی‌که دو مسیر به Bandwidth متفاوت داشته باشیم، با فرض یکسان‌بودن پارامتر Dealy روی هر دو مسیر، مسیری که Bandwidth بیشتر داشته باشد، متریک کمتری خواهد داشت.

۱.۱۳ مشخصات پروتوکول IGRP

همان‌طورکه ذکر شد، IGRP یک پروتوکول distance vector است. در این نوع پروتوکول‌ها هر مسیریاب تمام یا قسمتی از Routing Table خود را در زمانی منظم برای همسایه‌های خود می‌فرستد.

در مقابل distance vector protocol، پروتوکول‌های link state قرار دارند که اطلاعات محلی خود را به تمام Node های شبکه ارسال می‌کنند. بعداً خواهیم گفت که OSPF، IS-IS از نوع پروتوکول‌های link state می‌باشند. IGRP برای تعیین فاصله بین مسیریاب‌ها که شامل چند پارامترمی‌باشد، استفاده می‌کند، این پارامترها عبارتند از تأخیر موجود (delay)، پهنای باند مسیر (BW)، قابلیت اعتمادی‌که این مسیر وجود دارد (reliability) مقدار بار (load) که روی مسیر قرار دارد. همچنین برای هر یک از این پارامترها می‌توان وزنی تعیین کرد که اهمیت آن بیشتر از بقیه گردد؛ مثلاً: Bw می‌تواند از ۱۲۰۰ bps تا ۱۰ giga bps تغییر کند و این نکته، IGRP را برای شبکه‌هایی که مشخصات ساختاری آن‌ها تغییرات سریع ندارند مناسب می‌نماید.

برای انعطاف‌پذیری بیشتر، IGRP امکان ارسال داده از چند مسیر (multipath routing) را فراهم می‌کند؛ مثلاً: اگر یک مسیر سه برابر بهتر از مسیر دیگر باشد (به‌خاطر این‌که طول آن بر اساس پارامترهای ذکر شده، طول دیگری به دست آمده) اغلب داده‌ها از خط اولی فرستاده می‌شوند، ضمن این‌که اگر یکی از این خطها خراب شود امکان سویچ‌کردن به خطهای دیگر وجود دارد. اما این نکته را به خاطر داشته باشید که در multipath routing از بین مسیرهای موجود تنها آن‌هایی استفاده می‌شوند که طول آن‌ها در محدودهٔ شخصی از بهترین طول‌های موجود باشد.

۱.۱۴ فعال‌کردن IGRP

عیارسازی این پروتوکول مانند دیگر پروتوکول‌های دینامیک در دو مرحله صورت می‌گیرد:

- فعال‌کردن پروتوکول مسیریابی
- معرفی شبکه‌های وصل شده به روتر که با این پروتوکول مسیریابی کارمی کنند.

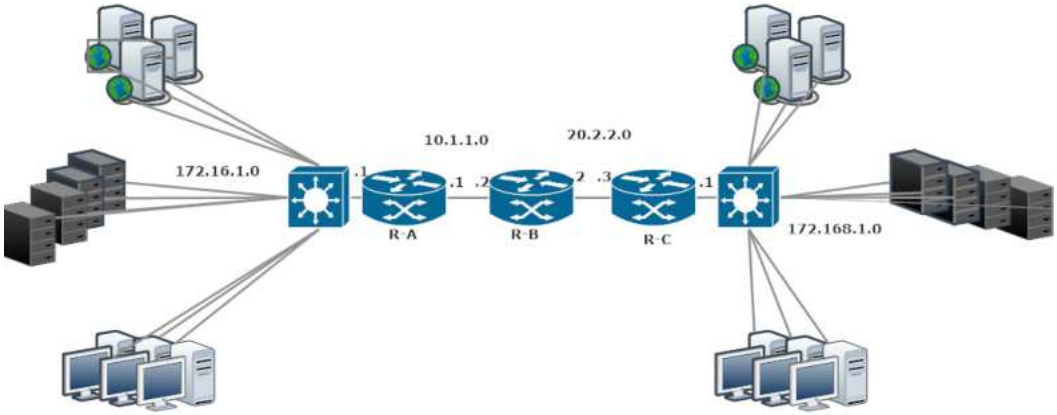
قدم اول: معرفی نوع پروتوکول مسیریابی می‌باشد که قرار است آن را روی روتر فعال کنید. برای این منظور فرمان زیر را در Globle Mode وارد می‌کنید:

```
Router(config)#router igrp autonomous-system
```

نوت: تمام کمپیوترهایی که قرار است با یکدیگر کار کنند و تبادل معلومات داشته باشند، باید در یک AS شماره یکسان قرار داشته باشند.

قدم دوم: می‌بایست به هر روتر شبکه‌های وصل‌شده را که قرار است در IGRP شرکت کنند، معرفی کنید. برای این منظور فرمان زیر را در Router-mode وارد می‌کنیم:

Router(config-router) #network network-number



شکل (۱-۵) فعال‌کردن IGRP

جدول (۲-۱) دستورهایی برای فعال‌کردن IGRP

R-A	R-B	R-C
R-A# CONF T	R-B# CONF T	R-C# CONF T
#router igrp 100	#router igrp 100	#router igrp
#network 172.16.0.0	#network 10.0.0.0	#network 192.168.1.0
#network 10.0.0.0	#network 20.0.0.0	#network 20.0.0.0

هر سه روتر A، B و C در یک AS با شماره ۱۰۰ قرار دارند و می‌خواهیم پروتوکول IGRP را روی روترهای این AS فعال کنیم؛ به‌طور مثال: راه‌اندازی IGRP را روی روتر A بررسی می‌کنیم.

گام اول، فعال‌کردن IGRP روی روتر می‌باشد. برای این منظور فرمان زیر را در globle mode وارد می‌کنیم:

```
Router(config)#router igrp 100
```

بعد از فعال‌شدن این پروتوکول، نوبت به معرفی شبکه‌هایی می‌رسد که این پروتوکول باید آن را به دیگر روترها معرفی کند. روتر A دارای دو شبکهٔ وصل‌شده با Network ID های ۱۷۲.۱۶.۰.۰ و ۱۰.۰.۰.۰ می‌باشد. بنابراین به‌صورت زیر آن‌ها را معرفی می‌کنیم:

```
Router(config-router)#network 172.16.0.0

Router(config-router)#network 10. 0.0.0
```

تا اینجا با مفاهیم اولیهٔ پروتوکول مسیریابی IGRP و نحوهٔ پیکربندی آن آشنا شدید. همان‌طورکه می‌دانید IGRP یک پروتوکول Distance-Vector می‌باشد، بنابراین برخلاف پروتوکول‌های Link-State توپولوژی شبکه را نگهداری نمی‌کند، بلکه تنها بهترین مسیرها به شبکه‌های محلی و غیر محلی را مشخص کرده و آن‌ها را در یک جدول تحت عنوان Routing Table نگهداری می‌کند. برای دیدن محتویات این جدول فرمان show ip route به‌کار می‌بریم. همان‌طوری‌که می‌دانید IGRP پروتوکولی است که Updateها را به‌صورت دورانی و به‌صورت Full Update ارسال می‌کند. همچنین IGRP دارای Timer های مختلفی می‌باشد که به‌کمک فرمان show ip protocol می‌توانید آن‌ها را مشاهده کنید. Timer ها در IGRP عبارتند از Updat, Invalid, Holddown و Flush که به‌صورت پیش‌فرض به ترتیب ۹۰،۲۷۰،۲۸۰ و ۶۳۰ می‌باشد. برای این‌که بفهمیم روترهایی که پروتوکول IGRP روی آن‌ها اجرا شده است، چه آپدیت‌هایی به هم می‌فرستند، از دستور زیر در Privileged mode استفاده می‌کنیم:

```
Router# debug IP IGRP events
```

با این دستور، کل معلومات پروتوکول IGRP پشت سر هم به‌صورت اتوماتیک نمایش داده می‌شود.

```
Router#debug IP IGRP transactions
```

این دستور به‌روز (Updates) بین دو روتر را که پروتوکول IGRP روی آن‌ها اجرا شده است، نمایش می‌دهد. برای غیر فعال‌کردن هر دو دستور از فرمان No Debug All استفاده کنید، البته با اجرای این دستور تمام دستوراتی که با debug نوشته شده‌اند، غیر فعال می‌شوند.

برای محاسبهٔ Bandwidth باید از فرمول زیر استفاده کنید:

$$\left[\left(K1.Bandwidth_E + \frac{K1.Bandwidth_E}{256 - Load} + K3.Delay_E\right).\frac{K5}{K4 + Reliability}\right].256$$

در فرمول بالا، حرف K را مشاهده می‌کنید. برای این‌که آن‌ها را پیدا کنیم باید از دستور Show IP Protocol استفاده کنیم.

```
Router#show ip protocol
Routing Protocol is "Eigrp 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates EIGRP metric weight K1=1, K2=0, K3=1,
K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
Automatic network summarization is in effect
Automatic address summarization:
Maximum path: 4
Routing for Networks:
192.168.1.0
192.168.2.0
Routing Information Sources:
Gateway Distance Last Update
Distance: internal 90 external 170
```

نکتهٔ بسیار مهم: این پروتوکول توسط سیسکو از نسخهٔ ۱۲.۳ ISO به بعد، جای خود را به پروتوکول EIGRP داده و از دنیای پروتوکول‌ها خداحافظی کرده است.

۱.۱۵ بررسی جدول مسیریابی IGRP

برای دیدن محتویات جدول مسیریابی کمند Show ip Route را در User Mode ویا Privileged Mode استفاده می‌کنیم. همان‌طورکه می‌دانید، جدول شامل لستی از شبکه‌های وصل و غیر وصل که به کمک پروتوکول IGRP به روتر معرفی شده است، می‌باشد.

شبکه‌های غیر محلی با علامت (I) مشخص شده و شبکه‌های وصل با علامت (C) مشخص می‌شود.

در مقابل هر شبکه که در جدول مسیریابی درج شده است، متریک محاسبه شده، که آن شبکه نیز در مقابل آن شبکه درج می‌باشد؛ به‌طور مثال: در شکل ذیل شبکهٔ ۲۰.۰.۰.۰ از طریق انترفیس سریال یک با متریک ۹۰۹۵۶ قابل دسترس می‌باشد.

```
R-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/1/0
I    20.0.0.0/8 [100/90956] via 10.1.1.2, 00:00:15, Serial0/1/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R-A#
```

شکل (۱-۶) IGRP Routing Tabl

خلاصه‌ی فصل اول

همان‌طورکه تابه اینجا با مفهوم Routing آشنا شدید،Routing پروسهٔ انتخاب مسیر برای دسترسی به شبکه‌های غیر محلی می‌باشد؛ بنابراین روتر با شناخت از Networkها و مسیرهای رسیدن به هر کدام و نگهداری این اطلاعات در یک جدول به‌عنوان یک مسیریاب ایفای نقش می‌کند. روتر باید بداند که اطلاعات شبکه‌های غیر محلی را از چه منابعی باید تهیه کند.

روتر باید بداندکه برای رسیدن به هر کدام از شبکه‌های غیر محلی چندین مسیر موجود است.

روتر باید بداندکه از میان تمامی مسیرهای موجود برای رسیدن به یک شبکهٔ غیر محلی کدام یک بهترین می‌باشد. و در نهایت روتر باید اطلاعات به‌دست‌آورده را در یک Database نگهداری کند تا با واردشدن یک پکت که آدرس مقصد آن شبکهٔ غیر محلی می‌باشد، هدایت در سریعترین زمان ممکن صورت گیرد.

IGRP (Interior Gateway Routing Protocol) یک پروتوکول مسیریابی Distance-Vector می‌باشد. بنابراین پروتوکولی است که اطلاعات شبکه‌های محلی و غیر محلی را در یک جدول مسیریابی نگهداری می‌کند. ویژگی عمدهٔ این پروتوکول دورانی‌بودن آن می‌باشد. متریک در این پروتوکول برخلاف RIP به چند پارامتر وابسته می‌باشد. پارامترهایی که در تعیین متریک نقش دارند، عبارت‌اند از: Reliability، Bandwidth، Delay، Load و MTU که به‌صورت پیش‌فرض IGRP در تعیین متریک فقط دو پارامتر Bandwidth و تأخیر (Delay) را دخالت می‌دهد. برای فعال‌کردن این پروتوکول روی یک روتر، دو مرحله باید انجام داد:

فعال‌نمودن پروتوکول مسیریابی؛

معرفی شبکه‌های وصل به روتری که با این پروتوکول مسیریابی کار می‌کند.

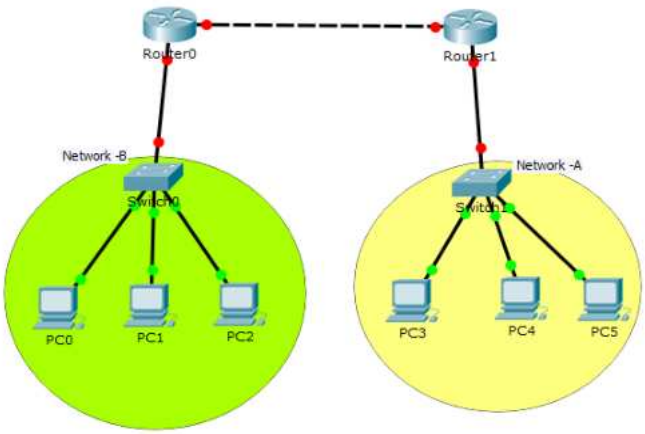
سوالات و فعالیت های فصل اول

۱. مسیریابی را تشریح نموده و نیز بگویید که چند نوع مسیریابی داریم.
۲. موارد استفاده Static Routing را به گونهٔ خلص تشریح نمایید.
۳. فرق بین Default Route و Static Route چیست؟ واضح سازید.
۴. چطور می‌توانیم که از طریق Static Routing دو شبکه را با هم وصل بسازیم؟
۵. کمنت ذیل را از نگاه لغوی تشریح نمایید و نیز بگوید که از هر کمنت چه وقت استفاده می‌شود.

Router(config)# ip route network-address subnet-mask {ip-address | exit-intf

فعالیت ها

- دو روتر را با استفاده از Static Route باهم وصل نمایید.
- یک شبکه را دیزاین نمایید که شامل دو روتر و توسط پروتوکول IGRP با هم معرفی شده باشد.
- شبکه‌های A و B ذیل را با استفاده از پروتکوول IGRP با هم وصل نمایید.



فصل دوم

پروتوکول EIGRP

هدف کلی: آشنایی محصلان با پروتوکول مسیریابی EIGRP و عملکرد آن.

اهداف آموزشی: پس از مطالعه این فصل محصلان انتظار می‌رود که:

۱. با پروتوکول مسیریابی EIGRP و عملکرد آن آشنا شوند.
۲. نحوهٔ تنظیم و پیکربندی پروتوکول مسیریابی EIGRP را بدانند.
۳. طریقهٔ تطبیق و تنظیم EIGRP را توضیح نمایند.

در فصل گذشته با روتینگ‌ها و نحوهٔ کارکرد آن آشنا شدیم. در این فصل روی موضوعاتی چون معرفی، نصب، و تفاوت عمدهٔ این پروتوکول با پروتوکول‌هایی مانند: IGRP و غیره تشریح شده است. ضمناً جدول‌های این پروتوکول و دستورات عمده‌یی که به‌خاطر فعال‌ساختن و بررسی جدول‌ها استفاده می‌شود، بحث خواهیم نمود.

۲.۱ معرفی پروتوکول EIGRP

قبل از این‌که این بحث را شروع کنیم، در مورد Administrative Distance کمی صحبت می‌کنیم:

Administrative Distance یک عدد مختص پروتوکول‌های شبکه و شبکه‌های وصل‌شده Connected است. به جدول زیر نگاه کنید:

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)

Administrator Distance معیاری است برای انتخاب یک پروتوکول، از بین پروتوکول‌های مختلف در یک شبکه، مثلاً؛ اگر به یک روتر از دو طرف معلومات برسد و یکی از این طرف‌ها Rip با ۱۲۰ AD و طرف دیگر با IGRP با ۱۰۰ AD است، برای انتخاب یکی از این مسیرها، مسیری که AD پایین‌تر دارد، انتخاب می‌شود و معلومات را از همان مسیر دریافت می‌کند.

AD مربوط به Static route که به‌صورت دستی وارد می‌کردیم، ۱ است در ادامه AD در شبکه را تغییر می‌دهیم و کارهای مختلفی روی آن انجام خواهیم داد.

پروتوکول EIGRP (Enhanced Interior Gateway Routing Protocol): یکی از محبوبترین پروتوکول‌ها در دنیای امروز است و فقط روی وسایل سیسکو کاربرد دارد، یکی از پرسرعت‌ترین پروتوکول‌ها است که سرعت Convergence یا هماهنگی بسیار بالا دارد.

۲.۲ ویژگی‌های پروتوکول EIGRP

از خانوادهٔ Distance Vector است، چون از یک جهت برای رسیدن به شبکهٔ مورد نظر استفاده می‌کند. از خانوادهٔ Link State هم است، چون نقشهٔ کامل شبکه را برای پیداکردن بهترین مسیر در دست دارد. این پروتوکول برگرفته از پروتوکول IGRP است که سیسکو آن را بازسازی کرده و سرعت آن را زیاد ساخته است و ویژگی‌های دیگری نیز به آن اضافه کرده است که از این قرار است:

- پشتیبانی از VLSM / CIDR؛
- پشتیبانی از پروتوکول‌های IP, IPX, APPLE TALK؛
- انتخاب بهترین مسیر از طریق الگوریتم انتشار مسیر Dual (Diffusing Update Algorithm)
- از دسته پروتوکول های IGPS که داخل یک AS کار می‌کند؛

۲.۳ جدول‌های پروتوکول EIGRP

پروتوکول EIGRP از چندین جدول تشکیل شده است:

۲.۳.۱ جدول Topology Database Table

کل نقشهٔ شبکه در این جدول ثبت می‌شود و یکی دیگر از ویژگی‌های آن، استفاده از مسیرهای Backbone در این جدول است، یعنی اگر مسیر اصلی down شود از مسیرهای دیگری که در این جدول ذخیره شده است، استفاده می‌کند.

۲.۳.۲ جدول Routing Table

در این جدول، بعد از محاسبات الگوریتم Dual، کوتاه‌ترین مسیر به شبکه به دست می‌آید و در این جدول قرار می‌گیرد.

۲.۳.۳ جدول Neighbors Table

در این جدول، معلومات روترهای همسایه که به‌صورت محلی به روتر اصلی وصل است، قرار می‌گیرد. زمانی‌که از الگوریتم EIGRP استفاده کنیم، این الگوریتم فقط برای اطلاع‌دادن از Update جدید از بسته‌های Hello Packet استفاده می‌کند و به‌خاطر همین از bandwidth کمتری استفاده می‌کنند، یعنی برخلاف الگوریتم‌های Distance Vector، وقتی در جدول Routing تغییر وارد می‌گردد، کل جدول را برای روترهای همسایه ارسال نمی‌کند، یعنی Periodic Update ارسال نمی‌کند و فقط همان تغییر را بدون تأخیر به دیگر روترها در شبکه اطلاع می‌دهد.

به این پروتوکول، پروتوکول Distance Vector پیشرفته هم می‌گویند به‌خاطر داشتن ویژگی‌های Distance Vector و Link State. برای محاسبهٔ Metric باید به MetricIGRP مراجعه کنید که دقیقاً همان Metric است و فقط باید عددی که به دست می‌آید در ۲۵۵ ضرب شود. فکتورهای انتخاب مسیر هم، مانند IGRP است، اما به‌صورت پیش‌فرض از Bandwidth و Delay برای انتخاب مسیر استفاده می‌شود.

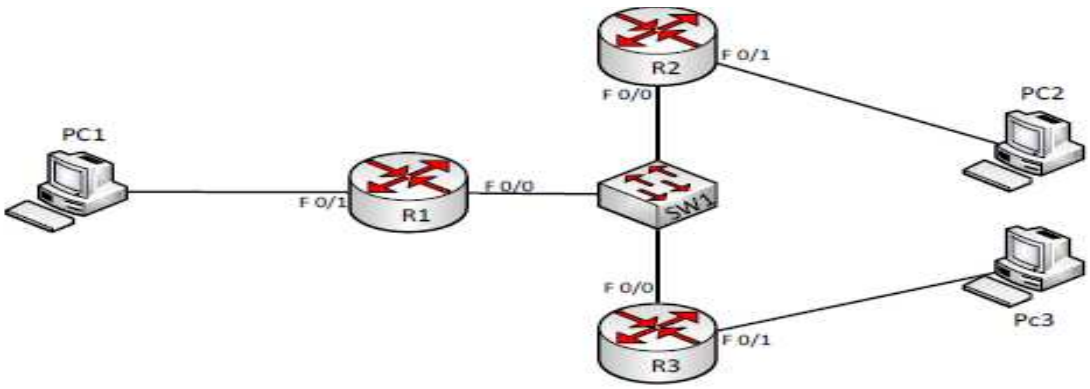
سرعت Convergence (هماهنگی با روترهای دیگر) به نسبت الگوریتم IGRP خیلی بیشتر است، به‌خاطر این‌که وقتی الگوریتم Dual به دنبال بهترین مسیر می‌گردد و مسیرهای دیگر را هم به همراه مسیر اصلی در جدول Routing ثبت می‌کند، اگر مسیر اصلی down شود، مسیر دیگر که به عنوان مسیر backup است، به جای آن مسیر شروع به کار می‌کند و این در صورتی است که الگوریتم Dual برای به‌دست‌آوردن بهترین مسیر، دوباره اجرا نمی‌شود، چون قبل از آن مسیر را پیدا کرده بود و این یکی از ویژگی‌های مهم این پروتوکول است.

نکته: به مسیر اصلی در EIGRP، Successor می‌گویند و به مسیر فرعی یا Feasible Successor نیز یاد می‌گردد.

۲.۴ کار با پروتوکول EIGRP

این پروتوکول برای شبکه‌های بزرگ، بسیار کاربرد دارد و بسیار خوب عمل می‌کند. برای فعال‌کردن این پروتوکول یک مثال را باهم انجام می‌دهیم.

مثال: سه روتر ۲۸۱۱، یک سویچ ۲۹۶۰ و سه کمپیوتر را به‌صورت زیر به هم وصل کنید.



شکل(۲-۱)شبکهٔ EIGRP

IP ها را به‌صورت جدول زیر وارد کنید:

جدول (۲-۱) لست IP Address ها.

	F 0/0	F0/1
R1	192.168.1.1/24	192.168.2.1/24
R2	192.168.2.2/24	192.168.3.1/24
R3	192.168.2.3/24	192.168.4.1/24
PC1	192.168.1.2/24	
PC2	192.168.3.2/24	
PC3	192.168.4.2/24	

بعد از واردکردن IPها در Interface مورد نظر و روشن‌کردن interface با دستور ping، شبکه را تست کنید تا وصل‌شدن به شبکهٔ روبه‌رو انجام شده باشد.

حال باید بین روترها، پروتوکول EIGRP را راه‌اندازی کنیم. برای این کار وارد R۱ می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router (config) #router Eigrp?

<1-65535> Autonomous system number
```

Router EIGRP را وارد کردیم و بعد از آن از علامت سؤال استفاده کردیم که به ما تعداد ASهای موجود را نشان می‌دهد. AS یا همان Administrative Distance، عددی برای ایجاد یک منطقه به‌خاطر ارتباط روترها باهم است؛ یعنی هر پروتوکول EIGRP در هر روتر از یک عدد مشابه استفاده کند که با روترهای دیگر در یک منطقه قرار می‌گیرند و باهم ارتباط دارند.

```
Router (config) #router eigrp 200
```

با دستور بالا، EIGRP 200 را ایجاد و وارد آن می‌شویم و بعد...

```
Router(config-router)#no auto-summary
```

همان‌طورکه در اول این درس بیان کردیم، EIGRP یک پروتوکول Classless است و برای همین از این دستور برای جلوگیری از ثبت IPها به‌صورت Class full جلوگیری می‌کنیم.

```
Router (config-router)# network 192.168.1.1?

A.B.C.D EIGRP wild card bits
```

این قسمت، برای واردکردن interfaceهای وصل‌شده connected به روتر است که کمی با پروتوکول‌های قبلی تفاوت دارد.

اول، دستور Network، بعد IP مورد نظر را به‌صورت کامل وارد می‌کنیم. در قدم بعدی، باید Mask Wild Card را وارد کنیم. این عدد برعکس Subnet Mask است که باید به‌صورت 255.0.0.0 وارد شود، یعنی قسمت آخر IP را که تغییر می‌کند، وارد کنیم که به‌صورت ذیل می‌شود:

```
Router (config-router) #network 192.168.1.1   0.0.0.255
```

شما می‌توانید به جای نوشتن Wild Card Mask فقط چهار صفر قرار دهید، به‌خاطر این‌که IPها ثابت است و تغییری ندارد و می‌خواهیم به‌صورت Classless به شبکه تزریق شود:

```
Router (config-router) #network 192.168.1.1   0.0.0.0

Router (config-router) #network 192.168.2.1   0.0.0.0
```

تا اینجا بر روی روتر R۱، پروتوکول EIGRP را با شمارهٔ AS ۲۰۰ راه‌اندازی کردیم و Networkهای مربوط به خودش را هم وارد کردیم.

نکته: وقتی Network را در یک پروتوکول تعریف می‌کنیم، به معنای این نیست که Network را به پروتوکول دادیم؛ به معنای این است که پروتوکول را روی این Network راه‌اندازی کردیم، پس به این نکته توجه کنید. تنظیمات را در روترهای دیگر هم انجام می‌دهیم.

تنظیمات روی روتر R۲

```
Router (config) #Router Eigrp 200
Router (config-router) #no auto-summary
Router (config-router) #network 192.168.2.2  0.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.1 (FastEthernet0/0) is up: new
adjacency
Router (config-router) #network 192.168.3.1  0.0.0.0
```

طوری‌که مشاهده می‌کنید در این روتر هم EIGRP ۲۰۰ تعریف کردیم، چون طوری که گفتیم روترها باید در یک EIGRP و یا در یک AS قرار گیرند تا باهم در ارتباط باشند.

همان‌طورکه مشاهده می‌کنید، بعد از واردکردن Network ۱۹۲.۱۶۸.۲.۱، سریع پیامی نمایش داده است که می‌گوید، الگوریتم Dual یک مسیر به شمارهٔ ۱۹۲.۱۶۸.۲.۱ پیدا کرده که این پروتوکول روی آن اجرا شده است.

در روتر R۳ هم تنظیمات مربوط به آن را وارد کنید:

```
Router (config) #router eigrp 200
Router (config-router) #no auto-summary
Router (config-router) #network 192.168.2.3 0.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.1 (FastEthernet0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.2 (FastEthernet0/0) is up: new adjacency
Router (config-router)#network 192.168.4.1 0.0.0.0
```

در این قسمت، به ما دو پیام نمایش داده شده که می‌گوید ۲ تا پروتوکول روی این Interfaceها فعال شده است.

تا اینجا روی همه روترها، پروتوکول EIGRP را اجرا کرده‌ایم، در این قسمت با اجرای دستور زیر جدول Routing را بررسی می‌کنیم:

دستور Show IP Route

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 - *candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route
Gateway of last resort is not set
D 192.168.1.0/24 [90/30720] via 192.168.2.1, 00:04:48, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
D 192.168.3.0/24 [90/30720] via 192.168.2.2, 00:04:47, FastEthernet0/0
C 192.168.4.0/24 is directly connected, FastEthernet0/1
```

با این دستور Show IP Route جدول routing نمایش داده شده است که اگر به جدول توجه کنید، دو شبکه را دریافت کرده که با حرف D شروع می‌شوند.

حرف D به معنای EIGRP است و نشان‌دهندهٔ این است که از روترهای دیگر این شبکه‌ها را شناخته ویا یاد گرفته، شبکه‌های پشت روترهای R۲ و R۳ را شناخته و یا یاد گرفته است.

در روترهای دیگر هم به همین صورت است.

دستور Show IP EIGRP Neighbors

برای نمایش همسایگی (Neighbors)، باید از دستور زیر در Privileged mode استفاده کنید:

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(Sec) (ms) Cnt Num
0 192.168.2.1 Fa0/0 13 00:44:14 40 1000 0 6
1 192.168.2.3 Fa0/0 11 00:39:02 40 1000 0 7
```

این دستور در روتر R۲ وارد شده است و نتیجهٔ آن را مشاهده می‌کنید، لست IPهایی را که با آن‌ها ارتباط همسایگی دارد، نمایش داده است.

دستور Show IP EIGRP Interface

این دستور برای نمایش معلومات Interface هایی است که پروتوکول EIGRP روی آن فعال شده است.

این دستور را در R۲ وارد می‌کنیم:

```
Router#show ip eigrp interface
IP-EIGRP interfaces for process 200
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa0/0 2 0/0 1236 0/10 0 0
Fa0/1 0 0/0 1236 0/10 0 0
```

به نتیجهٔ کار دقت کنید. اگر به Fa0/0 دقت کنید، نوشته است، PEER 2، یعنی این‌که از طریق Interface Fa0/0توانسته دو تا Neighbors را یاد بگیرد، Neighbors همان interface های روترهای همسایه هستند که روی آن‌ها EIGRP راه‌اندازی شده است.

دستور Show IP EIGRP Topology

این دستور کل معلومات جدول ساختار را به شما نمایش می‌دهد و می‌گوید که شبکه را از کدام مسیر دریافت کرده و...

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for AS 200
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,r - Reply status
P 192.168.2.0/24, 1 successors, FD is 28160
Via Connected, FastEthernet0/0
P 192.168.3.0/24, 1 successors, FD is 28160
Via Connected, FastEthernet0/1
P 192.168.4.0/24, 1 successors, FD is 30720
Via 192.168.2.3 (30720/28160), FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 30720
Via 192.168.2.1 (30720/28160), FastEthernet0/0
```

اگر به گزینهٔ اول نگاه کنید، می‌گوید که شبکهٔ ۱۹۲.۱۶۸.۲.۱ یک مسیر Successor است، یعنی یک مسیر اصلی است و از طریق interfaceFastEthernet 0/0 وارد همین روتر که داخل آن هستیم شده است.

بقیه هم به همین صورت است، پس نتیجه می‌گیریم که این جدول، کل interfaceهای را به ما نشان می‌دهد که EIGRP روی آن‌ها اجرا شده است.

دستور Show IP EIGRP Traffic

این دستور نشان‌دهندهٔ بسته‌های دریافتی و ارسالی، مانند زیر است:

```
Router#show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 100
Hellos sent/received: 0/0
Updates sent/received: 0/0
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 0/0
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
```

خلاصه‌ی فصل دوم

روتینگ پروتوکول EIGRP به‌روز (Updates) خودش را به‌صورت Multicast با آدرس IP اختصاص داده‌شدهٔ 244.0.0.10 می‌فرستد، Update Tiggered هست یعنی به محض به‌وجودآمدن تغییرات در شبکه آن را ارسال می‌کند. مانند این که یک لینک Down شود یا یک روتر از دسترس خارج شود یا یک روتر اضافه شود و....

از مفهومی به نام Wildcard Mask استفاده می‌کند؛ اما Wildcard Mask چیست و چه تفاوتی با Mask Subnet دارد؟ با جداکردن قسمت Network از قسم Host، مشخص می‌شد که در شبکهٔ ما چند آدرس IP وجود دارد؛ اما Wildcard Mask امکانی است که به ما داده شده تا بتوانیم چند آدرس IP را با هم یکجا تعریف کنیم.

در روتینگ پروتوکول EIGRP به دو دلیل جدول همسایگی در روتر تشکیل می‌شود:

- این‌که چک کنند همسایه‌ها زنده و Alive هستند؛
- پارامترهای همسایگی را با هم چک کنند.

با باقی روترها همسایگی تشکیل می‌دهد) از خصوصیات State Linkها بود. (اصل مسیر را ارسال می‌کند) از خصوصیات Vector Distanceها بود (اما فقط یکبار ارسال می‌کند و بعداً اگر تغییری در مسیرها ایجاد شد، فقط تغییر را ارسال می‌کند) از خصوصیات State Link ها(

جدولی به نام توپولوژی دارد (از خصوصیات State Link ها) و بهترین مسیر را از جدول توپولوژی انتخاب می‌کند و باقی مسیرها را در جدول توپولوژی نگه می‌دارد.

EIGRP (Enhanced interior Gateway Routing Protocol)، نسخهٔ پیشرفتهٔ IGRP می‌باشد که توسط شرکت سیسکو طراحی و ستندرد شده است.

