



دولت جمهوری اسلامی افغانستان
اداره تعلیمات تخنیکي و مسلکي
معاونیت امور اکادمیک
ریاست نصاب و تربیه معلم



پروژه انکشاف
مهارت‌های افغانستان



اداره تعلیمات
تخنیکي و مسلکي

روتینگ سویچینگ ۱ (Routing & Switching)

رشته: کمپیوتر ساینس - دیپارتمنت: شبکه

صنف ۱۴ - سمستر اول

سال: ۱۳۹۹ هجری شمسی



شناسنامه کتاب

نام کتاب: روتینگ سوئیچینگ ۱ (Routing & Switching)

رشته: کمپیوتر ساینس

تدوین کننده: روح الله ساحل

همکار تدوین کننده: سمیه عثمان

- کمیته نظارت: ندیمه سحر رئیس اداره تعلیمات تخنیکي و مسلکی
- عبدالحمید اکبر معاون امور اکادمیک اداره تعلیمات تخنیکي و مسلکی
- حبیب الله فلاح رئیس نصاب و تربیه معلم
- عبدالمتین شریفی آمر نصاب تعلیمی ریاست نصاب و تربیه معلم
- روح الله هوتک آمر طبع و نشر کتب درسی، ریاست نصاب و تربیه معلم
- احمد بشیر هیله من مسؤل انکشاف نصاب، پروژه انکشاف مهارت های افغانستان
- محمد زمان پویا، کارشناس انکشاف نصاب، پروژه انکشاف مهارت های 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 مدیر عمومی بورد تصحیح کتب درسی و آثار علمی

دیزاین: صمد صبا و سید کاظم کاظمی

چاپ کال: ۱۳۹۹ هجری شمسی

تیراژ: ۱۰۰۰

چاپ: اول

وبسایت: www.dmtvet.gov.af

ایمیل: info@dmvtvet.gov.af

حق چاپ برای اداره تعلیمات تخنیکي و مسلکی محفوظ است.



سرود ملی

| | |
|-----------------------|-------------------------------|
| دا وطن افغانستان دی | دا عزت د هر افغان دی |
| کور د سولې کور د تورې | هر بچی یې قهرمان دی |
| دا وطن د ټولو کور دی | د بلوڅو، د ازبکو |
| د پښتون او هزاره وو | د ترکمنو، د تاجکو |
| ورسره عرب، گوجر دي | پامیریان، نورستانیان |
| براهوي دي، قزلباش دي | هم ایماق، هم پشه یان |
| دا هیواد به تل ځلېږي | لکه لمر پر شنه آسمان |
| په سینه کې د آسیا به | لکه زړه وی جاویدان |
| نوم د حق مو دی رهبر | وایو الله اکبر وایو الله اکبر |



پیام اداره تعلیمات تکنیکی و مسلکی

استادان کرام و شاگردان نهایت ارجمند!

تربیت نیروی بشری ماهر، متخصص و کارآمد از عوامل کلیدی و انکار ناپذیر در توسعه اقتصادی و اجتماعی هر کشور محسوب می‌گردد و هر نوع سرمایه گذاری بزرگ در بخش‌های مختلف اقتصادی نیازمند به پلان گذاری و سرمایه گذاری در بخش نیروی بشری و توسعه 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 اداره تعلیمات تکنیکی و مسلکی از بدنه وزارت معارف جدا گردیده و به یک اداره مستقل ارتقا کرد. این اداره به عنوان متولی و مجری آموزش‌های تکنیکی و مسلکی در بخش‌های زراعت، صنعت، هنر و خدمات می‌باشد. این اداره که فراگیرترین نظام تعلیمی کشور در زمینه‌های متذکره محسوب می‌شود، تلاش می‌کند تا در حیطه وظایف و صلاحیت خود زمینه دستیابی به هدف‌های تعیین شده در قانون اساسی کشور را ممکن سازد و جهت رفع نیاز بازار کار، فعالیت‌های خویش را توسعه دهد در عین حال با توجه به ارتقای کیفیت این اداره به جنبه‌های کیفی فعالیت‌های خویش تأکید داشته، سعی می‌نماید مهارت فارغان لیسه‌ها و انستیتوت‌های مسلکی را با تکنالوژی معاصر همگام سازد.

نظام اجتماعی و طرز زندگی در افغانستان مطابق به احکام دین مقدس اسلام و رعایت تمامی قوانین مشروع و معقول انسانی عیار است؛ اداره تعلیمات تکنیکی و مسلکی جمهوری اسلامی افغانستان نیز با ایجاد زمینه‌های لازم برای تعلیم و تربیت جوانان و نوجوانان مستعد و علاقمند به حرفه آموزی، ارتقای مهارت‌های شغلی در سطوح مختلف مهارتی، تربیت کادرهای مسلکی و حرفوی و ظرفیت سازی تخصصی از طریق انکشاف و ایجاد مکاتب و انستیتوت‌های تکنیکی و مسلکی در سطح کشور با رویکرد ارزش‌های اسلامی و اخلاقی فعالیت می‌نماید؛ فلذا جهت نیل به اهداف عالی این اداره که همانا تربیه افراد ماهر و توسعه 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 تکنیکی و مسلکی محسوب می‌شود، پس باید همگام با تحولات و پیشرفت‌های علمی نوین و مطابق نیازمندی‌های جامعه و بازار کار تألیف گردد و دارای چنان ظرفیتی باشد که بتواند آموزه‌های دینی و اخلاقی را توأم با فراورده‌های علوم جدید با روش‌های نوین به شاگردان و محصلان انتقال دهد. کتابی را که اکنون در اختیار دارید، بر اساس همین ویژه‌گی‌ها تهیه و تألیف گردیده است. به این وسیله، صمیمانه آرزو مندیم که آموزگاران خوب، متعهد و دلسوز کشور با خلوص نیت، رسالت اسلامی و ملی خویش را ادا نموده و نوجوانان و جوانان کشور را به سوی قله‌های رفیع دانش و مهارت‌های مسلکی رهنمایی نمایند و از شاگردان و محصلان گرامی نیز می‌خواهیم که از این کتاب به درستی استفاده نموده، در حفظ و نگهداشت آن سعی بلیغ به خرج دهند. همچنان از مؤلفان، استادان، شاگردان و اولیای محترم شاگردان تقاضا می‌شود نظریات و پیشنهادات خود را در مورد این کتاب از نظر محتوا، ویرایش، چاپ، اشتباهات املایی، انشایی و تایپی عنوانی اداره تعلیمات تکنیکی و مسلکی کتباً ارسال نموده، امتنان بخشند. در پایان لازم می‌دانم در جنب امتنان از مؤلفان، مترجمان، مصححان و تدقیق کننده‌گان نصاب تعلیمات تکنیکی و مسلکی از تمامی نهادهای ملی و بین المللی که در تهیه، تألیف، طبع و توزیع کتب درسی زحمت کشیده و همکاری نموده‌اند، قدردانی و تشکر نمایم.

ندیمه سحر

رئیس اداره تعلیمات تکنیکی و مسلکی جمهوری اسلامی افغانستان

مقدمه ی

فصل اول: زیر شبکه (Subnetting) ۱

| | |
|-------|--|
| ۱.۱ | نسخه چهارم آی پی (IPv4) ۲ |
| ۱.۱.۱ | آدرسهای کلاس A ۳ |
| ۱.۱.۲ | آدرسهای کلاس B ۳ |
| ۱.۱.۳ | آدرسهای کلاس C ۴ |
| ۱.۱.۴ | Subnet Mask ۴ |
| ۱.۱.۵ | تبدیل اعداد از دیسیمال به باینری ۵ |
| ۱.۲ | زیر شبکه (Subnetting) ۸ |
| ۱.۲.۱ | فواید Subnetting ۹ |
| ۱.۳ | Subnet کردن آی پی آدرس کلاس A ۱۲ |
| ۱.۴ | Subnet کردن آی پی آدرس کلاس B ۱۴ |
| ۱.۵ | Subnet کردن آی پی آدرس کلاس C ۱۶ |
| ۱.۶ | Variable Length Subnetmask (VLSM) ۱۸ |

فصل دوم: سیستم عامل سیسکو (IOS (Internetwork Operating System) ۲۵

| | |
|-------|--|
| ۲.۱ | Internetwork Operating System (IOS) ۲۶ |
| ۲.۱.۱ | Set up mode ۲۶ |
| ۲.۱.۲ | CLI (Command Line Interface) محیط خط فرمان ۲۷ |
| ۲.۲ | مشخص کننده توانمندی ها و قابلیت های سیستم عامل روتر ۲۸ |
| ۲.۳ | مشخصه نحوه اجرا و مکان اجرای سیستم عامل ۳۰ |
| ۲.۴ | مشخصه نسخه و بروز رسانی Update سیستم عامل سیسکو (IOS) ۳۰ |
| ۲.۵ | ویژگی های سیستم عامل سیسکو (IOS) ۳۱ |
| ۲.۶ | IOS و ضرورت استفاده از آن ۳۱ |
| ۲.۷ | ماهیت اینترفیس IOS ۳۱ |
| ۲.۸ | ارتقای سیستم عامل دستگاه سیسکو ۳۲ |
| ۲.۹ | نسخه های IOS ۳۳ |
| ۲.۱۰ | مودهای عبار سازی خط فرمان CLI ۳۳ |

فصل سوم: روترهای سیسکو Cisco Routers ۳۸

| | |
|-------|--|
| ۳.۱ | سخت افزار روترهای سیسکو ۳۹ |
| ۳.۱.۱ | عناصر داخلی روتر (Router Internal elements) ۳۹ |
| ۳.۱.۲ | واحد پردازش مرکزی (CPU) ۴۰ |

| | | |
|----|--|-------|
| ۴۰ | حافظه اصلی (RAM) | ۳.۱.۳ |
| ۴۰ | حافظه پایداری (Non – Volatile RAM(NVRAM) | ۳.۱.۴ |
| ۴۱ | حافظه فلش (Flash memory) | ۳.۱.۵ |
| ۴۱ | گذرگاه (Buses) | ۳.۱.۶ |
| ۴۱ | حافظه ROM | ۳.۱.۷ |
| ۴۲ | سخت افزار خارجی روتر | ۳.۲ |
| ۴۲ | پوش (جعبه) Case | ۳.۲.۱ |
| ۴۳ | پورت های کنسول Console و AUX | ۳.۲.۲ |
| ۴۴ | خط اتصال (LAN Interface) | ۳.۲.۳ |
| ۴۵ | خط اتصال (WAN Interface) | ۳.۲.۴ |
| ۴۵ | بوت (Boot) شدن IOS روتر سیسکو | ۳.۳ |
| ۴۶ | مراحل بوت (Boot) شدن روتر سیسکو | ۳.۴ |
| ۴۸ | تنظیمات پیش فرض بالا آمدن یک Router default load | ۳.۵ |
| ۵۳ | تنظیمات ابتدایی روترهای سیسکو (Cisco Router Basic Configuration) | ۳.۶ |
| ۵۳ | راه های دسترسی به تجهیزات سیسکو | ۳.۶.۱ |
| ۵۶ | Telnet | ۳.۶.۲ |
| ۵۷ | Auxiliary Port | ۳.۶.۳ |
| ۵۷ | انواع Mode ها در CLI | ۳.۷ |
| ۶۰ | پیغام های خطا و معنای آن ها | ۳.۸ |
| ۶۱ | تغییر Hostname در روتر و سوئیچ | ۳.۹ |
| ۶۲ | پسورد گذاشتن روی Console یا User Mode | ۳.۱۰ |
| ۶۳ | Line VTY | ۳.۱۱ |
| ۶۳ | روش پسورد گذاشتن برای Enable Mode | ۳.۱۲ |
| ۶۳ | امن کردن پسورد Enable Mode | ۳.۱۳ |
| ۶۳ | روش پنهان کردن حروف پسورد | ۳.۱۴ |
| ۶۴ | تنظیم Interface های مسیریاب | ۳.۱۵ |
| ۶۶ | نمایش وضعیت خلاصه Port ها و Interface ها | ۳.۱۶ |
| ۶۶ | نوشتن توضیحات برای Port ها | ۳.۱۷ |
| ۶۶ | انتخاب چندین Interface هم زمان | ۳.۱۸ |
| ۶۷ | طریقه دادن IP به Interface های Router | ۳.۱۹ |
| ۶۷ | معرفی Shortcut های مهم در روتر (Router) | ۳.۲۰ |
| ۶۷ | ذخیره کردن تنظیمات در روتر | ۳.۲۱ |
| ۶۸ | طریقه Telnet نمودن به یک Router سیسکو | ۳.۲۲ |
| ۶۹ | Telnet از طریق Putty | ۳.۲۳ |
| ۷۴ | فصل چهارم: مسیریابی (Routing) | |
| ۷۵ | همگرایی (Convergence – Routing Update) | ۴.۱ |
| ۷۵ | مسیریابی آی پی (IP Routing) | ۴.۲ |

| | | |
|-----|---|--------|
| ۷۶ | تحويل مستقيم و غيرمستقيم | ۴.۳ |
| ۷۷ | جدول مسيريابی IP | ۴.۴ |
| ۷۷ | Interior Gateway Protocols پروتوكول های داخلی | ۴.۵ |
| ۷۸ | Exterior Gateway Protocol پروتوكول های بیرونی | ۴.۶ |
| ۷۸ | فاصله اداری (Administrative Distance) | ۴.۷ |
| ۷۹ | Metric متریک | ۴.۸ |
| ۸۰ | مسيريابی ثابت (Static Routing) | ۴.۹ |
| ۸۲ | مزایای استفاده از مسيريابی ثابت (Static Routing) | ۴.۹.۱ |
| ۸۲ | معایب استفاده از مسيريابی ثابت (Static routing) | ۴.۹.۲ |
| ۸۳ | Dynamic Routing | ۴.۱۰ |
| ۸۴ | مزایای استفاده از مسيريابی متغیر (Dynamic routing) | ۴.۱۰.۱ |
| ۸۴ | معایب استفاده از مسيريابی متغیر (Dynamic Routing) | ۴.۱۰.۲ |
| ۸۴ | Default Route | ۴.۱۱ |
| ۸۵ | Distance Vectore پروتوكول های | ۴.۱۲ |
| ۸۷ | Link State Routing Protocol های | ۴.۱۳ |
| ۸۹ | Hybrid Routing Protocol های | ۴.۱۴ |
| ۹۳ | فصل پنجم: سوئیچ سیسکو (Cisco Switch) | |
| ۹۴ | سوئیچ (Switch) | ۵.۱ |
| ۹۵ | انواع Switch ها | ۵.۲ |
| ۹۵ | Unmanageable Switches: سوئیچ های غیر قابل کنترل | ۵.۲.۱ |
| ۹۵ | Manageable Switches: سوئیچ های قابل کنترل | ۵.۲.۲ |
| ۹۶ | عناصر داخلی سوئیچ ها | ۵.۳ |
| ۹۶ | پردازنده مرکزی (CPU) | ۵.۳.۱ |
| ۹۶ | RAM | ۵.۳.۲ |
| ۹۶ | NV RAM | ۵.۳.۳ |
| ۹۷ | ROM | ۵.۳.۴ |
| ۹۷ | Flash | ۵.۳.۵ |
| ۹۸ | Cisco Switch Basic Configuration: تنظیمات اولیه سوئیچ های سیسکو | ۵.۴ |
| ۹۹ | Switch Basic Configuration: پیکربندی ابتدایی سوئیچ | ۵.۵ |
| ۱۰۳ | VLAN ۱: تنظیم انترفیس | ۵.۶ |
| ۱۰۵ | عملکرد سوئیچ و اصطلاحات رایج سوئیچینگ | ۵.۷ |
| ۱۰۵ | سوئیچ در لایه دوم (Data Link Layer) مدل OSI | ۵.۸ |
| ۱۰۶ | مهم ترین روش های مسيريابی سوئیچ | ۵.۹ |
| ۱۰۶ | Packet – Switching | ۵.۹.۱ |
| ۱۰۷ | میتودهای انتقال فریم در شبکه | ۵.۱۰ |
| ۱۰۷ | Cut – through | ۵.۱۰.۱ |
| ۱۰۷ | Store – and – Forward | ۵.۱۰.۲ |