EIGRP جزء دستهٔ پروتوکول IGP می‌باشد که در داخل AS کار می‌کند. EIGRP پروتوکول مسیریابی است که علاوه بر IP Routed Protocol، پروتوکول‌های IPX و Apple Talk را نیز پیشتبانی می‌کند روتری که با EIGRP کار می‌کند، معلومات خویش را درون سه جدول ذیل نگهداری می‌کند:

- Routing table
- Topology table
- Neighboring table

EIGRP برعلاوهٔ مسیر اصلی یک مسیر بدیل را نیز در Topology table خود نگهداری می‌کند که درصورت Down شدن مسیر اصلی، بدون اجرای مجدد الگوریتم DUAL مسیر دوم جاگزین مسیر اول شود، چون اجرای الگوریتم دوم زمان‌گیر می‌باشد و داشتن مسیر بدیل سرعت مسیریابی این پروتوکول را زیاد ساخته است.

سوالات فصل دوم

۱. فرق بین پروتوکول‌های IGRP و EIGRP را واضح سازید.

۲. در پروتوکول EIGRP تغییراتی که در شبکه وارد می‌شود، به چه شکل با دیگر Network ها شریک می‌شود؟

۳. Topology Table را تشریح نموده و نیز بگویید که چه وقت استفاده می‌شود.

۴. فرق بین Routing Table و Topology Table چیست؟ واضح سازید.

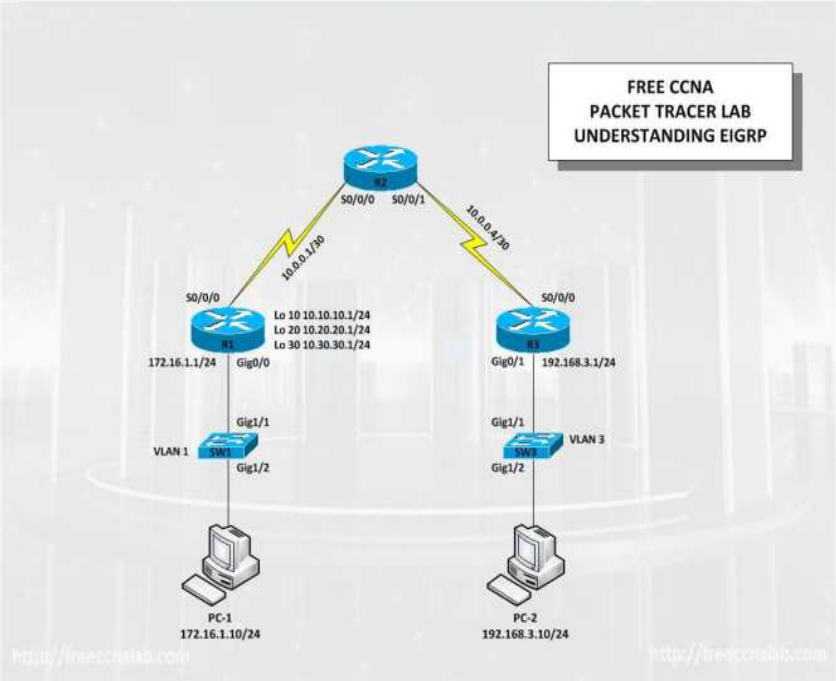
۵. توسط کدام کمنت می‌توانیم همسایه‌های یک روتر را ببینیم؟

۶. چطور می‌توانیم که پروتوکول EIGRP را روی روتر نصب نماییم؟

۷. Successor کدام مسیر است و موارد استفادهٔ آن را نیز تشریح نماید؟

فعالیت های فصل دوم

1. Hostname سویچ روتر را نظر به شکل تغییر بدهید.
2. تمام انترفیس‌های سوپچ و روتر را IP بدهد.
3. روترها را بررسی کنید و تنظیمات روی آن‌را فعال سازید.
4. دستور no domain-lookup را درسویچ‌ها فعال سازید.
5. درسویچ ها vlan3 وvlan1 را فعال کرده و پورت‌های مربوط به آن‌را شامل بسازید.
6. پروتوکول EIGRP 10 را در تمام روترها فعال سازید.
7. از دستور ping استفاده کنید و ارتباط بین Router1, Router2 وRouter3 را واضح سازید .
8. ازدستورshow ip route استفاده کنید وروتینگ های آنرا واضح سازید.



فصل سوم

پروتوکول مسیریابی OSPF

هدف کلی: آشنایی در مورد پروتوکول مسیریابی OSPF و عملکرد پیکربندی آن.

اهداف آموزشی: در پایان این فصل از محصلان انتظار میر رود که:

۱. با پروتوکول مسیریابی OSPF و عملکرد آن آشنا شوند.
۲. نحوهٔ تنظیم و پیکربندی پروتوکول مسیریابی OSPF را بدانند.
۳. طریقهٔ تطبیق و تنظیم OSPF را توضیح نمایند.

در این فصل پروتوکول مسیریابی OSPF را مورد بحث قرار می‌دهیم و OSPF همانند RIP,IGRP,EIGRP یک پروتوکول IGPs می‌باشد بنابراین دامنهٔ عملکرد آن در داخل AS می‌باشد و OSPF با دیگر پروتوکول‌های مسیریابی کاملاً متفاوت است. تفاوت عمدهٔ این پروتوکول عبارت است از تقسیم نمودن شبکهٔ بزرگ به Aeraها که در این فصل شما با پروتوکول OSPF از خانواده‌های link-state و نحوهٔ کار آن آشنا خواهید شد. بعداً به اصطلاح Areaها و میکانیزمی که چطور پروتوکول OSPF می‌تواند Areaها را ایجاد و باهم وصل نماید. در قدم دوم با پروسهٔ عملی‌سازی پروتوکول به‌شکل سیستماتیک آشنا خواهید شد.

۳.۱ پروتوکول OSPF

پروتوکول (Open Shortest Patch First) OSPF یک پروتوکول آزاد است و مختص به شرکت خاصی نیست و توسط سازمان IETF در سال ۱۹۸۸ نوشته شده است، مانند EIGRP نیست که فقط در روترهای سیسکو قابل اجرا باشد، بلکه در تمام روترهای شرکت‌های مختلف کاربرد دارد.

پس اگر شما در شبکه‌های خود از روترهای مختلف با برَندهای مختلف استفاده کنید، نمی‌توانید روی آن‌ها EIGRP اجرا کنید، بلکه فقط باید پروتوکول OSPF یا RIP روی آن‌ها اجرا کنید تا بتوانند باهم دیگر ارتباط برقرار کنند.

این پروتوکول از مجموعه پروتوکول‌های Link state و زیرمجموعهٔ پروتوکول‌های IGPs است، یعنی داخل یک AS کار می‌کنند. الگوریتمی که در این پروتوکول استفاده می‌شود، Dijkstra است.

OSPF که در این قسمت آن را بررسی می‌کنیم، OSPF Version ۲ است که با IPV۴ کار می‌کند و در آخر کتاب، در قسمت IPV۶از OSPF Version ۳ استفاده می‌شود.

OSPF از جدولی به نام Link-State Database استفاده می‌کند که کل معلومات شبکه یا نقشهٔ شبکه را برای انتخاب کوتاه‌ترین مسیر در خود ذخیره می‌کند و برای به‌دست‌آوردن کوتاه‌ترین مسیر از الگوریتمی به نام SPF استفاده می‌کند و بعد از پیداشدن مسیر، آن را در جدول دیگری به نام Routing Table ذخیره می‌کند.

OSPF برای ارسال آپدیت Update از بسته‌هایی به نام (Link-State Advertisement) LSA استفاده می‌کند که معلومات جدول خود را به نام Link-State Database به روترهای دیگر ارسال می‌کند. در فصل گذشتهٔ کتاب گفتیم که از پروتوکول‌های Distance Vector برای ارسال به‌روز Update کل جدول به روترهای همسایه استفاده می‌شد که به‌عنوان Periodic Update بود، اما در OSPF این چنین نیست.

اگر تغییری در جدول ایجاد شود، این تغییر بلافاصله از طریق LSA که در بالا توضیح دادیم به بقیهٔ روترها خبر داده می‌شود و خیلی کم از Bandwidth شبکه استفاده می‌کند، به این آپدیت، Triggered Update می‌گویند که تغییرات را بسیار سریع اعلام می‌کند.

باید گفت: این گونه هم نیست که OSPF نخواهد کل جدول را هرگز ارسال نکند، این کار را هر 30 دقیقه یکبار انجام می‌دهد که کل جدول Database را به شبکهٔ مورد نظر ارسال می‌کند.

این پروتوکول برای شبکه‌های بزرگ بسیار کارآمد است و در حال حاضر در حال استفاده در شبکه‌های بزرگ است.

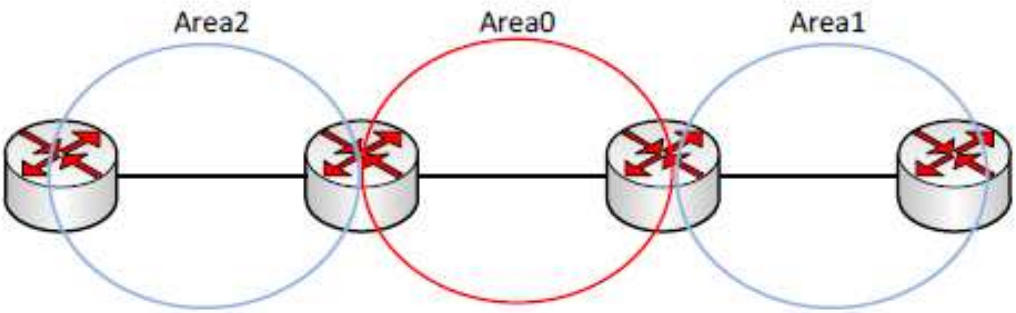
OSPF شبکه‌های بزرگ را به ناحیه‌های (Area) مختلف تقسیم می‌کند که دلایل خاص خودش را دارد:

با ایجاد ناحیه، سرعت کار این الگوریتم بسیار افزایش پیدا می‌کند.

کم‌حجم شدن جدول Routing به خاطر ایجاد ناحیه؛

مدیریت بر چند روتر بهتر از مدیریت بر چندین روتر است.

با ایجاد ناحیه، اگر یکی از روترها دست‌کاری شود یا مشکلی برای آن پیش آید، بقیهٔ روترها در ناحیهٔ دیگر بدون مشکل به کار خود ادامه می‌دهند.



شکل (۳-۱) OSPF areas

Backbone Area یا Area0 ناحیه‌یی است که Areaهای دیگر به آن متصل می‌شوند و تمام معلومات Areaهای دیگر باید از این Area رد شود، پس این Area به‌عنوان Backbone یا ستون فقرات شبکهٔ OSPF شناخته می‌شود به طور خلاصه می‌توان گفت این Area پادشاه همهٔ Area ها است.

نکته: اگر دسته‌بندی یا ناحیه در OSPF وجود نداشت، الگوریتم SPF که وظیفهٔ پیداکردن کوتاه‌ترین مسیر را انجام می‌دهد، با مشکل مواجه خواهد شد. چون جدول Database که گراف شبکه در آن قرار دارد، بسیار بزرگ می‌شود.

توجه داشته باشید که با ایجاد یک Area، الگوریتم SPF فقط در همان Area پروسس خود را انجام می‌دهد و بر کل شبکه تأثیر ندارد، پس الگوریتم SPF (Shortest Path First)، تنها در یک Area پروسس خود را انجام می‌دهد و زمانی که به نتیجه برسد، این نتیجه را با Areaهای دیگر در میان می‌گذارد.

۳.۲ انتخاب بهترین مسیر در OSPF

در OSPF انتخاب بهترین مسیر از طریق متریکی به نام Cost انجام می‌شود که از طریق الگوریتم SPF کوتاه‌ترین مسیر به دست می‌آید. به این نکته توجه داشته باشید که هر قدر Bandwidth یک خط بیشتر باشد، Cost آن کمتر است، پس Bandwidth رابطهٔ معکوس با Cost دارد.

۳.۳ راه‌اندازی پروتوکول OSPF

برای فعال‌کردن پروتوکول OSPF باید از دستور زیر به همراه یک Process ID استفاده شود:

```
Router (Config) # router ospf?

Process ID<1-65535>
```

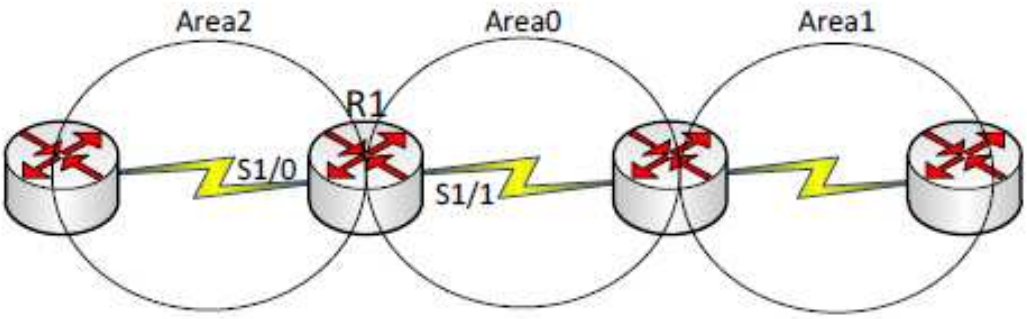
در پروتوکول EIGRP، شماره‌یی که اختصاص می‌دهیم، باید در همهٔ روترها یکی باشد، اما شماره‌یی که به پروتوکول OSPF داده می‌شود، لازم نیست که در همهٔ روترها یکی باشد، از شمارهٔ ۱ تا ۶۵۵۳۵ می‌توانید اختصاص دهید، پس مانند ASها نیستند که باید در همهٔ روترها یکی باشد.

این عدد فقط برای متفاوت‌کردن OSPF ها باهم است.

برای تعریف Network، باید از روش زیر استفاده کنید:

```
(config-router) #Network 192.168.1.1 0.0.0.0 area0Router
```

برای تعریف شبکه، IP Address را وارد می‌کنیم، بعداً Wild Card Mask را و بعد از آن مشخص می‌کنیم که این شبکه در کدام Area یا ناحیه قرار دارد. به شکل نگاه کنید، اگر توجه داشته باشید S1/1 مربوط به R1 در Area0 قرار دارد، پس اگر وارد این روتر شدیم در موقع تعریف شبکه در پروتوکول OSPF باید آن را داخل Area0 قرار دهیم؛ مثلاً: در سمت دیگر، روتر R1 پورت سریال S1/0 در Area2 قرار دارد که باید در تعریف شبکهٔ این پورت در Area2 قرار دهیم.



شکل (۳-۲) راه‌اندازی OSPF

در مورد Wild Card Mask که باهم در پروتوکول EIGRP گفتیم که این عدد برعکس Subnet Mask است و بعد از آن گفتیم که لازم نیست که Wild Card Mask بنویسید، فقط به جای Wild Card Mask از چهار تا صفر استفاده کنید.

۳.۴ Router ID

نشان‌دهندهٔ یک روتر در شبکهٔ OSPF است که برای ارتباط روترها باهم در پروتوکول OSPF از این نشانه استفاده می‌کنند.

از این به بعد Router ID را خلاصه می‌کنیم و از RID استفاده می‌کنیم.

این IP از بین IPهای یک روتر انتخاب می‌شوند که بزرگترین IP آدرس باشد. همان‌طورکه می‌دانید این Interface ها که IP روی آن‌ها Set شده است به‌صورت فزیکی می‌باشند و زمانی که Down شوند، بر روی کارکرد پروتوکول OSPF تأثیرگذار است و باعث مشکل در شبکه می‌شود. برای حل این مشکل باید از یک Interface مجازی استفاده کرد که هیچ وقت Down نمی‌شود. این Interface، loopback است که در قسمت‌های قبل از کتاب با این Interface کار کردیم.

نکته: اگر شما از چندین loopback استفاده کنید، RID از بین آن‌هایی انتخاب می‌شود که بالاترین IP Address را دارند.

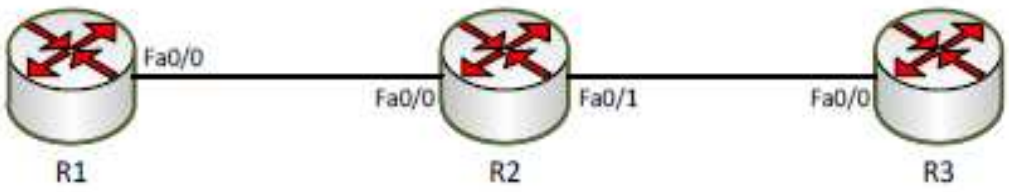
۳.۵ روترهای DR و BDR

در شبکه‌های تحت OSPF، روتری تحت عنوان DR (Designated Router) وجود دارد که همهٔ روترهای داخل یک Area، تمام معلومات و تغییرات را به این روتر می‌فرستند و این روتر به دیگر روترها اعلام می‌کند، یعنی این‌که هر روتر هر تغییری را به همهٔ روترها ارسال نمی‌کند که باعث ایجاد بار سنگین در شبکه شود؛ فقط معلومات خود را به روتر اصلی در شبکه، یعنی DR می‌فرستد و DR آن را پخش می‌کند.

اما اگر این روتر از کار بیفتد، چه باید کرد؟ اگر این روتر Down شود، روتری که BDR (Backbone Designated Router) است به جای آن کار می‌کند و تمام معلومات به این روتر ارسال می‌شود.

نکته: درصورتی‌که تغییری در شبکه OSPF رخ دهد، این تغییر از طریق (Link state Update) LSU به روترهای DR و BDR فرستاده می‌شود، پس توجه داشته باشید که هرچه در روتر DR وجود دارد در روتر BDR هم وجود دارد.

نکته: روترهای DR و BDR در هر Area وجود دارند، اما بین هر Subnet قرار دارند. به‌شکل زیر توجه کنید:

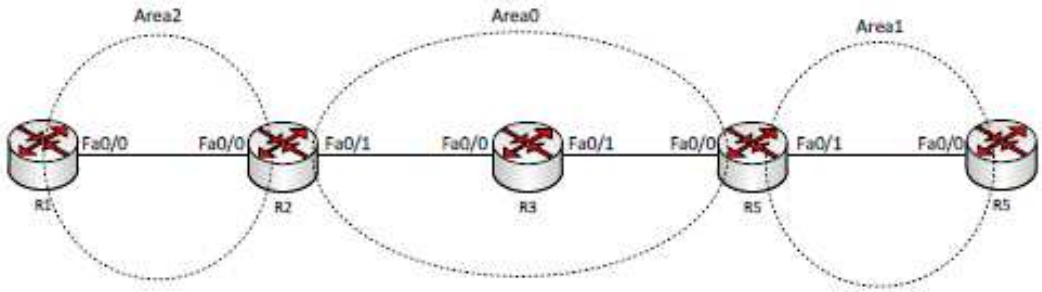


شکل(۳-۳) معرفی روترهای DR و BDR

روترهای DR و BDR بین دو Subnet انتخاب می‌شود، یعنی این‌که در شکل بالا بین روترهای R۱ و R۲ یک آدرس 172.16.1.0 وجود دارد که بین این دو روتر، روتری به‌عنوان DR انتخاب می‌شود که IP Address بزرگ‌تر داشته باشد، البته یک فکتور دیگر در انتخاب روترهای DR و BDR وجود دارد که خیلی مهمتر از بقیه فکتورها است و آن‌هم Priority است که اگر Priority یک روتر از روتر دیگر بزرگتر باشد، همان روتر به‌عنوان DR انتخاب می‌شود، اما به‌صورت پیش‌فرض Priority=۱ است و به‌خاطر همین از IP Address برای انتخاب روترهای DR و BDR استفاده می‌کنند.

مثال ۳: در این مثال، نحوهٔ راه‌اندازی پروتوکول OSPF را باهم کار می‌کنیم.

چهار روتر را به لست اضافه کنید و به‌صورت زیر به هم متصل نمایید:



	Fa0/0	Fa0/1	LoopBack
R1	172.16.1.1/16		150.1.1.1/24
R2	172.16.1.2/16	172.16.2.1/16	150.1.2.2/24
R3	172.16.2.2/16	172.16.3.1/16	150.1.3.3/24
R4	172.16.3.2/16	172.16.4.1/16	150.1.4.4/24
R5	172.16.4.2/16		150.1.5.5/24

بعد از تخصیص IP ها به‌صورت جدول بالا در روتر باید پروتوکول OSPF را راه‌اندازی کنیم:

روتر R۱:

```
Router(config) #router ospf 20
```

تعریف Router OSPF ۲۰ که ۲۰ یک شمارهٔ شناسایی برای این پروتوکول است‌که تأثیری در روند کار ندارد، اما باید تعریف شود.

```
Router(config-router) #router-id 150.1.1.1
```

در این قسمت باید RID روتر را تعریف کنید که این IP مربوط به Loopback interface است، پس بعد از ورود به پروتوکول OSPF در درجهٔ اول RID را تعریف کنید.

```
Router (config-router) #network 172.16.1.1 0.0.0.0 area 2
```

در این قسمت Networkهای مربوط به روتر را تعریف می‌کنیم و می‌گوییم که در کدام Area قرار دارد؛ مثلاً در این قسمت، Interface Fa۰/۰روتر R۱ در Area۲ قرار دارد. در تعریف Network، اول خود IP و بعد، Wild Card Mask مربوط به آن را وارد می‌کنیم. همان‌طورکه در مطالب قبل کتاب گفتیم، سعی کنید به جای Wild Card Mask از چهار صفر استفاده کنید (۰.۰.۰.۰). در بقیه روترها هم همین کار را انجام دهید:

روتر R۲:

```
Router (config) #router ospf 10
Router (config-router) #router-id 150.1.2.2
Router (config-router) #network 172.16.1.2 0.0.0.0 area 2
Router (config-router) #network 172.16.2.1 0.0.0.0 area 0
```

روتر R۳:

```
Router(config)#router ospf 10
Router(config-router)#router-id 150.1.3.3
Router(config-router)#net 172.16.2.2 0.0.0.0 area 0
Router(config-router)#net 172.16.3.1 0.0.0.0 area 0
```

روتر R۴:

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.4.4
Router(config-router)#net 172.16.3.2 0.0.0.0 area 0
Router(config-router)#net 172.16.4.1 0.0.0.0 area 1
```

روتر R۵::

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.5.5
Router(config-router)#net 172.16.4.2 0.0.0.0 area 1
```

در این قسمت، از طریق دستور Show ip Route، نگاهی به جدول Routing روتر R۱ می‌کنیم و این دستور را در Privileged mode وارد می‌کنیم:

```
Router#show Ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 - *candidate default, U - per-user static route, o – ODR
P - Periodic downloaded static route
Gateway of last resort is not set
150.1.0.0/24 is subnetted, 1 subnets
C 150.1.1.0 is directly connected, Loopback0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
O IA 172.16.2.0 [110/2] via 172.16.1.2, 00:14:31, FastEthernet0/0
O IA 172.16.3.0 [110/3] via 172.16.1.2, 00:11:56, FastEthernet0/0
O IA 172.16.4.0 [110/4] via 172.16.1.2, 00:08:42, FastEthernet0/0
Router(config)#
```

همان‌طورکه مشاهده می‌کنید، Networkهای که از طریق OSPF یاد گرفته است، به‌صورت O IA نمایش داده است که O IA، بیانگر OSPF inter area است و نشان‌دهندهٔ این است که این شبکه‌ها را از Area دیگری غیر از Area خود یاد گرفته است و اگر یک روتر در Area خود چیزی یاد بگیرد، آن را با حرف O ثبت می‌کند.

نکته: تمام دستوراتی که در Privileged mode اجرا می‌شوند، در Global mode هم اجرا می‌شوند، اما این کار باید از طریق اضافه‌کردن کلمهٔ do به اول دستور انجام شود. به مثال زیر توجه کنید:

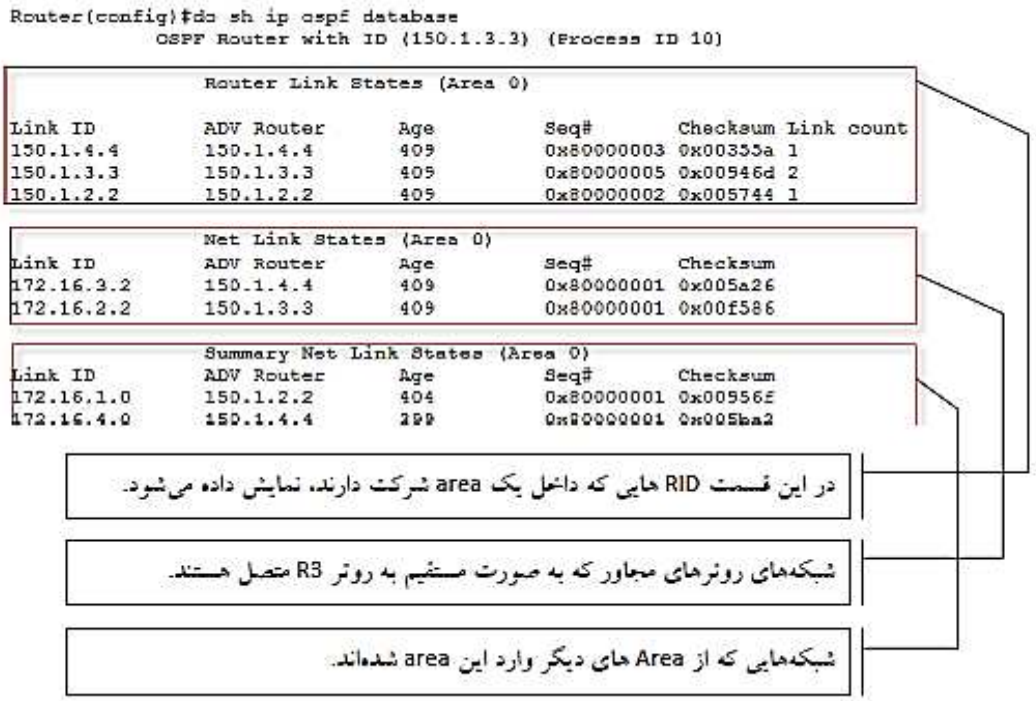
```
Router(config)#do sh ip int b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 172.16.2.2 YES manual up up
FastEthernet0/1 172.16.3.1 YES manual up up
Loopback0 150.1.3.3 YES manual up up
Vlan1 unassigned YES unset administratively down down
```

همان‌طورکه مشاهده می‌کنید، دستور Show ip interface brief را هم به‌صورت کوتاه‌شده و هم در Global mode با اضافه‌کردن کلمهٔ do اجرا کردیم، به همین سادگی، پس همیشه کلمهٔ do یادتان باشد و سعی کنید از این کلمه استفاده کنید تا سرعت کار بالا رود.

کلمهٔ do را زمانی استفاده می‌کنیم که بخواهیم دستوراتی را که در Privileged mode اجرا می‌شوند، در Global mode استفاده کنیم؛ مانند: دستور Ping که در Global mode اجرا نمی‌شود، اما اگر در اول این دستور، کلمهٔ do قرار گیرد، اجرا می‌شود.

۳.۶ دستور Show IP OSPF Database

این دستور را در روتر R۳ و در Global mode با اضافه‌کردن کلمهٔ do اجرا کنید:



دستور Show ip OSPF Interface

این دستور، interfaceهای فعال در پروتوکول OSPF را نمایش می‌دهد. در روتر R۳ این دستور را اجرا می‌کنیم:

```
Router#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
Internet address is 172.16.2.2/24, Area 0
Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 150.1.3.3, Interface address 172.16.2.2
Backup Designated Router (ID) 150.1.2.2, Interface address 172.16.2.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, adjacent neighbor count is 1
Adjacent with neighbor 150.1.2.2 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
Internet address is 172.16.3.1/24, Area 0
Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 150.1.4.4, Interface address 172.16.3.2
Backup Designated Router (ID) 150.1.3.3, Interface address 172.16.3.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, adjacent neighbor count is 1
Adjacent with neighbor 150.1.4.4 (Designated Router)
Suppress hello for 0 neighbor(s)
```

همان‌طورکه در بالا مشاهده می‌کنید، روترهای DR و BDR را مشخص کردیم. در بین روترهای R۲ و R۳، روتر R۳ به‌خاطر داشتن IP Address بزرگ‌تر به‌عنوان روتر DR انتخاب شده است و روتر R۲ به‌عنوان BDR انتخاب شده است و در بین روترهای R۳ و R۴ روتر R۴ به‌عنوان DR و روتر R۳ به‌عنوان BDR انتخاب شده است.

۳.۷ دستور Show ip OSPF Neighbor

```
Router# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
150.1.2.2 1 FULL/BDR 00:00:31 172.16.2.1 FastEthernet0/0
150.1.4.4 1 FULL/DR 00:00:31 172.16.3.2 FastEthernet0/1
```

با این دستور می‌توانید،DR یا BDR بودن روترهای همسایه را مشخص کنید. همان‌طوری که مشاهده می‌کنید این دستور در روتر R۳ اجرا شده و در نتیجهٔ آن به ما RID روترهای همسایه را نشان داده است و مشخص کرده است که روتر R۴ به‌عنوان DR و روتر R۲ به‌عنوان BDR انتخاب شده است.

۳.۸ دستور Show ip OSPF Border–routers

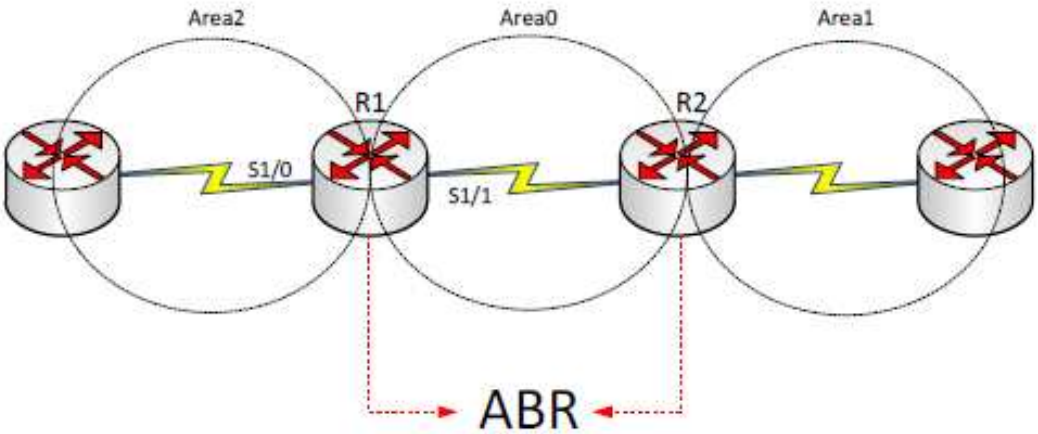
```
Router#show ip ospf border-routers
OSPF Process 10 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 150.1.2.2 [1] via 172.16.2.1, FastEthernet0/0, ABR, Area 0, SPF 1
i 150.1.4.4 [1] via 172.16.3.2, FastEthernet0/1, ABR, Area 0, SPF 1
```

این دستور، روترهای همسایه را به ما نشان می‌دهد و IP Address آن را مشخص می‌کند.

۳.۹ روتر ABR (Area Border Router)

به روتری می‌توانید که بین دو Area قرار دارد و کار انتقال معلومات از یک Area به Area دیگر را بر عهده دارد.

به شکل زیر توجه کنید:



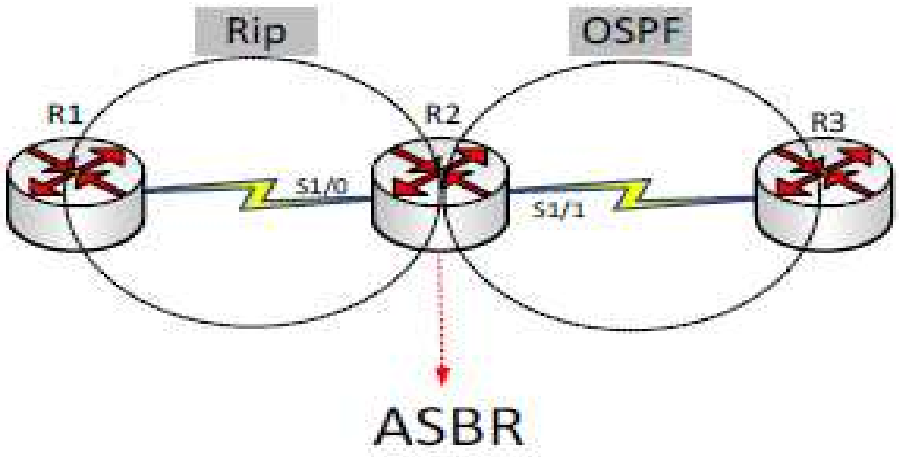
شکل ۳-۴ : معرفی روتر ABR

همان‌طورکه در شکل بالا مشاهده می‌کنید، روترهای R۱ و R۲ روترهایی هستند که بین دو Area قرار دارند و کار انتقال را انجام می‌دهند که به این روترها، روترهای ABR گفته می‌شود.