| | | |
|--|--|--------|
| ۱۰۷ | Fragment – Free | ۵.۱۰.۳ |
| ۱۰۷ | Switch Configuration | ۵.۱۱ |
| ۱۰۸ | جدول آدرس‌های Mac در سوئیچ | ۵.۱۲ |
| ۱۰۸ | Transparent Bridging | ۵.۱۳ |
| ۱۱۰ | روش‌های انتقال دیتا در شبکه | ۵.۱۴ |
| ۱۱۰ | واژه‌های بسته‌های اطلاعاتی (Packets) | ۵.۱۵ |
| ۱۱۱ | اجزای یک فریم | ۵.۱۶ |
| ۱۱۲ | جریان انتقال اطلاعات (از کامپیوتر مبدأ تا کامپیوتر مقصد) | ۵.۱۷ |
| ۱۱۲ | لایه Application | ۵.۱۷.۱ |
| ۱۱۳ | لایه Transport | ۵.۱۷.۲ |
| ۱۱۳ | لایه اینترنت (Internet) | ۵.۱۷.۳ |
| ۱۱۴ | عملیات در کامپیوتر مقصد | ۵.۱۸ |
| فصل ششم: پروتوکول STP (Spanning Tree Protocol) | | |
| ۱۱۸ | حلقه (Loop) | ۶.۱ |
| ۱۲۰ | Spanning Tree Protocol (STP) | ۶.۲ |
| ۱۲۱ | نیاز به پروتوکول STP | ۶.۲.۱ |
| ۱۲۴ | نحوه کار پروتوکول STP | ۶.۳ |
| ۱۲۵ | پروتوکول STP چگونه کار می‌کند؟ | ۶.۴ |
| ۱۲۶ | Hello BPDUs و Bridge | ۶.۵ |
| ۱۲۷ | انتخاب سوئیچ Root | ۶.۶ |
| ۱۲۹ | انتخاب Root Port برای هر سوئیچ | ۶.۷ |
| ۱۳۲ | انتخاب Designated Port در هر LAN Segment | ۶.۸ |
| ۱۳۳ | تبدیل کردن یک سوئیچ به Root | ۶.۹ |
| ۱۳۳ | غیر فعال کردن STP | ۶.۱۰ |
| فصل هفتم: شبکه محلی مجازی (VLAN) Virtual Local Area Network | | |
| ۱۳۷ | شبکه محلی مجازی (VLAN) | ۷.۱ |
| ۱۳۸ | دلیل استفاده از VLAN | ۷.۲ |
| ۱۴۰ | مزایای VLAN | ۷.۳ |
| ۱۴۱ | انواع VLAN | ۷.۴ |
| ۱۴۱ | عضویت ثابت (Static) | ۷.۴.۱ |
| ۱۴۲ | حالت ارتباط پورت در VLAN | ۷.۵ |
| ۱۴۲ | Access Link | ۷.۵.۱ |
| ۱۴۲ | Trunk Link | ۷.۵.۲ |
| ۱۴۳ | ایجاد VLAN | ۷.۶ |
| ۱۴۴ | پیکربندی VLAN (VLAN Configuration) | ۷.۷ |
| ۱۵۰ | بررسی VLAN ها | ۷.۸ |

| | | |
|-----|--|--------|
| ۱۵۱ | حذف کردن VLAN | ۷.۹ |
| ۱۵۱ | عضویت متغیر (Dynamic) | ۷.۹.۱ |
| ۱۵۲ | Trunk Port | ۷.۱۰ |
| ۱۵۳ | Tag زدن به هر فریم جهت انتقال در Trunk | ۷.۱۰.۱ |
| ۱۵۴ | پروتوکول (ISL) | ۷.۱۰.۲ |
| ۱۵۵ | پروتوکول ۸۰۲.۱ Q | ۷.۱۰.۳ |

فصل هشتم: پروتوکول معلومات مسیریابی RIP (Routing Information Protocol) ۱۵۹

| | | |
|-----|---|--------|
| ۱۶۰ | Routing Information Protocol (RIP) | ۸.۱ |
| ۱۶۰ | اصطلاحات مهم پروتوکول RIP | ۸.۲ |
| ۱۶۱ | ویژگی‌های پروتوکول RIP | ۸.۳ |
| ۱۶۱ | ویژگی‌های Loop Free در پروتکل RIP | ۸.۴ |
| ۱۶۱ | مسمومیت مسیر (Route Poisoning) | ۸.۴.۱ |
| ۱۶۲ | تقسیم افق (Split Horizon) | ۸.۴.۲ |
| ۱۶۲ | Hold Down Timer | ۸.۴.۳ |
| ۱۶۲ | Triggered (Flash) Updates | ۸.۴.۴ |
| ۱۶۲ | کارکرد پروتوکول RIP | ۸.۵ |
| ۱۶۳ | اعلان اطلاعات به روز (Advertising Update) | ۸.۶ |
| ۱۶۳ | رابطه غیر فعال (Passive Interface) | ۸.۷ |
| ۱۶۳ | شمارش هاپ (Hop Count) | ۸.۸ |
| ۱۶۴ | تایمرهای پروتوکول RIP (RIP Protocol Timer) | ۸.۹ |
| ۱۶۴ | انواع نسخه‌های (RIP) | ۸.۱۰ |
| ۱۶۴ | ویژگی‌های RIP Version ۱ | ۸.۱۰.۱ |
| ۱۶۴ | ویژگی‌های RIP Version ۲ | ۸.۱۰.۲ |
| ۱۶۴ | ویژگی‌های RIPng | ۸.۱۰.۳ |
| ۱۶۵ | تفاوت‌ها و شباهت‌های RIP v۱ و v۲ | ۸.۱۱ |
| ۱۶۵ | تنظیم و فعال کردن پروتوکول RIP | ۸.۱۲ |
| ۱۶۶ | مثال پیاده سازی پروتوکول RIP | ۸.۱۳ |
| ۱۶۸ | اختصاص آدرس IP به پورت‌های روترها (Router Interface): | ۸.۱۴ |
| ۱۶۹ | پیکربندی پورت‌های serial مسیریاب (Router۰): | ۸.۱۵ |
| ۱۶۹ | پیکربندی پورت‌های serial مسیریاب (Router۱): | ۸.۱۶ |
| ۱۷۰ | پیکربندی پورت‌های مسیریاب (Router۲): | ۸.۱۷ |

منابع ۱۷۴

مقدمه

با سپاس فراوان از الله متعال که برای ما توانایی داد تا بیاموزیم و به دیگران بیاموزانیم. ما در عصر زندگی می‌کنیم که در آن تکنالوژی و کمپیوتر، دنیای بزرگ را به دهکده کوچک مجازی تبدیل کرده است. کسانی که اینترنت را بنا نهاد، هیچ‌گاه تصور نمی‌کردند، روزی برسد که این شبکه دنیا را به تسخیر خود در آورد و به چنین گستردگی برسد. گسترش شبکه اینترنت به حدی است که بقای بسیاری از بنگاه‌های تجاری به در دسترس بودن شبکه اینترنت وابسته است. از طرفی گستردگی و پراگندگی این شبکه نیاز به یک مسیریابی دقیق و پیچیده را به وجود آورده است. اینترنت که تمام جهان را با هم وصل کرده، برای آسانی مدیریت و کنترل، از وسایل و پروتوکول‌های شبکه استفاده می‌کند.

این کتاب دارای هشت فصل می‌باشد که در فصل اول آن به Subnetting که شامل Subnet کلاس‌های A,B,C و VLSM است، به جزئیات تشریح شده است. در فصل دوم به سیستم عامل‌های سیسکو اشاره شده است که آن راه‌های مختلف برقراری ارتباط با روترهای سیسکو، ویژگی‌های سیستم عامل سیسکو، با محیط CLI و مودهای مختلف روترهای سیسکو آشنا می‌شوید. در فصل سوم روترهای سیسکو بررسی شده، با اجزای داخلی روترهای سیسکو، مراحل بوت شدن سیستم عامل روترهای سیسکو، با تنظیمات ابتدایی روتر، محیط CLI روتر و مودهای مختلف آن و با تنظیم انواع پسوندها و انترفیس‌های روتر به صورت اساسی آشنا می‌شوید. در فصل چهارم، روی مسیریابی یا روتینگ بحث صورت گرفته است که در آن به موضوعات اساسی مفاهیم اولیه روتینگ، الگوریتم‌های Default, Dynamic, Static و با عملکرد پروتوکول‌های مسیریابی (Distance vector Routing, Link State Routing, Hybrid Routing) اشاره شده است. در فصل پنجم این کتاب سوئیچ‌های سیسکو بررسی شده و موضوعات اجزای داخلی سوئیچ، تنظیمات ابتدایی آن، محیط CLI و مودهای آن، نحوه تنظیم انواع پسوندها، تنظیم انترفیس VLAN1 وظایف سوئیچ‌های لایه دوم و میتودهای انتقال فریم در شبکه تشریح شده است. در فصل ششم این کتاب، با پروتوکول STP تشریح شده و با موضوعات وقوع حلقه (Loop) در شبکه LAN، پروتوکول STP و راه‌اندازی آن اشاره شده است. در فصل هفتم موضوع VLAN بررسی شده است. در این فصل به ویژگی‌ها و نحوه تنظیم آن و نقش TRUNK در VLAN اشاره صورت گرفته است. در فصل هشتم این کتاب، با پروتوکول مسیریابی RIP آشنا می‌شوید و نحوه راه‌اندازی آن روی شبکه را یاد می‌گیرید.



هدف کلی کتاب

بعد از ختم موفقانه این کتاب، محصلین با موضوعات بسیار مهم شبکه؛ چون Sunetting، سیستم عامل وسایل سیسکو، سوچ ها و روترهای شرکت سیسکو، مسیریابی، استفاده از پروتوکول STP، مدیریت ترافیک با استفاده از VLAN و پروتوکول مسیریابی RIP به صورت اساسی آشنایی کامل حاصل خواهند کرد.

فصل اول

زیر شبکه (Subnetting)



هدف کلی: آشنایی و حصول معلومات در مورد عملیه subnetting و روش های آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. با عملکرد و هدف Subnetting آشنایی حاصل نمایند.
۲. شبکه را به بخش های کوچک (subnet) تقسیم نمایند.
۳. کلاس A نتورک را Subnet نمایند.
۴. کلاس B نتورک را Subnet نمایند.
۵. کلاس C نتورک را Subnet نمایند.
۶. باعملیه VLSM آشنا شوند.

در دهه‌های اخیر با پیشرفت تکنالوژی، وسایل زیادی از طریق اینترنت باهم وصل شدند که در عرصه‌های مختلف از آن استفاده می‌شود. این همه وسایل نیاز به IP دارند. از این رو شرکت IANA که مسئول توزیع IP در جهان است، با کمبود IP روبرو شد. برای حل این مشکل علمای بخش تکنالوژی دو راه حل را پیشنهاد کردند. راه حل کوتاه مدت عبارت از NAT و Subnetting و راه حل دراز مدت عبارت از IPv6 بود. چون فعلاً IPv4 به طور گسترده استفاده می‌شود، لازم است تا محصلین با هدف و عملکرد Subnetting آشنا شده، با استفاده از کلاس‌های مختلف IP، شبکه‌های بزرگ را به بخش‌های کوچک تقسیم کنند. هم‌چنان عملیه VLSM را به طور اساسی فراگرفته و در مثال‌های عملی استفاده کنند.

۱.۱ نسخه چهارم آی پی (IPv4)

قبل از اینکه به Subnetting بپردازیم، لازم است تا در مورد آی پی (IP) معلومات داشته باشیم، پس به همین خاطر اول در مورد آی پی نسخه چهارم معلومات مختصر ارائه می‌کنیم.

آی پی (IP) عبارت از آدرسی است که موقعیت یک وسیله (Device) را در شبکه معلوم می‌کند.

این آدرس‌ها دارای ساختار منطقی بوده و می‌توانیم آن را تغییر دهیم. توسط این آدرس‌ها می‌توانیم Network ها را شناسایی کنیم. آدرس‌های IP را به نام آدرس منطقی (Logical Address) نیز یاد می‌کند.

آدرس‌های IP دارای دو نسخه (Version) بوده که نسخه چهارم (IP v4) آن، هنوز هم مورد استفاده است. نسخه چهارم IP در سال 1981 معرفی گردید. نسخه‌یی که جدیداً معرفی گردیده، به نام نسخه ششم (IP v6) یاد می‌شود. مادر اینجا صرف نسخه چهارم آدرس‌های IP را مورد بحث قرار می‌دهیم.

آدرس‌های IP v4 دارای طول 32 بیت بوده و هر آدرس به چهار بخش جدا گردیده است. هر بخش دارای هشت بیت بوده که به نام Octet یاد می‌شود (Octet به معنی هشت است). هر Octet توسط نقطه از هم جدا می‌شود و هر Octet می‌تواند از صفر تا 255 قیمت بگیرد.

آدرس‌های IPv4 به پنج کلاس ذیل تقسیم می‌شود:

- آدرس‌های IP کلاس A
- آدرس‌های IP کلاس B
- آدرس‌های IP کلاس C
- آدرس‌های IP کلاس D
- آدرس‌های IP کلاس E

هر کلاس دارای صفات و استفاده جداگانه بوده و از همین سبب شناختن هر کلاس مهم می‌باشد. چطور این کلاس‌ها را شناخته می‌توانیم؟

این کلاس‌ها را از روی اولین Octet طرف چپ، طور ذیل شناخته می‌توانیم:

آدرس‌های IP کلاس A: اولین Octet آن از صفر تا 127

آدرس‌های IP کلاس B: اولین Octet آن از 128 تا 191

آدرس‌های IP کلاس C: اولین Octet آن از 192 تا 223

آدرس‌های IP کلاس D: اولین Octet آن از 224 تا 239

آدرس‌های IP کلاس E: اولین Octet آن از 240 تا 255

ما در Network بیشتر از سه کلاس اول (کلاس A، B و C) استفاده می‌کنیم. کلاس D برای Multicast و کلاس E ریزرف می‌باشد. در اینجا می‌خواهیم آدرس‌های کلاس A، B و C را بشناسیم.

۱.۱.۱ آدرس‌های کلاس A

از این آدرس‌ها اولین Octet طرف چپ آن برای Network و متباقی سه Octet آن برای Host می‌باشد. این آدرس‌ها برای Network‌های کلان استفاده می‌شود.

| Class A | Network | Host | Host | Host |
|---------|---------|------|------|------|
| Octet | 1 | 2 | 3 | 4 |

قیمت اولین Octet آن از صفر تا 127 می‌باشد.

نوت: آدرس صفر ریزرف بوده و آدرس 127 برای Loopback استفاده می‌شود.

۱.۱.۲ آدرس‌های کلاس B

از این آدرس‌ها دو Octet طرف چپ برای Network و دو Octet طرف راست آن برای Host می‌باشد. این آدرس‌ها برای Network‌های متوسط استفاده می‌شود.

| Class B | Network | Network | Host | Host |
|---------|---------|---------|------|------|
| Octet | 1 | 2 | 3 | 4 |

قیمت اولین Octet آن از 128 تا 191 می‌باشد.

۱.۱.۳ آدرس‌های کلاس C

از این آدرس‌ها سه Octet طرف چپ آن برای Network و یک Octet آن برای Host می‌باشد. این آدرس‌ها برای Network های کوچک استفاده می‌شود.

| Class C | Network | Network | Network | Host |
|---------|---------|---------|---------|------|
| Octet | 1 | 2 | 3 | 4 |

قیمت اولین Octet آن از 192 تا 223 می‌باشد.

۱.۱.۴ Subnet Mask

برای تشخیص بخش Network و بخش Host از Subnet Mask استفاده می‌شود. هر کلاس دارای Subnet Mask از قبل تعیین شده (Default) می‌باشد. Subnet Mask از قبل تعیین شده (Default) برای کلاس‌های A، B و C قرار می‌باشد:

برای کلاس A: 255.0.0.0

| | | | | |
|----------|----------|----------|----------|---------------|
| 255 | 0 | 0 | 0 | اعداد دیسیمل |
| 11111111 | 00000000 | 00000000 | 00000000 | ماعداد باینری |

برای کلاس B: 255.255.0.0

| | | | | |
|----------|----------|----------|----------|--------------|
| 255 | 255 | 0 | 0 | اعداد دیسیمل |
| 11111111 | 11111111 | 00000000 | 00000000 | اعداد باینری |

برای کلاس C: 255.255.255.0

| | | | | |
|----------|----------|----------|----------|--------------|
| 255 | 255 | 255 | 0 | اعداد دیسیمل |
| 11111111 | 11111111 | 11111111 | 00000000 | اعداد باینری |

تبدیل اعداد یکی از موضوعات مهم دیگری است که در Subnet کردن شبکه به ما بسیار کمک می‌کند؛ پس لازم است تا تبدیل اعداد از دیسیمل به باینری و برعکس آن یاد بگیریم.

۱.۱.۵ تبدیل اعداد از دیسیمال به باینری

برای اینکه بتوانیم یک آدرس IP را تحلیل کنیم و یا هم Subnet کنیم، باید تبدیل اعداد باینری به دیسیمال را بدانیم. هر قسمت دیسیمال آدرس IP را به یک عدد 8 بیتی باینری تبدیل خواهیم نمود و آن را در بیت‌های صفر تا 7 که هشت بیت می‌شود قرار می‌دهیم:

| بیت 0 | بیت 1 | بیت 2 | بیت 3 | بیت 4 | بیت 5 | بیت 6 | بیت 7 |
|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| 0 به توان 2 | 1 به توان 2 | 2 به توان 2 | 3 به توان 2 | 4 به توان 2 | 5 به توان 2 | 6 به توان 2 | 7 به توان 2 |
| بیت 0 | بیت 1 | بیت 2 | بیت 3 | بیت 4 | بیت 5 | بیت 6 | بیت 7 |

حال اگر بخواهیم یک عدد دیسیمال را به باینری تبدیل کنیم، عدد را به صورت متوالی به مقادیر بالا، از چپ به راست کسر می‌کنیم. در صورتی که مقادیر توانی، دو قابلیت کسر شدن از عدد باقیمانده را داشت، در جدول مربوطه عدد 1 و اگر نداشت عدد صفر را قرار می‌دهیم. جهت وضاحت بهتر می‌خواهیم عدد 249 را به باینری تبدیل نماییم:

$$\text{مرحله اول: } 249 - 128 = 121$$

بنابراین 128 در 249 وجود دارد، پس در جدول 1 قرار می‌دهیم

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| | | | | | | | 1 |

$$\text{مرحله دوم: } 121 - 64 = 57$$

بنابراین 64 داخل 121 وجود دارد، پس در جدول 1 قرار می‌دهیم

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| | | | | | | 1 | |
| | | | | | | | 1 |

مرحله سوم: $57 - 32 = 25$

بنابراین 32 داخل 57 وجود دارد، پس در جدول 1 قرار می‌دهیم

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|----|----|----|---|---|---|---|
| 1 | 1 | 1 | | | | | |

مرحله چهارم: $25 - 16 = 9$

بنابراین 16 داخل 25 وجود دارد، پس در جدول 1 قرار می‌دهیم

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|----|----|----|---|---|---|---|
| 1 | 1 | 1 | 1 | | | | |

مرحله پنجم: $9 - 8 = 1$

بنابراین 8 داخل 9 وجود دارد، پس در جدول 1 قرار می‌دهیم

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|----|----|----|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | | | |

مرحله ششم: $1 - 4 = \text{ERROR}$

بنابراین 4 داخل 1 وجود ندارد، پس در جدول 0 قرار می‌دهیم

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|----|----|----|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | | |

مرحله هفتم: $1 - 2 = \text{ERROR}$

بنابراین 2 داخل 1 وجود ندارد، پس در جدول 0 قرار می‌دهیم

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|----|----|----|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | |

مرحله آخر: $1 - 1 = 0$

بنابراین 1 داخل 1 وجود دارد، پس در جدول 1 قرار می‌دهیم

| | | | | | | | |
|-----|----|----|----|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |

از محاسبه بالا می‌توان گفت که عدد دیسیمل 249 برابر با عدد باینری 11111001 است.

تبدل اعداد باینری به دیسیمل

| | | | | | | | |
|----|----|----|----|----|----|----|-----|
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |

در جدول بالا دیده می‌شود که از طرف چپ به راست قیمت اعداد باینری هر رقم دو برابر رقم قبلی است. لذا، اولین رقم دارای قیمت $20 = 1$ ، دومین رقم دارای قیمت $21 = 2$ سومین رقم دارای قیمت $22 = 4$ ، چهارمین رقم دارای قیمت $23 = 8$ و... است.

حال با استفاده از جدول بالا عدد باینری 101011102 را به عدد دیسیمل تبدیل می‌کنیم.

حل: اعداد باینری داده شده را به ترتیب از طرف چپ در جدول قرار می‌دهیم و قیمت آن را جمع می‌کنیم
مرحله اول: عدد اول را در جدول قرار می‌دهیم، دیده می‌شود که قیمت آن 1 است.

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| 1 | | | | | | | |

مرحله دوم: عدد دوم را در جدول قرار می‌دهیم، دیده می‌شود که قیمت آن 0 است.

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| 1 | 0 | | | | | | |

مرحله سوم: عدد سوم را در جدول قرار می‌دهیم، معلوم می‌شود که قیمت آن 4 است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| 1 | 0 | 1 | | | | | |

مرحله چهارم: عدد چهارم را در جدول قرار می دهیم، معلوم می شود که قیمت آن صفر است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|----|----|----|-----|

| | | | | | | | |
|---|---|---|---|--|--|--|--|
| 1 | 0 | 1 | 0 | | | | |
|---|---|---|---|--|--|--|--|

مرحله پنجم: عدد پنجم را در جدول قرار می دهیم، معلوم می شود که قیمت آن 16 است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|----|----|----|-----|

| | | | | | | | |
|---|---|---|---|---|--|--|--|
| 1 | 0 | 1 | 0 | 1 | | | |
|---|---|---|---|---|--|--|--|

مرحله ششم: عدد ششم را در جدول قرار می دهیم، معلوم می شود که قیمت آن 32 است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|----|----|----|-----|

| | | | | | | | |
|---|---|---|---|---|---|--|--|
| 1 | 0 | 1 | 0 | 1 | 1 | | |
|---|---|---|---|---|---|--|--|

مرحله هفتم: عدد هفتم را در جدول قرار می دهیم، معلوم می شود که قیمت آن 64 است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|----|----|----|-----|

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | |
|---|---|---|---|---|---|---|--|

مرحله هشتم: عدد هشتم را در جدول قرار می دهیم، معلوم می شود که قیمت آن 0 است

| | | | | | | | |
|---|---|---|---|----|----|----|-----|
| 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|---|---|---|---|----|----|----|-----|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|

در اخیر همه قیمت ها را باهم جمع می کنیم.

$$(1)+(0)+(4)+(0)+(16)+(32)+(64)+(0)=11710$$

پس گفته می توانیم که عدد $101011102 = 11710$ است.

۱.۲ زیر شبکه (Subnetting)

عبارت از تقسیم کردن یک شبکه بزرگ به شبکه های کوچک فرعی می باشد. هدف از Subnetting این است که یک محدوده (Range) از IP Addresses را که به ما تعلق دارد، به چند Range آدرس مجزا تقسیم کنیم تا بتوانیم از هر Range، جداگانه استفاده کنیم. مثلاً: ممکن است بخواهیم برای کاهش ترافیک، شبکه را به چند بخش (Segment) تقسیم کنیم و بین بخش های روتر (Router) قرار دهیم.

۱.۲.۱ فواید Subnetting

- کم کردن ترافیک و بالابردن کارکرد شبکه.
- افزایش توان مدیریتی شبکه و در نتیجه حل مشکل، آسانتر.
- کوچک شدن اندازه Routing table و در نتیجه بالا رفتن سرعت هم‌گرایی (Convergence) شبکه.

مثال: شبکه 192.168.129.0 که subnet mask آن 255.255.255.0 است به دو بخش تقسیم کنید؟

حل: در قدم اول شبکه داده شده یا بخش (Network ID) و بخش Subnet mask را به باینری تبدیل می کنیم. با استفاده از فورمول ساده ذیل، اگر زیر شبکه (subnet) خواسته شده بود، استفاده می کنیم:

Number of Subnet needed $2^n \geq$

n در فورمول فوق تعداد بیت‌هایی است که باید از سمت راست از Host قرض بگیریم و به Network اضافه کنیم.

چون از ما دو زیر شبکه خواسته شده است، پس اگر یک بیت را از Host قرض بگیریم دو زیر شبکه به ما می‌دهد.

یعنی 21=2

Network ID: 192.168.129.0

Subnet mask: 11111111.11111111.11111111.10000000 /255.255.255.128

| | Network | | | Host |
|--------------|-----------------|-----------------|-----------------|-----------------|
| Network ID | 1 1 0 0 0 0 0 0 | 1 0 0 0 0 0 0 0 | 1 0 0 0 0 0 0 1 | 0 0 0 0 0 0 0 0 |
| Default mask | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 0 0 0 0 0 0 0 0 |

1 1 1 1 1 1 1 1

1 0 0 0 0 0 0 0

↓

Subnet

↓

| | Network | | | Host |
|--------------|-----------------|-----------------|-----------------|-----------------|
| Network ID | 1 1 0 0 0 0 0 0 | 1 0 0 0 0 0 0 0 | 1 0 0 0 0 0 0 1 | 0 0 0 0 0 0 0 0 |
| Default mask | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 1 0 0 0 0 0 0 0 |

شکل (۱-۱) بیت‌های شبکه و Host

همانطور که مشاهده می کنید، به اندازه یک بیت به سمت Host پیش روی کرده ایم. درواقع به اندازه یک بیت از بخش Host قرض گرفته شده و مقدار آن از صفر به یک تبدیل شده است. بنابر این تعداد بیت های بخش Host هفت بیت و یک بیت به عنوان بیت Subnet انتخاب می شود.

در شبکه فرعی اول داریم

192.128.129.0 – 255.255.255.128

192.128.129.1 – 255.255.255.128

192.128.129.2 – 255.255.255.128

192.128.129.3 – 255.255.255.128

سرانجام، آخرین آی پی آدرس

192.128.129.127 – 255.255.255.128

نوت: اولین آی پی آدرس مربوط به Network ID و آخرین آی پی آدرس مربوط به Broadcast address می باشد که به کامپیوترها داده نمی شود. و متباقی آدرس هایی که در بین Network ID و Broadcast address قرار دارند، همه آن ها آدرس های معتبر (Valid) می باشد که می تواند به کامپیوترها داده شود. برای محاسبه Network ID تمام بیت های Host را صفر می سازیم و برای پیدا کردن Broadcast Address تمام بیت های Host را یک می سازیم.

در شبکه فرعی دوم داریم:

192.128.129.128 – 255.255.255.128

192.128.129.129 – 255.255.255.128

192.128.129.130 – 255.255.255.128

192.128.129.131 – 255.255.255.128

و بالاخره آخرین آی پی آدرس

192.128.129.255 – 255.255.255.128

نوت: اولین آی پی آدرس مربوط به Network ID و آخرین آی پی آدرس مربوط به Broadcast address می باشد که به کامپیوترها داده نمی شود. متباقی آدرس هایی که در بین Network ID و Broadcast address قرار دارند، همه آن ها آدرس های معتبر (Valid) می باشد که می تواند به کامپیوترها داده شود.

هر دو شبکه فرعی که از شبکه 192.128.129.0 با Subnet mask 255.255.255.0 به وجود آمده‌اند، در شکل ذیل نشان داده شده است.

| | Network | | | Host |
|---|----------|----------|----------|----------|
| Network ID | 11000000 | 10000000 | 10000001 | 00000000 |
| <p>If subnet is 00000000 then</p> <p>Network ID : 192.168.129.0</p> <p>First valid host : 192.168.129.1</p> <p>Last valid host : 192.168.129.126</p> <p>Broadcast address : 192.168.129.127</p> <p>If subnet is 10000000 then</p> <p>Network ID : 192.168.129.128</p> <p>First valid host : 192.168.129.129</p> <p>Last valid host : 192.168.129.254</p> <p>Broadcast address : 192.168.129.255</p> | | | | |

شکل (۱-۲) شبکه‌های فرعی

تعداد بیت‌های بخش Subnet به اندازه یک بیت می‌باشد و تعداد حالت‌هایی که یک بیت می‌تواند داشته‌باشد، دو حالت است، یک و صفر.

بنابر این به کمک تعداد بیت‌های Subnet می‌تواند، تعداد Network‌های ایجاد شده را تشخیص داد. در این مثال یک Network با 256 عدد آدرس به دو Sub network هر کدام با تعداد 128 عدد آدرس تبدیل شده است. در این مثال، بیت هشتم از Octet می‌تواند هم مقدار یک و هم مقدار صفر بگیرد، بنابر این با توجه به مقادیر یک و صفری که بیت هشتم گرفته است، دو حالت زیر را خواهد داشت:

1. صفر

بیت هشتم صفر و هفت بیت دیگر می‌تواند مقدار یک و صفر به خود گیرد، بنا بر این رنج IP addresss که می‌توانیم داشته باشیم، با حساب صفر بودن بیت هشتم، 192.168.129.1 الی 192.168.129.127 خواهد بود. در این حالت Network ID تغییر نکرده و همان 192.168.129.0 خواهد بود، با این تفاوت که رنج IP addressها تغییر کرده است.

2. یک

بیت هشتم یک و هفت بیت دیگر می‌توانند مقدار یک و صفر به خود بگیرند، بنا بر این رنج IP address که با شرایط جدید می‌توانیم داشته باشیم با حساب یک بودن بیت هشتم، 192.168.129.129 الی 192.168.129.254 خواهد بود.

همانطور که می‌دانید برای تعیین Network Address باید در IP address بیت‌های که نشان دهنده Host هستند، مقدار صفر بگیرند. زیرا Network Address با حساب یک‌بودن بیت هشتم، 192.168.129.128 خواهد بود. و تعداد IP Address‌های که می‌توان در این شبکه استفاده کرد با حذف کردن حالت‌های مربوط به Network Address و Broadcast Address، 126 آدرس خواهد بود.

بنابراین در مثال بالا با استفاده از Subnetting یک Network به دو تا Network تبدیل شده و تعداد Host‌ها نیز به دو بخش تقسیم شده است.

۱.۳ Subnet کردن آی‌پی آدرس کلاس A

مثال: آی‌پی آدرس کلاس A داده شده است می‌خواهیم آن را به تعداد 4 شبکه فرعی تقسیم (subnet) نماییم:

50.0.0.0- 255.0.0.0

مرحله اول: اول آی‌پی آدرس داده شده را به باینری تبدیل می‌کنیم و با استفاده از فورمول، بخش‌های ذیل را معلوم می‌کنیم:

- تعداد Subnet با استفاده از فورمول 2^n و 2^h عبارت از تعداد subnet است.
- تعداد Host با استفاده از فورمول 2^n و 2^h عبارت از Host است.
- افزایش (Increment) عبارت از تعداد Host در یک subnet است (2^h).
- Octet (که در آن محاسبه صورت می‌گیرد معلوم می‌کنیم)

مرحله دوم: آدرس داده شده را به باینری تبدیل می‌کنیم.

Ip address 00110010.00000000.00000000.00000000

Subnet mask 11111111.00000000.00000000.00000000

چون از ما 4 subnet خواسته شده، پس قیمت n ما می‌شود 2؛ یعنی دو بیت از Host قرض می‌گیریم و به شبکه اضافه می‌کنیم. Subnet mask جدید ما به شکل ذیل تبدیل می‌شود.

Subnet mask 11111111.11000000.00000000.00000000 /255.192.0.0

مرحله سوم: تعداد Host‌ها را در هر subnet با استفاده از فورمول 2^h-2 معلوم می‌کنیم.

Subnet mask 11111111.00000000.00000000.00000000

چون قیمت h در این مثال 22 است پس در هر subnet به تعداد 4194304 آی‌پی وجود دارد.

مرحله چهارم: برای آسانی کار در octet که هم صفرها و هم یک‌ها باشد، محاسبه خود را انجام می‌دهیم که افزایش (increment) در octet دوم 64 می‌باشد.