۳.۱۰ روتر ASB (Autonomous System Border Router)

این روتر کار انتقال معلومات از یک پروتوکول یا یک Domain دیگر به داخل OSPF را انجام می‌دهد.

به‌شکل زیر توجه کنید:



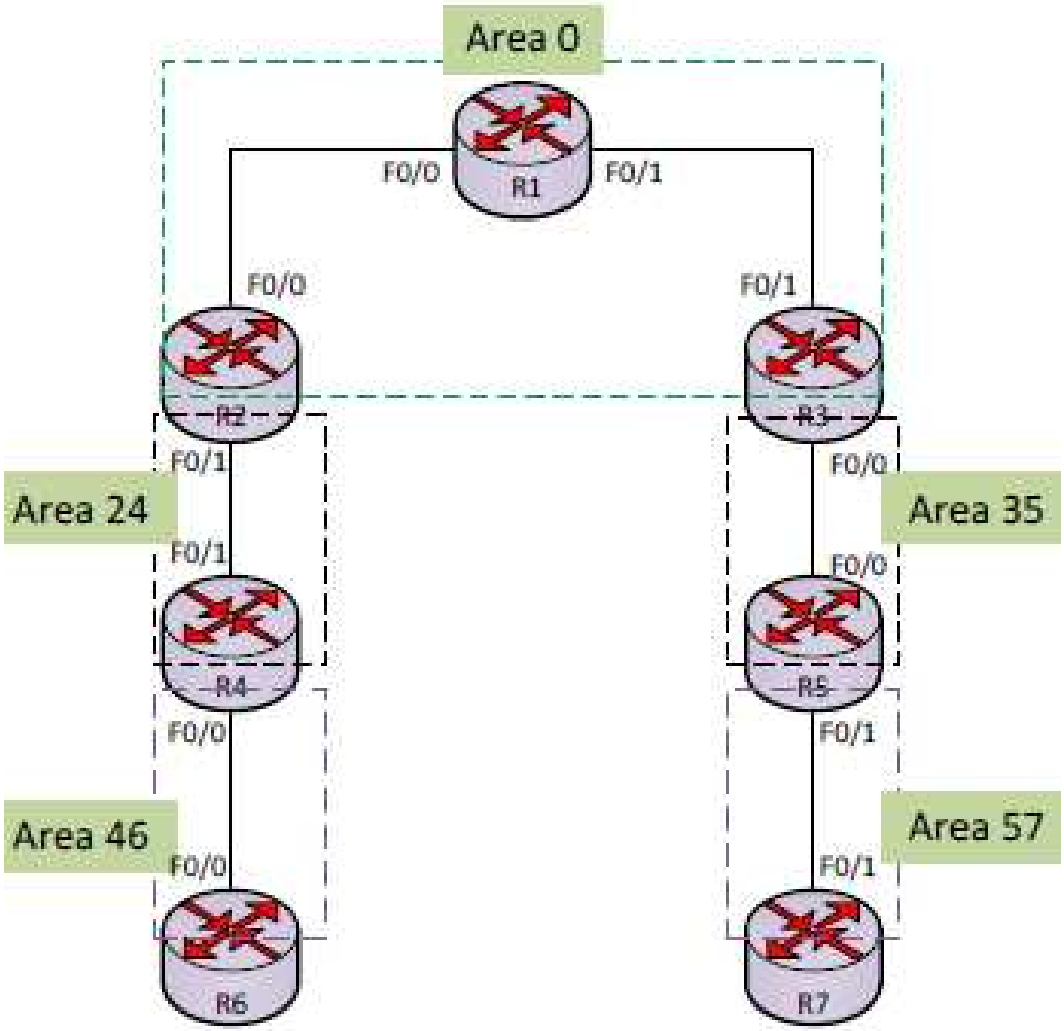
شکل ۳-۵ : معرفی روتر ASB

در این شکل روتر R۲ بین دو پروتوکول قرار دارد و کار ترجمه یا Redistribute را انجام می‌دهد و به‌عنوان روتر ASBR شناخته می‌شود.

۳.۱۱ کار با Virtual Link در OSPF

همان‌طورکه قبلاً بیان کردیم، تمام Areaها باید به Area۰ متصل باشند تا بتوانند معلومات خود را انتقال دهند. اگر این Areaها به‌صورت مستقیم، مانند شکل زیر به Area۰ متصل نباشند، نمی‌توانند دیتاها را انتقال دهند.

برای درک این موضوع یک مثال را باهم بررسی می‌کنیم:



در این مثال، Areaهای 46 و 57 نمی‌توانند معلومات خود را در شبکه ارسال کنند، به این علت که به Area0 متصل نیستند. برای حل این مشکل از Area 24.35 که بین این دو Area قرار دارد، کمک می‌گیریم و یک لینک مجازی بین Area ها ایجاد می‌کنیم. برای این کار باید وارد روترهای مرزی شویم که در این مثال برای متصل‌شدن Area46 به Area0 از روترهای R4 و R2 کمک می‌گیریم و Virtual link را روی این دو فعال می‌کنیم تا یک پل از Area46 به Area0 زده باشیم.

جدول IP Address به‌صورت زیر است:

Router	F0/0	F0/1	LoopBack
R1	1.1.12.1/24	1.1.13.1/24	100.1.1.1/24
R2	1.1.12.2/24	1.1.24.2/24	100.2.2.2/24
R3	1.1.35.3/24	1.1.13.3/24	100.3.3.3/24
R4	1.1.46.4/24	1.1.24.4/24	100.4.4.4/24
R5	1.1.35.5/24	1.1.57.5/24	100.5.5.5/24
R6	1.1.46.6/24	...	100.6.6.6/24
R7	...	1.1.57.7/24	100.7.7.7/24

بعد از واردکردن IP Address در روترها باید پروتوکول OSPF را روی تک تک روترها فعال کنیم، وارد روتر R۱ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.1.1.1
Router(config-router)#network 1.1.12.1 0.0.0.0 area 0
Router(config-router)#network 1.1.13.1 0.0.0.0 area 0
```

همان‌طورکه مشاهده می‌کنید، پروتوکول OSPF را روی این روتر فعال و شبکه‌های مربوط به آن معرفی کردیم؛ در بقیهٔ روترها هم به‌صورت زیر عمل می‌کنیم:

وارد روتر R۲ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.2.2.2
Router(config-router)#network 1.1.12.2 0.0.0.0 area 0
Router(config-router)#network 1.1.24.2 0.0.0.0 area 24
```

وارد روتر R۳ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.3.3.3
Router(config-router)#network 1.1.13.3 0.0.0.0 area 0
Router(config-router)#network 1.1.35.3 0.0.0.0 area 35
```

وارد روتر R۴ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.4.4.4
Router(config-router)#network 1.1.24.4 0.0.0.0 area 24
Router(config-router)#network 1.1.46.4 0.0.0.0 area 46
```

وارد روتر R۵ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.5.5.5
Router(config-router)#network 1.1.35.5 0.0.0.0 area 35
Router(config-router)#network 1.1.57.5 0.0.0.0 area 57
```

وارد روتر R۶ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.6.6.6
Router(config-router)#network 1.1.46.6 0.0.0.0 area 46
```

وارد روتر R۷ شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.7.7.7
Router(config-router)#network 1.1.57.7 0.0.0.0 area 57
```

بعد از اتمام کار، اگر وارد روتر R۶ و R۷ شوید و دستور Show ip Route را وارد کنید، متوجه می‌شوید هیچ شبکه‌یی را از طریق OSPF یاد نگرفته است.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 - *candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route
Gateway of last resort is not set
1.0.0.0/24 is subnetted, 1 subnets
C 1.1.46.0 is directly connected, FastEthernet0/0
```

همان‌طورکه مشاهده می‌کنید، هیچ شبکه‌یی را از طریق پروتوکول OSPF یاد نگرفته است، به‌خاطر این که Area ۴۶ و Area ۵۷ به Area۰ متصل نیستند. برای حل این مشکل یک پُل به Area۰ مزنیم.

۳.۱۲ ایجاد Virtual link

برای ایجاد این ارتباط، باید وارد روترهای R۲ و R۴ و روترهای R۳ و R۵شوید و دستور ساخت Virtual link را وارد کنید:

وارد روتر R۲ شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 24 virtual-link 100.4.4.4
```

همان‌طورکه مشاهده می‌کنید، اول وارد OSPF ۱ شدیم که قبلاً ایجاد کردیم و بعد با دستور Area۰ virtual-link ۱۰۰.۴.۴.۴ به روتر گفتیم که یک virtual link ایجاد کند. برای ارتباط با روتر روبرو که مرز بین Area دیگر است، این کار را باید در طرف روبرو هم انجام دهیم، یعنی روتر R۴.

وارد روتر R۴ شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)# area 24 virtual-link 100.2.2.2
```

بعد از این که در روتر R۴ هم این دستور را وارد کردید، ارتباط بین Area ۴۶ و Area۰ توسط این ارتباط برقرار می‌شود. برای درک این موضوع وارد روتر R۶ شوید و دستور Show ip route را وارد کنید:

```
Router# show Ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 - *candidate default, U - per-user static route, o - ODR
P - Periodic downloaded static route
Gateway of last resort is not set
 24/1.0.0.0is subnetted, 5 subnets
O IA 1.1.12.0 [110/3] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA 1.1.13.0 [110/4] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA 1.1.35.0 [110/5] via 1.1.46.4, 00:00:56, FastEthernet0/0
C 1.1.46.0 is directly connected, FastEthernet0/0
O IA 1.1.57.0 [110/6] via 1.1.46.4, 00:00:56, FastEthernet0/0
```

روتر R۶ تمام آدرس‌های شبکه را از طریق OSPF یاد گرفته است. در ادامه باید همین کار را در طرف دیگر نیز وارد کنید، یعنی بین روترهای R۳ و R۵:

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.5.5.5
```

وارد روتر R۵: شوید و دستور زیر را وارد کنید:

بعد از اتمام کار، تمام روترها در شبکه قابل شناسایی هستند و می‌توانند همدیگر را ببینند.

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.3.3.3
```

خلاصه‌ی فصل سوم

First Short Path First (OSPF) یک پروتوکول از دستهٔ پروتوکول‌های IGPs می‌باشد بنابراین پروتوکولی است که در داخل AS معتبر بوده و مسیریابی را انجام می‌دهد. از طرفی OSPF جزء پروتوکول‌های Link State می‌باشد. و توپولوژی شبکه را به‌صورت درختی درآورده که خود رأس و ریشهٔ این درخت می‌باشد، سپس این توپولوژی به‌دست‌آورده را در یک State-Link Database نگهداری می‌کند. پس از تکمیل Database State-Link به کمک الگوریتمی تحت عنوان Dijkstra یا همان Algorithms SPF کوتاه‌ترین مسیرها را تعیین و در Routing Table خود نگهداری می‌کند OSPF برخلاف پروتوکول‌های Distance-Vector، Periodic نمی‌باشد. این بدان معنی است که روتر کل اطلاعات Routing Table اش را به‌صورت Periodic Update به روترهای مجاورش ارسال نمی‌کند، بلکه فقط تغییراتی را که در Link-State Database رخ دهد، به روترهای دیگر اطلاع می‌دهد. بنابراین هر کدام از روترها با اصلاح‌کردن Link-State Database خود الگوریتم SPF را اجرا کرده و Routing Table خود را می‌سازند. ویژگی دیگر این پروتوکول، این است که شبکهٔ بزرگ را به Area تقسیم می‌کند که این تقسیمات باعث مدیریت خوب و جدول مسیریابی کوچک می‌شود و نیز از مصرف Bandwith بیشتر جلوگیری می‌کند.

سوالات فصل سوم

۱. موارد استفاده Router ID را واضح سازید.

۲. برتری‌های پروتوکول OSPF نظربه دیگر پروتوکول‌ها چیست؟ شرح سازید.

۳. پروسهٔ ایجاد DR/BDR را در یک مثال عملی واضح سازید.

۴. Administrative Distance پروتوکول OSPF چند است؟ و نیز بگویید که AD به خاطر کدام هدف استفاده می‌شود.

۵. یک شبکه Area Single را با استفاده از پروتوکول OSPF بسازید که شامل سه روتر باشد.

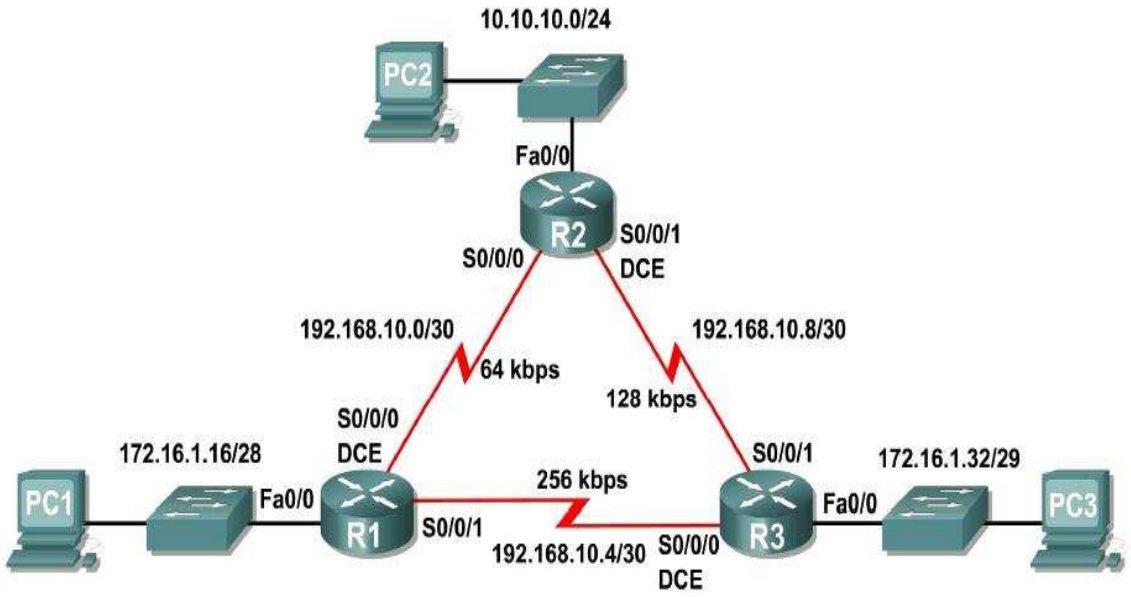
۶. دستور ذیل به‌خاطر چی استفاده می‌شود واضح بسازید:

Router(Config)#interface loopback number

۷. بسته‌های پروتوکول OSPF را نام ببرد.

فعالیت های فصل سوم

- شبکه را نظر به‌شکل زیر دیزاین کنید. آدرس‌های تمام انترفیس‌ها را نظر به جدول و subnet که داده شده، آن را انجام دهید و پورت‌های آن را فعال سازید.
- Hostname سویچ روتر را نظر به‌شکل تغییر بدهید.
- روترها را بررسی کنید و تظیمات روی آن را فعال سازید.
- دستور no domain-lookup را در سویچ‌ها و روتر فعال سازید.
- پروتوکول OSPF را در تمام روترهایی که در شکل ذیل داده است فعال سازید.
- از دستور ping استفاده کنید و ارتباط بین Router را واضح سازید.
- از دستور show ip route استفاده کنید و مسیرهای لینک‌های route شده را شرح دهید.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A
	S0/0/0	192.168.10.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A
	S0/0/0	192.168.10.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

فصل چهارم

VALN

هدف کلی: در ختم فصل محصلان قادر خواهند بود تا با Trunk, VLAN و نحوۀ عملکرد آن و با پروتوکول‌های *ISL* و *۸۰۲.۱Q*آشنا شده عیارسازی و تطبیق آن را اجرا نمایند.

اهداف آموزشی: در پایان این فصل از محصلان انتظار می رود که:

۱. Trunk و نحوۀ عملکرد آن را در انتقال اطلاعات میان VLAN شرح دهند.
۲. با پروتوکول‌های ISL و ۸۰۲.۱Q آشنایی حاصل نمایند.
۳. با نحوۀ تنظیم پروتوکول‌های ISL و ۸۰۲.۱Q آشنا شوند.
۴. Native VLAN را بدانند.

در این فصل VLAN (Virtual LAN Protocol) مورد بحث قرار می‌دهیم زمانی‌که چندین کمپیوتر را به یک سویچ متصل می‌کنیم، آن‌ها به راحتی می‌توانند باهم ارتباط داشته باشند و از منابع شبکه استفاده کنند. اما تعداد زیاد کمپیوترها می‌تواند حجم کاری سویچ را افزایش دهند، یعنی این‌که تمام سویچ‌ها در یک منطقهٔ کاری باهم در ارتباط هستند و امنیت در این نوع شبکه‌ها بسیار پایین می‌آید، اما می‌توان با تقسیم یک منطقه به چندین منطقه، امنیت را افزایش داد و ترافیک شبکه را به راحتی کنترول کرد.

مثال: شما مدیر شبکهٔ یک شرکت هستید و این شرکت از ۳ بخش حساب‌داری، فروش و اداری تشکیل شده است و می‌خواهید این چند اتاق را توسط سویچ وصل کنید که با متصل‌کردن تمام کمپیوترهای این اتاق‌ها، آن‌ها به هم متصل می‌شوند و می‌توانند به منابع شبکه دسترسی داشته باشند. با این کار ترافیک روی سویچ افزایش پیدا می‌کند، چون تمام این کمپیوترها در یک Broadcast Domain قرار دارند و امنیت در این شبکه به خاطر دسترسی اطلاعات پایین می‌آید. شما که مدیر شبکه هستید، باید کاری انجام دهید که این اتاق‌ها از هم جدا شوند؛ مثلاً: کمپیوتر اتاق حساب‌داری نتواند با اتاق اداری ارتباط برقرار کند. خوب این کار توسط VLAN انجام می‌شود که تمام کمپیوترهای اتاق حساب‌داری را می‌توان در یک منطقه قرار داد که باهم در ارتباط باشند و با اتاق‌های دیگر نتوانند در ارتباط باشند.

۴.۱ مفهوم VLAN

تمامی پورت‌هایی است که در یک محیط Broadcast Domain قرار دارند. این بدان معنی است که تمامی Device هایی که به این سویچ متصل هستند، همگی در یک LAN قرار دارند، بنابراین می‌توانند به راحتی به یکدیگر دسترسی داشته باشند. قرارگیری تمامی منابع شبکه مانند Server ها، کاربران انترنت در یک LAN واحد مشکلاتی را به دنبال دارد که نتیجهٔ آن به شرح ذیل است:

- ترافیک بالا؛
- امنیت پایین.

به عبارتی در چنین شبکه‌یی نمی‌توان مدیریت روی ترافیک و امنیت داشت. درحالی‌که اگر یک Broadcast Domain را به چندین Broadcast Domain تقسیم کنیم، ترافیک کاهش یافته و محلی شده و دسترسی‌ها محدود می‌شود. در واقع با تبدیل‌کردن یک LAN به چندین LAN یا همان VLAN نتایج زیر حاصل می‌شود:

- خوردشدن Broadcast Domain؛
- کاهش ترافیک؛
- محدودکردن سطح دسترسی.

فرض کنید تعدادی کمپیوتر در یک LAN قرارداشته باشند. بنابراین، همهٔ این کمپیوترها به راحتی با یکدیگر ارتباط دارند. اما درصورتی‌که یک LAN را به چندین VLAN تبدیل کنید، کمپیوترهایی که در یک VLAN قرار دارند، نمی‌توانند با VLANهای دیگر ارتباط برقرار کنند.

۴.۲ VLAN

VLAN گرفته‌شده از Virtual LAN یا LANهای مجازی می‌باشد، که هر VLAN یک Logical LAN یا یک Logical Subnet می‌باشد و یک حوزهٔ Broadcast مستقل را تشکیل می‌دهد. تمامی پورت‌های یک سویچ به‌صورت Default در یک Broadcast Domain قرار دارند. با تعریف VLAN،Broadcast Domain به نواحی منطقهٔ کوچک‌تری تقسیم می‌شود؛ لذا هر کدام از VLAN ها یک Broadcast Domain جدید خواهند بود. Nodeهای موجود در هر کدام از VLANها به راحتی با یکدیگر تبادل اطلاعات خواهند داشت. مشکل زمانی پیش می‌آید که شما بخواهید دسترسی به یک VLAN را برای بعضی از VLANها برقرار کنید. در واقع می‌خواهید ارتباط بین یک یا چند VLAN را برقرار کنید. برای این منظور کافی است که از یک Device لایهٔ سوم استفاده کنید، طوری که ترافیک را از یک VLAN به سمت VLAN دیگر هدایت کند.

۴.۳ Physical Subnet

تعدادی کمپیوتر و تجهیزات شبکه می‌باشند که به وسیلهٔ کیبل یا به‌صورت Wireless به هم متصل شده‌اند و متباقی دستگاه‌ها یک physical subnet در یک رنج آدرس لایهٔ ۳ قرار دارند.

۴.۴ Logical subnet

شامل کمپیوترها و دستگاه‌هایی هستند که صرف از نظر محل قرارگیری فزیکی به پورت‌های یک یا چندین سویچ که تمام‌شان عضو یک VLAN می‌باشند، متصل شده‌اند و متباقی دستگاه‌ها و کمپیوترهای یک Logical Subnet در یک رنج آدرسی لایهٔ 3 قرار خواهند داشت. VLAN یکی از توانمندی‌های مربوط به سویچ‌ها می‌باشد که به شما این امکان را می‌دهد تا کمپیوترهای متصل به یک سویچ یا چندین سویچ را به‌صورت منطقی درگروه‌های خاص قرار دهید، طوری که ترافیک این گروه از یکدیگر جدا شوند و در این حالت هر گروه یا هر VLAN تبدیل به یک حوزهٔ Broadcast مجزا خواهد شد. هر VLAN با یک شماره که به VLAN ID معروف می‌باشد، شناسایی خواهد شد. VLAN IDها یا شمارهٔ VLANها رنجی بین 1 تا 1005 می‌باشندکه VLAN 1 و VLAN1002 تا VLAN1005 ریزرف شده‌اند.

VLAN 1002 تا: VLAN 1005 این VLANها برای توانمندی‌های مربوط به Token Ring و FDDI Switching ریزرف شده‌اند.

نکته: هر سویچ قابلیت پشتیبانی از VLAN را نخواهد داشت ولی Switch های Cisco توانمندی VLAN را پشتیبانی می‌کنند.

برای ایجاد یک VLAN در سویچ وارد مود Global می‌شوید و دستور زیر را وارد می‌کنید:

```
Switch(config)# vlan?
<1-1005> ISL VLAN IDs 1-1005
```

همان‌طورکه مشاهده می‌کنید، بعد از تعریف vlan علامت سؤال قرار دادیم، که به ما تعداد vlanهای قابل ایجاد را نمایش دهد. یعنی می‌توانیم از 1 تا 1005 عدد vlan در یک سویچ تعریف کنیم. توجه داشته باشید که vlan 1 را نمی‌توانید ایجاد کنید، چون به‌صورت پیش‌فرض تمام پورت‌های سویچ در این vlan قرار

```
Switch(config)#vlan 20
Switch(config-vlan)#Name Kabul
```

دارد و به‌خاطر همین است که تمام پورت‌ها باهم در ارتباط هستند.

در این دستور Vlan شماره ۲۰ تعریف شده است و بعد از آن، یک اسم از طریق دستور Name تعریف نمودیم. برای مشاهدهٔ Vlan که تعریف کردیم و نام این Vlan از دستور زیر استفاده می‌کنیم:

```
Switch#show vlan brief
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
 20 Kabul active
 1002 fddi-default active
 1003 token-ring-default active
1004 fddinet-default active 1005trnet-default active
```

همان‌طور که مشاهده می‌کنید، Vlan ۲۰ با نام Kabul تعریف شده است و وضعیت آن فعال است. اگر به Vlan ۱ نگاهی کنید، متوجه می‌شوید که تمام پورت‌های سویچ در این Vlan قرار دارد.

قراردادن پورت‌ها داخل Vlan مورد نظر: این کار به دو صورت انجام می‌پذیرد:

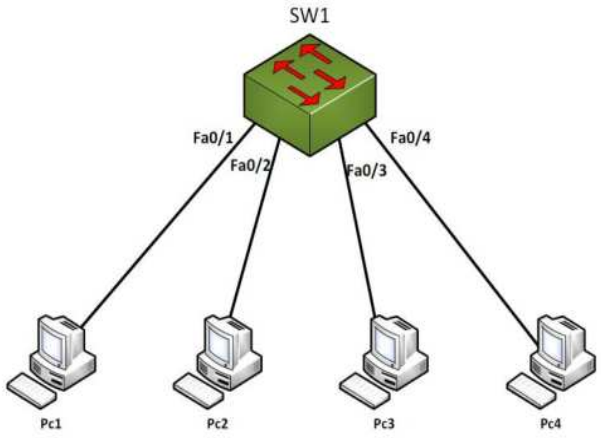
- Static Vlan: این روش به‌صورت دستی است و می‌توانیم هر پورتی را در Vlan مورد نظر خود قرار دهیم، این روش یکی از امن‌ترین روش‌ها است

- Dynamic Vlan: در این روش نسبت دادن پورت به یک Vlan از طریق دستی صورت نمی‌گیرد، بلکه از طریق یک سرور مرکزی با نام (Vlan Membership Policy Server) VMPS ایجاد و مدیریت می‌شوند.

در این قسمت، نحوهٔ قراردادن پورت‌های یک سویچ را در یک Vlan باهم بررسی می‌کنیم. هر پورت سویچ از دو Mode تشکیل شده است:

- Mode Access
- Mode Trunk

تمام پورت‌های یک سویچ به‌صورت پیش‌فرض در مود access قرار دارد. برای این‌که یک پورت را به یک Vlan ارتباط دهید، باید از این مود استفاده کنید؛ مثال:



شکل (۱,۴) Vlans

یک سویچ و ۱ PC را به صفحه اضافه و آن‌ها را به هم متصل کنید و طبق جدول صفحهٔ بعد به کمپیوترها آدرس دهید:

Station	IP Address	Subnet Mask
PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0
PC3	192.168.1.3	255.255.255.0
PC4	192.168.1.4	255.255.255.0

بعد از این‌که این آدرس‌ها برای کمپیوترها داده شد، اگر ارتباط بین PCها را تست کنید، متوجه می‌شوید که تمام آن‌ها باهم در ارتباط می‌باشند. حال می‌خواهیم از طریق Vlan ارتباط 1 کمپیوتر PC1و PC2 را با PC3 و PC4 جدا کنیم. برای این کار در داخل سویچ دو Vlan تعریف می‌کنیم:

Station	IP Address	Subnet Mask
PC1	Fa/0/1	10
PC2	Fa/0/2	10
PC3	Fa/0/3	20
PC4	Fa/0/4	20

طبق جدول، Pc ها را داخل Vlanهای مورد نظر قرار می‌دهیم؛ برای این کار وارد پورت‌هایی می‌شویم که کمپیوتر مورد نظر به آن متصل است؛ مثال: در بالا PC1به پورت Fa0/1متصل است که این پورت باید در Vlan 10قرار بگیرد:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

همان‌طور که مشاهده می‌کنید، در قسمت اول وارد پورت Fa0/1شدیم و بعد از آن از دستور Switchport mode access استفاده کردیم تا مود بر روی Access تنظیم شود و بعد از آن از دستور Switchport access Vlan 10استفاده کردیم تا این پورت را وارد Vlan 10 کنیم. متباقی پورت‌ها هم به‌صورت زیر انجام می‌شود.

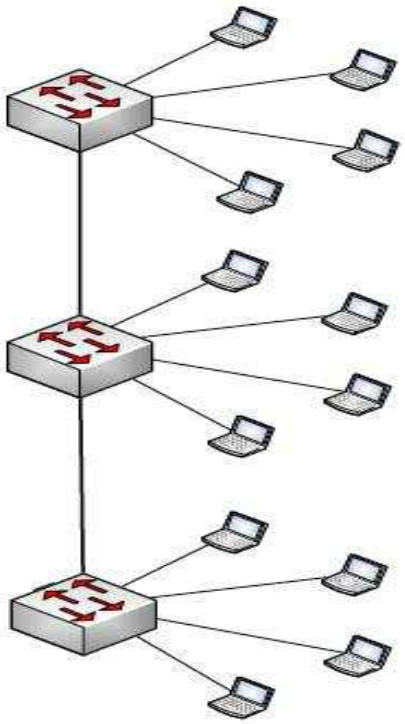
```
Switch(config)#int f0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10

Switch(config-if)#int f0/3
Switch(config-if)# switchport mode access
 Switch(config-if)# switchport access vlan 20

Switch(config-if)#int f0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

بعد از اتمام کار از طریق PC4،PC1 را Ping کنید که متوجه می‌شوید این کار امکان‌پذیر نیست و آنهم به خاطر جداکردن آن‌ها و قراردادن داخل دو vlan جدا است و فقط PC1و PC2 می‌توانند همدیگر را ببینند و باهم در ارتباط باشند، چون در یک Vlan قرار دارند.

۴.۵ Trunk Mode



قبل از تعریف این مود، یک مثال برای درک بهتر این موضوع تعریف می‌کنیم؛ شما مدیر شبکهٔ یک ساختمان هستید و این ساختمان از سه طبقه تشکیل شده است و در هر طبقه از یک سویچ برای وصل‌کردن کمپیوترها استفاده شده است و تمام سویچ‌ها به هم متصل شده‌اند. نکتهٔ مهم در این قسمت این است که در هر طبقه بخش حساب‌داری، اداری و فروش وجود دارد و می‌خواهیم تمام بخش‌های هر ساختمان باهم در ارتباط باشند؛ برای این کار شما در هر طبقه، مانند مثال قبل برای هر بخش یک Vlan تعریف می‌کنید و پورت‌ها را داخل Vlan مورد نظر قرار می‌دهید، اما یک مشکل وجود دارد، این که سویچ باید با vlan های دیگر در طبقات مختلف در ارتباط باشند. برای حل این مشکل باید از Trunk استفاده کرد، Trunk روشی برای انتقال Vlanها در سویچ‌های مختلف است و با استفاده از آن، این مشکل به راحتی حل می‌شود.

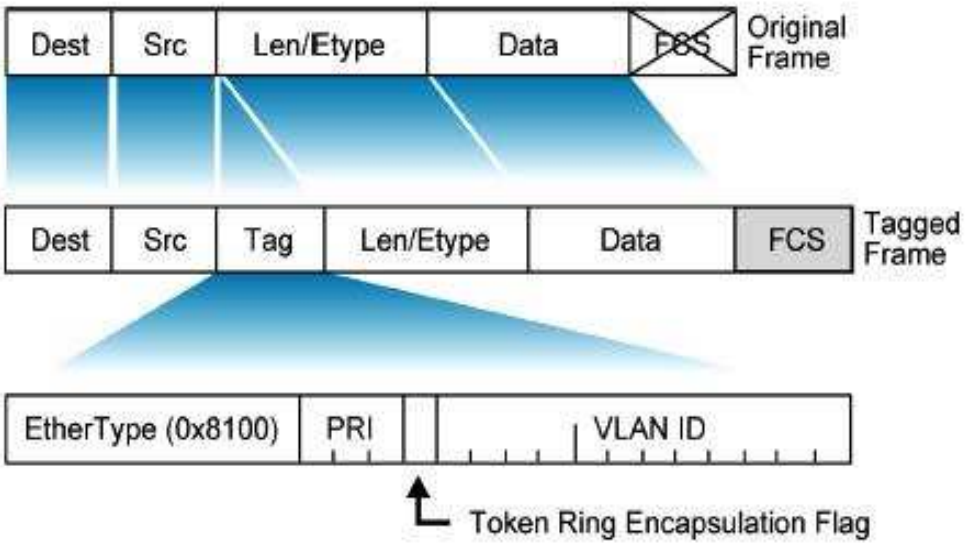
Tag زدن روی فریم‌ها

برای انتقال Vlanها در مود Trunk دو روش وجود دارد که از طریق آن یک Vlan شناسایی می‌شود:

- ISL(Inter-Switch Link Protocol)
- 802.1Q

ISL: یک استندرد برای بسته‌بندی فریم‌ها برای انتقال در یک مسیر یا همان Trunk که این استندرد مربوط به شرکت سیسکو بوده و به‌صورت پیش‌فرض در دستگاه‌های لایهٔ دوم این شرکت فعال است.

802.1Q: یک استندرد Open Source است و مربوط به شرکت خاصی نیست و اگر در شبکهٔ خود از سویچ‌های شرکت‌های متفاوت استفاده می‌کنید، برای برچسپ‌زدن روی فریم‌ها باید از این استندرد استفاده کنید. این پروتوکول ساختار فریم‌ها را تغییر می‌دهد.



۴.۶ فعال‌کردن پروتوکول ISL

این پروتوکول به‌صورت پیش‌فرض روی سویچ‌های شرکت سیسکو فعال است.

فعال‌کردن پروتوکول 802.1Q

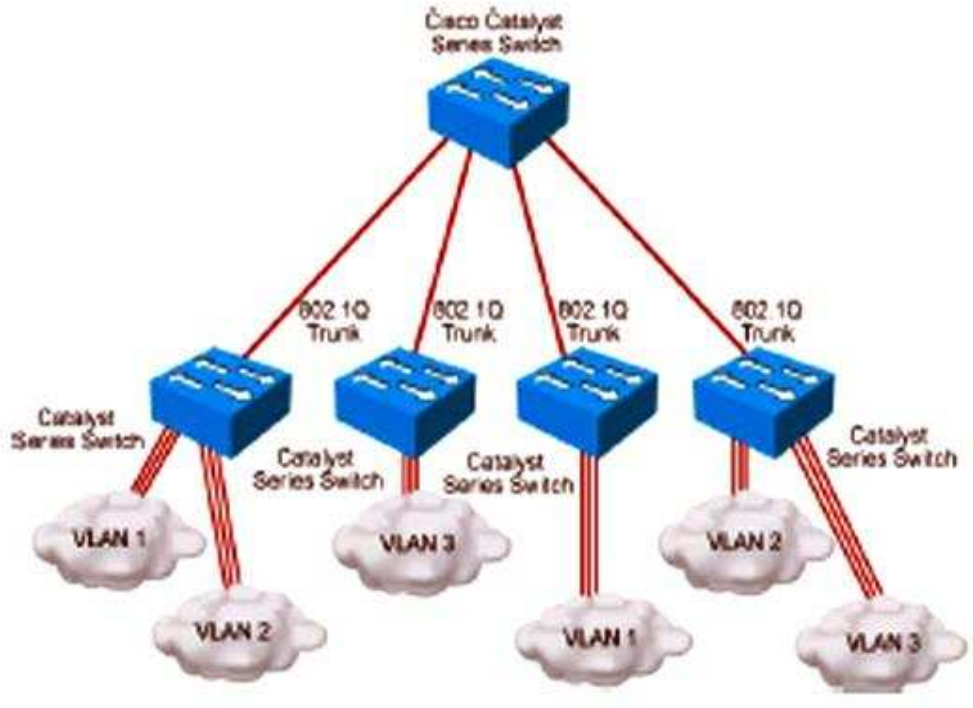
برای فعال‌کردن این پروتوکول باید وارد interface مورد نظر شوید و دستور زیر را وارد کنید:

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

با اجرای این دستورات، یک سویچ تمام Vlanها را برچسپ‌گذاری می‌کند و از خود عبور می‌دهد. شاید شما بخواهید به سویچ بگویید که فقط Vlanهای خاصی از وی عبور کنند؛ برای این منظور از دستور زیر استفاده می‌کنیم:

```
Switch(config-if)#switchport trunk allowed vlan 10
```

با این دستور فقط Vlan ۱۰ حق عبور دارد و متباقی Vlan ها از این سویچ عبور نمی‌کنند. پس یک پورت در سویچ زمانی Trunk می‌شود که بخواهید Vlanها را بین دو دستگاه سویچ جابجا کنید. به شکل زیر توجه کنید:



شکل (۲,۴) VLAN

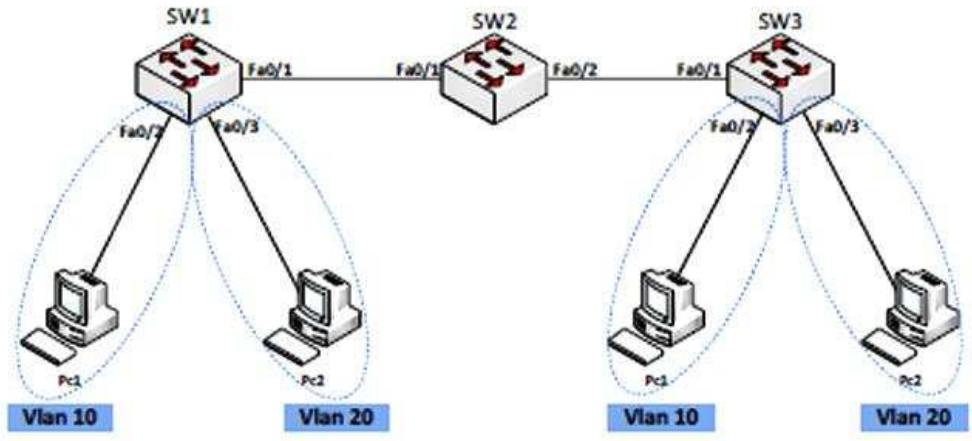
در این شکل، سویچ‌ها به هم متصل شده‌اند و سویچ‌هایی که در زیر قرار دارند از Vlanهای مختلف تشکیل شده‌اند. برای ارتباط Vlan۱ به Vlan۱ در سویچ دیگر، باید پروتوکول Trunk را روی پورت‌های سویچ که به سویچ اصلی متصل است، اجرا کنیم و بعد ستور ۸۰۲.۱Q را نوشته کنیم تا عملیات برچسپ‌گذاری روی Vlanها را انجام دهد.

۴.۷ Native Vlan

همان‌طور که قبلاً گفتیم در تمام سویچ‌ها Vlan۱ وجود دارد و قادر به ایجاد ویا حذف آن نیستیم، اما وقتی چندین سویچ را با پروتوکول Trunk،۸۰۲.۱Q می‌کنید، در زمان انتقال Vlan ۱ بین سویچ‌ها روی آن‌ها هم برچسپ‌گذاری می‌شود و همین کار باعث استفاده بیش از حد bandwidth شبکه می‌شود و برای جلوگیری از این کار باید روی پورت که Trunk شده است، دستور زیر را وارد کنیم:

```
Switch(config-if)# switchport trunk native vlan 1
```

با این کار، Vlan۱ در پروتوکول Trunk انتقال داده نمی‌شود.



Station	Ip Address	SubnetMask
Pc1	192.168.1.1	255.255.255.0
Pc2	192.168.1.2	255.255.255.0
Pc3	192.168.1.3	255.255.255.0
Pc4	192.168.1.4	255.255.255.0

بعد از این‌که Ip Addressها را در pc ها وارد کردیم، نوبت به تعریف Vlan در سویچ است. در داخل هر یک از سویچ‌ها، Vlanهای ۱۰ و ۲۰ را به‌صورت زیر تعریف می‌کنیم:

```
Switch(config)#vlan 10
Switch(config)# vlan 20
```

بعد از تعریف Vlan باید پورت‌های متصل به Pc را داخل Vlanهای مشخص‌شده قرار دهیم؛ مثال: PC۱باید در ۱۰ Vlan قرار بگیرد؛ برای این کار وارد سویچ و بعد، وارد interface fa0/2که به PC۱متصل است، می‌شویم و آن را طبق دستور زیر داخل ۱۰ Vlan قرار می‌دهیم:

```
Switch(config)#int f0/2
 Switch(config-if)#switchport mode access
 Switch(config-if)#switchport access vlan 10
```

متباقی پورت‌های سویچ را که به pc متصل است، داخل Vlan قرار می‌دهیم.

```
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

پورت‌های سویچ ۳ را به صورتی که در بالا انجام دادیم، داخل Vlan قرار می‌دهیم. بعد از این‌که این کار را انجام دادید، یک Ping از PC۱ به PC۳ بگیرید و مطمئن باشید که جواب نمی‌گیرید، به‌خاطر این که

پروتوکول Trunk روی پورت‌های سویچ فعال نشده و به‌خاطر این ارتباط برقرار نمی‌شود. وارد SW۱شوید و پورتی را که به طرف SW۲ می‌رود،Trunk کنید:

```
Switch(config)#Interface Fa0/1

Switch(config-if)#switchport mode trunk
```

بعد از این کار، مدل برچسپ‌گذاری روی فریم‌ها را باید مشخص کنید که ISL باشد یا ۸۰۲.۱Qکه در برنامهٔ Paket Tracer به‌صورت از قبل تعیین‌شده dot۱Q است و ISL وجود ندارد که این کار از شرکت سیسکو بعید است، چون در سویچ ۲۹۵۰ استندرد ISL وجود ندارد، استندردی که مربوط سیسکو است. متباقی پورت‌های متصل به سویچ‌های دیگر را Trunk کنید:

```
Sw2
Switch(config)#Interface Fa0/1
Switch(config-if)#switchport mode trunk
Switch(config)#Interface Fa0/2
Switch(config-if)#switchport mode trunk
SW3
Switch(config)#Interface Fa0/1
Switch(config-if)#switchport mode trunk
```

بعد از این کار، ارتباط بین Vlanها برقرار می‌شود و PC۱با PC۳ باهم ارتباط برقرار می‌کنند. بعد از این مثال، سؤالی برای شما ایجاد می‌شود که اگر تعداد سویچ‌ها زیاد باشد و ما بخواهیم داخل هر کدام از سویچ‌ها vlan تعریف کنیم، کار بسیار وقت‌گیر است. آیا روش دیگری هم وجود دارد؟ بلی، روش دیگری هم وجود دارد که می‌توانیم در یک سویچ یا هر سویچی در شبکهٔ Vlan تعریف کنید. این Vlanها به‌صورت خودکار وارد سویچ دیگر می‌شوند که به این روش VTP(VLAN Trunking Protocol) می‌گویند.

۴.۸ Inter Vlan Routing

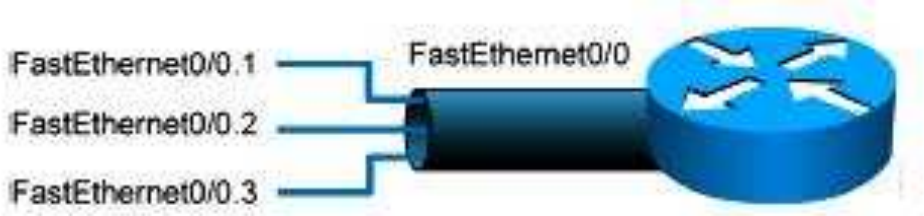
آیا این موضوع به ذهن شما رسیده که وقتی دو کمپیوتر در دو Vlan متفاوت قرار دارند، راهی وجود دارد که این دو بتوانند باهم در ارتباط باشند؟، بلی این راه از طریق Inter vlan Routing امکان‌پذیر است، یعنی از طریق یک روتر ارتباط Vlanهای تعریف‌شده در سویچ را باهم برقرار می‌کنیم.

همان‌طور که می‌دانید سویچ‌های لایهٔ ۲، مانند ۲۹۵۰ قادر به انجام عملیات روتینگ نمی‌باشند و برای همین از روتر برای انجام عملیات روتینگ بین Vlanها استفاده می‌شود. ارتباط Vlanهای مختلف هم می‌تواند از طریق روتر انجام شود و هم از طریق سویچ‌هایی که در لایهٔ ۳ کار می‌کنند.

به شکل زیر توجه کنید؛ برای انجام عملیات روتینگ روی روتر فقط از یک interface فزیکی استفاده می‌شود و برای ارتباط با vlanها از پورت‌های مجازی استفاده می‌کنند که قابلیت Encapsulation را دارند. روتر برای انجام عملیات روتینگ باید یک انترفیس داخل Vlan داشته باشد، یعنی اگر ۴ تا vlan

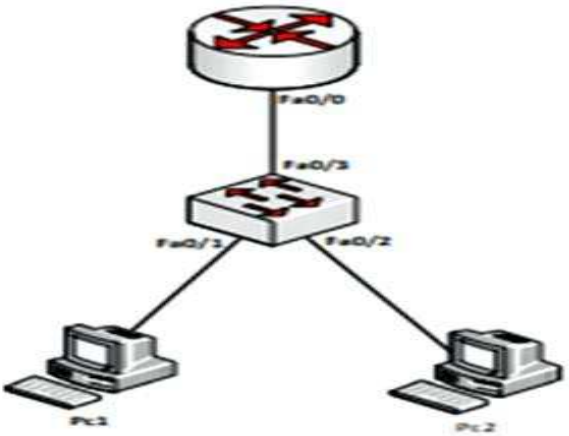
داریم، باید ۴ تا پورت روتر را به سویچ اتصال دهیم که باعث به هدر رفتن پورت‌های روتر و افزایش هزینه می‌شود و به‌خاطر همین از یک انترفیس فزیکی به همراه انترفیس مجازی داخل آن استفاده می‌کنند.

شکل ۴-۳ : Inter Vlan Routing



مثالی از Inter Vlan Routing:

مانند شکل یک روتر، سویچ و دو PC را به صفحه اضافه کنید و به‌صورت زیر به هم متصل کنید:



وارد سویچ شوید و پورت متصل به روتر را در Trunk قرار دهید، چون مسئول انتقال Vlanها است:

```
Switch (config) #interface fast Ethernet 0/3
Switch (config-if) #switchport mode trunk
Switch (config-if) #switchport trunk encapsulation dot1q
```

همان‌طور که می‌دانید dot۱Q روی سویچ‌های ۱۱۴۴ به‌صورت پیش‌فرض فعال است و لازم به واردکردن دستور switchport trunk encapsulation dot۱Qنیست.

بعد از این کار، دو vlan با شماره‌های 100 و 200 تعریف کنید.

```
Switch (config) #vlan 100
Switch (config-vlan) #ex
Switch (config) #vlan 200
```

پورت‌های متصل به pc را داخل Vlan قرار دهید، PC1داخل Vlan 100 و PC2 داخل Vlan.200

```
Switch (config) #int f0/1
Switch (config-if) #sw m ac
Switch (config-if) #sw ac vlan 100
Switch (config-if)#int f0/2
Switch (config-if)#sw m ac
Switch (config-if)#sw ac vlan 200
```

حالا وارد روتر شوید و کارهای زیر را انجام دهید: در این سناریو، ما احتیاج به دو انترفیس مجازی داریم. پورت سویچ به پورت Fa0/0متصل است، پس انترفیس مجازی به‌صورت زیر تعریف می‌شود:

```
Router(config)#int f0/0.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#int f0/0.200
Router(config-subif)#encapsulation dot1Q 200
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#int f0/0
```

به دقت به دستورات توجه کنید؛ در قدم اول int f0/0.100را نوشتیم که با این دستور، وارد انترفیس مجازی با شمارهٔ 100 که روی Interface f0/0قرار دارد، شدیم. بعد از آن، روش برچسپ‌زدن را مشخص کردیم، چون در مرحلهٔ Trunk روی سویچ، dot1Q را انتخاب کردیم. در این قسمت هم، بعد از encapsulation باید dot1Q قرار داشته باشد. بعد از آن، عدد 100 که نمایان‌گر Vlan 100 است و ارتباط مستقیم با Vlan 100 دارد و در ادامه، address ip مورد نظر را وارد کردیم و همین کار را در پورت مجازی interface f0/0.200 هم انجام دادیم؛ اما با تغییر شمارهٔ Vlan و شمارهٔ ip، بعد از ختم کار وارد انترفیس فزیکی می‌شویم و آن را فعال می‌کنیم.

نکته: دستور NO Shutdown را در انترفیس مجازی وارد نکنید، چون پورت اصلی نیست و برای ارتباط باید پورت فزیکی یا اصلی روشن شود.

در این قسمت وارد pcها می‌شویم و Ip Address و Default Gateway را برای آن‌ها تعریف می‌کنیم.

برای PC۱ به این صورت تعریف می‌کنیم:

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

برای PC۲ به این صورت تعریف می‌کنیم:

IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1

بعد از ختم کار، دو pc که در Vlanهای مختلف قرار دارند، می‌توانند همدیگر را ببینند.

اگر از PC۲، PC۱را Pnig کنیم، به‌صورت زیر جواب می‌دهد:

```
PC>ping 192.168.1.2
 Pinging 192.168.1.2 with 32 bytes of data:
 Request timed out.
 Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=10ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

خلاصه‌ی فصل چهارم

به‌منظور کنترول و مدیریت ترافیک و افزایش security در یک شبکه LAN باید آن را به تعدادی Broadcast Domain تقسیم کرد به طوری که هر کدام از این Broadcast Domainهای جدید یک Virtual LAN ویا VLAN خواهند بود. هر کدام از VLANها شامل تعدادی پورت خواهند بود که این پورت‌ها می‌توانند همگی از یک سویچ ویا از تعدادی سویچ انتخاب شده باشند. نحوهٔ عضویت در هر کدام از VLANها به دو صورت امکان‌پذیر می‌باشد:

- Static VLAN
- Dynamic VLAN

درصورتي‌که پورت‌ها را به‌صورت Static عضو VLANها کنید و در صورت تغییر در شبکه باید هر کدام از آن‌ها را به‌صورت دستی تغییر دهید. در روش Dynamic، node های یک شبکه بر اساس آدرس‌های فزیکی یا منطقی ویا پروتوکول‌های مختلف دسته‌بندی می‌شوند و مدیریت آن‌ها توسط یک Server انجام می‌شود.

Trunk عبارت از یک مسیر ارتباطی مشترک است که انتقال ترافیک تمام VLANها را انجام می‌دهد و پورتی که این ترافیک را عملاً انتقال می‌دهد، پورت Trunk نامیده می‌شود. با این پورت بسته‌های مختلف به نشانه‌های مختلف را می‌توان از یک مسیر واحد ارسال کرد. این پروتوکول جهت نشانی بسته‌ها دو استندرد را استفاده می‌کند که عبارت‌اند از:

- ISL
- 802.1 Q

ISA پروتوکول مخصوص به سیسکو بوده و روی تجهیزات سیسکو به‌صورت پیش‌فرض فعال می‌باشد درحالی‌که 802.1 Q یک استندرد عمومی بوده و مربوط کدام کمپنی خاص نمی‌باشد و درصورتی‌که در یک شبکه سویچ‌هایی از شرکت‌های متفاوتی داشته باشید، باید از این پروتوکول جهت Frame Tagging استفاده کنید.

سوالات فصل چهارم

۱. VLAN را تعریف نموده و نیز بگوید که به خاطر کدام هدف استفاده می‌شود.

۲. پروتوکول ۸۰۲.۱Q چطور فعال می‌گردد واضح سازید.

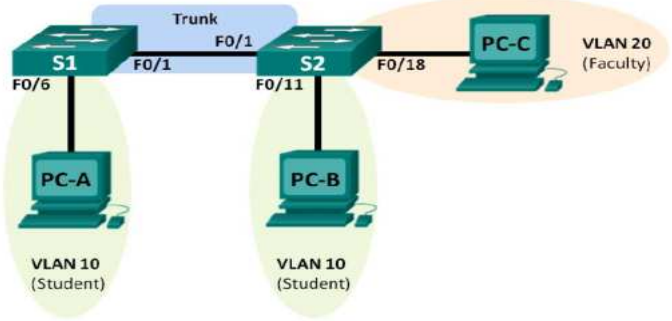
۳. موارد استفادهٔ Trunk Mode را شرح نمایید.

۴. فرق بین Trunk Mode و Native Vlan را تشریح نمایید.

۵. فرض کنید که ما امکانات ساختن VLANها را در سویچ نداریم به نظر شما به کدام مشکل رو به رو خواهم شد؟

۶. پروسهٔ فعال‌ساختن VLAN را سلسله‌وار تشریح نمایید.

- شبکه‌یی را نظر به شکل ذیل دیزاین کرده و VLANهای مربوطه آن را بسازید و انترفیس‌هایی را نظر به جدول و subnet که داده شده، انجام دهید و پورت‌های آن را فعال سازید.
- Hostnam سویچ و کمپیوتر را نظر به شکل تغییر بدهید.
- Vlan به نام‌های faculty, student و management ساخته و پورت‌های آن را نظر به شکل شامل آن VLAN بسازید.
- دستور no domain-lookup را در سویچ‌ها فعال سازید.
- پورت استفاده‌شده در بین دو سویچ را Trunk۸۰۲.۱Q کنید.



Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

فصل پنجم

پروتوکول VTP

هدف کلی: آشنایی با VTP و روش‌های عیارسازی آن.

اهداف آموزشی: در پایان این فصل از محصلان انتظار می رود که:

۱. پروتوکول VTP را تعریف نمایند.
۲. عملکرد پروتوکول VTP و مودهای آن را بدانند.
۳. پروتوکول VTP را عیارسازی نمایند.

در درس‌های گذشته با مفهوم VLAN و Trunk در یک شبکه Ethernet آشنا شدید. با بزرگ‌شدن یک شبکه و افزایش تعداد سویچ‌ها، تغییرات جزئی در هر کدام از VLANها ویا ساختن یک VLAN جدید منجر به ایجاد تغییر در متباقی سویچ‌ها می‌شود؛ بنابراین مدیریت منابع در این شبکه با مشکلات بسیار زیادی همراه خواهد بود. سیسکو برای رفع این مشکل VTP را ارائه کرده است. VTP طرح مدیریت گروهی سویچ‌ها را معرفی می‌کند. بنابراین VTP با تعریف کردن یک ناحیه که شامل تعدادی سویچ می‌باشد و تعریف Client و Server در این شبکه، تغییرات روی Server را اعمال کرده و سپس به اطلاع دیگر سویچ‌ها می‌رساند بنابراین اطلاع‌رسانی در مورد VLANها و تغییرات آن‌ها در این شبکه خیلی راحت‌تر و سریع‌تر خواهد شد. برای روشن‌شدن مطلب ابتدا با اصطلاحات مربوط به VTP که در این فصل شما به این پروتوکول آشنا خواهید شد و همچنان به فعال‌سازی و عملکرد آن در یک شبکه و Modeهای مختلف آن آشنا خواهید شد.

۵.۱ مشخصات پروتوکول VTP

در درس‌های گذشته با مفهوم VLAN و TRUNK در یک شبکه آشنا شدید. با توسعه‌یافتن یک شبکه و افزایش تعداد سویچ، تغییر جزئی در هر کدام از VLANها ویا ساختن یک VLAN جدید منجر به ایجاد تغییر در بقیه سویچ‌ها می‌شود. بنابراین مدیریت منابع زیاد در یک شبکه، با مشکل جدی روبه‌رو خواهیم شد. و کمپنی سیسکو به‌خاطر حل این مشکل پروتوکول VTP را معرفی کرده است.

VTP طرح مدیریت گروهی سویچ‌ها را معرفی می‌کند بنابراین VTP با تعریف‌کردن یک ناحیه که شامل تعدادی از سویچ‌ها می‌باشد، می‌تواند مدیریت خوب‌تری را بالای شبکه داشته باشد که به‌خاطر فهمیدن بیشتر این پروتوکول، لازم است موضوعات ذیل را مطالعه نماییم:

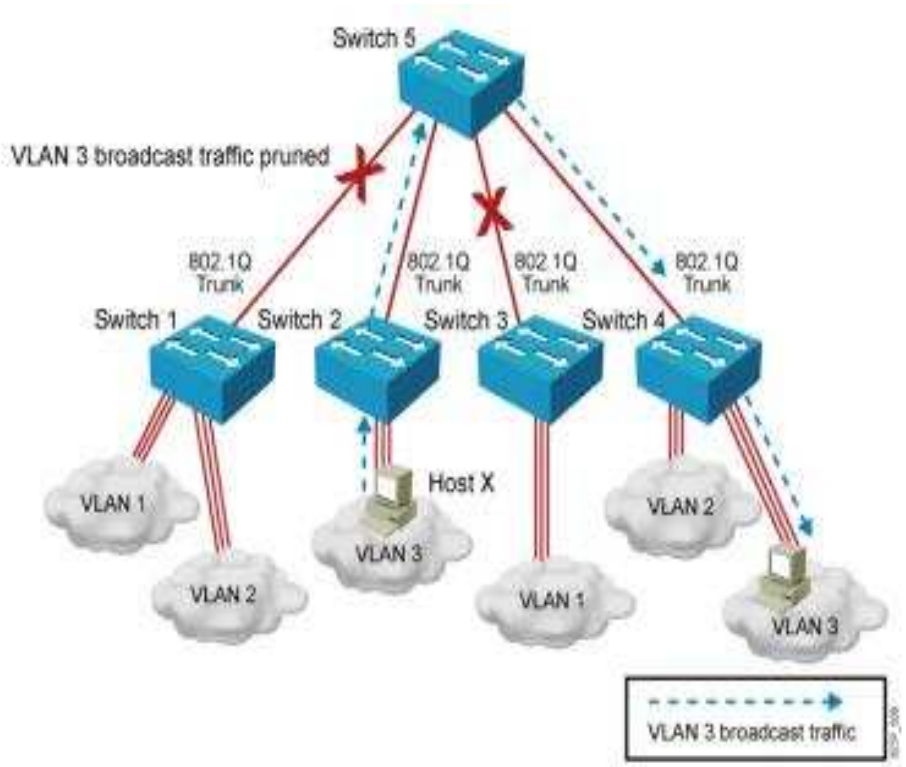
۵.۲ VTP Domain

به ناحیه‌یی گفته می‌شود که سویچ‌های داخل آن عضو هستند و Vlan های خود را با همدیگر به اشتراک می‌گذارند. سویچ‌ها تنها می‌توانند در یک VTP Domain عضو شوند و نمی‌توانند Vlanهای خود را با VTP domain دیگری به اشتراک بگذارند.

۵.۳ VTP pruning

قابلیتی است که می‌توان به وسیلهٔ آن ترافیک اضافه مثل Broadcast را کاهش داد. به این صورت که سویچ تمام پورت‌های Trunk خود را چک می‌کند و مشخص می‌کند که از هر پورت به چه VLAN هایی می‌رسد. به‌طور پیش‌فرض این ویژگی غیر فعال است. در صورت فعال‌کردن این ویژگی روی یک سویچ این ویژگی رو تمام سویچ‌های دومین فعال خواهد شد.

در شکل زیر به سویچ ۲ یک pc متصل است و در ۳ Vlan قرار دارد و می‌خواهد با pc دیگر در سویچ ۴ ارتباط برقرار کند. همان‌طور که می‌دانید سویچ، بعد از رسیدن درخواست به پورت، خود آن را به‌صورت Broadcast برای دیگر سویچ‌ها که به آن‌ها Trunk شده است، ارسال می‌کند؛ اما با فعال‌کردن VTP Pruning این کار انجام نمی‌شود و فقط پیام Broadcast به سویچ‌هایی ارسال می‌شود که یکی از پورت‌های آن‌ها در Vlan مورد نظر قرار داشته باشد.



شکل ۱،۵ (VTP Pruning)

۵.۴ کاربا (VLAN Trunking Protocol)

این پروتوکول توسط شرکت سیسکو ارائه شده است، اما انحصاری نیست و شرکت‌های دیگر می‌توانند از این پروتوکول استفاده کنند. این پروتوکول برای مدیریت Vlanها و ایجاد امنیت به‌کار برده می‌شود. VTP به مدیر شبکه اجازهٔ ایجاد، حذف و تغییر نام را می‌دهد. چند ویژگی این پروتوکول عبارتند از:

ساختمان‌بندی Vlanها به‌صورت سریع در تمام سویچ‌ها؛

نظارت کامل بر کار Vlanها در یک زمان؛

ایجاد vlan به‌صورت Plug-and-Play؛

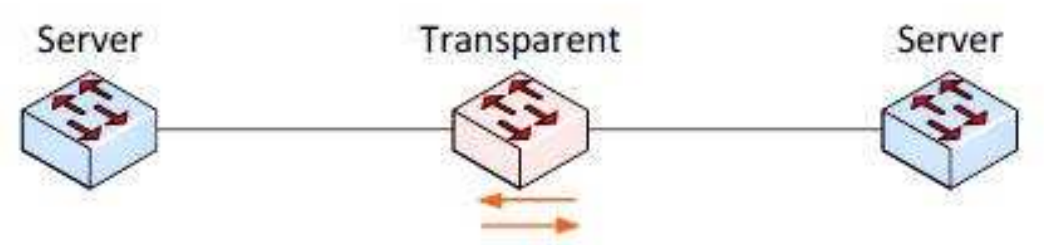
VTP دارای سه حالت است:

Server Mode: در این حالت یک سویچ می‌تواند Vlanها را ایجاد، حذف و به‌طور کامل مدیریت کند که به‌صورت پیش‌فرض تمام سویچ‌ها در مود Server قرار دارند.

ClientMode: در این حالت سویچ به سرور گوش می‌دهد و نمی‌تواند یک Vlan را ایجاد، حذف و مدیریت کند و همه چیز از طریق Server به آن اعمال می‌شود.

TransparentMode: این سویچ فقط Vlan هایی را که به وی می‌رسد، از خود عبور می‌دهد و کاری روی آن‌ها انجام نمی‌دهد، اما این سویچ می‌تواند Vlan را تعریف ویا حذف کند؛ اما به کسی اعلام نمی‌کند که این Vlanهای من است؛ کلاً سویچ مستقل است و تمام کارها را خودش انجام می‌دهد. به شکل صفحهٔ بعد توجه کنید.

در بین دو سویچ Server یک سویچ transparent قرار گرفته است. این سویچ فقط Vlan هایی را که از دو سرور برای آن ارسال می‌شود، به سویچ دیگر انتقال می‌دهد و کاری روی این Vlanها انجام نمی‌دهد؛ اما خودش می‌تواند vlan ایجاد کرده و روی آن‌ها کار کند؛ ولی VLanهای مربوط به خودش را به کسی نمی‌دهد.



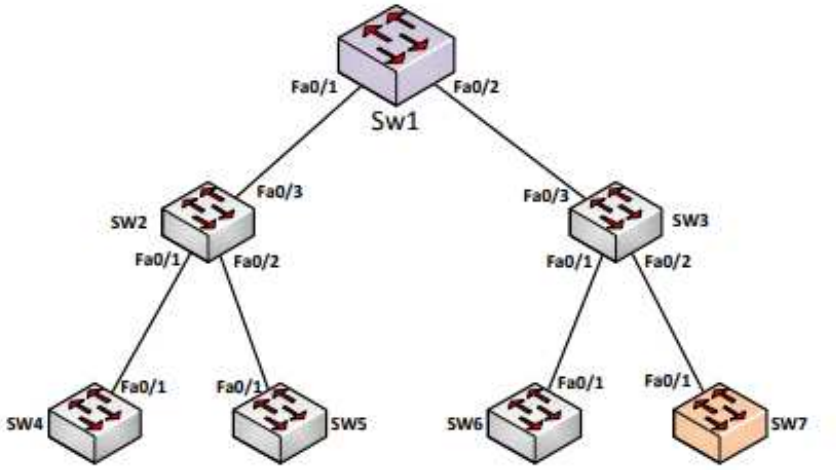
شکل ۵-۲ : معرفی سویچ transparent

۵.۵ فعال‌کردن VTP

برای فعال‌کردن Vtp باید از دستورات زیر در سویچ استفاده کنیم:

```
Switch# configure terminal
Switch(config)# vtp mode [server | client | transparent]
Switch(config)# vtp domain domain-name
Switch(config)# vtp password password
Switch(config)# vtp pruning
Switch(config)# end
```

با یک مثال این دستورات را داخل آن به کار می‌بریم:



در این مثال، سویچ ۲ به‌عنوان سرور و سویچ ۷ به‌عنوان Transparent و بقیه، به‌عنوان Client هستند. همیشه به یاد داشته باشید که قبل از ایجاد VTP، حتماً تمام پورت‌های سویچ‌هایی را که به هم متصل هستند، در وضعیت Trunk قرار دهیم تا Vlanها بتوانند بین سویچ‌ها حرکت کنند، پس در پورت‌های سویچ‌ها که به سویچ دیگری متصل است، دستور زیر را وارد می‌کنیم؛ مثال: در سویچ یک پورت fast۰/۱ آن با پورت fast۰/۳ سویچ دو در ارتباط است و باید این پورت‌ها در وضعیت Trunk قرار بگیرند:

```
Switch(config)#int f0/1

Switch(config-if)#switchport mode trunk
```

بعد از این‌که در تمام سویچ‌ها، پورت‌ها را در وضعیت Trunk قرار دادیم، نوبت به ایجاد VTP است. برای این کار وارد سویچ ۲ می‌شویم و دستورات زیر را وارد می‌کنیم:

```
Switch(config)# vtp mode server
Switch(config)# vtp mode server
```

با دستور بالا این سویچ به‌عنوان سرور انتخاب می‌شود، البته این وضعیت به‌صورت پیش‌فرض فعال است.