مرحله پنجم: اولین subnet عبارت است از

50.0.0.0 – 255.192.0.0 (Network ID)

50.0.0.1 – 255.192.0.0

50.0.0.2 – 255.192.0.0

بالاخره، آخرین آی‌پی ما قرار ذیل است:

50.63.255.255 – 255.192.0.0 (Broadcast address)

مرحله ششم: subnet دوم عبارت است از

50.64.0.0 - 255.192.0.0 (Network ID)

50.64.0.1 - 255.192.0.0

50.64.0.2 – 255.192.0.0

بالاخره، آخرین آی‌پی ما در این subnet قرار ذیل است:

50.127.255.255 – 255.192.0.0 (Broadcast address)

مرحله هفتم: subnet سوم عبارت است از:

50.128.0.0 – 255.192.0.0 (Network ID)

50.128.0.1 – 255.192.0.0

50.128.0.2 – 255.192.0.0

50.128.0.3 – 255.192.0.0

بالاخره، آخرین آی‌پی ما در این subnet قرار ذیل است.

50.191.255.255 – 255.192.0.0 (Broadcast address)

مرحله هشتم: subnet چهارم عبارت است از:

50.192.0.0 – 255.192.0.0 (Network ID)

50.192.0.1 – 255.192.0.0

50.192.0.2 – 255.192.0.0

50.192.0.3 – 255.192.0.0

بالاخره، آخرین آی پی ما در این subnet قرار ذیل است:

50.255.255.255 – 255.192.0.0 (Broadcast address)

۱.۴ Subnet کردن آی پی آدرس کلاس B

شبکه داده شده را به 30 subnet تقسیم کنید؟

175.160.0.0

مرحله اول: اول آی پی آدرس داده شده را به باینری تبدیل می کنیم و با استفاده از فورمول، بخش های ذیل را معلوم می کنیم.

- تعداد Subnet (با استفاده از فورمول 2^n) عبارت از تعداد subnet است.
- تعداد Host (با استفاده از فورمول $2^h - 2$) عبارت از Host است.
- افزایش (Increment) عبارت از تعداد Host در یک subnet است (2^h).
- Octet (که در آن محاسبه صورت می گیرد، معلوم می کنیم)

مرحله دوم: آدرس داده شده را به باینری تبدیل می کنیم.

Ip address 10101111.10100000.00000000.00000000

Subnet mask 11111111.11111111.00000000.00000000

چون از ما 30 subnet خواسته شده، پس قیمت n ما 5 می شود؛ یعنی 5 بیت از Host قرض می گیریم و به شبکه اضافه می کنیم. Subnet mask جدید ما به شکل ذیل تبدیل می شود:

Subnet mask 11111111.11111111.11111000.00000000 /255.255.248.0

مرحله سوم: تعداد Host ها را در هر subnet با استفاده از فورمول $2^h - 2$ معلوم می کنیم:

Subnet mask 11111111.11111111.11111000.00000000

چون قیمت h در این مثال 11 است، پس در هر subnet به تعداد 2048 آی پی وجود دارد.

مرحله چهارم: برای آسانی کار در octet که هم صفرها و هم یک‌ها باشد، محاسبه خود را انجام می‌دهیم که افزایش (increment) در octet سوم 8 می‌باشد.

مرحله پنجم: اولین subnet عبارت است از:

175.160.0.0 – 255.255.248.0 (Network ID)

175.160.0.1 – 255.255.248.0

175.160.0.2 – 255.255.248.0

175.160.0.3 – 255.255.248.0

و بالاخره، آخرین آی‌پی ما قرار ذیل است:

175.160.7.255 – 255.255.248.0 (Broadcast address)

مرحله ششم: دوم subnet عبارت است از

175.160.8.0 – 255.255.248.0 (Network ID)

175.160.8.1 – 255.255.248.0

175.160.8.2 – 255.255.248.0

175.160.8.3 – 255.255.248.0

بالاخره، آخرین آی‌پی ما در این subnet قرار ذیل است:

175.160.15.255 – 255.255.248.0 (Broadcast address)

در این مثال 32 ، subnet وجود دارد، آخرین subnet را هم محاسبه می‌کنم و محاسبه subnet‌های باقی‌مانده به محصلین عزیز واگذار می‌شود.

مرحله آخر: Subnet ، 32 ام عبارت است از:

175.160.248.0 – 255.255.248.0 (Network ID)

175.160.248.1 – 255.255.248.0

175.160.248.2 – 255.255.248.0

175.160.248.3 – 255.255.248.0

بالاخره، آخرین آی پی ما در این subnet قرار ذیل است:

175.160.255.255 – 255.255.248.0 (Broadcast address)

۱.۵ Subnet کردن آی پی آدرس کلاس C

شبکه داده شده را به 8، subnet تقسیم کنید.

200.50.60.0 255.255.255.0

مرحله اول: اول آی پی آدرس داده شده را به باینری تبدیل می کنیم و با استفاده از فورمول بخش های ذیل را معلوم می کنیم.

- تعداد Subnet (با استفاده از فورمول 2^n) عبارت از تعداد subnet است.
- تعداد Host (با استفاده از فورمول $2^h - 2$) عبارت از Host است.
- افزایش (Increment) عبارت از تعداد Host در یک subnet است (2^h).
- Octet (که در آن محاسبه صورت می گیرد، معلوم می کنیم)

مرحله دوم: آدرس داده شده را به باینری تبدیل می کنیم.

Ip address 11001000.00110010.00111100.00000000

Subnet mask 11111111.11111111.11111111.11100000

چون از ما 8 subnet خواسته شده، پس قیمت n ما 3 می شود، یعنی 3 بیت از Host قرض می گیریم و به شبکه اضافه می کنیم. Subnet mask جدید ما به شکل ذیل تبدیل می شود.

Subnet mask 11111111.11111111.11111111.11100000 /255.255.255.224

مرحله سوم: تعداد Host ها را در هر subnet با استفاده از فورمول $2^h - 2$ معلوم می کنیم.

Subnet mask 11111111.11111111.11111111.11100000

چون قیمت h در این مثال 5 است؛ پس در هر subnet به تعداد 32 آی پی وجود دارد.

مرحله چهارم: برای آسانی کار در octet که هم صفرها و هم یکها باشد، محاسبه خود را انجام می دهیم که افزایش (increment) در octet اول 32 می باشد.

مرحله پنجم: اولین subnet عبارت است از

200.50.60.0 – 255.255.255.224 (Network ID)

200.50.60.1 – 255.255.255.224

200.50.60.2 – 255.255.255.224

200.50.60.3 – 255.255.255.224

بالاخره، آخرین آی پی ما قرار ذیل است:

200.50.60.31 – 255.255.255.224 (Broadcast address)

مرحله ششم: subnet دوم عبارت است از:

200.50.60.32 – 255.255.255.224 (Network ID)

200.50.60.33 – 255.255.255.224

200.50.60.33 – 255.255.255.224

200.50.60.35 – 255.255.255.224

بالاخره، آخرین آی پی ما قرار ذیل است:

200.50.60.63 – 255.255.255.224 (Broadcast address)

مرحله هفتم: subnet سوم عبارت است از:

200.50.60.64 – 255.255.255.224 (Network ID)

200.50.60.65 – 255.255.255.224

200.50.60.66 – 255.255.255.224

200.50.60.67 – 255.255.255.224

بالاخره، آخرین آی پی ما قرار ذیل است:

200.50.60.95 – 255.255.255.224 (Broadcast address)

آخرین subnet این مثال عبارت است از:

200.50.60.224 – 255.255.255.224 (Network ID)

200.50.60.225 – 255.255.255.224

200.50.60.226 – 255.255.255.224

200.50.60.227 – 255.255.255.224

بالاخره، آخرین آی پی ما قرار ذیل است:

200.50.60.255 – 255.255.255.224 (Broadcast address)

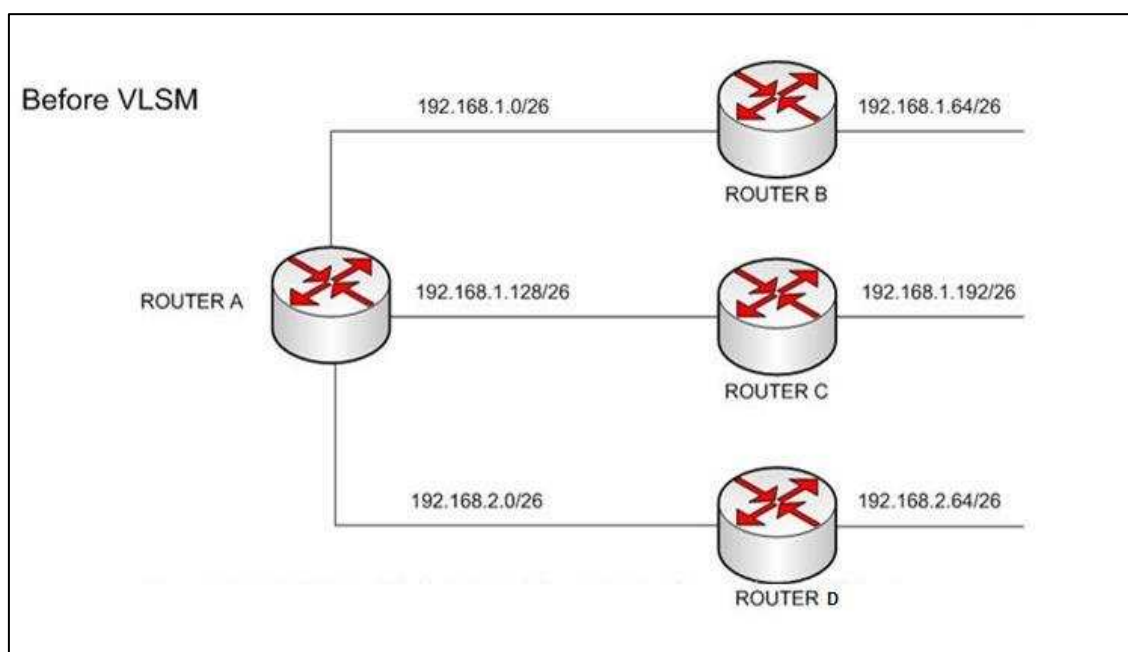
۱.۶ Variable Length Subnetmask (VLSM)

VLSM در استاندارد RFC 1812 تعریف شده و اجازه استفاده از Subnet Mask های با اندازه مختلف در خلال یک آدرس با کلاس استاندارد را به ما می دهد؛ به بیان ساده: استفاده بهتر از فضای آدرسی که در اختیارمان قرار داده شده است.

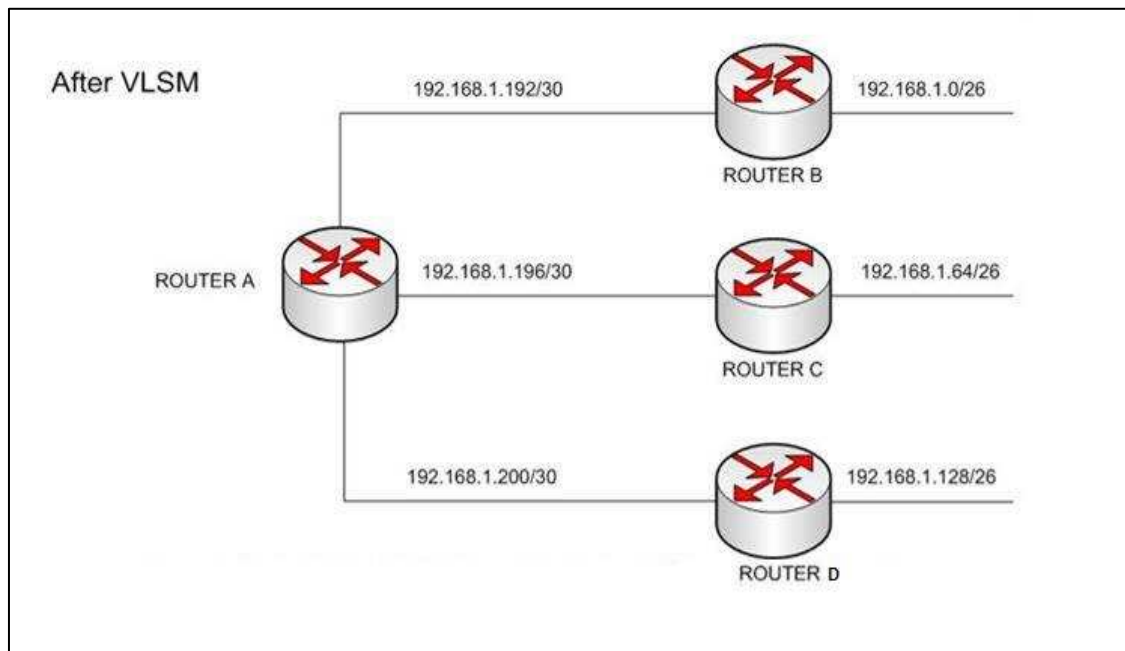
مزیت های VLSM شامل دو مورد مهم زیر است:

- استفاده هرچه بهتر از فضای آدرس که در اختیار ما قرار گرفته است.
- استفاده از خصوصیت Route Summarization.

همان طوری که در مورد اول اشاره شد، با استفاده از VLSM می توان از فضای آدرسی که در اختیار ما قرار داده می شود، به بهترین شکل ممکن استفاده کرد. این اشکال، مثال ساده ای را قبل و بعد از VLSM نشان می دهد.



شکل (۳-۱) شبکه بدون VLSM



شکل (۴-۱) شبکه با VLSM

در مثال فوق روتر (A) که به روترهای دیگر (B, C, D) وصل شده است. در هر یک از این سایت‌ها حد اکثر تعداد 50 عدد کامپیوتر وجود دارد و بنابراین Subnet Mask، 26/ را نظر به فورمول که قیمت $h=6$ است انتخاب نمودیم. در شکل (3-1) که از VLSM استفاده نشده است، فقط می‌توان یک Mask که برابر با 255.255.255.192 بوده و حد اکثر 62 آدرس را برای هریک از شبکه‌ها ارائه می‌دهد، در تمام شبکه‌ها به کاربرد. به خاطری که تعداد شبکه‌های ما با Subnet‌های مورد استفاده باید از دو آدرس در کلاس C استفاده نماییم، در این صورت آدرس‌های زیاد در شبکه ضایع خواهد شد.

در شکل (4-1) آدرس‌دهی شبکه را با استفاده از VLSM انجام داده‌ایم. در این مثال شبکه‌های دور (Remote) از 26/ و شبکه‌های روتر A از 30/ به عنوان Mask استفاده می‌کند و در این صورت فقط یک آدرس در کلاس C برای آدرس‌دهی تمام دستگاه‌های شبکه، مورد نیاز خواهد بود که در نتیجه از ضایع شدن آبی‌آدرس‌های زیاد جلوگیری خواهد شد.

مراحل آدرس‌دهی با روش VLSM:

۱. آن شبکه یا Segment را که دارای بیشترین تعداد کامپیوتر بوده، مشخص می‌کنیم.
۲. بهترین Mask ممکن را برای بزرگ‌ترین شبکه تعیین می‌نماییم.
۳. شبکه‌های ایجاد شده به وسیله Mask تعیین شده را می‌نویسیم.

۴. برای شبکه‌هایی که دارای تعداد کمپیوترهای کمتری هستند، یکی از شبکه‌های ایجاد شده را تخصیص داده و متناسب با مقدار کمپیوترهای موجود در آن شبکه، Mask مناسب را تعیین می‌کنیم.

۵. شبکه‌های جدیدی که ایجاد شده است، دوباره می‌نویسیم.

محاسبات انجام شده در حقیقت تقسیم کردن شبکه‌یی است که خود تقسیم شده است، به شبکه‌های کوچک‌تر و در صورت ضرورت تقسیم‌بندی دوباره آن‌ها می‌باشد. در این صورت است که از فضای آدرس که در اختیار ما قرار دارد، می‌توانیم به بهترین صورت استفاده کنیم.

مثال:

شبکه 255.255.255.0 _ 190.50.60.0 داده شده است. آن را به سه شبکه، در شبکه (A) 60 کمپیوتر، در شبکه (B) 30 کمپیوتر و در شبکه (C) 6 کمپیوتر وجود دارد؛ طوری که کمترین ضایعات آی‌پی آدرس داشته باشد.