```
Switch(config)#vtp domain cisco.com
Changing VTP domain name from NULL to cisco.com
```

در این قسمت هم، نام دومین را به cisco تغییر می‌دهیم، توجه داشته باشید که تمام سویچ‌ها برای ارتباط باهم باید در یک domain قرار داشته باشند.

رمز عبور را برای این VTP فعال می‌کنیم که گزینهٔ مهمی در ارتباط با سویچ‌های دیگر است. با قراردادن رمز عبور، کسی دیگر نمی‌تواند بدون اجازه، خودش را عضو این Domain کند. سعی کنید رمز عبور را به‌صورت پیچیده وارد کنید.

```
Switch(config)#vtp password 123
Setting device VLAN database password to 123
```

با دستورات بالا VTP را روی سویچ ۱ فعال کردیم و این سویچ به‌عنوان سویچ سرور نقش اصلی را در این شبکه بازی می‌کند. بقیه سویچ‌ها به جز سویچ ۷ باید در مود VTP Client قرار بگیرند و اطلاعات را از VTP Server دریافت کنند:

سویچ ۲:

```
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#vtp domain cisco.com
Domain name already set to cisco.com
```

سویچ ۳:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سویچ ۴:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سویچ ۵:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سویچ ۶:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سویچ:۷

```
Switch(config)#vtp m Transparent
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

بعد از اتمام کار، نوبت به تعریف Vlan در سویچ ۱ می‌رسد که سویچ سرور است. در این سویچ، Vlan های ۲۰۰،۱۰۰، ۳۰۰ را تعریف می‌کنیم. با اجرای دستور show vlan brief، می‌توانید لست Vlanهای ساخته‌شده را مشاهده کنید.

```
Switch#show vlan brief
VLAN Name Status Ports
 ----------------------------------------------------------------
 1default active 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
 100VLAN0100 active
 200VLAN0200 active
 300 VLAN0300 active
 1002fddi-default active
 1003token-ring-default active
 1004fddinet-default active
 1005trnet-default active
```

تا اینجا در سویچ یک، Vlanها را تعریف کردیم، چون این سویچ سرور است. سویچ‌های باقی‌مانده به علت VTP Client بودن Vlan ها را از سویچ سرور دریافت می‌کنند. اگر شما در سویچ ۶ دستور show vlan brief را اجرا کنید، تمام vlan هایی را که در سویچ یک ساختیم را در این سویچ هم نمایش می‌دهد:

```
Switch#show vlan brief

VLAN Name                        Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                      active    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
100  VLAN0100                    active
200  VLAN0200                    active
300  VLAN0300                    active
1002 fddi-default                active
1003 token-ring-default              active
1004 fddinet-default             active
1005 trnet-default               active
```

اگر در سویچ ۷ این دستور را وارد کنید، چیزی مشاهده نمی‌کنید، چون این سویچ در مود Transparent قرار گرفته است که آن را توضیح دادیم.

۵.۶ دستور SHOW VTP STATUS

با این دستور اطلاعاتی را دربارهٔ VTP و اجزای آن که روی سویچ برقرار شده است، نمایش می‌دهد:

```
Switch#show vtp status
VTP Version: 2
Configuration Revision: 3
Maximum VLANs supported locally: 255
Number of existing VLANs: 8
VTP Operating Mode: Server
VTP Domain Name: cisco.com
VTP Pruning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation: Disabled
MD5 digest: 0x5C 0xF1 0xFA 0x4C 0xCB 0x3F 0xB8 0xD3
Configuration last modified by 0.0.0.0 at 3-1-93 00:40:23
Local updater ID is 0.0.0.0 (no valid interface found)
```

دستور show vtp counters:

اطلاعاتی است که هر ۳۰۰ ثانیه توسط Server به بقیه سویچ‌ها در شبکه ارسال می‌شود.

```
Switch#show vtp counters
VTP statistics:
Summary advertisements received    : 45
Subset advertisements received     : 14
Request advertisements received    : 9
Summary advertisements transmitted : 24
Subset advertisements transmitted  : 14
Request advertisements transmitted : 0
Number of config revision errors   : 3
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk        Join Transmitted Join Received   Summary advts received from
                                               non-pruning-capable device
---------- --------------- --------------- --------------------------
```

Summary advertisements: این دستور تعداد بسته‌های ارسالی و دریافتی پروتوکول VTP را به ما نشان می‌دهد.

Subset advertisements: شامل تغییرات در یک vlan است و توسط server VTP ارسال می‌شود.

دستور show vtp password: رمز عبور قرار داده‌شده روی vtp password را نمایش می‌دهد.

خلاصه‌ی فصل پنجم

توسعه‌یافتن یک شبکه و افزایش تعداد سویچ‌ها نیاز به مدیریت خوب‌تر را ایجاب می‌کند. زیرا در یک شبکه با اندازهٔ بزرگ، تغییرات جزئی؛ مانند تغییر هر کدام VLAN ها ویا ساختن یک VLAN جدید نیاز به تغییر در باقی سویچ‌ها دارد و این کار باید به‌صورت دستی توسط مدیر شبکه انجام شود. بنابراین مدیریت منابع در این شبکه با مشکلات بسیار زیاد روبه‌رو خواهد بود که راه حل این همه مشکلات پروتوکول VTP می‌تواند باشد.

VTP طرح مدیریت گروهی سویچ‌ها را معرفی می‌کند؛ بنابراین VTP با تعریف‌کردن یک ناحیه که شامل تعدادی سویچ‌ها می‌باشد و تعریف Client و Server در این شبکه، تغییرات را روی سرور عملی کرده و پس به اطلاع دیگر سویچ‌ها می‌رساند.

سوالات فصل پنجم

۱. پروتوکول VTP را تعریف نمایید.

۲. فرق بین پروتوکول VTP و Trunking را در یک مثال واضح سازید.

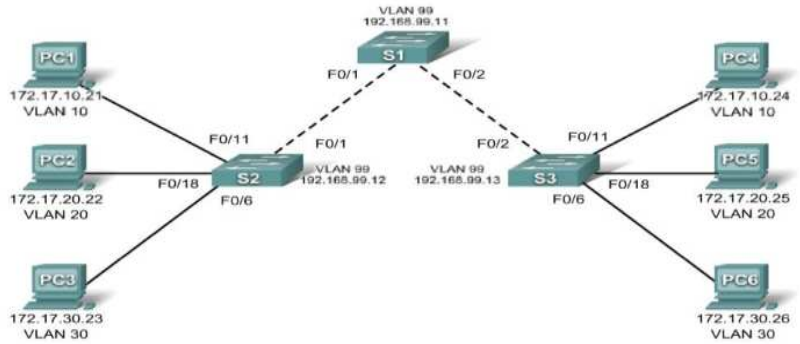
۳. توسط کدام کمنت می‌توانیم پروتوکول VTP را نصب نماییم؟

۴. موارد استفادهٔ VTP Pruning را در مثال تشریح نمایید.

۵. VTP Domain چیست؟ به‌صورت خلص تشریح نمایید.

فعالیت های فصل پنجم

- شبکه‌یی را نظر به شکل ذیل دیزاین کرده و VLANهای آن را بسازید و پروتوکول VTP را روی سویچ‌های آن فعال کنید و انترفیس‌ها را نظر به جدول و subnet که داده شده، انجام دهید. SW۱ را بحیث سرور و متباقی آن را به حیث Client معرفی کنید.
- ساختن vlan۹۹؛
- ساختن vtp server و vtp Client؛
- ساختن آدرس‌های کمپیوترها (assing ip address for pc).



Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

فصل ششم

Access List

هدف کلی: آشنایی و حصول معلومات در مورد Access Control List و انواع آن.

اهداف آموزشی: در پایان این فصل از محصلان انتظار می رود که:

۱. با Access Control List و اهداف آن معرفی شوند.
۲. با انواع Access Control List آشنا شوند.
۳. با نحوۀ تنظیم انواع Access Control List آشنا شوند.
۴. Access Control List را مدیریت و خطایابی نمایند.

تا اینجا کار با روتینگ، vlan و دیگر پروتوکول‌ها آشنا شدیم. حال نوبت به کنترول ترافیک شبکه و تعیین مجوزهای دسترسی برای ترافیک‌ها است؛ مثال: آیا شبکهٔ ۱۰.۱۰.۱۰.۲ اجازه دارد برای ما ترافیک بفرستد یا خیر؟ ما در Access List ها یاد می‌گیریم که چطور ترافیک شبکه را مدیریت کنیم و اعمال فیلترینگ داشته باشیم. ما می‌توانیم با استفاده از Access List برای یک روتر تعریف کنیم که چه ترافیک‌هایی اجازهٔ ورود به روتر و چه ترافیک‌هایی اجازهٔ خروج از روتر را دارند.

هم‌چنان موضوعات مربوط به Access List ابتدایی و Access List پیشرفته استندرهای مربوطه و استفادهٔ Access List به‌خاطر امن‌ساختن پورت‌ها، و به‌شکل کلی عملی‌سازی Access List بین روترهای سیسکو تشریح شده است.

۶.۱ لست دسترسی Access List

از Access List برای مدیریت ترافیک در شبکه استفاده می‌شود؛ مثلاً: شما می‌توانید به یک یا چند کمپیوتر اجازهٔ دسترسی به منابع خاصی از شبکه را ندهید که یکی از مهم‌ترین بخش‌های کار در شبکه است. در کل دو نوع Access List در شبکه وجود دارد که به شماره‌های مختلف مشخص شده‌اند.

لست دسترسی استندرد (Access List Standard) باشماره‌های ۱ تا ۹۹ و ۱۳۰۰ تا ۱۹۹۹
لست دسترسی پیشرفته (Access List Extended) باشماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹

۶.۲ لست دسترسی استندرد (Standard Access List)

این نوع Access Listها از شماره‌های ذکرشده در بالا استفاده می‌کنند و فقط ترافیک‌های مربوط به منبع را مورد بررسی قرار می‌دهند. با نحوهٔ کار این Access List آشنا می‌شویم.

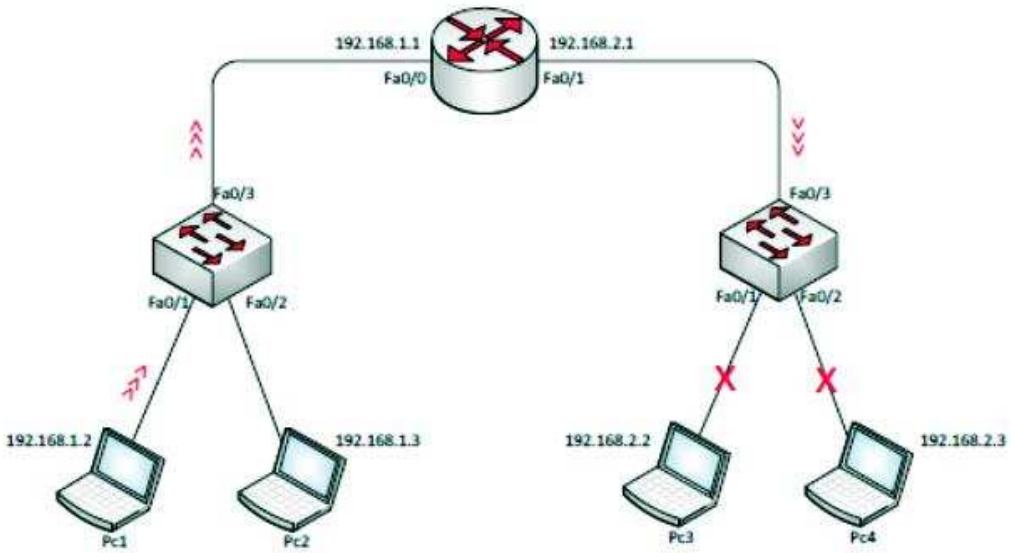
۶.۲.۱ Deny

این دستور در access List برای جلوگیری از دسترسی یک Node خاص به یک شبکهٔ دیگر است که بسیار پرکاربرد و خطرناک است، به دلیل این که با یک اشتباه، نصب یا کل شبکه از کار می‌افتد.

۶.۲.۲ Permit

این دستور ضد دستور Deny است و برای دسترسی به شبکه کاربرد دارد.

در این مثال می‌خواهیم از دسترسی PC۱به PC۳ و PC۴ جلوگیری کنیم.



وارد روترشده و دستورات زیر را وارد می‌کنیم:

```
Router (config)#ip access-list standard dpc1
```

در قسمت اول باید access List را تعریف کنیم؛ هم می‌توانیم با نام و هم می‌توانیم با شماره آن را تعریف کنیم که در این قسمت از نام dPC۱استفاده شده. شما می‌توانید، هر اسم دیگری در این قسمت قرار دهید. ویا از شماره استفاده کنید، اما همیشه سعی کنید از نام استفاده کنید که مدیریت آن آسان باشد.

```
Router(config-std-nacl)#deny 192.168.1.2 0.0.0.0
```

با این دستور ip address مربوط به PC۱را Deny می‌کنیم. اگر توجه کنید، در قسمت اول، دستور deny و بعد Ip address مربوط به PC۱و بعد از آن که مهم است از Wildcard Mask تأکیدی استفاده می‌کنیم. یعنی استفاده از چهار صفر که تأکید بر deny کردن همین Ip را دارد. اگر wild Card Mask را به‌صورت 255.0.0.0 وارد کنیم، یعنی تمام Ip addressها در رنج 192.168.1.0 فیلتر شود، پس سعی کنید از wild Card Mask تأکیدی استفاده کنید.

```
Router(config-std-nacl)#permit any
```

بعد از Deny حتماً از Permit استفاده کنید، چون هر زمان که از Deny استفاده می‌کنید، سایر شبکه‌ها هم Deny می‌شود و به‌خاطر همین از Permit Any استفاده می‌کنیم تا سایر شبکه‌ها اجازهٔ دسترسی داشته باشند.

بعد از تعریف کامل access List باید به روتر بگوییم که این فیلترینگ را روی کدام پورت انجام بدهد، پس وارد روتر می‌شویم. اگر توجه کنید، می‌خواهیم دسترسی PC۱به PC۳ و PC۴ جلوگیری کنیم، پس باید در پورت Fa0/1 روتر دستور زیر را وارد کنیم:

```
Router (config) # int f0/1
Router (config-if) #ip access-group dpc1 out
```

به دستور توجه کنید، Ip access-group را تعریف و بعد از آن، نام List Access را که ایجاد کرده‌ایم، وارد می‌کنیم، گفتیم ترافیک این access list در زمان خروج از انترفیس، فیلتر شود. اگر به جای out، گزینهٔ in را انتخاب می‌کردید، یعنی که شما access List را برای شبکهٔ 192.168.2.0 نوشته کردید، که این امر اشتباه است و این list access قابل اجرا نیست و حال اگر از PC۱به PC۳ و PC۴،Ping کنید، با پیام زیر مواجه می‌شوید:

```
PC>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

و حالا اگر از طریق PC۲ بخواهید PC۳ و PC۴ را Ping کنید، چنین جواب خواهید گرفت:

```
PC>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data
Reply from 192.168.2.3: bytes=32 time=1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.2.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in mille-seconds: Minimum = 0ms, Maximum = 1ms,
Average = 0ms
```

برای قراردادن توضیحات روی یک Access List، باید از دستور Remark استفاده کرد:

```
Router (config-std-nacl) # remark Access List Deny Pc1
```

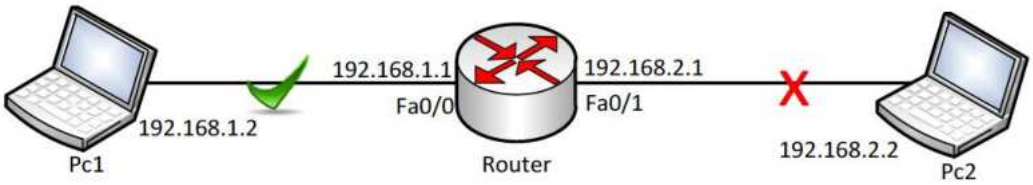
برای دیدن این دستور باید وارد Running-Config شوید تا این پیام برای شما نمایش داده شود.

```
Router# show Running-Config access-list
20 remark Access List Deny Pc1
```

۶.۳ لست دسترسی پیشرفته (Extended Access List)

این نوع Access List از شماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹ تشکیل شده است و می‌تواند ترافیک مربوط به منبع و مقصد را مورد بررسی قرار دهد، حتی می‌توانید پروتوکول‌ها یا برنامه‌های خاص را Deny یا Permit کنید.

مثال: در این مثال می‌خواهیم Telnet را روی روتر اجرا کنیم و access List بنویسیم که از دسترسی PC۲ به Telnet جلوگیری کند.



وارد روتر می‌شویم و به‌صورت زیر عمل می‌کنیم:

```
Router (config) #ip access-list extended Dpc2tel
```

یک access List extended با نام DPC2tel را ایجاد کردیم که شما می‌توانید به جای این نام، از نام دلخواه یا از شماره‌های ذکرشده در قسمت قبل استفاده کنید.

```
Router (config-ext-nacl) # deny tcp 192.168.2.0 0.0.0.255 any eq 23
```

در این قسمت برای Deny کردن PC۲ برای جلوگیری از Telnet، باید از از پروتوکول Tcp و پورت ۲۳ که مربوط به Telnet است را Deny کنید. در زیرجدول مربوط به پروتوکول‌ها و شمارهٔ پورت‌ها مشخص شده است:

```
Router (config-ext-nacl) # deny tcp 192.168.2.0 0.0.0.255 any eq 23
```

Decimal	Keyword	Description	Protocol
0		Reserved	
1-4		Unassigned	
20	FTP-DATA	FTP (data)	TCP
21	FTP	FTP	TCP
23	TELNET	Terminal connection	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Host name server	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		Unassigned	
160-223		Reserved	
162		FNP	UDP
224-241		Unassigned	
242-251		Unassigned	

چون در این جا قرار است که Telnet را برای PC۲ بسته کنیم. از پروتوکول TCP طبق جدول و از پورت ۲۳ که مربوط به Telnet است، استفاده می‌کنیم. پس به این صورت نوشته کنیم که Deny شود، پروتوکول TCP را برای شبکهٔ ۱۹۲.۱۶۸.۲.۰ با Wild Card mask، ۲۵۵.۰.۰.۰ و با پورت ۲۳ که مربوط به Telnet است.

نکته: بعد از این کار، تمام ترافیک مربوط به شبکه ۱۹۲.۱۶۸.۲.۰ فیلتر می‌شود، به‌خاطر این باید از دستور زیر در آخر کار برای Permit دادن به متباقی شبکه استفاده کنیم.

```
Router (config-ext-nacl) #permit ip any any
```

با این کار، PC۲ می‌تواند با روتر ارتباط داشته باشد و فقط پروتوکول Telnet بسته شده است. اگر یادتان باشد در access List standard همه ترافیک مربوط به یک دستگاه فیلتر می‌شد و حق دسترسی به هیچ عنوان نداشت، اما در access Extended چنین نیست. تنها PC۲ نمی‌تواند Telnet کند. برخلاف، می‌تواند روتر را ping کند.

در ادامه باید این access List را روی پورت روتر فعال کنیم:

```
Router (config-if) #ip access-group Dpc2tel in
```

پس این دستور به این صورت خوانده می‌شود که Ip access-group DPC۲telرا بر روی این پورت به‌صورت ورودی فعال کن، ورودی یعنی که PC۲ درحال ورود به روتر است. اگر از PC۲ به روتر Telnet کنیم، جواب نمی‌دهد.

```
PC>telnet 192.168.2.1
Trying 192.168.2.1…
 %Connection timed out; remote host not responding
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in mille-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

۶.۴ دستور Show access–list

این دستور، تعداد access List های موجود روتر را با جزئیات نمایش می‌دهد:

```
Router (config) #do sh ip access-list
Extended IP access list Dpc2tel
```

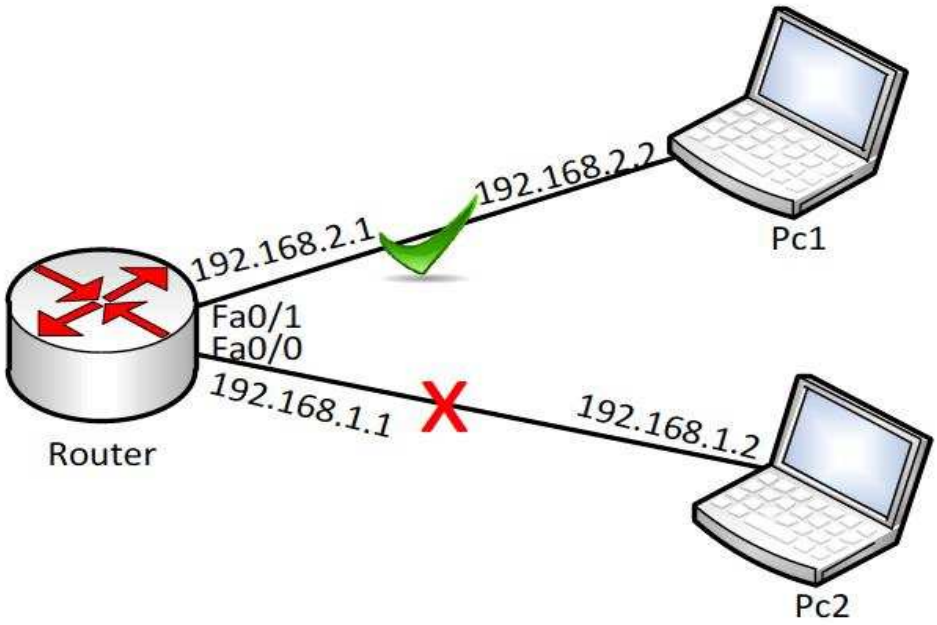
توجه داشته باشیدکه دستورات به‌صورت خلاصه‌شده وارد شده است و چون در مود Global هستیم، در اول دستور از do استفاده کردیم.

```
Router#show access-lists Dpc2tel
Extended IP access list Dpc2tel
deny tcp 192.168.2.0 0.0.0.255 any eq telnet (24 match(es))
permit ip any any (8 match(es))
```

در ادامه از access-List بسیار استفاده می‌کنیم. این دستور، یک دستور اساسی در سیسکو است.

۶.۵ استفاده از Access–List درپورت مجازی VTY

شما می‌توانید با تعریف یک Access List و فعال‌کردن آن در پورت Vty به یک ip اجازهٔ Telnet بدهید، یا ندهید. برای انجام این کار به مثال زیر توجه کنید:



شکل ۶-۱ : راه اندازی ACL در پورت VTG

مانند شکل بالا، یک روتر و دو pc را به صفحه اضافه و به هم متصل کنید و به پورت‌های مورد نظر ip دهید.

وارد روتر شوید و access-List زیر را وارد کنید:

```
Router(config)#ip access-list standard 10
Router (config-std-nacl) #permit 192.168.1.0 0.0.0.255
```

در دستورات بالا، یک access-List استندرد با شمارهٔ ۱۰ تعریف کردیم و بعد از آن به شبکهٔ ۱۹۲.۱۶۸.۱.۰ اجازهٔ دسترسی دادیم و زمانی که یک Permit برای یک شبکه تعریف می‌کنیم، متباقی شبکه‌ها Deny می‌شوند.

بعد از ایجاد Access –List، وارد پورت Line Vty می‌شویم و Telnet را روی پورت‌ها فعال می‌کنیم:

```
Router(config)#line vty 0 15
Router (config-line) #password 123
Router (config-line) #login
Router(config-line) #access-class 10 in
```

در دستور اول، وارد پورت Vty ۰ ۱۵ می‌شویم و بعد رمز عبور را بر روی پورت‌ها قرار می‌دهیم، سپس با دستور login می‌گوییم که در زمان telnet شدن، رمز عبور را درخواست کند و بعد از آن، با دستور access-class به این پورت می‌گوییم که در زمان telnet شدن، فقط ip address هایی را قبول کن که access-list ۱۰ می‌گوید. بعد از اتمام کار، اگر از طریق PC۱به روتر Telnet کنید، جواب می‌گیرید، اما از طریق PC۲ این امکان وجود ندارد.

خلاصه‌ی فصل ششم

از Access List برای مدیریت ترافیک در شبکه استفاده می‌شود؛ مثلاً؛ شما می‌توانید به یک یا چند کمپیوتر اجازهٔ دسترسی به منابع خاصی از شبکه را ندهیدکه یکی از مهم‌ترین بخش‌های کار در شبکه است. معمولاً دو نوع Access List داریم؛

نوع اول Access List Standard استندرد که از شماره‌های باشماره‌های ۱ تا ۹۹ و ۱۳۰۰ تا ۱۹۹۹ فقط ترافیک‌های مربوط به منبع را مورد بررسی قرار می‌دهند.

نوع دوم Access List Extended پیشرفته از شماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹ تشکیل شده است و می‌تواند ترافیک مربوط به منبع و مقصد را مورد بررسی قرار دهد، حتی می‌توانید پروتوکول‌ها یا برنامه‌های خاص را Deny یا Permit کنید.

سوالات و فعالیت های فصل ششم

۱. Access list چطور روی یک روتر فعال می‌گردد؟

۲. چند نوع Access List داریم؟ هر کدام آن را نام ببرد.

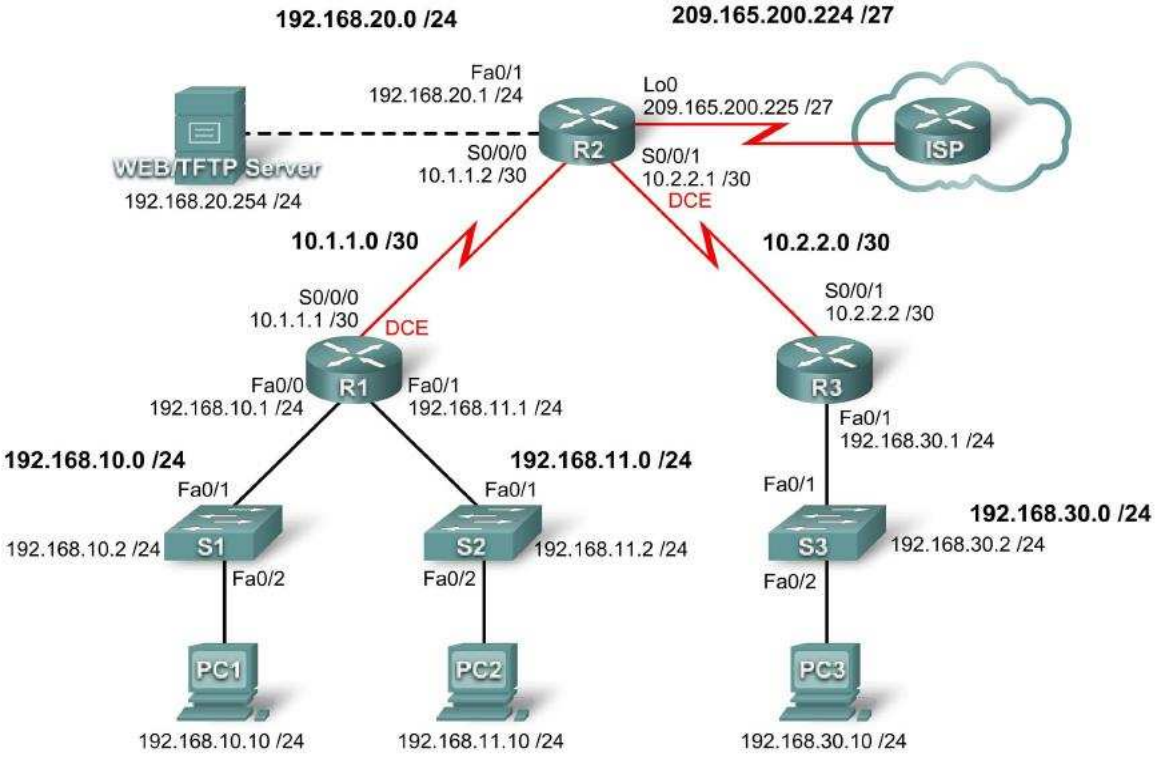
۳. هدف فعال‌ساختن Access List را شرح دهید.

۴. فواید و نواقص Access List واضح سازید.

۵. توسط کدام کمنت می‌توانم روی روتر خویش Access List را فعال نماییم؟

فعالیت ها

- شبکه‌یی را نظر به شکل ذیل دیزاین کرده و پروتوکول access list را فعال کنید و انترفیس‌ها را نظر به شکل و جدولی که داده شده فعال سازید.
- کنسول روترها را پس‌ورد بدهید.
- Dns-lookup را غیر فعال کنید.
- ACL را بالای روتر سوم انجام بدهید.
- پروتوکول OSPF 0 را بالای روترها انجام بدهید.
- Loopback interface را بالای روتر دوم فعال سازید.
- جهت اطمینان از ارتباط روترها از دستور ping استفاده نمایید.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	Fa0/1	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	Fa0/1	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
S1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1
R2	Fa0/1	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	Fa0/1	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
S1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1

فصل هفتم

(NAT) Network Address Translation

هدف کلی: آشنایی با NAT و انواع آن.

اهداف آموزشی : در پایان این فصل از محصلان انتظار می رود که:

۱. NAT را تعریف نمایند.
۲. عملکرد NAT را بدانند.
۳. با انواع NAT و نحوۀ تنظیم آن آشنایی حاصل نمایند.

Network Address Translat (NAT) میکانیزم ترجمهٔ آدرس‌های Invalid به آدرس‌های valid می‌باشد همان‌طور که می‌دانید، آدرس‌های Valid، آدرس‌هایی هستند که توسط Region های مختلف IANNA راجسترشده و منحصربه‌فرد می‌باشند. از آنجایی‌که تعداد IPV۴ محدود می‌باشد، بنابراین نمی‌توان به هر Station در دنیا یک IP راجسترشده نسبت داد. پس راه حل مشکل کمبود تعداد IP راجسترشده چی می‌تواند باشد؟

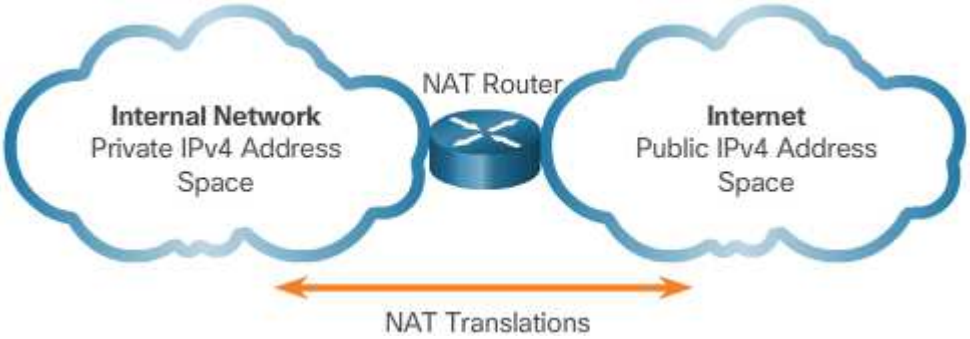
IPV۶ راه حل تعداد محدود IPV۴ می‌باشد. اما مسأله اینجاست که استفاده از آن و گسترده‌شدنش زمان‌بر است. بنابراین، نمی‌تواند یک راه حل کوتاه‌مدت باشد. راه حل دیگر، استفاده از ترجمهٔ آدرس‌ها یا همان NAT می‌باشد. در واقع NAT با ترجمه‌کردن تعدادی از آدرس‌های Invalid به آدرس ویا آدرس‌های راجسترشده این مشکل را حل کرده است. اما این تنها کاربرد NAT نیست؛ بلکه یکی دیگر از کاربردهای NAT برقراری امنیت در شبکه می‌باشد. در واقع یکی از راه‌های دور نگه‌داشتن شبکهٔ محلی از دسترس هکرها، پنهان‌کردن دستگاه‌ها به کمک آدرس غیر واقعی است. بنابراین با ترجمه‌کردن آدرس واقعی یک Station به آدرس دیگر می‌توان امنیت این دستگاه را برقرار کرد. بنابراین به‌طور کلی می‌توان گفت NAT میکانیزم ترجمه آدرس‌های Invalid یک شبکه به آدرس‌های راجسترشده می‌باشد. در این فصل با نحوهٔ عملکرد NAT و انواع آن آشنا خواهید شد.

۷.۱ NAT (Network Address Translation)

همان‌طوری که می‌دانید IP هایی که در داخل شبکهٔ خود استفاده می‌کنیم، invalid می‌باشد و برای ارتباط با دنیای انترنت باید به یک Ip valid تبدیل شوند. در دنیای انترنت از روشی به نام NAT استفاده می‌کنیم و Nat زمانی مورد استفاده قرار می‌گیرد که در یک شبکه استفاده‌کننده‌هایی که دارای آدرس‌های معتبر نیستند نیاز به برقراری ارتباط با انترنت را دارند.

NAT یا Network Address Translation پروتوکول یا روشی است که برای تبدیل IP آدرس‌های شخصی به آدرس‌های معتبر (Public) استفاده می‌شود. این پروتوکول در لایهٔ سوم OSI مودل کار می‌کند.

از آنجایی‌که تعداد آدرس‌های IPV۴ محدود می‌باشد، بنابراین نمی‌توان به هر Station در دنیا یک IP آدرس راجسترشده را توضیح کرد. پس راه حل این مشکل، یعنی کمبود تعداد IPهای راجسترشده، پروتوکول NAT می‌باشد. این پروتوکول، تعداد آدرس‌های غیر معتبر (Private) را که از یک طرف به یک انترفیس سرور NAT متصل است، در قالب یک آدرس معتبر (Encapsulation) به سمت انترفیس خروجی که به انترنت متصل است، ارسال می‌کند. به زبان ساده؛ زمانی از این سرویس استفاده می‌کنیم که تعدادی کمپیوتر را بخواهیم از طریق یک آدرس Public به انترنت متصل نماییم.



شکل ۱,۷ (Network Address Translations)

همان‌طورکه می‌دانید، آدرس‌های Public آدرس‌هایی هستند که توسط Regionهای مختلف در نقاط مختلف جهان راجستر می‌شوند. در واقع آدرس‌های IPV۴ و IPV۶توسط این Regionها راجستر می‌شوند درصورتی‌که از آدرس‌های IPV۶استفاده شود، بناءً به ساختار آن احتمال تمام‌شدن این آدرس تقریباً غیر ممکن می‌باشد، اما مشکل زمانی پیش می‌آید که از IPV۴ استفاده کنیم. در واقع نمی‌توان به هر Station در شبکه یک آدرس Public دریافت کرد. نظر به تعریف این پروتوکول، شبکه‌ها را به دو دستهٔ کلی تقسیم می‌نماییم:

- Inside Network
- Outside Network

Inside Network به شبکه یا شبکه‌هایی گفته می‌شود که دارای آدرس‌های Private باشند. در واقع شبکهٔ داخلی که آدرس Stationهای مختلف آن توسط Regionها راجستر نشده است.

Outside Network به شبکه‌هایی گفته می‌شود که دارای آدرس‌های راجسترشده باشند. انترنت مجموعه‌یی از شبکه‌های با آدرس‌های راجسترشده می‌باشد.

۷.۲ انواع NAT

همان‌طورکه می‌دانید NAT وظیفهٔ ترجمهٔ آدرس‌های Private به آدرس‌های Public را به عهده دارد. بنابراین با توجه به این‌که این ترجمه چگونه انجام می‌شود، NAT را می‌توان به سه دستهٔ کلی زیر دسته‌بندی کرد:

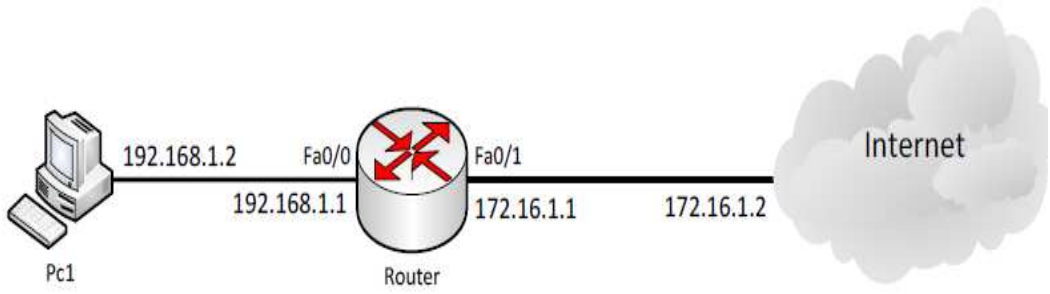
- Static NAT
- Dynamic NAT
- Dynamic NAT with overload

۷.۳ Static NAT

همان‌طور که از نامش پیدا است، عملیات ترجمه به‌صورت دستی صورت می‌گیرد. در واقع به‌صورت دستی به NAT Router گفته می‌شود که کدام آدرس Private را به چه آدرس Public ترجمه کند.

بنابراین به‌صورت دستی یک تناظر یک‌به‌یک بین آدرس‌های شخصی و آدرس‌های رسمی شکل می‌گیرد. درنتیجه درصورتی‌که یک Station نیاز به ارتباط با شبکهٔ بیرونی داشته باشد، NAT Router یک آدرس Public را به این آدرس متناظر کرده و از این به بعد این آدرس در شبکه‌های بیرونی قابل شناخت می‌باشد.

مثالی از Static NAT:



در این مثال PC۱می‌خواهد به انترنت متصل شود و به خاطر invalid بودن IP آن باید ترجمهٔ آدرس Ip valid انجام شود. وارد روتر شوید و دستورات زیر را وارد کنید:

```
Router (config) # ip nat inside source static 192.168.1.2 172.16.1.2
```

این دستور می‌گوید که IP NAT را روی شبکهٔ داخلی و روی مبدأ فعال کن و به‌صورت دستی (Static) به شمارهٔ ۱۹۲.۱۶۸.۱.۲ را به IP Valid ۱۷۲.۱۶.۱.۲ تبدیل کن.

بعد وارد انترفیس Fa0/0 که به سمت شبکهٔ داخلی است می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config-if)#ip nat inside
```

به این دستور NAT روی این انترفیس فعال می‌شود. در انترفیس دیگر Fa0/1 که به سمت شبکهٔ Out side است، دستور زیر را وارد می‌کنیم:

```
Router(config-if)#ip nat Outside
```

بعد از اتمام کار IP مربوط به PC۱برای رفتن به شبکه، انترنت تبدیل می‌شود، می‌تواند با دستور زیر NAT فعال‌شده روی روتر را مشاهده کنید:

```
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 192.168.1.2 172.16.1.2 ---
```

با دستور زیر اطلاعات کامل از NAT روی روتر به دست خواهید آورد:

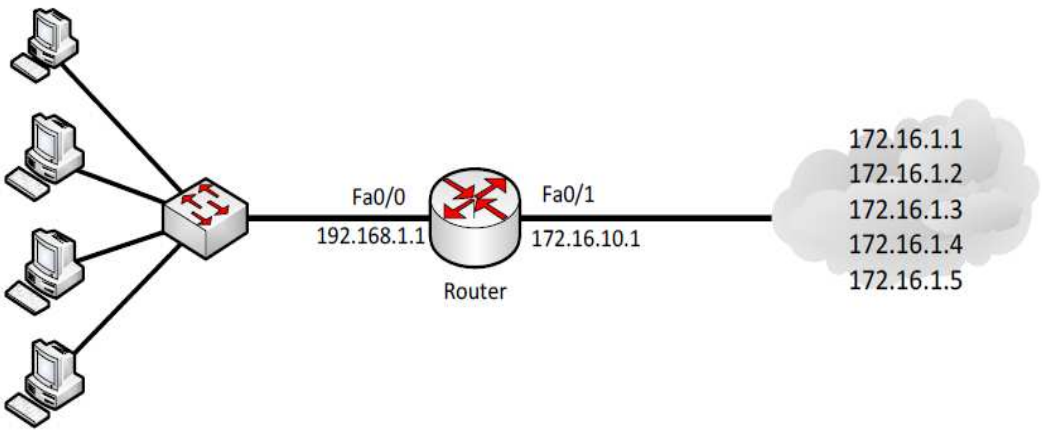
```
Router# show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 0 Misses: 14
Expired translations: 0
```

۷.۴ Dynamic NAT

Dynamic NAT نیز همانند Static NAT است؛ اما با این تفاوت که در NAT به‌صورت Dynamic می‌توانیم یک یا چندین IP را به چندین IP ترجمه کنیم؛ اما چرا چندین IP به چندین IP؟

فرض کنید شما Admin یک ISP هستید و به دلیل کمبود IP نیاز به NAT دارید. به‌طور مثال شما دارای 10 Valid IP و 100 Invalid IP که باید به آن‌ها ترجمه کنید. ممکن است تا کنون برای شما پیش آمده باشد که کاربر (User) تماس گرفته و اعلام نارضایتی کند از این که مدت‌های طولانی برای دانلود یک فایل از سایت Rapidshare.com باید انتظار بکشد. این به دلیل این است که سایت Rapidshare.com تمامی یوزرهای شما را به چشم یک کاربر می‌بیند. برای رفع این مشکل می‌توانیم 10 آدرس معتبر را به 100 آدرس غیر معتبر ترجمه کنیم که تا حدود زیادی مشکل را حل خواهد کرد.

در Dynamic NAT معمولاً آدرس‌های معتبر را به وسیلهٔ IP nat pool مشخص و آدرس‌های غیر معتبر را توسط یک access-list مشخص می‌کنیم. دلیل استفاده از access-list ایجاد امنیت بیشتر است. حال با یک مثال به نحوهٔ ایجاد یک Dynamic NAT می‌پردازیم. با دقت به این مثال توجه کنید، تا به خوبی با مطالب آن آشنا شوید.



برای استفاده از Dynamic Nat نخست از همه دو چیز تعریف می‌کنیم، یکی IP Pool که مجموعهٔ IPهای Valid که در این مثال پنج تا است، را در خود نگه‌می‌دارد و بعد باید یک Access List برای IP داخل شبکه خود تعریف کنیم و در آخر این دو را با هم ترکیب کنیم.

وارد روتر شوید و دستور زیر را وارد کنید:

این دستور را به این صورت بخوانید: IP NAT Pool ایجاد کن با نام OIP، که می‌توانید هر نام دیگری هم قرار دهید و بعد از آن باید IPهای Valid را وارد کنید که در قسمت اول، شروع IP و در قسمت بعدی، پایان IP را مشخص کنید، مانند دستور بالا و در قسمت آخر هم Net mask آن را وارد کنیدکه همان Wild Card mask است. تا این قسمت، ip nat pool را تعریف کردیم و برای ادامه باید access-list را برای شبکهٔ داخلی تعریف کنیم:

```
Router (config) #access-list 10 permit 192.168.1.0 0.0.0.255
```

IPهای داخلی شبکه را در یک access-list قرار می‌دهیم که اجازهٔ دسترسی به شبکه را به آن‌ها داده‌ایم.

حالا نوبت این است که این دو را به هم ارتباط دهیم:

```
Router(config)#ip nat inside source list 10 pool oip
```

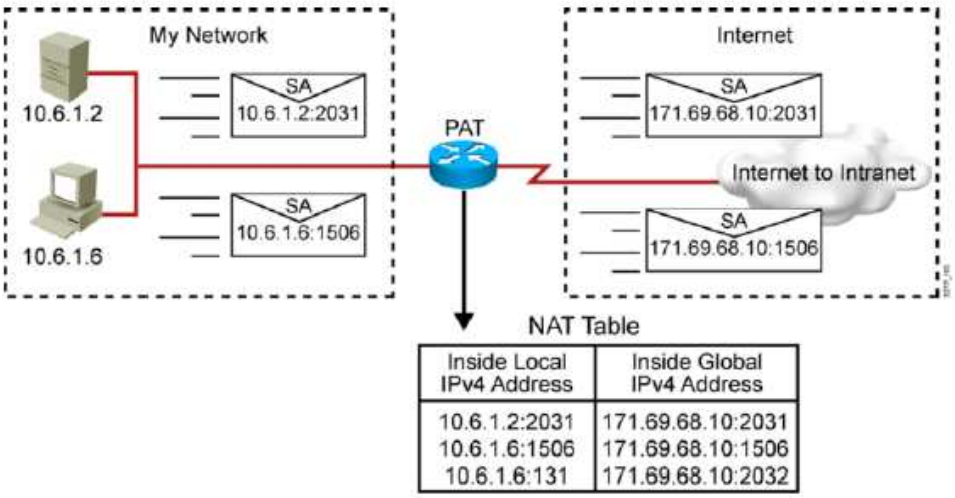
با این دستور، access-list ۱۰ با pool oip ارتباط برقرار می‌کند و در زمان خروج IPهای تعریف‌شده در access-list به IP تعریف‌شده در Pool oip تبدیل می‌شوند. بعد از این کار وارد انترفیس می‌شویم و دستورات زیر را وارد می‌کنیم:

```
Router(config)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#int f0/1
Router(config-if)#ip nat outside
```

۷.۵ Dynamic Nat with Overload (PAT)

این روش یکی از بهترین روش‌ها درحال حاضر است، به دلیل این که شما احتیاج به یک IP Valid را دارید و تمام IP Invalid داخل شبکهٔ شما از طریق یک IP Valid ترجمه می‌شود؛ اما با استفاده از پورت،

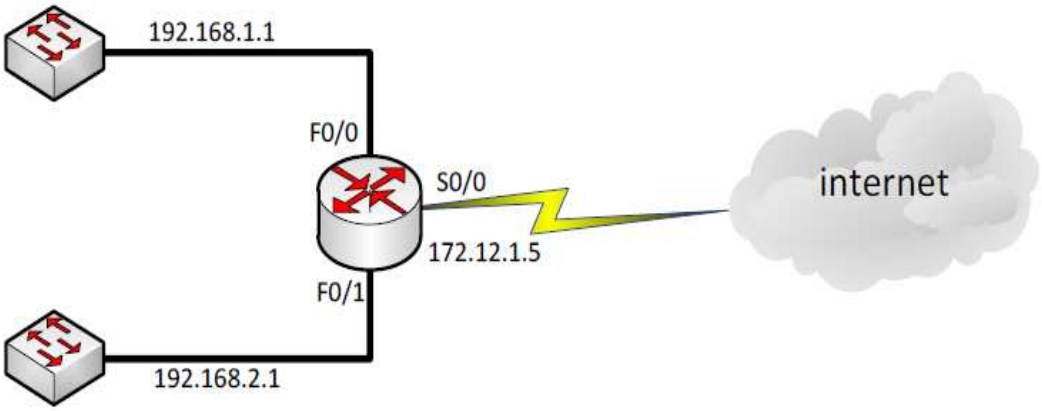
یعنی این‌که وقتی InvalidIP می‌خواهد به انترنت راه پیدا کند، از طریق همان IP Valid و به همراه یک پورت به انترنت راه پیدا می‌کند. در ادامه به‌صورت کامل با این موضوعات کار می‌کنیم.



شکل (۲,۷)PAT Translations

۷.۶ مثالی از Port Address Translation (PAT)

در این قسمت نیاز به یک IP Valid است و از طریق پورت IPها را از هم جدا می‌کند. به شکل ذیل توجه کنید:



در این شکل، دو شبکهٔ داخلی داریم که باید برای هر کدام یک access-list بنویسیم.

```
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

با دستور بالا، access-list شمارهٔ یک ایجاد شده است که IPهای Invalid شبکه‌های داخلی را در خود قرار داده است. وارد روتر می‌شویم و دستور زیر را وارد می‌کنیم:

```
Ip nat inside source list 1 interface Serial0 overload
```

با تعریف دستور بالا access-list با شمارهٔ ۱ که ایجادکرده ایم، انتخاب و روی انترفیس Serioal۰ که به طرف شبکهٔ خارجی است، فعال می‌کنیم و در آخر دستور از Overload استفاده می‌کنیم که در زمان خروج، IP را به همراه یک پورت به بیرون ارسال می‌کند.

بعد از آن وارد انترفیس‌های روتر می‌شویم و NAT را فعال می‌کنیم:

```
ip nat inside
```

نحوهٔ پاک‌کردن آدرس‌های موجود در جدول NAT:

```
Router#clear ip nat translation*
```

با این دستور، کلاً درس‌های موجود در جدول Nat حذف خواهد شد.

```
Router#clear ip nat translations inside a.b.c.d outside e.f.g.h
```

با این دستور یکی از رکوردهای ایجادشده از جدول Nat حذف خواهد شد.

امنیت همزمان، همراه با عملی‌سازی پروتوکول Dynamic NAT، یک فایروال به‌صورت اتومات بین شبکهٔ داخلی و شبکه‌های خارجی ایجاد می‌گردد. NAT صرفاً امکان ارتباط به کامپیوترها را که در حوزهٔ داخلی می‌باشند خواهد داد.

این بدان معنا است که یک کمپیوتر موجود در خارج از شبکهٔ داخلی، قادر به ارتباط مستقیم با یک کمپیوتر موجود در حوزهٔ داخلی نبوده، مگر این‌که ارتباط فوق توسط کامپیوتر شما مقداردهی اولیه گردد. شما به راحتی قادر به استفاده از انترنت، دریافت فایل‌ها، و غیره خواهید بود؛ ولی افراد خارج از شبکه نمی‌توانند با استفاده از آدرس IP شما به کامپیوتر شما متصل شوند.

برخی از روترهای مبتنی بر NAT امکان فیلترینگ و ثبت ترافیک را ارائه می‌دهند. با استفاده از فیلترینگ می‌توان سایت‌هایی را که پرسونل یک سازمان از آن‌ها استفاده می‌نمایند، کنترول کرد. با ثبت ترافیک یک سایت می‌توان از سایت‌های بازشده توسط کاربران آگاهی و گزارشات متعددی را بر اساس اطلاعات ثبت‌شده ایجادکرد.

خلاصه‌ی فصل هفتم

پروتوکول NAT میکانیزم ترجمهٔ آدرس می‌باشد جهت برقراری ارتباط با انترنت ویا جهت امن‌ساختن شبکه استفاده می‌شود. پروتوکول NAT با ترجمه‌کردن آدرس‌های Private به آدرس‌های راجسترشده کار ترجمه را انجام می‌دهد. این ترجمه می‌تواند یک‌به‌یک ویا یک‌به‌چند باشد، بنابراین می‌توان با توجه به نحوهٔ ترجمه، NAT را به سه دستهٔ کلی تقسیم کرد:

- Static NAT
- Dynamic NAT
- Dynamic NAT with Overload

Static NAT ترجمهٔ یک‌به‌یک آدرس‌ها را انجام می‌دهد و دو روش آخر ترجمه یک‌به‌چند را انجام می‌دهند.

روتر، اطلاعات لازم برای ترجمه را در یک جدول نگهداری می‌کند و ترجمه بر اساس آن صورت می‌گیرد. در حالتی که Static NAT را استفاده کنیم، بدون تغییر باقی می‌ماند درحالی‌که اگر از Dynamic NAT ویا Dynamic with overload NAT استفاده شود، این جدول تغییر می‌کند.

سوالات فصل هفتم

۱. NAT چیست؟ انواع آن را نام بگیرید.

۲. فرق بین Dynamic Nat و Static Nat را بیان کنید.

۳. پروتوکول NAT در امنیت شبکه چه اهمیت دارد؟

۴. ترجمهٔ یک‌به‌یک توسط کدام نوع NAT صورت می‌گیرد؟

۵. دلیل اصلی به‌میان‌آمدن پروتوکول NAT را تشریح کنید.

- شبکه‌یی را نظر به شکل ذیل بسازید؛ انترفیس‌ها را فعال و ارتباط بین آن را شناسایی کنید.
- Static Nat را فعال کنید.
- Dynamic Nat را فعال کنید.
- یک وب‌سرور شبیه‌سازی‌شده بر روی ISP ایجاد کنید.

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (Simulated Server)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

فصل هشتم

WAN Connection

اهداف کلی: آشنایی با انواع ارتباطات در شبکهٔ گسترده و پروتوکول های آن.

اهداف آموزشی : در پایان این فصل از محصلان انتظار می رود که:

۱. انواع ارتباطات در شبکهٔ گسترده را بدانند.
۲. با عملکرد پروتوکول PPP آشنایی حاصل نمایند.
۳. با عملکرد پروتوکول HDLC آشنایی حاصل نمایند.
۴. پروتوکول PPP را عیارسازی نمایند.
۵. پروتوکول HDLC را عیارسازی نمایند.

شبکهٔ گستردهٔ (wan) یک شبکهٔ کمپیوتری است که ناحیهٔ جغرافیایی نسبتاً وسیعی را پوشش می‌دهد. (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قارهٔ دیگر) این شبکه‌ها معمولاً از امکانات انتقال خدمات‌دهندگان عمومی، مانند شرکت‌های مخابراتی استفاده می‌کنند؛ به عبارت کمتر رسمی، این شبکه‌ها از مسیریاب‌ها و لینک‌های ارتباطی عمومی استفاده می‌کنند. شبکه‌های گسترده از نظر محدودهٔ تحت پوشش با شبکه‌های شخصی (به انگلیسی PAN) شبکه‌های محلی به انگلیسی (LAN) شبکه‌های دانشگاهی به انگلیسی (CAN) شبکه‌هایی که چند ساختمان یک سازمان را پوشش می‌دهند (یا شبکه‌های کلان شهری) به انگلیسی ((MAN که معمولاً محدود به یک اتاق، یک ساختمان، فضای چند دانشکده یا یک شهر می‌باشند، قابل مقایسه هستند. بزرگ‌ترین و شناخته‌شده‌ترین مثال از یک شبکهٔ گسترده، شبکه انترنت است. سرویس‌هایی که با آن‌ها می‌توانیم شبکه‌های خود را در نقاط مختلف به هم متصل کنیم و توسط مخابرات ارائه می‌شود، به شرح زیر است:

Leased Line
Circuit Switching
Packet Switching
Cell Switching
Label switching

۸.۱ Leased Line

عبارتند از یک ارتباط نقطه‌به‌نقطه و مستقیم که توسط Service Provider ارائه می‌شود. Leased Line ارتباطی است که همواره برقرار می‌باشد و با مشخص‌بودن دو سر آن به‌عنوان یک ارتباط اختصاصی به‌عنوان یک ارتباط Secure توسط Service Provider ارائه می‌شود. bandwitdth این ارتباط می‌تواند تا ۴۵ Mbps باشد.

۸.۲ Circuit–Switched

در این روش همان‌طور که از نامش پیداست یک مدار مجازی بین دو Station نهایی تعریف می‌شود. در سویچینگ مداری ابتدا ارتباط بین دو Station نهایی برقرار شده و سپس اطلاعات منتقل می‌شود. نمونهٔ شبکه سویچینگ مداری، شبکهٔ تلفن می‌باشد. در این شبکه بعد از برقراری ارتباط بین دو نقطهٔ نهایی، یک ارتباط فزیکی برقرار شده و طرفین می‌توانند به مکالمه و حتی انتقال دیتا بپردازند و تا زمانی‌که طرفین به‌صورت کامل این ارتباط را قطع نکنند، این مدار آزاد نخواهد شد. بنابراین می‌توان گفت که یکی از نقاط ضعف سویچینگ مداری، اشغال کانال‌های فزیکی حتی در زمانی که هیچ‌گونه اطلاعاتی رد و بدل نمی‌شود، است. این بدان معنا است که با محدودبودن ظرفیت سویچینگ و با اشغال‌شدن یک کانال، حتی اگر طرفین برای مدتی انتقال سیگنال نداشته باشند، کانال اشغال خواهد ماند. شبکهٔ تلفن معمولی و شبکهٔ ISDN نمونه‌یی از سویچینگ مداری هستند.

۸.۳ Packet–Switched

در این روش برخلاف سویچینگ مداری، مداری بین دو Station نهایی برقرار نمی‌شود، بلکه در این روش اطلاعات به بسته‌های کوچکی تقسیم شده و به همراه یک سری اطلاعات کنترولی به شبکهٔ سویچینگ پکتی تحویل داده می‌شود؛ بنابراین سویچ‌های مختلف با درنظرگرفتن بهترین مسیر، پکت را هدایت کرده و به مقصد می‌رسانند؛ لذا در این روش منابع شبکه درگیر برقراری یک مدار دایمی بین دو Station نهایی نخواهند شد. برای نمونه می‌توان شبکه‌های relay-Frame و X.25 را به‌عنوان شبکهٔ سویچینگ پکتی معرفی کرد.

۸.۴ Switching Label

در این روش که سریع‌ترین روش موجود است بر روی بسته‌ها برچسپ‌گذاری و انتقال معلومات می‌شود. این روش در لایهٔ ۲، یعنی لایهٔ پیوند اطلاعات کار می‌کند. استفاده از برچسپ‌گذاری و Multiport فناوری‌های جدید در این زمینه هستند.

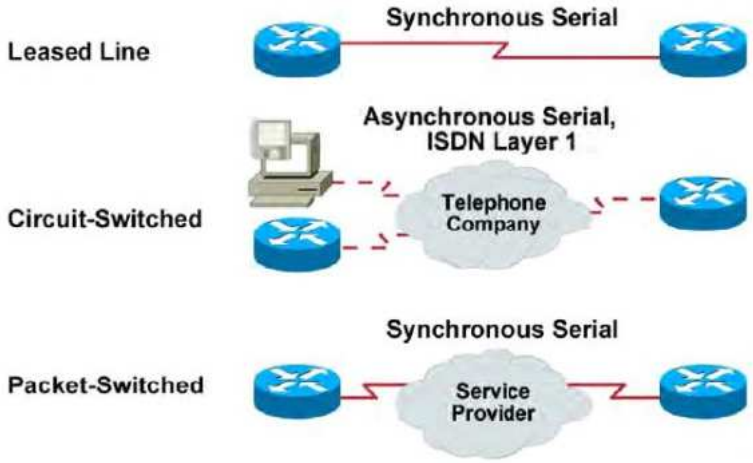
Serial انترفیس: از دید لایهٔ فزیکی به ارتباط یک روتر با شبکهٔ WAN، انترفیس Serial روتر و یک کیبل نیاز می‌باشد. انترفیس Serial، انترفیسی است که در آن انتقال دیتا به‌صورت متوالی (Serial) صورت می‌گیرد این بدان معنا است که در هر زمان یک سیگنال روی کانال ارتباطی ارسال می‌شود، بنابراین bitهای معلومات پشت سر هم روی خط حرکت خواهند کرد. روترهای سیسکو استانداردهای زیر را برای انترفیس Serial حمایت می‌کنند:

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530

انترفیس Serial که به آن انترفیس WAN نیز گفته می‌شود، یک پورت ۶۰Pin می‌باشد که (DB-۶۰) و به آن یک کُنکتور (DB-۶۰) متصل می‌شود. در صورت ارتباط روتر با شبکهٔ WAN می‌بایست از کیبل استفاده شود که از یک سو دارای کانکتوری (DB-۶۰) باشد که به انترفیس Serial روتر متصل شود و از سوی دیگر می‌توان با توجه به سرویسی که استفاده می‌شود، کانکتور مشخصی داده باشد.

انترفیس‌های سریال نیز دو نوع هستند. نوع اول DCE یا Data Communication Equipment قابلیت Clocking و تغییر User Data به فارمت Service Provider را دارا هستند. مشهورترین مثال آن CSU/DSU است. نوع دوم DTE یا Data Terminal Equipment هستند.DTE برای عملیات به DCE نیاز دارد همان‌طور که در شکل مشاهده می‌کنید DSU/CSU ویا مودم به‌عنوان سخت‌افزاری است که دیتای دریافتی از روتر را قابل ارسال به شبکهٔ WAN می‌کند. در انتقال سریال دیتا می‌بایست سرعت

انتقال دیتا در انترفیس سریال گیرنده و فرستند یکسان باشد. در واقع می‌بایست Clock Rate یا همان نرخ ارسال دیتا در انترفیس سریال فرستنده و گیرنده یکسان باشد. DTE یا همان Data terminal equipment، که در این شکل روتر در نظر گرفته شده است، نیاز به تعیین Clock Rate از سوی مودم ویا CSU/DSU دارد تا سرعت ارسال دیتا بر اساس نرخ مشخص‌شده باشد. DCE یا همان Data terminal equipment که معمولاً یک مودم یا یک CSU/DSU می‌باشد وظیفهٔ تبدیل اطلاعات دریافتی از یک DTE به فارمت قابل قبول شبکهٔ WAN را به عهده دارد و از طرفی DCE وظیفهٔ تعیین Clock Rate را به عهده دارد؛ بنابراین انترفیس‌های Serial می‌توانند نقش DTE ویا DCE را داشته باشند. به‌طور مثال در استندارد EIA/TIA-۵۳۰ روتر فقط می‌تواند DTE باشد.



شکل: (۸، ۱) ارتباط Wan connection type

۸.۵ بررسی پروتوکول‌های WAN در لایهٔ دوم

همان‌طور که می‌دانید در شبکهٔ Ethernet دیتا به‌صورت فریم‌های Ethernet بسته‌بندی شده و سپس در اختیار لایهٔ فزیکی قرار داده می‌شود. در شبکهٔ WAN نیز قبل از این‌که اطلاعات تحویل بستر ارتباطی WAN شود، در فریم‌های مشخصی بسته‌بندی می‌شود. پروتوکول‌های لایهٔ دوم در شبکهٔ WAN نحوهٔ این بسته‌بندی را مشخص می‌کنند. با توجه به سرویس و استندردی که استفاده می‌شود، پروتوکول‌های لایهٔ دوم خاصی می‌بایست استفاده کرد. همان‌طور که در شکل مشاهده می‌کنید، متناسب با انواع شبکه‌های WAN، پروتوکول‌های متفاوتی به‌منظور بسته‌بندی اطلاعات استفاده می‌شود.

۸.۶ بررسی پروتوکول‌های مربوط به Line Leased یا خطوط اجاری

پروتوکول‌های مربوط به خطوط Leased به دو دسته تقسیم می‌شوند:

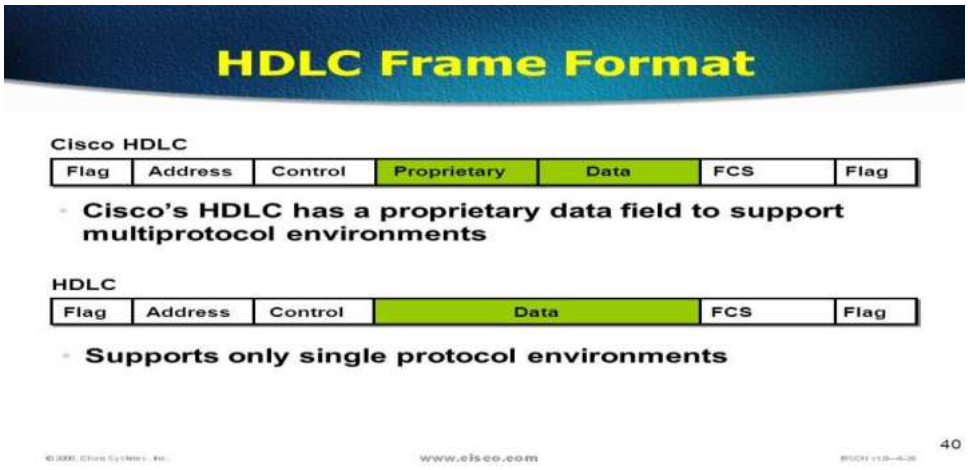
- HDCL
- PPP

۸.۷ بررسی پروتوکول HDLC

HDLC یک پروتوکول WAN Encapsulation است که در لایهٔ دوم کار می‌کند. ساده‌ترین پروتوکولی است که شما می‌توانید جهت ارتباط دو Remote Office بر روی خط‌های اجاره‌یی از آن بهره ببرید.

نسخه‌های HDLC یا High-Level Data Link Control

HDLC دو نسخه دارد. یک نسخهٔ استندرد که همهٔ ما صرف نظر از این‌که از چه برَند Router استفاده می‌نماییم، آن را می‌شناسیم. نسخهٔ دیگر، ورژن اختصاصی کمپنی سیسکو است که با نام Cisco Proprietary Version مشهور است و تنها در تجهیزات سیسکو وجود دارد. اگر نگاهی به فریم‌های هر دو نسخهٔ HDLC بیندازید، متوجه می‌شوید که تنها تفاوت این دو در یک فیلد اضافه به نام Proprietary یا اختصاصی است.



شکل (۸، ۲) نسخه‌های HDLC Frame Format

۸.۸ ضعف HDLC چیست؟

با وجود سادگی این پروتوکول، Administratorها کم‌تر از آن استفاده می‌کنند. دلیل این موضوع آن است که در HDLC هیچ میکانیزم Authentication وجود ندارد. اکنون استفاده از HDLC در بسیاری از سازمان‌ها به هیچ عنوان منطقی نیست.