حل:

نظر به مراحل گفته شده (1 و 2) بزرگ‌ترین شبکه ما دارای 60 پایه کمپیوتر بوده که با توجه به آدرس داده شده، Mask مناسب به صورت 255.255.255.192 190.50.60.0 خواهد بود که 62 عدد آی‌پی آدرس را ارائه می‌دهد. در مراحل 3 شروع به نوشتن شبکه‌های ایجادی با استفاده از Mask جدید می‌کنیم:

قیمت $h = 6$ است.

1- 190.50.60.0 255.255.255.192

2- 190.50.60.64 255.255.255.192

3- 190.50.60.128 255.255.255.192

4- 190.50.60.192 255.255.255.192

چهار شبکه ایجاد شد که در هر شبکه به تعداد 62 آی‌پی آدرس معتبر وجود دارد. subnet اول را به شبکه (A) اختصاص می‌دهیم.

Subnet دوم را به شبکه (B) خود نظر به تعداد کمپیوتر دوباره تقسیم می‌کنیم و دو subnet آخری به شبکه‌های دیگر قابل استفاده می‌باشد. قیمت $h = 5$ است.

حال، شبکه دوم خود را مانند مراحل فوق تقسیم می کنیم که subnetmask آن تغییر می کند.

192.50.60.64 255.25.255.224

190.50.60.96 255.255.255.224

.....

Subnet اول که 30 آی پی آدرس را به ما می دهد، به شبکه (B) خود اختصاص می دهیم و subnet دوم را برای شبکه (C) خود که دارای 6 کامپیوتر می باشد، دوباره تقسیم می کنیم.

که این دفعه، قیمت $h = 3$ است. شبکه با subnetmask جدید به وجود می آید.

190.50.60.96 255.255.255.248

نوت: در تقسیم بندی آخری، شبکه ما به 32 شبکه فرعی تقسیم می شود که subnet اول آن را به شبکه (C) خود اختصاص داده و subnet های متباقی برای شبکه هایی که جدیداً ایجاد می شود، قابل استفاده می باشد.



آی‌پی‌آدرس (IP address) یک آدرس منطقی است که در یک شبکه برای تعیین موقعیت یک وسیله استفاده می‌شود. دارای دو بخش مهم است که عبارت از بخش شبکه و بخش Host است. این آدرس منطقی به پنج کلاس تقسیم‌بندی شده که کلاس‌های (A, B, C) برای استفاده عموم، کلاس D برای Multicast و کلاس E آن ریزرف می‌باشد.

Subnetmask جداکننده بخش شبکه و بخش Host در یک آی‌پی‌آدرس می‌باشد. بنابر رشد سریع اینترنت شرکت IANA که مسئول توزیع آی‌پی بود، با کمبود آی‌پی‌آدرس مواجه شد. علمای بخش تکنالوژی برای حل این مشکل دو راه حل پیشنهاد کردند. راه حل اولی NAT و subnetting بود و راه حل بنیادی ایجاد IPv6 بود.

در Subnetting یک شبکه بزرگ به شبکه‌های کوچک تقسیم می‌شود.
برای تعیین تعداد شبکه‌های فرعی (subnet) از فورمول ذیل استفاده می‌شود.

$$2^n \geq \text{Number of Available subnet}$$

حرف n تعداد بیت‌هایی را که از بخش (Host) قرض گرفته شده و به بخش (Network) اضافه شده است، نشان می‌دهد.

در صورتی که IP‌های قابل استفاده مورد نظر باشد، از فورمول ذیل استفاده می‌شود:

$$2^h - 2 \geq \text{Number of Available IP Address}$$

حرف h تعداد بیت‌هایی را نشان می‌دهد که در بخش Host باقی مانده است.
اما مشکل که در subnetting وجود داشت، این بود که شبکه را به سائزهای مساوی تقسیم می‌کرد و سبب ضایع شدن آی‌پی‌آدرس می‌گردید.

بعداً VLSM ایجاد شد که مشکل ضایع شدن آی‌پی را به حد اقل رساند. این برنامه طوری عمل می‌کند که آی‌پی‌ها را نظر به ضرورت شبکه اختصاص می‌دهد. در هر شبکه Network ID و Host address قابل استفاده نمی‌باشد.



- (۱) کلاس‌های IPv4 را با مثال شرح دهید.
- (۲) هدف اصلی Subnetting چیست توضیح دهید.
- (۳) عملیۀ Subnetting را بالای IP کلاس A اجرا کنید.
- (۴) عملیۀ Subnetting را بالای IP کلاس B اجرا کنید.
- (۵) عملیۀ Subnetting را بالای IP کلاس C اجرا نمایید.
- (۶) فورمول حداقل IP‌های قابل استفاده در یک شبکه را واضح سازید.
- (۷) فورمول تعداد Subnet‌های موردنیاز در یک شبکه را واضح سازید.
- (۸) عملیۀ VLSM را مختصراً توضیح دهید.
- (۹) خصوصیات مهم VLSM را توضیح دهید.
- (۱۰) مراحل آدرس‌دهی با روش VLSM را خلاص توضیح دهید.



- ۱- IP Address 10.0.0.0 255.0.0.0 به شش شبکه فرعی تقسیم کنید.
- ۲- IP Address 150.120.0.0 255.555.0.0 را به شبکه 15 شبکه فرعی تقسیم کنید.
- ۳- IP Address 192.168.10.0 255.255.255.0 را به 50 شبکه فرعی تقسیم کنید.
- ۴- IP Address 180.30.150.0 255.255.255.0 را طوری به شبکه‌های فرعی تقسیم کنید که هر شبکه فرعی دارای 40 آی‌پی‌آدرس معتبر (valied) داشته باشد.
- ۵- IP Address 192.168.5.0 255.255.255.0 را با استفاده از مراحل VLSM، Subnet نمایید. طوری که سه شبکه LAN با تعداد IP های 110، 55 و 22 را در نظر بگیرید و باید کمترین ضایع آی پی (IP) را داشته باشید.

فصل دوم

سیستم عامل سیسکو

IOS (Internetwork Operating System)



هدف کلی: آشنایی با سیستم عامل سیسکو (IOS) با محیط CLI و مدهای (Modes) آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. راه‌های مختلف برای برقراری ارتباط با تجهیزات Cisco را تشریح نمایند.
۲. ویژگی‌های سیستم عامل سیسکو (IOS) را مشخص کرده بتوانند.
۳. محیط CLI و مدهای آن را توضیح داده بتوانند.

سیستم عامل سیسکو، مختص به شرکت سیسکو می باشد. برای تجهیزات ارتباطی این شرکت قرار دارد و از آن برای کنترل روتینگ و سویچینگ دستگاه ها در شبکه های بزرگ استفاده می شود. سیستم عامل IOS مجموعه کاملی از ابزارها و فرامین است که به مسئول شبکه کمک می کند تا روتر یا سوئیچ سیسکو را پیکربندی و مدیریت نماید. برای تمامی مدیران شبکه آشنایی با IOS برای مدیریت و پیکربندی دستگاه های نظیر روتر یا سوئیچ الزامی است. قبل از اینکه بخواهیم به مسائل آموزشی سیسکو بپردازیم، شناخت سیستم عامل سیسکو (IOS) لازم است.

۲.۱ Internetwork Operating System (IOS)

عبارت از هسته مرکزی روتر (Router) و سویچ (Switch) های شرکت سیسکو می باشد. این سیستم عامل همانند سیستم عامل های دیگر وظیفه ذخیره و بازیابی فایل، مدیریت حافظه و مدیریت سرویس های مختلف را به عهده دارد. این سیستم عامل فاقد محیط گرافیکی بوده و مبتنی بر خط فرمان (CLI) می باشد؛ بنابراین دارای یک واسطه کاربری (UI) می باشد که به کمک آن دسترسی به دستورات و پیکربندی وسایل سیسکو امکان پذیر می باشد.

IOS سیسکو در دو mode پیکربندی می شود:

۱. Set up mode

۲. CLI

۲.۱.۱ Set up mode

هنگامی که روتر و یا بعضی از سویچ های سیسکو برای بار اول راه اندازی می کنید وارد set up mode شده، می توانید تنظیمات اولیه را انجام دهید.

در اینجا توضیحاتی در باره سخت افزار دستگاه، تعداد و نوع پورت ها وجود دارد. اما مسئله مهم، خط آخر است. در این خط پرسیده می شود که آیا قصد داریم عیار کردن دستگاه را ادامه بدهیم. اگر جواب ما Y - Yes باشد و انتر بزنیم، عملاً وارد یک رشته از پرسش و پاسخ خواهیم شد که باعث انجام یک عیار سازی اولیه طبق استانداردهای مدنظر خود سیسکو می شود. در صورتی که قصد داشته باشیم که تنظیمات را مشخصاً انجام داده و وارد این پرسش و پاسخ نشویم، حرف N - NO را انتخاب کرده و دکمه انتر را فشار می دهیم.

```
IOS Command Line Interface

unable
to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may
be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of
memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/
no]:
```

شکل (۱-۲) محیط خط فرمان

۲.۱.۲ (Command Line Interface) CLI محیط خط فرمان

عبارت از محیطی است که می‌توانید تنظیمات بیشتری را روی روتر (Router) و سویچ (Switch) انجام دهید. CLI یک محیط قدرتمند text base است که استفاده کننده (user) دستورات مورد نظر خود را تایپ می‌کند. البته باید بگوییم که محیط خط فرمان (CLI) تنها روش پیکربندی وسایل سیسکو نیست. این وسایل را بعدها از طریق مرورگر وب و یا حتی با یک سلسله نرم‌افزارهای مدیریت شبکه نیز می‌توان عیار سازی یا مدیریت کرد. اما از مرورگرها و نرم‌افزارها زمانی می‌توان استفاده کرد که وسیله سیسکوی مدنظر، دارای IP Address باشد. شکل ذیل محیط CLI را نشان می‌دهد.

```
IOS Command Line Interface

Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>ena
Router>enable
Router#
Router#
Router#confi
Router#configure
Router#configure terminal
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

شکل (۲-۲) مودهای خط فرمان

۲.۲ مشخص‌کننده توانمندی‌ها و قابلیت‌های سیستم عامل روتر

مصرف اول: به معنای این می‌باشد که نسخه IOS موجود، برای قابلیت IP Routing به صورت ویژه طراحی شده است. مقادیر و حروفی که به صورت معمول شما می‌توانید در این قسمت مشاهده کنید، معمولاً به شکل ذیل می‌باشد:

a – aapn

a² – atm

a³ – SNA Switching

b – appletakl

c – Communication Servers etc

I – ip

J – enterprise

l – IPX

n – Novell

f – firewall

p – Service Provider

v – voice

مصرف دوم: دسته‌یی از قابلیت و ویژگی‌ها می‌باشد که یک طراح یا مدیر شبکه باید متناسب با نیازها و طراحی خود از این ویژگی‌ها استفاده نماید. تفاوت در انتخاب این گروه از ویژگی‌ها تفاوت چشم‌گیری در قیمت خرید تجهیزات ایجاد می‌کند.

IB Bass

IP Services

Advanced IP Services

Enterprise Services

Advanced Enterprise Services

۱. **IP Base:** همان گونه که احتمالاً حدس می‌زنید، این IOS بسیار پایداری و دارای حداقل امکانات است که معمولاً به صورت رایگان و به همراه دستگاه به شما ارائه می‌شود.

نکته: Enterprise Base یا entbase بسیار شبیه به IP – Base است با این تفاوت که Multi – Protocol است و از پروتوکول‌های مختلفی؛ چون: (Various IBM Protocol, AppleTalk, IPX) پشتیبانی می‌کند. سیسکو در بسیاری از دستگاه‌های جدید خود این نسخه را به عنوان IOS رایگان اولیه ارائه می‌کند.

۲. **IP – Services:** در این IOS امکانات فراوانی از جمله (EIGRP / OSPF, BGP, GLBP, QOS, NAT, HA, VRF – Lite, Net flow, Advance Multicast) و غیره را در اختیار دارید که به همین دلیل باید ابتدا نیاز این سرویس‌ها را احساس کنید، سپس اقدام به انتخاب IOS خود نمایید.

۳. **Advanced IP Services:** این IOS خود دربرگیرنده انواع ذیل است. بنابراین به امکانات سه IOS زیر دقت کنید. همه آن‌ها بر علاوه امکاناتی؛ چون تنظیمات امنیتی بسیار پیشرفته IPV6، سرویس‌های مخصوص ارائه‌دهندگان سرویس‌های بزرگ (Service Provider Services) و ... در این IOS وجود دارند.

مجموعه این IOS عبارت انداز:

- **Advanced Security:** شامل امکاناتی؛ چون (VPN, DES Enct, IPSec, IDS, IOS Firewall, SSH و ...) می‌باشد.
- **SP Services:** شامل امکاناتی؛ چون (MPLS و SSH, ATM, VOATM) می‌باشد.
- **IP Voice:** شامل امکاناتی؛ چون (VOIP, VOFR, IP Telephone) می‌باشد.

۴. **Enterprise Services:** برای دانستن امکانات این مجموعه، کافیست مجموعه‌های (Enterprise Base, IP Voice و SP Services) را با قابلیت‌هایی؛ چون ارائه سرویس‌های Service Provider و پشتیبانی کامل از IBM. اضافه کنید

۵. **Advanced Enterprise Services:** (Enterprise Services و Advanced IP Services) یا بهتر است بگوییم Full Cisco IOS Software. کامل‌ترین سیستم‌عامل سیسکو (IOS) بوده که دارای قیمت بسیار بالایی می‌باشد و کاربرد خاص خود را دارد.

۲.۳ مشخصه نحوه اجرا و مکان اجرای سیستم عامل

این قسمت نشان دهنده محل قرارگیری IOS حرف (m) و نوع فشرده سازی آن حرف (z) است.

دیگر گزینه های موجود برای محل قرارگیری عبارت انداز:

m: در حافظه RAM

r: در حافظه ROM

f: در حافظه Flash

i: محل قرارگیری IOS در هنگام بوت و اجرای دستورات عوض می شود.

دیگر گزینه های موجود برای فشرده سازی عبارت انداز:

z: فشرده سازی Zip

z: فشرده سازی mzip

w: فشرده سازی با الگوریتم STAC

۲.۴ مشخصه نسخه و بروز رسانی Update سیستم عامل سیسکو (IOS)

اعداد مانند 3.12 یا 28-122 به معنای نسخه IOS و نمایانگر آخرین Patch یا بسته به روز رسانی که روی آن وجود دارد، می باشد.

مشخصه نهایی

اول تر از همه بدانید که ممکن است، در اینجا ترکیبی از یک یا چند تا از حروف T و S و E و B را مشاهده کنید. هر یک بیانگر موضوعاتی می باشد که در ذیل آن را توضیح می دهیم.

T. برخی ویژگی های جدید اضافه شده و برخی نقایص و ایرادات (دقت کنید نقایص و ایرادات و خطاها نه صرفاً باگ های کوچک) برطرف شده اند.

S. برخی ویژگی های محکم کاری ها (Consolidation) و تهدیدات امنیتی، رفع بعضی نقایص و ایرادات.

E. نشان می دهد این IOS مربوط به سازمان های بزرگ و Service Provider ها است. در این نسخه برخی ایرادات رفع شده اند. ضمن اینکه امکاناتی مخصوص Service Provider ها، و تنظیمات و قابلیت های پیشرفته (Security، Firewall، Voice و QOS) اضافه شده اند.

B. برخی امکانات مخصوص سرویس های (+ Broadband) رفع برخی نقایص و مشکلات.

K9. این علامت بدین معناست که شما می‌توانید Encryption داشته باشد با کلیدی به طول بیش از 64 بایت.

۲.۵ ویژگی‌های سیستم‌عامل سیسکو (IOS)

عملکرد اصلی Cisco IOS این است که ارتباطات اطلاعات بین دستگاه‌های شبکه را فعال می‌نماید.

- عملیات روتینگ و سوئیچینگ (مسیریابی و تعویض)
- قابلیت توسعه و تغییر پیکربندی شبکه
- دستیابی ایمن به منابع شبکه
- امنیت ترافیک شبکه Network Security
- رمزگذاری Encryption
- احراز هویت Authentication
- قابلیت Firewall
- اجرای خط مش Policy Enforcement

IOS دارای نسخه‌های متفاوتی است که هر نسخه دارای ویژگی‌ها و خصوصیات منحصر به فرد خود می‌باشد؛ ولی ساختار اولیه دستورات پیکربندی در همه آن‌ها مشابه می‌باشد.

۲.۶ IOS و ضرورت استفاده از آن

یک روتر یا سوئیچ بدون وجود یک سیستم‌عامل، قادر به انجام وظایف خود نمی‌باشد- مانند یک کامپیوتر. شرکت سیسکو سیستم‌عامل Cisco IOS را برای محصولات شبکه‌یی خود طراحی و پیاده‌سازی نموده است. نرم‌افزار فوق، جزء جدا ناپذیر در معماری نرم‌افزار روترهای سیسکو می‌باشد و همچنین به‌عنوان سیستم‌عامل در سوئیچ‌های Catalyst ایفای وظیفه می‌کند. بدون وجود یک سیستم‌عامل، سخت‌افزار قادر به انجام هیچ‌گونه عملیاتی نخواهد بود.

۲.۷ ماهیت اینترفیس IOS

نرم‌افزار IOS از یک اینترفیس خط دستوری و یا CLI (Command – Line Interface) استفاده می‌نماید. IOS یک تکنالوژی کلیدی است که از آن در اکثر خطوط تولید محصولات شرکت سیسکو استفاده می‌شود. عملکرد IOS با توجه به نوع دستگاه‌های بین شبکه‌یی متفاوت می‌باشد. برای دستیابی به محیط IOS از روش‌های متعددی استفاده می‌شود.

Console Session: در این روش با استفاده از یک اتصال سریال (Serial) با سرعت پایین، کامپیوتر و یا دستگاه ترمینال را مستقیماً به پورت کنسول روتر متصل می‌کنند.

ارتباط Dialup: در این روش با استفاده از مودم و از طریق پورت کمکی (AUX) با روتر ارتباط برقرار می‌شود. سرویس شبکه‌یی خاص بر روی روتر پیکربندی شده است.

استفاده از Telnet: در این روش می‌باید حداقل یکی از اینترفیس‌ها با یک آدرس IP پیکربندی شود و Virtual Terminal Session برای Login و رمز عبور پیکربندی شده باشد. برای دستیابی به بخش رابطه کاربر روتر و یا سوئیچ از یک برنامه ترمینال استفاده می‌شود.

Hyper Terminal متداول‌ترین گزینه در این رابطه می‌باشد. Cisco IOS سیستم‌عامل قدرتمند با تمام ویژگی‌ها و توانایی‌های لازم است که در عین قدرتمندی بسیار ساده و کارآمد طراحی شده است. به خاطر داشته باشید که سیستم‌عامل قادر است تا تمام مسیرهای سیسکو را راه‌اندازی نماید، باید از تمام ویژگی‌های آن‌ها حمایت کند تا بتواند با استفاده از آن، هر مسیر را در هر محیط تنظیم و پیکربندی کرد. این سیستم‌عامل فرامین توابع زاید و بی‌مصرفی که به‌صورت ندرت مورد استفاده قرار بگیرد، ندارد.

۲.۸ ارتقای سیستم‌عامل دستگاه سیسکو

تغییر و نصب IOS با سیستم‌عامل سوئیچ و روتر سیسکو یکی از مواردی است که توسط مدیر شبکه کمپیوتری یک سازمان صورت می‌گیرد. دلیل این کار را می‌توان در موارد ذیل خلاصه کرد:

- مانند بقیه نرم‌افزارها، سیستم‌عامل دستگاه‌ها نیز دارای نقاط ضعف امنیتی هستند که به‌مرور زمان توسط تولیدکنندگان شناسایی شده و در نسخه‌های جدید سیستم‌عامل اصلاح می‌شوند.
- اضافه شدن امکانات جدید به سیستم‌عامل، همواره مدنظر ایجادکنندگان سیستم‌عامل بوده است.
- همیشه به‌روزر بودن (update) و به‌روز نگه‌داشتن دستگاه‌ها به‌عنوان یک اصل مهم در وظیفه مدیران است.

۲.۹ نسخه‌های IOS

هر سیستم مسیریاب (Router) با نسخه‌ای اصل Cisco IOS عرضه می‌شود و به‌طور ذاتی حداقل از یکی از پروتوکول‌های مسیریابی مانند (IP و IPX) حمایت می‌کند. حال وقتی می‌خواهید آن را به‌گونه‌ی ارتقا دهید که هم‌زمان بخواهید از هر دو پروتوکول حمایت کند، باید نسخه IP / IPX Feature Pack را تهیه و نصب کنید. برخلاف سیستم‌عامل PC که نسخه‌ای اصلاحی (Service Pack) فقط سیستم‌عامل را ارتقا داده و از آن نواقص را رفع می‌کند.

Feature Pack نسخه‌ای ارتقا دهنده نیست؛ بلکه به‌طورمعمول کل سیستم را در خود دارد و از نو آن را نصب می‌کند. لذا وقتی یک Feature Pack را به روی مسیریاب خود نصب می‌کنید، باید مطمئن شوید که این نسخه تمام قابلیت‌ها و عملکردهای مطلوب شما را در خود دارد؛ مثلاً: اگر شما بر روی سیستم خود نسخه‌ی که از Pack IP Feature دارید و می‌خواهید سیستم خود را به نسخه‌های که از IPX نیز حمایت کند، ارتقا دهید؛ (یعنی هر دو را هم‌زمان داشته باشید) باید IP / IPX Feature Pack را از ابتدا نصب کنید و نمی‌توانید IPX Pack Feature را اضافه به سیستم قبلی مانند Service Pack در PC نمایید.

۲.۱۰ مودهای عیارسازی خط فرمان CLI

نخستین مود به نام User Mode و یا Exec Mode یاد می‌شود. وقتی وارد CLI شویم، مستقیماً وارد این مود می‌شود. علامت این مود > است؛ یعنی نام Device که در برابرش علامت > قرارگرفته است. مانند Router>

این مود صرفاً حالت دروازه ورودی را دارد و از طریق آن وارد کنسول می‌شویم. در این مود دستورهای کمی وجود دارد و برای رفتن به مود بالاتر از دستوری Enable استفاده می‌کنیم. مود بالاتر به نام‌های (Enable Mode و یا Privilege Mode) یاد می‌شود. هرگاه در برابر نام Device، علامت # وجود داشته باشد، یعنی در این مود قرار داریم. دستوراتی بیشتری در این مود قابل استفاده هستند. مانند Router#

با دستور Configure Terminal به مود بالاتر و قوی‌تری به نام Config Mode یا Global Mode رفته می‌توانیم. اکثر دستورات اصلی و اجرایی در این مود قابل استفاده می‌باشد. کار این مود به‌صورت ذیل است:

Router (Config) #

در شکل زیر، می‌توان چگونگی حرکت از User Mode به Global Mode را مشاهده کرد:

Router>

Router>enable

Router#

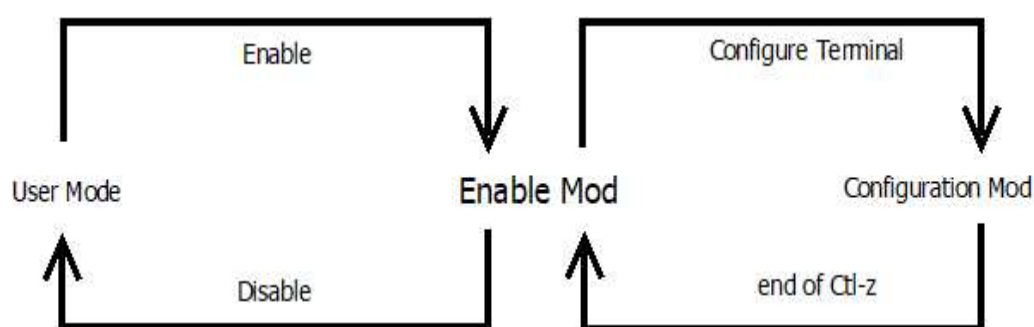
Router# configure terminal

Router (config)#

اگر بخواهیم از یک مود به مود قبلی برگردیم، در همه مودها می‌توان از دستور Exit استفاده کرد. یعنی در هر مودی که باشیم، توسط دستور Exit می‌توانیم به مود قبلی باز گردیم.

البته دستورات دیگری نیز وجود دارد. اگر دقت کرده باشید، برای اینکه از User Mode به Privilege Mode برویم، دستورات enable را وارد می‌کردیم. دقیقاً با دستور disable هم می‌توانیم معکوس این حرکت را انجام دهیم، یعنی از Privilege Mode به User Mode باز گردیم، از Global Mode هم می‌توانیم با وارد کردن دستور end به Privilege Mode برگردیم.

کلید ترکیبی Ctrl + Z ما را از هر مود مستقیماً به Privilege Mode برمی‌می‌گرداند. شکل ذیل را در نظر بگیرید.



شکل (۲-۳) مودهای محیط خط فرمان

تایپ دستورات در محیط خط فرمان (CLI) ساده است. شما لازم نیست که دستور Configure Terminal را به صورت کامل وارد کنید، کافی است وارد کنید. Conf t در اینجا خود editor متوجه می‌شود که منظور از این دستور خلاصه، دستور Configure Terminal می‌باشد. یا به جای enable صرفاً کافی است وارد کنید: ena. خود editor بقیه دستور را حدس می‌زند و اجرا می‌کند. اگر دستوری که قصد نوشتن آن را دارید، اختصاصاً مربوط به همان مود باشد، کافی است یکی دو حرف اول را تایپ کنید، کلید TBA را از صفحه کلید فشار دهید تا خود editor بقیه آن دستور را تکمیل نماید. همچنان شما می‌توانید از کمک (help) استفاده کنید. در هر مودی که باشید با تایپ علامت (?) تمام دستورات آن مود به شما نمایش داده می‌شود.



(IOS) سیستم عامل وسایل شرکت سیسکو می باشد. از آن برای کنترل روتینگ و سوئیچینگ دستگاه ها در شبکه های بزرگ و کوچک استفاده می شود. سیستم عامل IOS مجموعه یی کامل از ابزارها و فرامینی است که به مسئول شبکه کمک می کند تا Router یا Switch سیسکو را پیکربندی و مدیریت کند.

عمدتاً هر یک از سیستم عامل های روتر یا سوئیچ سیسکو، بنابر قابلیت ها و امکانات دسته بندی می شوند و این تفاوت بیانگر قیمت هر یک از آنها است. IOS سیسکو دارای محیط خط فرمان (CLI) قدرتمند است. نام استفاده کننده (User) می تواند، تمام دستورات خود را در آن بنویسد. دارای سه مود مهم می باشد که مود اول آن به نام user mode مود دوم آن به نام privilege mode و مود سوم آن به نام Global mode یاد می شود.

IOS سیسکو دارای قابلیت های زیادی می باشد که چند قابلیت آن را ذکر می کنیم:

۱) عملیات Routing و Switching (مسیریابی و تعویض)؛

۲) قابلیت توسعه و تغییر پیکربندی شبکه؛

۳) دستیابی امن به منابع شبکه؛

۴) امنیت ترافیک شبکه Network Security

۵) رمزگذاری Encryption

۶) احراز هویت Authentication

۷) قابلیت فایروال Firewall

برای دستیابی به محیط IOS از روش های Console Session، Dialup و Telnet استفاده وسیع صورت می گیرد.



- (۱) سیسکو IOS را مختصراً تشریح نمایید.
- (۲) سیسکو IOS را با معرفه Advanced Enterprise Services را تشریح نمایید.
- (۳) ویژگی‌های سیستم عامل سیسکو (IOS) را برشمارید.
- (۴) قابلیت‌های سیستم عامل سیسکو (IOS) را شرح دهید.
- (۵) ماهیت IOS – Interface را شرح دهید.
- (۶) روش‌های دستیابی به محیط IOS را شرح دهید.
- (۷) محیط خط فرمان (CLI) را واضح سازید.
- (۸) مودهای محیط خط فرمان (CLI) را شرح دهید.
- (۹) برای رفتن از User Mode به مود بالاتر از کدام دستور استفاده می‌شود؟ واضح سازید.
- (۱۰) Config – mode را به‌طور خلاصه واضح سازید.



۱. با استفاده از packet tracer تنظیمات مودهای مختلف محیط خط فرمان، در روتر اجرا نمایید.
۲. کارکرد نسخه‌های مختلف سیستم عامل روتر را باهم مقایسه نمایید.
۳. ویژگی‌های سیستم عامل روتر را در گروپ‌های کوچک با هم صنفیان خود بحث نمایید.

فصل سوم

روترهای سیسکو Cisco Routers



هدف کلی: آشنایی با روتر، تنظیم‌های ابتدایی روتر و محیط CLI.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. اجزای داخلی روتر را توضیح داده بتوانند.
۲. مراحل Boot شدن IOS را توضیح داده بتوانند.
۳. تنظیمات ابتدایی روتر را انجام داده بتوانند.
۴. محیط CLI روتر و Mode‌های آن را توضیح کرده بتوانند.
۵. انواع پسوندها را تنظیم کرده بتوانند.
۶. نحوه تنظیم اینترفیس‌های روتر را تشریح کرده بتوانند.

در این فصل اجزای داخلی روترهای سیسکو را تحت مطالعه قرار می‌دهیم. شرکت سیسکو روترهای خود را در انواع و مدل‌های مختلفی ارائه می‌کند که تفاوت این مدل‌ها در قابلیت‌های سخت‌افزاری آن‌ها نهفته است. انجینران و طراحان شبکه باید با این نوع تفاوت‌ها آشنایی حاصل نمایند. تا وقتی از یک سلسله (series) خاص از روترها صحبت می‌شود. باید بدانیم که با چه ترکیب سخت‌افزاری سروکار داریم، مثلاً: وقتی بدانیم در یک سلسله (series) از روترها از ISDN پشتیبانی نمی‌شود. دیگر وقت خود را برای تنظیم و پیکربندی آن تلف نخواهیم کرد. مراحل بوت (Boot) شدن سیستم عامل روتر و تنظیمات ابتدایی روتر توضیح داده شده است. محیط خط فرمان (CLI) در روتر و مودهای آن تشریح شده، انواع مختلف پسوردها در روتر و تنظیم انترفیس‌ها به صورت اساسی تشریح شده است.

۳.۱ سخت افزار روترهای سیسکو

سخت افزار عبارت از تمام اجزای روتر که قابلیت لمس کردن را داشته باشد، به نام سخت افزار یاد می‌شود. سخت‌افزار روتر را می‌توانیم به دو بخش تقسیم کرد:

۱. سخت‌افزار داخلی: سخت‌افزار داخلی یک روتر شبیه به ساختار داخلی یک کامپیوتر شخصی می‌باشد و قطعاتی؛ مانند RAM و CPU مدارات داخلی (chip) را شامل می‌باشد و بر روی مادربرد روتر به شکل ثابت نصب می‌باشند.