۸.۹ فعال‌نمودن HDLC

پروتوکول HDLC به‌صورت پیش‌فرض روی انترفیس‌های Serial در تجهیزات سیسکو فعال می‌باشد. همان‌طور که می‌دانید پروتوکول HDLC به‌عنوان پروتوکول لایهٔ دوم بـر روی خطـوط Line-Leased بـه کـار گرفتـه می‌شود. بنابراین درصورتی‌که در دو سر این کانال ارتباطی تجهیزات سیسکو مورد استفاده قـرار گیـرد، این پروتوکول به‌منظور کپسوله‌کردن دیتا اسـتفاده خواهـد شـد. درحـالی‌کـه اگـر هـر دو سـوی ایـن کانـال تجهیزات سیسکو استفاده نشود می‌بایست از پروتوکول PPP به‌عنوان پروتوکول لایهٔ دوم استفاده کرد. برای مشاهدهٔ نوع encapsulation جاری بر روی انترفیس سریال روتر از فرمان show interface استفاده می‌کنیم. بـرای تعریـف پروتوکول HDLC روی انتـرفیس Serial، ابتـدا وارد Mode مربـوط بـه انتـرفیس Serial شـده و سپس فرمان زیر را وارد می‌کنید؛ به‌طور مثال: hdlc encapsulation بر روی انترفیس S۰ را با دستور زیر مشاهده می‌کنیم:

```
RouterA#sh int s0
```

اگر روش encapsulation بر روی یک انترفیس سریال عوض شده بود، شما می‌توانید با صادرکردن دستور encapsulation hdlc از طریق مود interface configuration آن را مجدد به hdlc برگردانید.

```
RouterA#config t
RouterA(config)#int s0
Router(config-if)#encapsulation hdlc
```

۸.۱۰ بررسی پروتوکول PPP

این پروتوکول که در یک ارتباط Point To Point کاربرد دارد، دارای دو لایهٔ زیر است:

- NCP یا Network Control Protocol: این پروتوکول وظیفهٔ بسته‌بندی یا کپسول‌کردن پروتوکول‌های لایهٔ Network، مانند IP و IPX را دارد.
- LCP Link Control Protocol: وظیفهٔ این پروتوکول، کنترول برقراری ارتباط بین دو نقطه است.

این لایه دارای ویژگی‌های زیر است:

۸.۱۱ Authentication

در این قسمت، مجوز برقراری ارتباط بین دو نقطه در ارتباط Point to Point بررسی می‌شود. برای تأیید اعتبار از دو روش استفاده می‌کند؛ بـه طـور مثـال: در یـک ارتبـاط نقطـه‌بـه‌نقطـه ماننـد Line-Leased که دو روتر در دو سر آن واقع شده است، ارتباط لایهٔ دوم زمانی برقرار می‌شـود کـه طـرفین مجوز برقراری ارتباط را بررسی کرده باشند. تأیید اعتبار توسط پروتوکول PPP به دو فارمت امکان‌پذیر است:

(Password Authentication Protocol) PAP
(Challenge Handshake Authentication Protocol) CHAP

در زیرلایهٔ LCP مشخص می‌شود که طرفین با چه مدتی عملیات Authentication را انجام می‌دهند.

Compression: این گزینه وظیفهٔ فشرده‌کردن دیتا در مبدأ و خارج‌کردن از حالت فشردگی در مقصد را به عهده دارد. این ویژگی به‌منظور افزایش ظرفیت یک لینک PPP به کار برده می‌شود.

Error Detection: میکانیسمی به‌منظور کشف خطا و جلوگیری از وقوع Loop می‌باشد.

Multilink: به کمک این ویژگی انترفیس‌هایی از روتر که PPP روی آنها فعال باشد می‌توانند در Balance کردن پکت‌ها روی Linkهای متفاوت نقش داشته باشند.

۸.۱۲ پروتوکول‌های تأیید اعتبار در PPP Authentication

همان‌طور که گفته شد دو میتود و در واقع دو پروتوکول وظیفهٔ تأیید اعتبار (Authentication) در PPP را به عهده دارند. تأیید اعتبار توسط پروتوکول PPP به دو فارمت امکان‌پذیر می‌باشد:

- (Password Authentication Protocol) PAP
- Challenge Handshake Authentication Protocol) CHAP

بنابراین زمانی که شما پروتوکول PPP را انتخاب می‌کنید، می‌بایست مشخص کنید از چه میتودی برای تأیید اعتبار استفاده خواهید کرد. در ادامه با هر دو میتود و نحوهٔ تنظیم آنها روی انترفیس‌های Serial یک روتر آشنا خواهید شد.

۸.۱۲.۱ PAP

بعد از این‌که فاز اول PPP، یعنی برقراری ارتباط براساس لایه دوم صورت پذیرفت می‌بایست Authentication صورت گیرد. PAP میتودی است که عملیات تأیید اعتبار را در دو مرحله انجام می‌دهد.

به علت سادگی این پروتوکول پس‌ورد به‌صورت Text Clear بر روی Link ارسال می‌شود. بنابراین از نظر امنیتی در سطح پایینی عمل می‌کند. درصورتی‌که تأیید اعتبار بخواهد به‌صورت کمی پیچیده‌تر انجام گیرد، نیاز به پردازش بیشتری می‌باشد و این از سرعت برقراری یک ارتباط می‌کاهد، درنتیجه زمانی‌که در تأیید اعتبار نیازی به دقت بالا نباشد، از این میتود استفاده می‌شود.

۸.۱۲.۲ CHAP

پروتوکول CHAP از یک میکانیزم سه مرحله‌یی برای شناخت و تأیید اعتبار استفاده می‌کند:

گام اول: بعد از مبادلهٔ پکت‌های LCP و برقراری لینک PPP، Message Challenge توسط درخواست‌کننده ارتباط Router Local به Router Remote ارسال می‌شود.

گام دوم: Router Remote پس از دریافت Message و بعد از به‌کاربردن الگوریتم MD۵ روی پس‌ورد، مقدار جدید را که حاصل الگوریتم MD۵ می‌باشد، با یک Message Response به Router Local ارسال می‌کند.

گام سوم: Router Local پس‌وردی را که نزد خود داشته است، به کمک الگوریتم MD۵ تبدیل به مقداری می‌کند و سپس مقدار حاصله را با مقدار دریافت‌شده توسط Message Response مقایسه کرده و در صورت یکسان‌بودن دو مقدار، تأیید اعتبار در این ارتباط به Router Remote اطلاع داده می‌شود.

مروری بر مراحل تنظیم‌کردن PPP روی یک لینک نقطه به نقطه:

بعد از این که پروتوکول PPP به‌عنوان پروتوکول لینک Point-to-Point انتخاب شد، می‌بایست آن را روی انترفیس مربوطه فعال کرد. به کمک فرمان PPP encapsulation روی انترفیس Serial پروتوکول PPP فعال می‌شود. بعد از فعال‌کردن پروتوکول PPP می‌بایست Authentication و میتود مورد نظر انتخاب و سپس تنظیم شود.

نحوهٔ تنظیم پروتوکول PPP: وارد مود انترفیس شده و فرمان زیر را وارد می‌کنید:

```
Router(config-if)#encapsulation ppp
```

۸.۱۳ نحوهٔ تنظیم Authentication در پروتوکول PPP

پس از فعال‌شدن پروتوکول PPP روی انترفیس Serial می‌بایست Authentication و میتود مورد نظر را روی انترفیس serial فعال کرد.

مشخص‌کردن یک نام برای روتر:

```
Router(config)#hostname name
```

۸.۱۴ مشخص کردن (Username) و (Password):

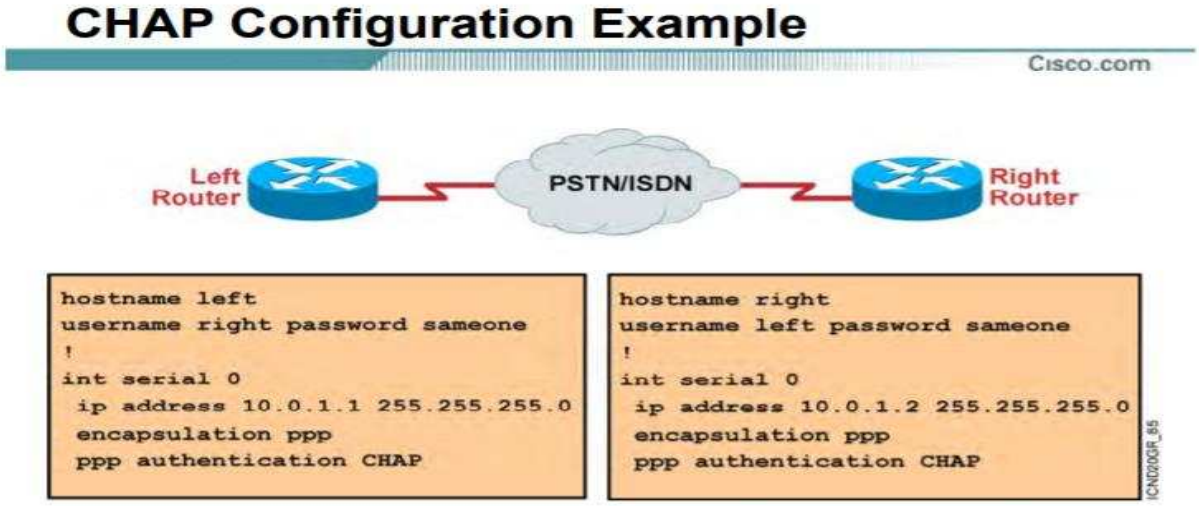
نکته: در تنظیم Authenticatin روی یک لینک نقطه‌به‌نقطه، می‌بایست Username نام روتر طرف مقابل و پس‌ورد روی هر دو روتر یکسان باشد.

```
Router(config)#username name password password
```

تعیین نوع پروتوکول Authentication، به عبارتی مشخص‌کردن PAP یا CHAP

Router(config-if)#ppp authentication{chap | chap pap | pap chap | pap}

مثالی از تنظیم CHAP: شکل فوق نحوهٔ تنظیم پروتوکول PPP با میتود تأیید اعتبار CHAP را نشان می‌دهد. در هر دو روتر پس از مشخص‌شدن Hostname می‌بایـست Username و Password را روی هـر کـدام از روترها مشخص کرد. Username نام روتر مقابل و پس‌ورد روی هر دو روتر یکسان

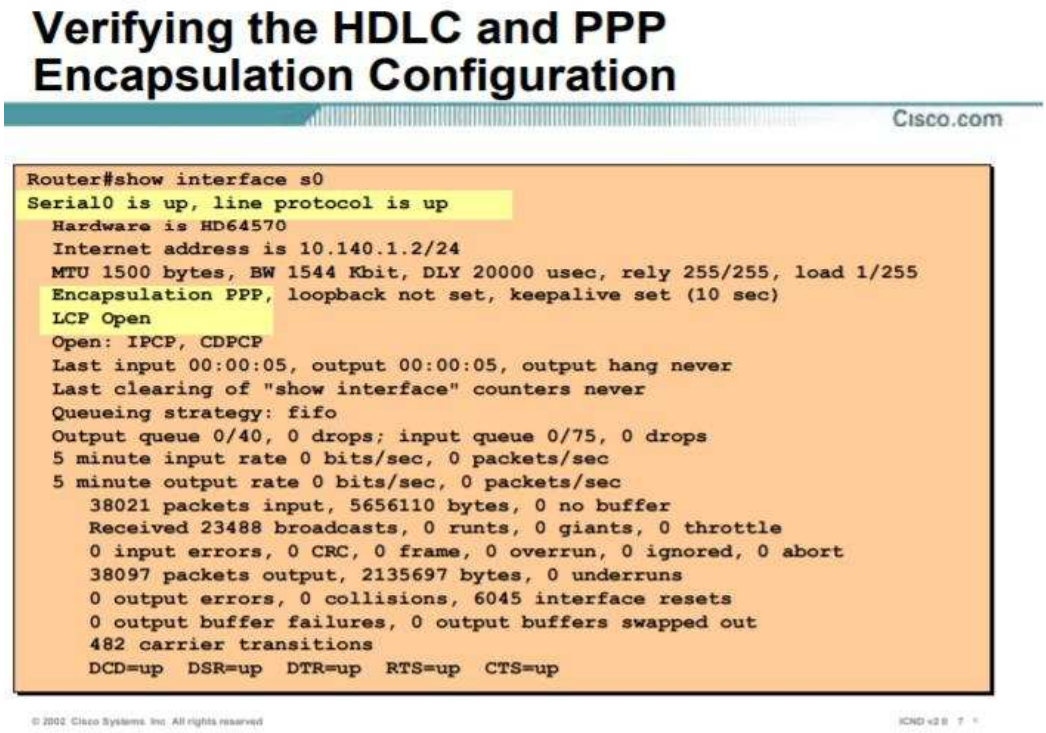


می‌باشد.

شکل: ۳,۸ نحوهٔ تنظیم پروتوکول PPP با میتود تأیید اعتبار CHAP

۸.۱۵ بررسی عملکرد پروتوکول PPP ویا HDLC

به کمک فرمان interface show می‌توان نوع پروتوکول لایهٔ دوم و میتود Authentication را که روی آن انتـرفیس تنظیم شده است، مشاهده کرد. به کمک این فرمان می‌توانید State هر کـدام از زیرلایـه‌های پروتوکول PPP را مشاهده کنید.



شکل (۸، ۴) مشاهدهٔ زیرلایـه‌های پروتوکول PPP

خلاصه‌ی فصل هشتم

WAN و سرویس‌های مختص به شبکهٔ WAN به‌منظور انتقال دیتا و تبادل اطلاعات شبکه‌های مختلف در ناحیه‌های مختلف جغرافیایی، استندرد و طراحی شده‌اند. ارتباطات WAN دارای انواع مختلفی می‌باشند. طوری‌که در یکی از دسته‌های زیر قرار می‌گیرند:

- Leased-Line
- Circuit-Switched
- Packet-Switched

بر اساس دسته‌بندی فوق، پروتوکول‌های WAN در لایهٔ دوم نیز طبقه‌بندی می‌شوند؛ به‌طور مثال: پروتوکول PPP و HDLC پروتوکول‌هایی هستند که به‌منظور فریم‌بندی اطلاعات قبل از تحویل به لایهٔ فزیکی استفاده می‌شوند و هر دو جزء پروتوکول‌های دو دستهٔ Leased-Line و Circuit-Switched هستند. از دید لایهٔ فزیکی به‌منظور برقراری ارتباط یک روتر با شبکهٔ WAN، به انترفیس Serial روتر و یک کیبل نیاز می‌باشد. بنابراین، این کیبل از یک طرف دارای کانکتور(DB-۶۰) به‌منظور اتصال به روتر و از سوی دیگر با توجه به سرویس WAN، نوع کانکتور متفاوتی خواهد داشت. روترهای سیسکو پنج استندرد متفاوت را به‌منظور ارتباط با شبکهٔ WAN حمایت می‌کنند. این پنج استندرد عبارتند از:

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530

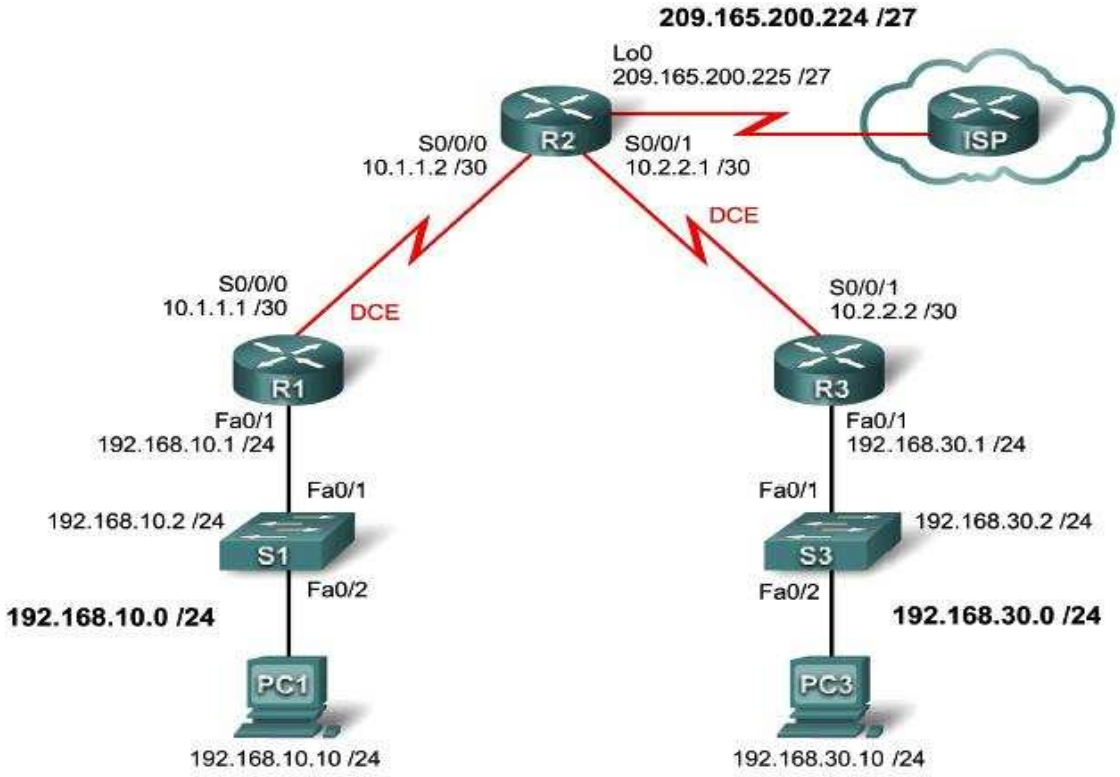
از آن‌جایی که انترفیس Serial دیتا را به‌صورت متوالی ارسال و دریافت می‌کند، بنابراین می‌بایست نرخ ارسال و دریافت دیتا بین گیرنده و فرستنده یکسان باشد؛ لذا Clock Rate با همان نرخ ارسال اطلاعات در واحد زمان توسط یکی از طرفین تعیین می‌شود. در ارتباطات سریال Clock Rate توسط DCE تعیین می‌شود، و این DTE می‌باشد که Clock Rate مشخص‌شده را پذیرفته و با آن دیتا را ارسال و دریافت می‌کند.

سوالات فصل هشتم

- موارد استفادهٔ WAN Connection ها را واضح سازید.
- فرق بین Packet Switching و Circuit Switching را بیان نمایید.
- فرق بین پروتوکول‌های PPP و HDCL را برشمارید.
- شبکه‌های جهانی را تشریح نمایید.

فعالیت های فصل هشتم

- شبکه وکیبل‌های آن را نظر به شکل ذیل دیزاین کرده و پروتوکول OSPF را بالای تمامی روترها انجام بدهید.
- انترفیس‌ها را فعال کنید.
- تنظیمات point to point encapsoltion را بالای پورت سریال serial فعال کنید.
- در مورد کمنت debug ppp negotiation و debug ppp packet تحقیق کنید و بیاموزید.
- تنظیمات PPP PAP و CHAP را فعال سازید.



فصل نهم

Frame Relay

هدف کلی: آشنایی محصلان با عیار سازی Frame Relay.

اهداف آموزشی: در پایان این فصل از محصلان انتظار می رود که:

۱. با عملکرد و ویژگی‌های Frame Relay آشنایی حاصل نمایند.
۲. پارامترهای Frame Relay را بدانند.
۳. Frame Relay را عیارسازی نمایند.

در این فصل Frame Relay را مورد بحث قرار می‌دهیم. نحوهٔ برقراری یک ارتباط لایهٔ دوم توسط Frame Relay و سیگنال‌های مورد استفاده از Frame Relay.

این پروتوکول از دستهٔ پروتوکول‌های Switching Packet است. Bandwidth آن عموماً ۵۶ کیلوبایت تا ۴۵ مگابایت است. هر مسیری که در frame Relay ایجاد می‌شود، به‌عنوان یک VC (Virtual Circuit) در نظر گرفته می‌شود. اگر این مسیر دایمی باشد، به‌عنوان PVC (Permanent Virtual Circuit) گفته می‌شود و اگر موقتی باشد به آن (Switched Virtual Circuit) است که اصولاً از PVC برای ارتباط بین دو مسیر استفاده می‌کنند.

۹.۱ Frame Relay

Frame Relay پروتوکول لایهٔ Data Link و یک سرویس (Connection Oriented) اتصال‌گرا می‌باشد. Frame Relay با تعریف‌کردن مدار، ارتباطات منطقی بین نقاط انتهایی برقرار می‌کنند. بنابراین با این تکنیک از یک کانال فزیکی می‌تواند چندین مدار مجازی (VC) عبور داد هر کدام از این مدارهای مجازی مشخص‌کنندهٔ دو نقطهٔ انتهایی می‌باشند. در شبکهٔ Relay Frame هر کدام از نقاط انتهایی به‌عنوان DTE و سویچ‌های شبکهٔ Frame Relay به‌عنوان DCE انتخاب می‌شوند. بنابراین انترفیس‌های Serial به عنوان DTE عمل کرده و با نرخ ارسال اطلاعات که توسط سویچ‌های شبکهٔ Frame Relay تعیین می‌شود، به ارسال دیتا می‌پردازد. در شبکهٔ Relay Frame ما با دو دسته مدار بین نقاط انتهایی رو به‌رو هستیم:PVC و SVC.

PVC مداری است که همواره برقرار می‌باشد، بنابراین می‌بایست برای برقراری این ارتباط هزینهٔ بیشتری پرداخت کرد، این درحالی است که مدار SVC، مداری است که هنگامی که نیاز به برقراری ارتباط باشد فعال می‌شود. بنابراین از مدارات PVC جهت برقراری ارتباطات سویچ‌ها در Service Provider و از مدارات SVC جهت ارتباط Customerها با Service Provider استفاده می‌شود.

- DCE: که در سمت سرویس‌دهنده ویا مخابرات است که کار سویچینگ و Clocking را انجام می‌دهند.
- DET: که در سمت سرویس‌گیرنده یا مشتری وجود دارد و ارتباط با شبکهٔ WAN را برقرار می‌کند.

مفهموم DLCI: هر VC توسط یک عدد که به آن عدد (Data-Link Connection Identifier)DLCI از دیگر VCها متمایز می‌شود. از طریق این عدد، IP Address ها را هدایت و کنترول می‌کنیم، توجه داشته باشید؛ این عدد bit ۱۰است.

Frame Relay یک شبکهٔ Broadcast نیست، بلکه یک شبکهٔ (Non-broadcast Multi-access) NBMA است و تمام اعضای شرکت‌کننده در یک ارتباط Frame Relay، باید یک ip در یک رنج داشته باشند.

۹.۲ LMI (Local Management Interface)

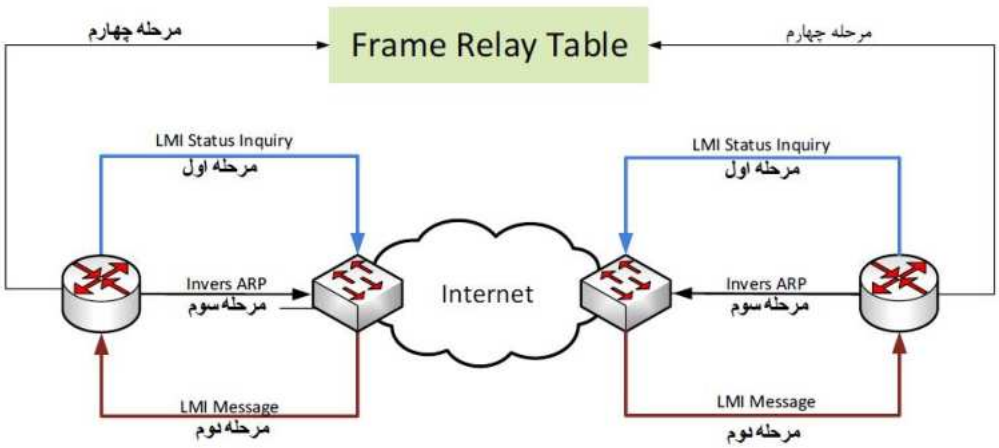
استندردی است که بر روی ارتباط بین DCE و DTE نظارت و کنترول می‌کند که بر سه نوع است:

- Cisco
- Ansi
- Q.933

در ارتباط Frame Relay باید استندرد به کار برده‌شده یکی باشد.

Inverse Arp: این عبارت عدد DLCI مربوط به یک Interface را در به‌صورت خودکار در فریم Frame Relay قرار می‌دهد.

چگونه ارتباط از طریق Frame Relay انجام می‌شود؟ به شکل زیر دقت کنید؛ هر مرحله از آن را با هم بررسی می‌کنیم:



شکل ۹-۱ : مراحل برقراری ارتباط frame relay

برای ایجاد ارتباط Frame Relay باید روتر به یک سویچ Frame Relay متصل شود. به این سویچ‌ها CSU/DSU می‌گویند. بعد از ارتباط، مرحله‌های بالا را باهم مورد بررسی قرار می‌دهیم.

مرحلهٔ اول: روتر یک پیام LMI Status Inquiry به سویچ مخفف FR (FR مخفف Frame Relay) می‌فرستد و درخواست ایجاد یک مدار مجازی VC را می‌کند.

مرحلهٔ دوم: در این مرحله، سویچ FR یک LMI Massage را برای روتر ارسال می‌کند که در این پیام، شمارهٔ DLCI مربوط به همان شبکه‌هایی که روتر در آن قرار دارد، به روتر داده می‌شود. از طریق این شماره، می‌توان در مدار مجازی VC با روتر شبکهٔ دیگر ارتباط برقرار کند.

نکته: LMI Massage هر ۲۴ ثانیه یکبار بین سویچ و روتر انجام می‌شود.

مرحلهٔ سوم: در این مرحله روتر بعد از دریافت DLCI در مرحلهٔ قبل، یک Invers ARP را به روترهای مقابل خود ارسال می‌کند و خود را به آن‌ها معرفی می‌کند.

نکته: روتر هر ۶۰ ثانیه یکبار پیام Invers ARP را برای تمام DLCIهای خود ارسال می‌کند.

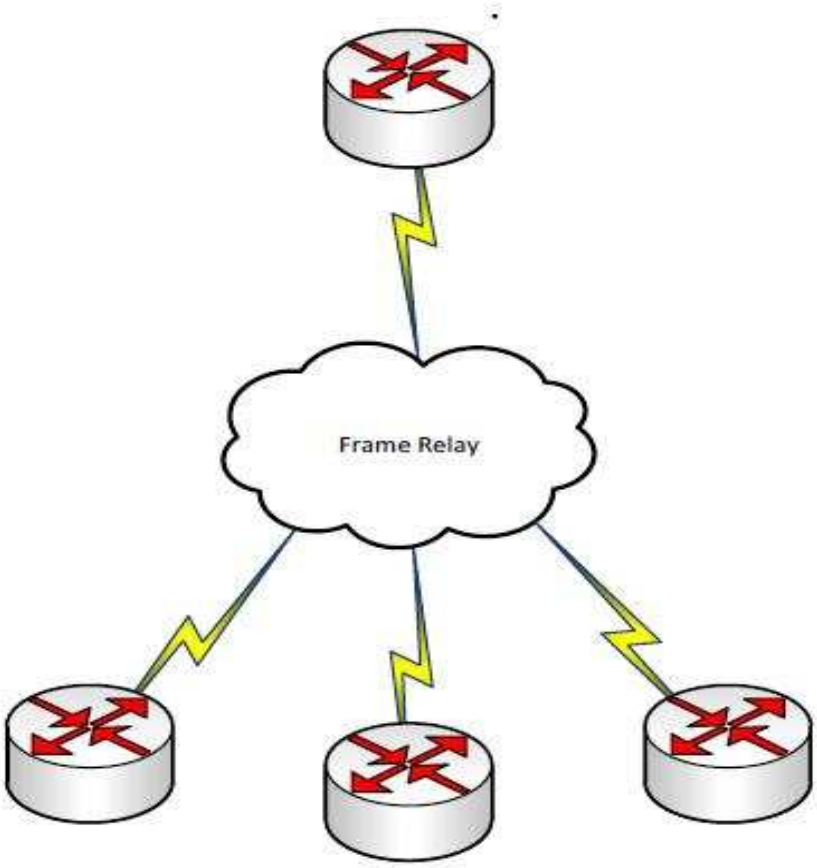
مرحلهٔ چهارم: روترها بعد از دریافت پیام Invers ARP که حاوی اطلاعات DLCI و IP Address است، آن‌ها را در جدولی به نام Frame Relay Map قرار می‌دهد.

۹.۳ کار با Frame Relay:

شبکهٔ Frame Relay از نظر هندسی و توپولوژی به سه دسته تقسیم می‌شوند:

۹.۳.۱ Hub and Spoke

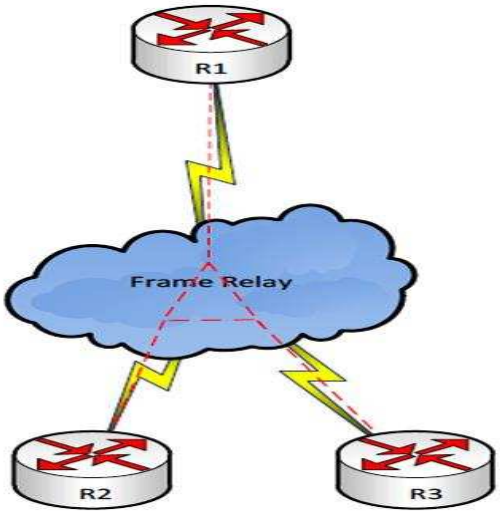
در این توپولوژی، یک روتر می‌تواند از طریق پورت‌های Sub interface خود به روترهای دیگر متصل شود، مانند شکل زیر:



شکل ۹-۲ : توپولوژی Hub and Spoke

۹.۳.۲ توپولوژی FullMesh

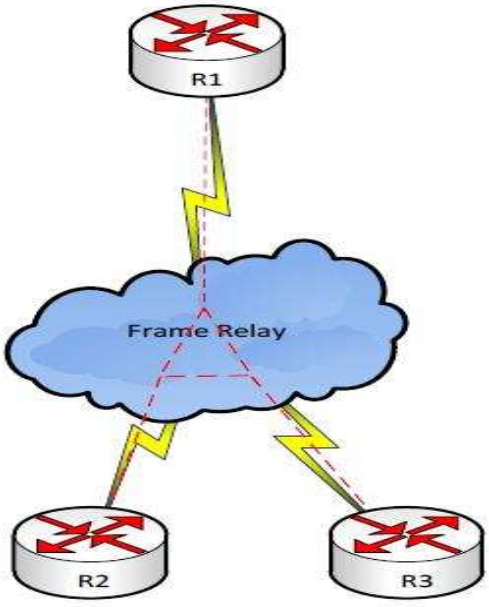
در این توپولوژی هر روتر دارای یک ارتباط با روترهای دیگر دارد. یا دارای یک مدار مجازی VC با روترهای دیگر می‌باشد.



شکل ۹-۳ : توپولوژی FullMesh

۹.۳.۳ توپولوژی Mesh Partial

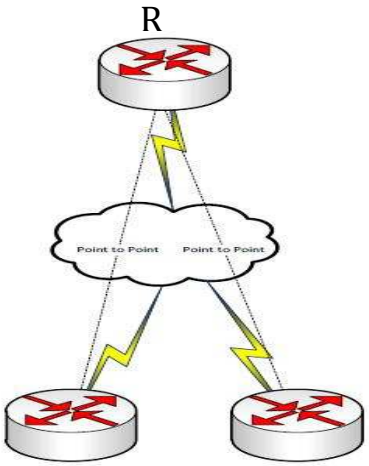
در این توپولوژی یک روتر به تمام روترهای دیگر در شبکه Frame Relay متصل است.



شکل ۹-۴: توپولوژی Mesh partial

ساختن انترفیس مجازی یا Sub Interface به دو صورت انجام می‌گیرد:

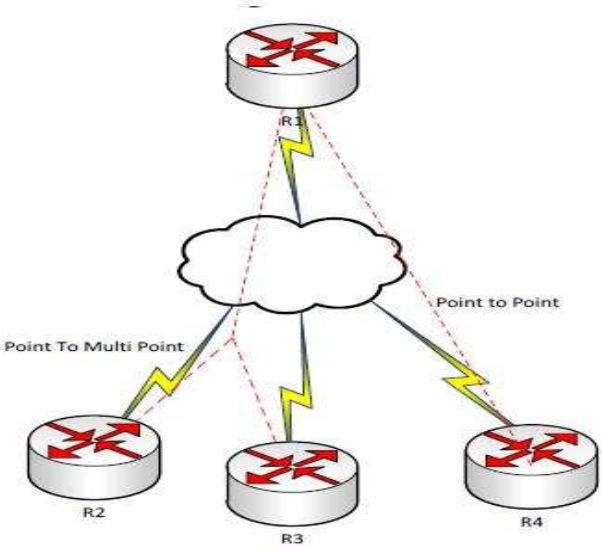
- Point to Point
- Point to Multi Point



شکل ۹-۵: انترفیس مجازی Point to Point

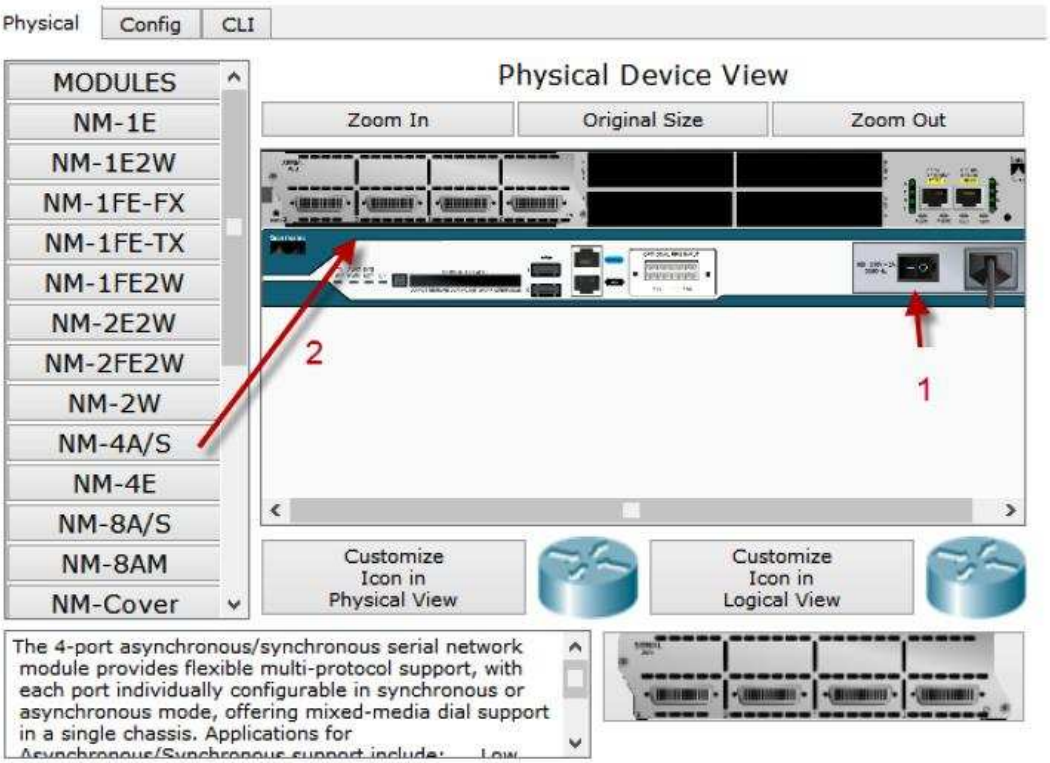
در مود Point To Point، یک روتر با روتر دیگر به‌صورت مستقیم در ارتباط است. هر روتر با روتر مقابل خود در یک رنج یا Subnet قرار دارند.

در مود Point To Multipoint، یک روتر می‌تواند با چند روتر دیگر در یک رنج قرار دا شته با شد و باهم در ارتباط باشـند. در شـکل زیر R۱ با روترهای ۲ و ۳ در یک رنج قرار دارند و به‌صـورت Point To Multipoint در ارتباط هستند و روتر ۱ با روتر ۴ به‌صورت point to point می‌باشند.



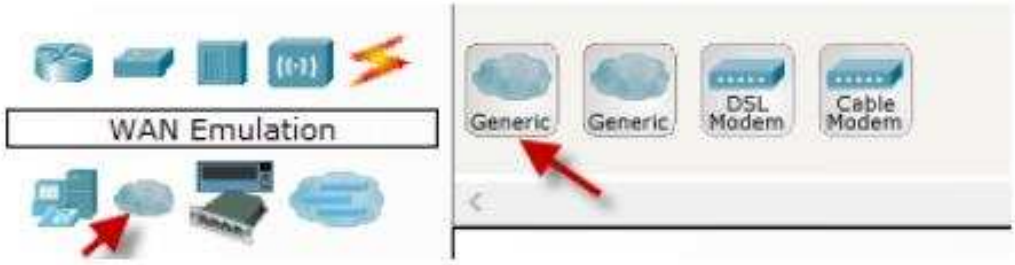
شکل ۹-۶: انترفیس مجازی Point to Multi-Point

در این مثال می‌خواهیم کار با Frame Relay را به‌صورت عملی بررسی کنیم. برنامهٔ Packet Tracer را باز می‌کنیم و سه روتر ۲۸۱۱ به لست اضافه نموده و به هر کدام از آن‌ها یک ماژول سریال اضافه می‌کنیم، به‌صورت زیر:

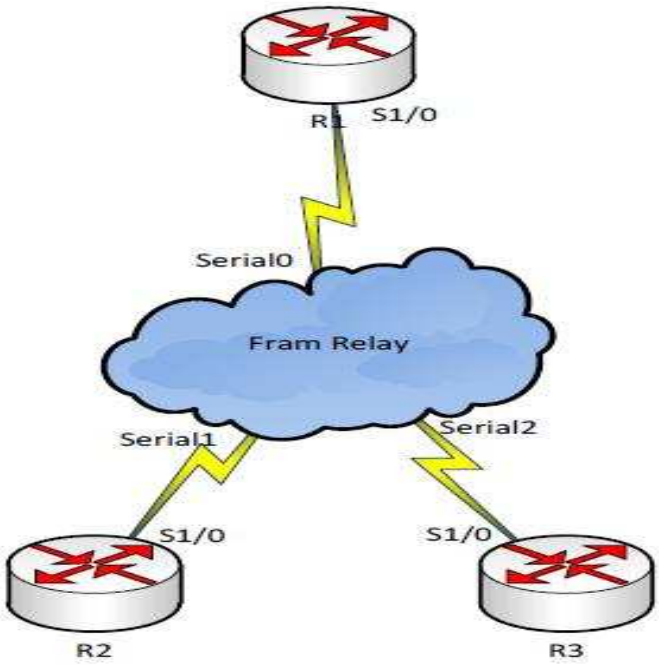


شکل ۹-۷: برنامه packet tracer

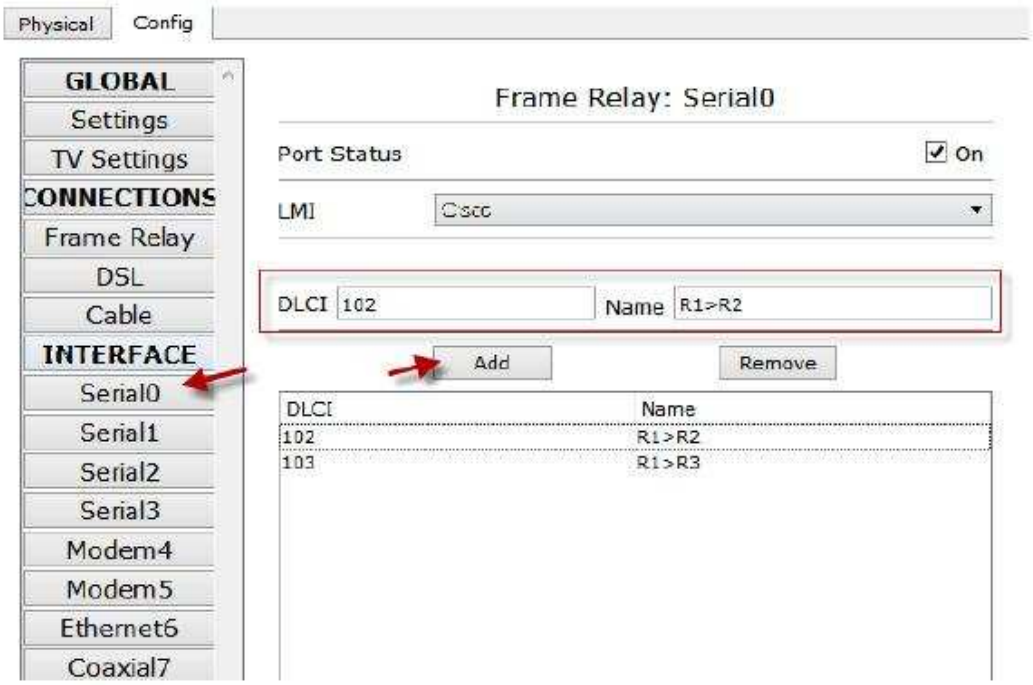
مانند شکل، بر روی روتر کلیک و در تب Physical اول روتر را طبق شمارهٔ یک خاموش می‌کنیم و بعد از لست سمت چپ ماژول -A/S۴NM را می‌کشیم و در جای مشخص‌شده در شمارهٔ ۲ قرار می‌دهیم و بعد، روتر را روشن می‌کنیم. در باقی روترها هم این کار را انجام می‌دهیم، بعد باید سویچ Frame Relay را به لست اضافه کنیم، برای این کار، طبق شکل زیر بر روی Wan Emulation کلیک و گزینهٔ Generic را به صفحه اضافه می‌کنیم:



مانند شکل زیر آن‌ها را از طریق کیبل سریال به هم متصل کنید:



بعد از این کار داخل Generic می‌شویم و بر روی پورت‌های سریال که در شکل به روترها متصل کردیم، کلیک می‌کنیم:

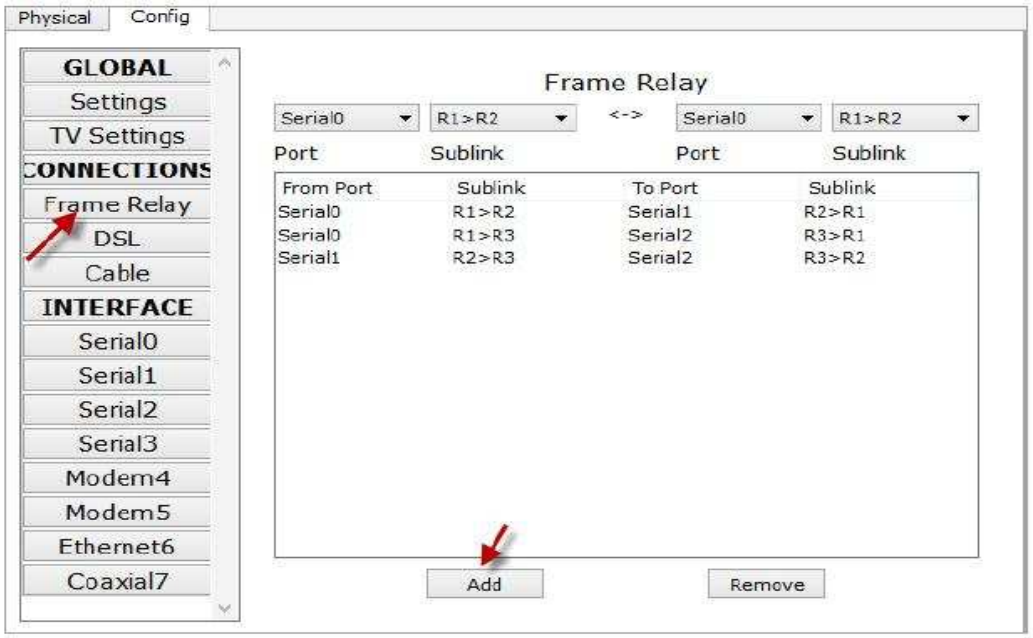


مانند شکل بالا روی سریال شمارهٔ صفر کلیک کردیم، اگر در شکل توجه کنیم، سریال صفر به روتر R۱ متصل است و باید DLCI یا مدار منطقی بین روترها را ایجاد کنیم. در DLCI شمارهٔ ۱۰۲ را داخل

می‌کنیم که عدد ارتباطی بین روتر ۱ و ۲ است و در قسمت Name می‌توانیم مشخص کنیم. این عدد ارتباط بین کدام روتر است؛ مثلاً: R۱>R۲ برای روترهای R۱ و R۳ هم DlCI را مشخص می‌کنیم، می‌نویسیم ۱۰۳ که عددی بین روتر ۱ و ۳ است. در شمارهٔ سریال ۱ که به روتر ۲ متصل است، اعداد زیر را وارد می‌کنیم:

در پورت سریال شمارهٔ ۲ اطلاعات زیر را وارد می‌کنیم:

بعد از این، کار بر روی قسمت Frame Relay کلیک می‌کنیم و عملیات زیر را انجام می‌دهیم:



مانند شکل، بر روی Frame Relay کلیک می‌کنیم، شما باید ارتباط بین روترها را مشخص کنید؛ مثلاً: کیبل سریال صفر با نام R۱ >R۲ به کیبل سریال ۱ با نام R۱ R۲ < متصل می‌شود، در کل مانند شکل عمل کنید.

بعد از آماده‌شدن کار باید Frame Relay را روی روترها فعال کنیم. روش‌های متفاوتی برای این کار وجود دارد. که باهم این روش‌ها را بررسی می‌کنیم. روش اول به‌صورت اتوماتیک انجام می‌گیرد و با فعال‌کردن

Frame Relay به‌صورت خودکار، روترهای مجاور شناسایی می‌شوند. وارد روتر R۱ شوید و دستورات زیر را وارد کنید:

```
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip add 1.1.123.1 255.255.255.0
```

در دستورات بالا وارد انترفیس سریال ۱/۰ شدیم و encapsulation frame-relay این دستور را فعال کردیم و بعد از آن IP Address مربوط به این انترفیس را وارد کردیم.

وارد روتر R۲ شوید و دستورات زیر را وارد کنید:

```
R2(config)#int s1/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#ip add 1.1.123.2 255.255.255.0
```

وارد روتر R۳ شوید و دستورات زیر را وارد کنید:

```
R3(config)#int s1/0
R3(config-if)#encapsulation frame-relay
R3(config-if)#ip add 1.1.123.3 255.255.255.0
```

بعد از این کار و با فعال‌کردن Frame Relay به‌صورت خودکار توسط روشی به نام invers ARP، باقی روترهای متصل به این Frame Relay را شناسایی می‌کند و برای مشاهدهٔ جدول FR از دستور زیر استفاده کنید:

```
R1#show frame-relay map
Serial1/0 (up): ip 1.1.123.2 dlci 102, dynamic, broadcast, CISCO, status defined, active
Serial1/0 (up): ip 1.1.123.3 dlci 103, dynamic, broadcast, CISCO, status defined, active
```

همان‌طور که مشاهده می‌کنید با دستور Show frame-relay map، لست روترهای متصل از طریق FR به ما نمایش داده شد، اگر به پایان هر دستور نگاه کنید، گزینهٔ Active را مشاهده می‌کنید که نشان‌دهندهٔ فعال‌بودن خط است و می‌توانید به Ip addressهای مورد نظر Ping کنید. در غیر این صورت اگر گزینهٔ دیگری باشد، یعنی ارتباط با روتر دیگر برقرار نشده است.

نکته: همان‌طور که گفتیم، روش Invers ARP هر ۶۰ ثانیه یک‌بار بین روتر و سویچ FR فعال می‌شود تا فعال‌بودن خط و شمارهٔ DLCI را چک کند و همین امر باعث ایجاد ترافیک بیهوده در آن می‌شود، برای حل این مشکل باید از Static Frame Relay استفاده و Invers ARP را خاموش کنید، به‌صورت زیر:

۹.۴ فعال‌کردن Static Frame Relay

نکته: نرم افزار Packet Tracer این روش را پشتیبانی نمی‌کند، اما این روش را با هم بررسی می‌کنیم که روی بقیه نرم‌افزارها مانند GNS که در آن بحث خواهد صورت گرفت، اجرا می‌شوند: وارد روتر R۱ شوید و دستورات زیر را وارد کنید:

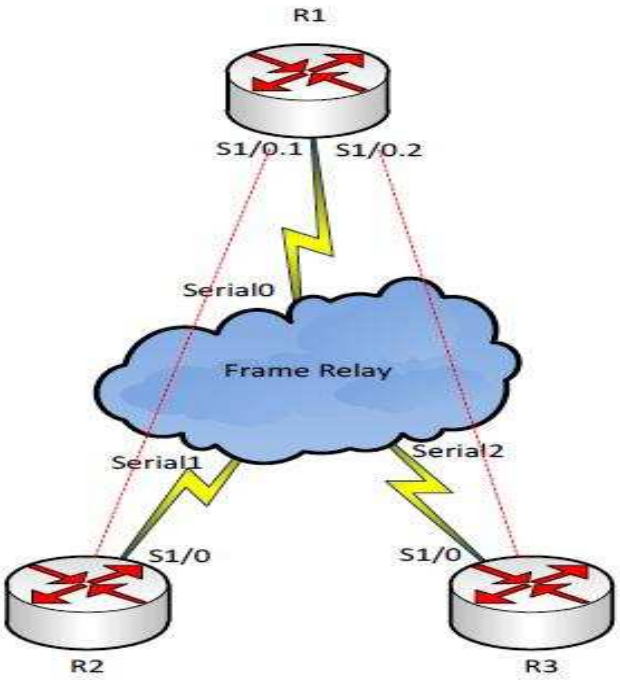
```
R1(config)#int s1/0
R1(config-if)#Encapsulation Frame-relay
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#frame-relay map ip 1.1.123.2 102 broadcast
R1(config-if)#frame-relay map ip 1.1.123.3 103 broadcast
```

به دستورات بالا توجه کنید، وارد انترفیس سریال ۱/۰ شدیم و Frame Relay را فعال کردیم و بعد از آن با دستور no frame-relay inverse-arp این روش را غیر فعال کردیم که به‌صورت خودکار عمل نکند در ادامه با دستور frame-relay map ip ۱.۱.۱۲۳.۲ ۱۰۲ broadcast یکی، IP Address های روترهای دیگر را Map می‌کنیم شمارهٔ ۱۰۲ هم به‌عنوان DLCI مربوط به روتر ۲ است و در آخر باید از عبارت"broadcast " استفاده کنیم، به‌خاطر این‌که به‌صورت پیش‌فرض split-horizon که در بحث‌های قبلی روی آن کار کردیم از به‌روز Update کردن Routing جلوگیری می‌کند) به این صورت که از طریق انترفیسی که آن Route را دریافت کرده، دوباره به همان انترفیس برنمی‌گرداند (برای مثال، اگر روتر R۱ یک آپدیت به سمت R۲ می‌فرستد R۲ نمی‌تواند یک به‌روز Update به R۱ ارسال کند، به خاطر این‌که هر دوی آن‌ها از طریق یک انترفیس آپدیت‌ها را ارسال و دریافت می‌کنند. با استفاده از عبارت "broadcast" ما به R۲ می‌گوییم که یک کاپی از هر broadcast یا multicast را که از طریق انترفیس خودت دریافت می‌کنی، به مدار مجازی (virtual circuit) که با مقدار DLCI اختصاص داده شده، در دستور "frame-relay map" ارسال کن. در واقع یک پکت کاپی‌شده به‌صورت unicast نه broadcast ارسال می‌شود که بعضی اوقات نیز با نام "pseudo-broadcast" نیز شناخته می‌شود. برای روتر بعدی هم می‌نویسیم frame-relay map ip ۱.۱.۱۲۳.۳ ۱۰۳ broadcast و در باقی روترها هم همین کار را انجام می‌دهیم و به این صورت، روترها به‌صورت دستی همدیگر را شناسایی می‌کنند.

۹.۵ Hub and Spoke

این روش به این صورت است که یک روتر به‌عنوان روتر اصلی انتخاب می‌شود و باقی روترها فقط به این روتر متصل می‌شوند و از طریق این روتر به متباقی روترها دسترسی پیدا می‌کنند. موضوعی که در این روش به چشم می‌خورد Sub Interface است که برای هر یک از روترها به‌صورت Point To Point یا Point To Multi Point تعریف می‌شود.

به شکل زیر توجه کنید:



شکل ۹-۸: راه اندازی توپولوژی hub and spoke

در این شکل روتر R۱ از دو Sub interface برای ارتباط با روترهای R۲ و R۳ استفاده می‌کند که روش تنظیم‌کردن آن به‌صورت زیر است:

وارد روتر R۱ شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.1 point-to-point
Router(config-subif)#frame-relay interface-dlci 102
Router(config-subif)#ip add 255.255.255.0 1.1.123.1
```

اول وارد انترفیس S۱/۰ می‌شویم و Frame Relay را فعال می‌کنیم و بعد از آن با دستور Exit خارج شده و با دستور int s۱/۰.۱point-to-point وارد انترفیس مجازی می‌شویم. point-to-point نشان‌دهندهٔ ارتباط مستقیم با روتر روبه‌رو است. یعنی این‌که دو روتر در یک Subnet کار می‌کنند. بعد از واردشدن باید ip address را وارد کنیم که به‌صورت ip add ۱.۱.۱۲۳.۱ ۲۵۵.۲۵۵.۲۵۵.۰ وارد می‌کنیم.

همان‌طورکه مشاهده کردید، این ارتباط با روتر R۲ بوده و برای R۳ هم به‌صورت زیر عمل می‌کنیم:

```
Router(config)#int s1/0.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 103
Router(config-subif)#ip add 1.1.124.1 255.255.255.0
```

بعد از واردکردن دستورات در روتر R۱ باید در روترهای دیگر هم دستورات را وارد کنیم:

وارد روتر R۲ شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
 Router(config-if)#exit
Router(config)#int s1/0.1 point-to-point
Router(config-subif)#frame-relay interface-dlci 201
Router(config-subif)#ip add 1.1.123.2 255.255.255.0
Router(config-subif)#int s1/0 Router(config-if)#no shut
```

وارد interface S1/0 شدیم و بعد از آن Frame Relay را با دستور encapsulation Frame Relay فعال کردیم بعد با دستور Exit از انترفیس اصلی خارج شده و با دستور point-to-point int s1/0.1 وارد انترفیس مجازی int s1/0.1 شدیم و همین انترفیس را در روتر 1 ایجاد کردیم. بعد از آن از دستور frame- Relay interface-dlci 201 استفاده می‌کنیم که ارتباط با روتر R1 از طریق DLCI 201 برقرار شود و بعد از آن از دستور ip add 1.1.123.2 255.255.255.0 استفاده می‌کنیم که ip address است که در رنج روتر R1 قرار دارد، توجه داشته باشید بعد از واردکردن دستورات، حتماً وارد پورت شوید و آن را فعال کنید؛ به هیچ وجه در پورت مجازی این کار را انجام ندهید.

وارد روتر R۳ شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int s1/0.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 301
Router(config-subif)#ip add 1.1.124.2 255.255.255.0
```

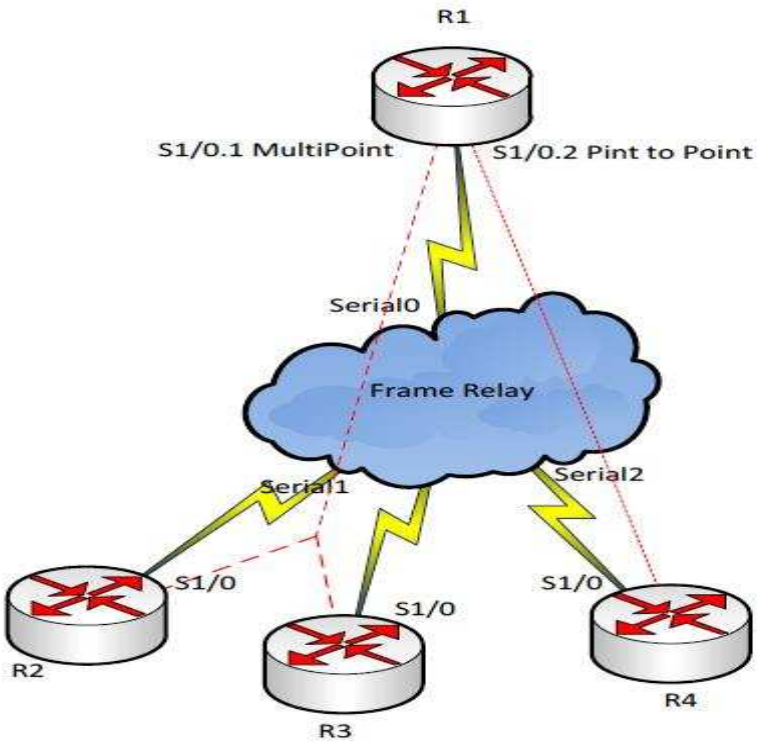
بعد از پایان کار، وارد روتر یک شوید و دستور زیر را داخل کنید:

```
Router#show frame-relay map
Serial1/0.1 (up): point-to-point dlci, dlci 102, broadcast, status defined, active
Serial1/0.2 (up): point-to-point dlci, dlci 103, broadcast, status defined, active
```

همان‌طور که مشاهده می‌کنید دو مسیر به لست اضافه شده است. از روتر R۱ می‌توانید به روترهای R۲ و R۳ ارتباط داشته باشید، اما روتر R۲ نمی‌تواند به روتر R۳ ارتباط داشته باشد! این موضوع به خاطر این است که هیچ روتینگ پروتوکولی بین آن‌ها اجرا نشده است، برای این کار روی هر روتر، پروتوکول EIGRP اجرا و Network ها را به این پروتوکول معرفی می‌کنیم.

۹.۶ ایجاد Hybrid Topology

به شکل زیر توجه کنید:



شکل ۹-۹ : راه اندازی hybrid topology

در شکل قبلی، روترهای R۱ و R۲ و R۳ به‌صورت MultiPoint به هم متصل هستند و در یک شبکه قرار دارند و روترهای R۱ و R۴ هم به‌صورت Point To Point به هم متصل هستند و در یک شبکه قرار دارند.

```
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
R1(config)#int s1/0.123 multipoint
R1(config-subif)#frame-relay interface-dlci 102
R1(config-subif)#frame-relay interface-dlci 103
R1(config-subif)#ip add 1.1.123.1 255.255.255.0
```

وارد روتر R۱ شوید و دستورات زیر را وارد کنید:

در مرحلهٔ اول، وارد انترفیس فزیکی می‌شویم و Frame Relay را اجرا و پورت را روشن می‌کنیم، بعد از آن از پورت خارج می‌شویم و با دستور int s1/0.123 multipoint وارد انترفیس مجازی با عملکرد MultiPoint می‌شویم و DLCIهای مربوط به روترهای دیگر را که در این شبکه می‌خواهند قرار بگیرند، وارد می‌کنیم. بعد IP Address را برای این پورت مجازی وارد می‌کنیم.

برای پورت مجازی دیگر که به روتر R۴ متصل و اتصال آن به‌صورت Point To Point است، دستورات زیر را وارد می‌کنیم:

```
R1(config)#int s1/0.124 point-to-point
R1(config-subif)#frame-relay interface-dlci 104
R1(config-subif)#ip add 1.1.124.1 255.255.255.0
```

وارد روتر R۲ شوید و دستور زیر را وارد کنید:

```
R2(config-if)# encapsulation frame-relay
R2(config-if)#no sh
R2(config)#int s1/0.123 multipoint
R2(config-subif)#frame-relay interface-dlci 201
R2(config-subif)#frame-relay interface-dlci 203
R2(config-subif)#ip add 1.1.123.2 255.255.255.0
```

در این روتر همان‌طور که مشاهده می‌کنید،DLCIهای مربوط به روترهای R۱ و R۳ را وارد کردیم و IP Address را وارد کردیم که دو روتر دیگر هم در این رنج قرار دارند.

یک نکتهٔ بسیار مهم این است که حتماً از Multipoint استفاده کنید تا ارتباط بین روترها باهم برقرار شود.

وارد روتر R۳ شوید و دستورات زیر را وارد کنید:

```
R2(config-if)# encapsulation frame-relay
R2(config-if)#no sh
R2(config)#int s1/0.123 multipoint
R2(config-subif)#frame-relay interface-dlci 301
R2(config-subif)#frame-relay interface-dlci 302
R2(config-subif)#ip add 1.1.123.3 255.255.255.0
```

در این روتر، DLCI مربوط به روترهای R۱ و R۲ را وارد کردیم و یک IP address در رنج روترهای دیگر وارد کردیم.

وارد روتر R۴ شوید و دستورات زیر را وارد کنید:

```
Router> Router>en
Router#conf t
Router(config)#int s0/1
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.124 point-to-point
Router(config-subif)#frame-relay interface-dlci 401
Router(config-subif)#ip address 255.255.255.0 1.1.124.2
Router(config-subif)#int s1/0
Router(config-if)#no sh
```

تا اینجا تنظیمات روی تمام روترها انجام شده است. برای مشاهدهٔ جدول Frame Relay از دستور زیر استفاده کنید:

```
R1(config-if)#do sh fram map
Serial1/0.123 (up): ip 1.1.123.2 dlci 102, dynamic, broadcast, CISCO, status defined, active
Serial1/0.123 (up): ip 1.1.123.3 dlci 103, dynamic, broadcast, CISCO, status defined, active
Serial1/0.124 (up): point-to-point dlci, dlci 104, broadcast, status defined, active
```

همان‌طور که مشاهده می‌کنید، خط‌های دوم و سوم مربوط به روترهای R۲ و R۳ است و خط چهارم مربوط به روتر R۴ است که به‌صورت point-to-point به آن متصل شدیم.

خلاصه‌ی فصل نهم

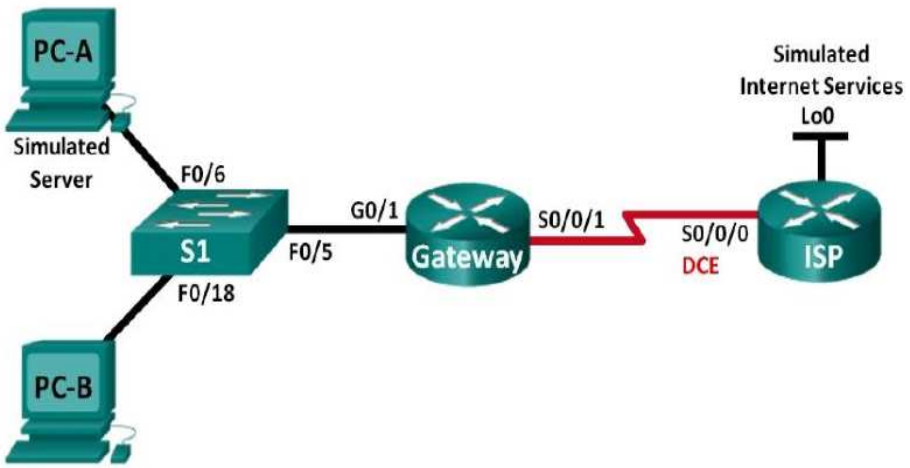
Frame Realy پروتوکول لایهٔ دو می‌باشد که دارای میکانیزم Packet Switching است. این پروتوکول به کمک تعریف یک مدار مجازی (Virtual Circuit) و با استفاده مشخصه‌یی به نام DLCI اطلاعات لایهٔ شبکه را دریافت نموده و آن‌ها را در بسته‌های Frame Realy جابه‌جا کرده و به لایهٔ فزیکی (Physical Layer) می‌دهد.

DLCI (High-Level Data Link Control) مشخصهٔ محلی می‌باشد که مشخص می‌کند بالای دیگر مدارهای مجازی کدام روتر قرار دارد، که تا بتواند Frame Realy تصمیم ارسال بسته‌ها را به لایهٔ بعدی بگیرد.

سوالات فصل نهم

۱. Frame Relay به‌خاطر کدام هدف در شبکه‌های کمپیوتری استفاده می‌شود؟
۲. ساختن انترفیس مجازی به چند طریق امکان‌پذیر است؟ هر کدام آن را تشریح نمایید.
۳. چطور می‌توانیم Static Frame Relay را فعال نماییم؟
۴. مراحل ایجاد Hybrid Topology در یک مثال واضح سازید.
۵. کمنت show frame-relay map به خاطر کدام هدف استفاده می‌شود؟

- شبکه‌یی را بسازید. نظر به شکل ذیل Frame Relay بالای روتر فعال کنید.
- Subinterface frame relay را در روترها ایجاد کنید.
- Dns-lookup را غیر فعال کنید.
- Line console را پس‌ورد بدهید و آن را encrypt کنید.
- Syncronastion را line console ایجاد کنید.



Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (Simulated Server)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

(References) منابع

1. Todd Lammle, S. O., &kevin, W. (2015). CCNA Routing and Switching.
2. (http//cisco.com)
3. Wendel, O. & Scott, H. (2016). CCNA Routing and Switching ICND2 200-105 Official Cert Guide.
4. Empson, P.G., Hans, R. (2015).CCNP Routing and Switching Portable Command Guide Scott/ Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.
5. Todd Lammle. (2017). CCNA Cisco CertifiedNetwork Associate Study Guide/ISBN: 0-7821-2647-2 Manufactured in the United States of America.