۲. سخت‌افزار خارجی (قابل مشاهده): سخت‌افزار خارجی هم شامل پورت‌های اتصال به روتر برای پیکربندی پورت اتصال به برق و کلید خاموش و روشن کردن روتر، اینترفیس‌های مخصوص شبکه‌های (LAN، کارت‌های توسعه برای WAN و جعبه اصلی روتر) بوده و از بیرون قابل مشاهده است.

۳.۱.۱ عناصر داخلی روتر (Router Internal elements)

استفاده از روترها در شبکه به امری متداول تبدیل شده است. یکی از دلایل مهم گسترش استفاده از روتر، ضرورت اتصال یک شبکه به چندین شبکه دیگر (انترنت و یا سایر سایت‌هایی از راه دور) در عصر حاضر است. نام در نظر گرفته شده برای روترها، متناسب با کاری است که آنان انجام می‌دهند، ارسال دیتا (data) از یک شبکه به شبکه دیگر؛ مثلاً: در صورتی که یک شرکت دارای یک شعبه در کابل و یک دفتر دیگر در ننگرهار باشد، به منظور اتصال آنان به یکدیگر می‌توان از یک خط Leased اختصاصی که به هریک از روترهای موجود در دفاتر متصل می‌شود، استفاده نمود. بدین ترتیب، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود، از طریق روتر صورت می‌گیرد و تمامی ترافیک‌های غیرضروری دیگر، فیلتر و در پهنای باند (Bandwidth) و هزینه‌های مربوطه، صرفه‌جویی می‌شود.

۳.۱.۲ واحد پردازش مرکزی (CPU)

واحد پردازش مرکزی مسئولیت اجرای دستورالعمل‌ها در سیستم عامل سیسکو را برعهده دارد. مقداردهی اولیه (Initialization)، عملیات (Routing Process) و غیره از جمله وظایف یک پردازنده می‌باشد. بسیاری از روترهای سیسکو از پردازنده‌های نوع RISC موتورلا خانواده 68000 استفاده می‌کنند که سرعتی در حدود 200 مگاهرتز را دارا می‌باشند. این پردازنده‌ها برای عملیات محاسباتی پیچیده که روتر بدان احتیاج دارد، بسیار مناسب هستند. یکی از ویژگی‌های این نوع پردازنده‌ها (CPUs) آن است که با توان مصرفی بسیار پایین، عملکرد مناسبی از خود نشان می‌دهند. از آنجایی که پردازنده (CPU) روتر انرژی زیادی مصرف نمی‌کند؛ لذا حرارت زیاد تولید نمی‌کند. این ویژگی مهم باعث می‌شود که مسیریاب (Router) های سیسکو به پکه‌های خنک کننده پردازنده نیاز نداشته باشند. همین ویژگی باعث می‌شود که روترهای سیسکو، بی‌سر و صدا، کم مصرف و از لحاظ حجمی، کوچک و ظریف باشند.

۳.۱.۳ حافظه اصلی (RAM)

از این حافظه به منظور ذخیره اطلاعات جدول روتینگ، صف‌های بسته‌های اطلاعاتی، اجرای پیکربندی (Configuration Implementation) و Cache، سوئیچینگ سریع استفاده می‌شود. در اکثر روترها، حافظه RAM، فضای زمان اجرا (Runtime) برای نرم افزار IOS و زیر سیستم‌های مربوطه را فراهم می‌نماید. حافظه RAM منطقاً به دو بخش (حافظه پردازنده اصلی و حافظه ورودی و خروجی مشترک) تقسیم می‌شود.

از حافظه ورودی و خروجی مشترک (Shared) توسط اینترفیس‌ها و به منظور ذخیره موقت بسته‌های اطلاعاتی استفاده می‌شود. با توجه به تکنالوژی استفاده شده در ساخت اینگونه حافظه‌ها، پس از خاموش کردن و یا روشن شدن دوباره روتر، اطلاعات موجود در حافظه RAM حذف می‌شود. حافظه‌های فوق معمولاً از نوع (DRAM حافظه RAM) پویا بوده و می‌توان با افزودن ماژول‌های DIMMs ظرفیت آنان را تغییر و افزایش داد.

۳.۱.۴ حافظه پایدار (Non – Volatile RAM(NVRAM)

این نوع حافظه از نوع حافظه‌های پرسرعت است و همان گونه که از نامش پیداست پایدار می‌باشد، یعنی با خاموش شدن یا دوباره روشن شدن (Restart) روتر، اطلاعات آن از بین نمی‌رود. اطلاعات مربوط به فایل start-up Configuration روتر در این حافظه قرار می‌گیرد.

فایل Start-up Configuration درواقع همان فایل پیکربندی روتر است و تمام اطلاعات پیکربندی روتر را که شما انجام داده‌اید، در خود دارد.

سیستم عامل روتر سیسکو یا به اختصار IOS به هنگام BOOT کردن روتر از روی این فایل تمام اطلاعات قبلی پیکربندی روتر را می خواند و آن اطلاعات را بر روی روتر اعمال می کند.

۳.۱.۵ حافظه فلش (Flash memory):

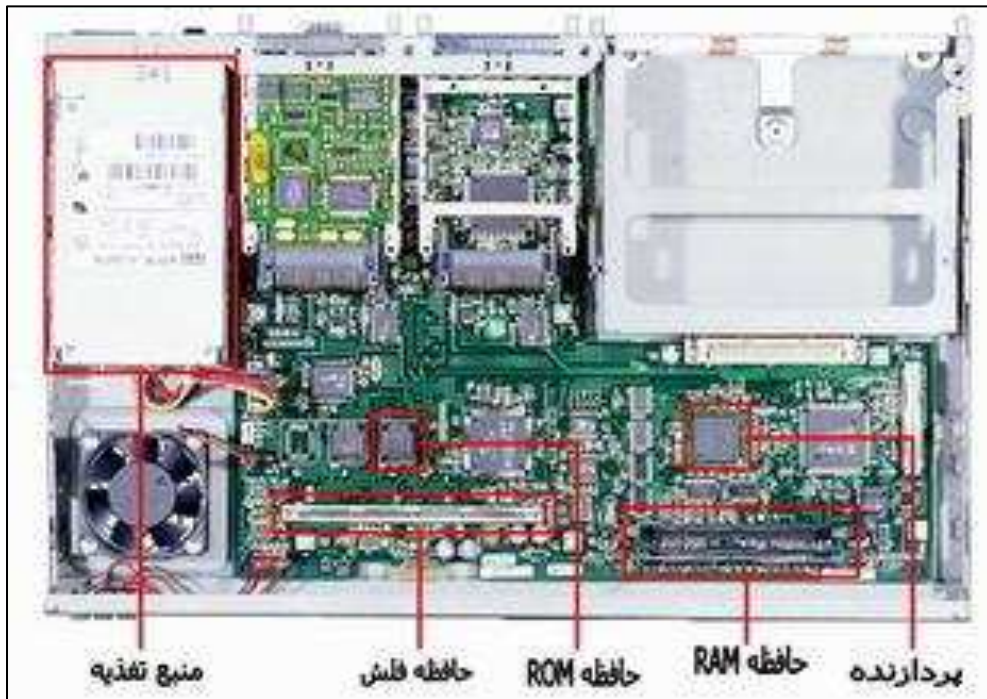
از این نوع حافظه ها به منظور ذخیره نسخه کامل نرم افزار IOS استفاده می شود. روتر معمولاً IOS پیش فرض خود را از حافظه فلش دریافت می نماید. با توجه به تکنولوژی استفاده شده در ساخت اینگونه حافظه ها، همواره می توان نرم افزار ذخیره شده داخل آنان را ارتقا و با یک نسخه جدید جایگزین نمود IOS. ممکن است به صورت فشرده و یا معمولی ذخیره شده باشد. در اکثر روترها یک نسخه اجرایی از IOS در زمان راه اندازی روتر، به حافظه RAM انتقال می یابد. در سایر روترها IOS ممکن است مستقیماً از طریق حافظه فلش اجرا شود. با افزودن و یا تعویض ماژول های SIMMs و یا کارت های PCMCIA، می توان ظرفیت حافظه فلش را ارتقا داد. در شماره ماژول مسیریاب های سیسکو، هرگاه بعد از نام ماژول علامت R درج شده باشد، بدین معناست که راه اندازی و اجرای برنامه های روتر، از طریق RAM داخلی انجام می شود.

۳.۱.۶ گذرگاه (Buses)

اکثر روترها شامل یک گذرگاه سیستم و یک گذرگاه پردازنده می باشد. از گذرگاه سیستم به منظور مبادله اطلاعات بین پردازنده و اینترفیس ها و یا تجهیزات جانبی نصب شده در یکی از سلات (Slot) های سیستم، استفاده می شود. گذرگاه فوق مسئولیت مبادله بسته های اطلاعاتی به اینترفیس ها را برعهده دارد (دریافت و ارسال). گذرگاه پردازنده توسط پردازنده و به منظور دستیابی عناصر از طریق حافظه اصلی روتر استفاده می شود. این گذرگاه مسئولیت مبادله دستورالعمل ها و دیتا (data) به یک آدرس خاص از حافظه را برعهده دارد (ذخیره و بازیابی).

۳.۱.۷ حافظه ROM

از این نوع حافظه به منظور ذخیره دائم کد خطیابی (Debugging) راه انداز (ROM Monitor) استفاده می شود. مهم ترین وظیفه حافظه ROM، تست و عیب یابی سخت افزار در زمان راه اندازی روتر و استقرار نرم افزار IOS از حافظه فلش به داخل حافظه RAM می باشد. برخی روترها دارای یک نسخه خاص و سبک تر از IOS می باشند. می توان از آن به عنوان یک گزینه و منبع جایگزین در زمان راه اندازی روتر استفاده نمود. اطلاعات موجود در اینگونه حافظه ها را نمی توان حذف نمود و در صورت نیاز به ارتقا، باید مدار مجتمع و یا ای سی (Integrated circuit) مربوطه را تعویض نمود. نوع عناصر و محل نصب آنان در روترها با توجه به ماژول آنان می تواند متفاوت و متغیر باشد. شکل زیر عناصر اصلی داخلی در یک روتر 2600 را نشان می دهد.



شکل (۳-۱) نمای عناصر داخلی روتر

برعلاوه اجزای فوق، می‌توان توانایی روترهای سیسکو را با اضافه نمودن مادیول‌های مختلف با خدمات بیشتر عیار نمود و بلند برد.

۳.۲ سخت‌افزار خارجی روتر

۳.۲.۱ پوش (جعبه) Case

شاید صحبت در رابطه با پوش یک پورت، عجیب به نظر برسد، ولی باید توجه کرد که برای طراحی بدنه یک روتر، بسیاری مورد توجه قرار گرفته است تا استفاده از آن برای مهندسان شبکه راحت باشد. بدنه در روترهای سیسکو دارای رنگ آمیزی خاصی است و نشان (logo) شرکت معمولاً در سمت چپ قرار دارد. و شماره سلسله (series) مربوط به آن روتر در سمت راست قرار می‌گیرد. معمولاً روترهایی که در آن شماره سلسله (series) و نشان شرکت در پیش روی بدنه قرار می‌گیرند، برای نصب در Rack طراحی شده‌اند و به مدل‌های تجاری از روترهای سیسکو تعلق دارند. البته در مدل‌هایی که برای شبکه‌های کوچک طراحی می‌شوند، شماره سلسله (series) بر قسمت بالایی بدنه روتر قرار دارد و این نوع از روترها برای قرارگرفتن بر روی میز یا نصب بر روی دیوار طراحی شده‌اند. در روترهای سیسکو معمولاً پورت‌های اتصال و دکمه خاموش و روشن در عقب بدنه قرار دارد و برای هر پورت یک جفت چراغ LED برای تعیین وضعیت پورت‌ها در کنار هر پورت در نظر می‌گیرند و به آن‌ها پانال وضعیت (State panel) می‌گویند. پانال وضعیت (panel state) در روترهای تجاری (Enterprise) در پشت روتر و در روترهای خانگی و کوچک معمولاً در روی بدنه قرار دارد.

این چراغ‌ها (پانل وضعیت) برای تشخیص اتصال درست کیبل‌ها، در هرپورت و همچنین تعیین نرخ خطا به روی پورت‌های اینترنت یا WAN مورد استفاده قرار می‌گیرند.



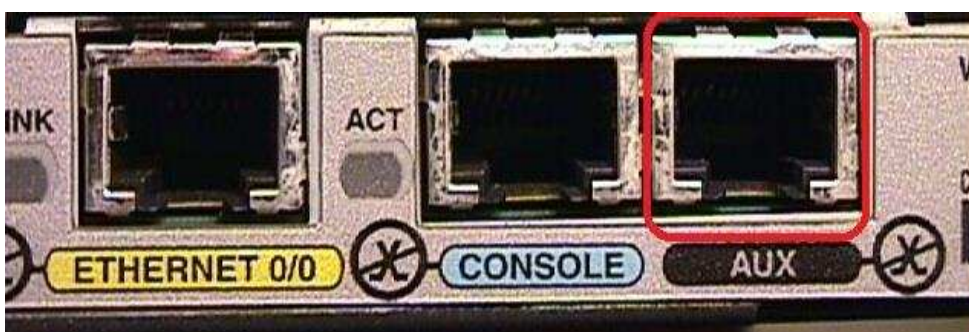
شکل (۲-۳) بدنه (جعبه) Case روتر

۳.۲.۲ پورت‌های کنسول Console و AUX

از جمله پورت‌هایی است که در پشت روترهای سیسکو قرار دارند. پورت کنسول اولین راه برقراری ارتباط با روتر سیسکو محسوب می‌شود. از طریق وصل یک کیبل مخصوص، به نام Rollover Cable به این پورت، می‌توانید روتر را به یک کامپیوتر متصل کرده و از طریق آن کامپیوتر اقدام به پیکربندی روتر نمایید. پورت کنسول از لحاظ ظاهری شبیه به پورت RJ-45 می‌باشد؛ اما تفاوت‌هایی از لحاظ کارکرد با آن دارد، به همین دلیل برای اتصال کامپیوتر به پورت کنسول، کیبل مخصوصی وجود دارد که به همراه روتر به شما فروخته می‌شود. همچنین با استفاده از پورت Auxiliary یا به اختصار AUX. شما می‌توانید یک مودم را به روتر (Router) تان وصل کرده و کاربر نیز با اتصال به این مودم از طریق اتصال از راه دور اقدام به پیکربندی روتر نماید.



شکل (۳-۳) انجام‌های کیبل ارتباطی Console



شکل (۴-۳) ساختمان پورت‌های AUX، کنسول و اترنت

۳.۲.۳ خط اتصال (LAN Interface)

از این نوع خط اتصال (Interface) برای اتصال روتر به شبکه‌های محلی، مانند Token Ring Ethernet و یا شبکه‌های محلی مبتنی بر فیبر نوری (FDDI) استفاده می‌شود.

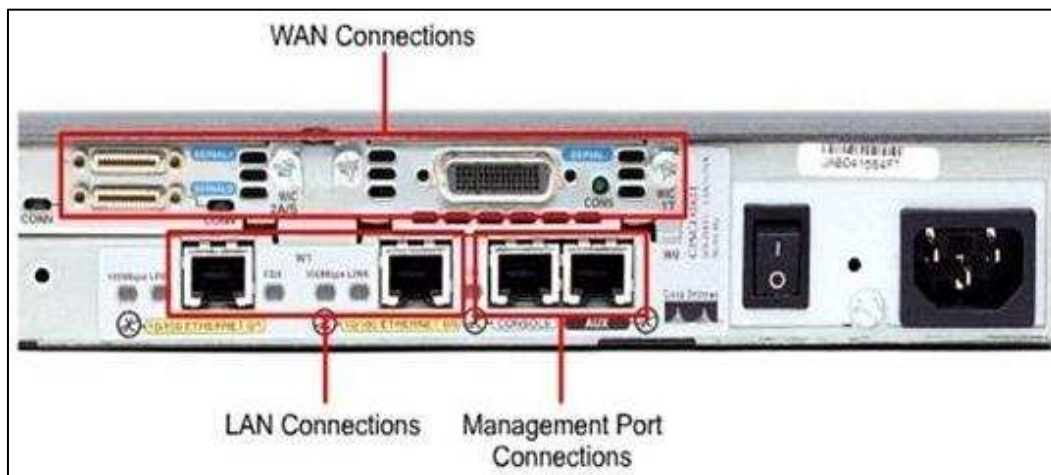
بسته به نوع و شماره سلیله (series) یک روتر، انترفیس‌های متفاوتی برای اتصال به شبکه‌های محلی وجود دارند که از این میان می‌توان به (Ethernet Interface، Fast Ethernet و Gigabit Ethernet Interface) و همچنین به اینترفیس‌های مخصوص کیبل‌های فیبر نوری اشاره کرد.

انترفیس‌های فوق دارای (chip) کنترلی خاصی می‌باشند که منطق لازم برای اتصال روتر به محیط انتقال شبکه محلی را ارائه می‌نمایند. درواقع عملکرد هر کدام از این نوع انترفیس‌ها همانند کارت شبکه محلی می‌باشد.

۳.۲.۴ خط اتصال (WAN Interface)

بسیاری از روترهای سیسکو قابلیت اتصال به WAN به اختصار WIC نامیده می‌شود، از قبل در محل مربوط، نصب شده است. اغلب کارت‌های اتصال به WAN شامل T1E1 و ISDN می‌باشند و شما می‌توانید از طریق این پورت‌ها به شبکه‌های شهری و یا Ethernet متصل شوید. در اغلب روترهایی که پورت اتصال به WAN را ندارند، یک تیغه فلزی قابل برداشتن، در پشت آن‌ها وجود دارد که شما می‌توانید با برداشتن آن تیغه و قراردادن یک کارت توسعه WAN در محل پورت مربوطه، اقدام به ارتقای روتر خود نمایید. انواع کارت توسعه WAN که می‌توان در یک روتر سیسکو نصب و اضافه کرد، به سلسله (series) و مدل روتر بستگی دارد. روترها از اینترفیس SERIAL برای برقراری ارتباط با استفاده از تکنالوژی ISDN و از اینترفیس T1E1 برای برقراری ارتباط با استفاده از تکنالوژی خطوط استیجاری T1/E1 Lease line مخابرات بهره می‌برند. هر دو تکنالوژی ارتباط، از بستر مخابراتی شبکه‌های شهری (WAN) برای رد و بدل دیتاها استفاده می‌کنند.

همچنین روترها می‌توانند برای اتصال به Ethernet از کارت توسعه مودم آنالوگ یا کارت توسعه ASDL استفاده کنند. البته باید توجه کرد که امروزه استفاده از تکنالوژی مودم آنالوگ، برای اتصال به Ethernet منسوخ شده است.



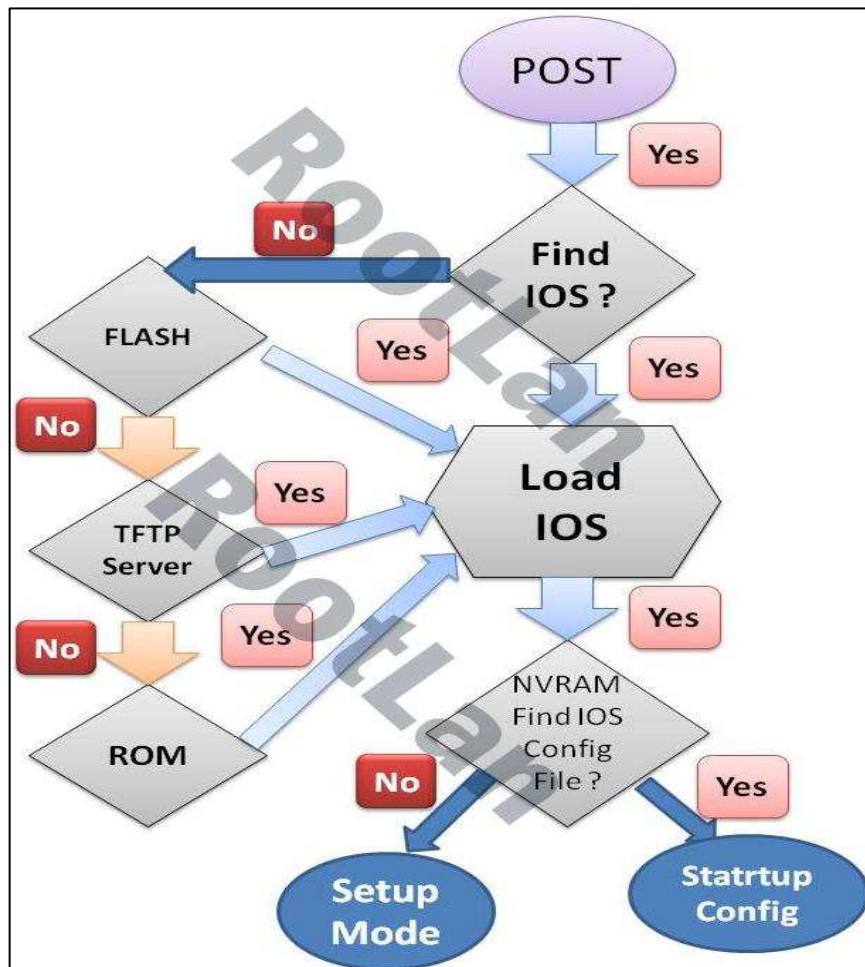
شکل (۳-۵) پورت‌های مدیریتی، WAN و LAN

۳.۳ بوت (Boot) شدن IOS روتر سیسکو

همانطور که می‌دانید، تجهیزاتی مانند روتر و سویچ، دقیقاً مشابه سخت‌افزارهایی اند که شما در کمپیوترهای خانگی یا لپتاپ‌ها دارید. آن‌ها هم یک سیستم کمپیوتری هستند که به جای اینکه در قالب یک لپتاپ یا Case ما از آنها استفاده کنیم، در قالب یک وسیله سخت‌افزاری به شکل یک وسیله (Appliance) از آنها استفاده می‌کنیم.

همه تجهیزات برای خودشان پروسه دارند که از زمان روشن شدن دستگاه تا رسیدن به سیستم عامل مربوطه انجام می‌شود. به این پروسه در اصطلاح روترهای سیسکو، Cisco Boot Sequence یا ترتیب بوت

(Boot) روترهای سیسکو گفته می‌شود. در این پروسه، سخت‌افزارهای سیستم بررسی می‌شوند و در صورت نیاز نرم‌افزارهای وابسته به آنها نیز اجرا می‌شوند تا تمامی آزمایش‌ها بر روی دستگاه قبل از رسیدن به سیستم‌عامل یا همان IOS انجام شده باشد. این پروسه شامل مراحل زیر می‌باشد:



شکل (۳-۶) مراحل بوت (Boot) شدن روتر سیسکو

۳.۴ مراحل بوت (Boot) شدن روتر سیسکو

۱. مانند یک سیستم معمولی کمپیوتری، روتر به محض روشن شدن پروسه Post که مخفف Power On Self – Test است را انجام می‌دهد. Post تمامی سخت‌افزارهای موجود بر روی دستگاه را تست می‌کند و از صحت عملکرد آنها اطمینان حاصل می‌کند. برای مثال تمامی Interface‌های یک روتر تست می‌شوند. نرم‌افزار یا بهتر بگوییم میان افزاری که پروسه POST را در روترها انجام می‌دهد، هم در حافظه ROM ذخیره شده است و هم از همین حافظه اجرا می‌شود.

۲. در مرحله بعدی برنامه‌یی به نام bootstrap که در ROM ذخیره شده است و برای اجرای نرم‌افزارها استفاده می‌شود، مقدار یا Value مربوط به Configuration Register را بررسی می‌کند تا محل

Load کردن IOS روتر را پیدا کند. Value پیش فرض Configuration Register عدد Hexadecimal به شکل x21020 می باشد.

زمانی که Value به شکل x21020 باشد، به این معناست که روتر باید سیستم عامل IOS روتر را از Image که در حافظه Flash روتر وجود دارد، Load کند و همچنین start-up Configuration خود را با سرعت 9600 baud rate برای پورت کنسول تعریف کند. اگر Value به شکل x21020 باشد، بعد از این که این مرحله تمام شد، bootstrap نرم افزار IOS را از حافظه Flash می خواند و Load می کند.

نکته: وظیفه اصلی برنامه Bootstrap، شناسایی سخت افزارها و پیدا کردن نرم افزار IOS روتر و سپس Load کردن Image این نرم افزار است. به صورت پیش فرض، در تمامی روترهای سیسکو IOS از حافظه Flash که روی روترها قرار دارد، Load می شود.

محل دیگری که می توان IOS های روترهای سیسکو را قرارداد تا از آن Load شوند، TFTP سرور است که معمولاً بر روی یک کامپیوتر قرار می گیرد. اگر برنامه Bootstrap نتواند یک Image معتبر پیدا کند، به عنوان ROM Monitor عمل خواهد کرد.

محیط ROM Monitor در واقع یک محیطی CommanZ است که شما می توانید برای برخی از پیکربندی های روتر خود، از قبیل دانلود کردن Image سیستم عامل IOS از TFTP سرور و یا بهبودی یافتن، Recover کردن رمزهای عبور فراموش شده و یا حتی تغییر دادن Configuration Register و برخی دیگر از تنظیمات از آن استفاده کنید.

نکته: منظور از ROMMON، سیستم عاملی بسیار سبک و ساده و با اندک قابلیت ها می باشد. یکی از کاربردهای این سیستم عامل و اجرای آن این است که می توانید در داخل آن اقدام به کپی نمودن فایل IOS به داخل Flash نمایید- در زمانی که فایل IOS قبلی به صورت اتفاقی حذف شده باشد. از دیگر استفاده های آن می توان به انجام عملیات بازیابی رمز عبور یاد کرد.

توجه داشته باشید که شما قادر به هیچگونه دخل و تصرفی در مراحل 1 و 2 نخواهید بود و این در حالیتیست که می توانید مراحل 3 و 4 را دستخوش تغییر قرار دهید. به عنوان مثال، می توان یک Router را به گونه ای پیکربندی نمود که به جای جستجو برای اجرای یک IOS در فضای Flash، اقدام به چنین کاری در یک فضای به اشتراک گذاشته شده در شبکه، مانند یک (TFTP) نماید. همچنین شما می توانید یک Router را طوری پیکربندی نمایید که به جای اجرای فایل startup-config موجود در flash، اقدام به بارگذاری و اجرای آن از طریق فایلی در فضای به اشتراک گذاشته شده در شبکه نماید.

۳. بعد از این مرحله، نرم افزار IOS به دنبال یک Configuration-File معتبر که در NVRAM ذخیره شده باشد، می رود. به این فایل startup-config هم گفته می شود. اگر در این میان در NVRAM فایل

Startup Configuration وجود داشت، روتر از طریق این فایل تنظیمات و دستورات را می‌خواند، اما اگر فایلی در NVRAM پیدا نشد، سیستم عامل IOS روتر System Configuration Setup را نمایش می‌دهد.

۱. زمانی که Startup Configuration به صورت کامل Load شد، IOS به شما خط فرمان User Mode روتر را نمایش می‌دهد.

۳.۵ تنظیمات پیش فرض بالا آمدن یک Router default load

انتخاب IOS از سوی یک Router به دو عامل زیر بستگی دارد:

۱. تنظیمات مرتبط با قابلیت configuration-register

۲. پیکربندی صورت گرفته بر اساس دستور boot system

تنظیم پیش فرض در نظر گرفته شده برای قابلیت Configuration Register عدد 0x2101 می‌باشد، به منظور مشاهده آن، از دستور زیر استفاده کنید:

Router# show version | include register



شکل (۳-۷) تنظیم پیش فرض برای رجیستر

شما می‌توانید با مراجعه به این مستند، معنای عدد مذکور را بیابید. به تصویر زیر که از این مستند استخراج شده است، دقت کنید:

| | |
|--------|---|
| 0x2102 | Ignores Break Books into ROM if initia boot fails 9600 console baud rate default value for mosr platforms |
|--------|---|

بر اساس دستور زیر می‌توانید دریابید که چه IOS‌های در حال حاضر بر روی دستگاه مورد نظر وجود دارند. توجه داشته باشید که در مثال زیر، دستگاه مورد نظر در خانواده محصولات Cisco Router 2800 می‌باشد:

```
Router#show flash: | include c2800
```

```
12 67926080 Apr 2 2015 14:21:46 +00:00 c2800nm-adventerprisek9-mz.151-4.M10.bin
```

```
29 67929600 Nov 4 2016 12:11:22 +00:00 c2800nm-adventerprisek9-mz.151-4.m12a.bin
```

شکل (۳-۸) سیستم عامل روتر

همانطور که در مثال فوق مشاهده می‌نمایید، بر روی Flash دو IOS وجود دارد. لطفاً به اعداد درج شده در کنار فایل‌های IOS دقت کنید. در صورت عدم انتخاب IOS جهت لود شدن از طریق دستور Boot System، در فایل IOS که عدد مرتبط شده با آن کوچک‌تر باشد، اولیت بالاتری جهت لود شدن در هنگام بالا آمدن Router دارد. همچنین به منظور مشاهده IOS که در حال حاضر، Router موردنظر از آن جهت بالا آمدن استفاده نموده است، می‌توانید از دستور زیر استفاده کنید:

```
Router#
```

```
Router#show version | include image
```

```
System image file is "flash0:c2900-universalk9-mz.SPA.151-1.M4.bin"
```

```
Router#
```

بررسی تنظیمات موردنیاز جهت بوت نمودن Router از طریق فایل IOS موجود در Flash دستگاه: در ادامه می‌خواهیم با فرض وجود چندین فایل IOS بر روی Flash یک Router، آن را وادار کنیم که از یک IOS خاص عملیات بوت شدن را به انجام برساند. بدین منظور می‌توانید از دستور Boot System استفاده کنید. به مثال زیر نگاه کنید:

```
Router(config)#
```

```
Router(config)#boot system flash c2800-adventerprisek9-mz.151-4.m12a.bin
```

بررسی تنظیمات موردنیاز جهت بوت نمودن Router از طریق فایل IOS موجود در شبکه

حداقل دو سناریو را می‌توان مورد بررسی قرار داد که بوت نمودن Router از طریق فایل IOS موجود در شبکه می‌تواند برای آن‌ها مفید باشد. در سناریوی اول، فرض کنید که فضای خالی موجود بر روی Flash آنقدر کوچک است که امکان نگهداری از فایل IOS مورد نظر را ندارد. همچنین فرض کنید که در زیر ساخت شبکه سازمان خود از تعداد زیادی Router استفاده می‌کنید. در این صورت، بدون نیاز به کپی کردن فایل IOS بر روی هریک آن‌ها، می‌توان آن‌ها را به‌گونه‌ای پیکربندی نمود که فایل IOS موردنظر شما را از فضای در نظر گرفته‌شده در شبکه، دانلود و سپس به اجرا در آورند.

در هر دو سناریوی فوق، بوت نمودن Router از طریق فایل IOS موجود در شبکه می‌تواند مفید واقع شود و در ادامه به چگونگی انجام این کار اشاره شده است:

```
Router(config)#boot system ?  
WORD    TFTP filename or URL  
flash   Boot from flash memory  
tftp     Boot from a tftp server
```

همانطور که در شکل فوق مشاهده می‌کنید، یکی از گزینه‌های موجود، استفاده از پروتوکول TFTP می‌باشد. در مثال زیر به چگونگی پیکربندی Router موردنظر جهت استفاده از TFTP Server اشاره شده است:

```
Router(config)#boot sys  
Router(config)#boot system tftp c2800nm-adventerprisek9-mz.151-4.ml2a.bin.192.168.1.2
```

پیکربندی فوق مشخص می‌نماید که Router موردنظر به دنبال کدام IOS بر روی کدام TFTP Server باشد. البته توجه داشته باشید که این تنها نیمی از عملیات پیکربندی بوده و این بدان علت است که به صورت پیش فرض، تنظیمات صورت گرفته بر روی قابلیت Configuration Register به گونه‌یی می‌باشد که Router همواره به دنبال یافتن فایل IOS بر روی فضای ذخیره سازی Flash خود می‌باشد. لذا به منظور ادامه عملیات پیکربندی، باید با تغییر تنظیمات Configuration Register از حالت پیش فرض به عبارت X210F اقدام نمایید، به شکل زیر نگاه کنید:

```
Router(config)#  
Router(config)#config-register 0x210F
```

نکته دیگری که باید به آن توجه داشته باشید، این است که باید اطمینان حاصل کنید که Router مورد نظر، امکان دسترسی به TFTP Server را دارد. بدین منظور بر اساس مثال زیر، ابتدا بر روی یکی از interface‌های موجود بر روی Router مورد نظر، پیکربندی زیر را به انجام می‌رسانیم:

```
Router(config)#interface FastEthernet 0/0  
Router(Config-if)#ip address 192.168.1.1 255.255.255.0  
Router(Config-if)#no Shutdown
```

حال با ذخیره تنظیمات صورت گرفته، روی روشن کردن Router، به صحت فعالیت‌های انجام شده خود پی خواهیم برد، به شکل زیر توجه کنید:

```
1 Loading c2800nm-Adventerprisek9-mz.151-4.M12a.bin from 192.168.1.2 (Via Fast Ethernet0/0):  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
[ OK - 6792600 bytes]
```

همانطور که در شکل فوق مشاهده می‌کنید، عملیات load شدن IOS از طریق پروتوکول TFTP با موفقیت صورت پذیرفت.

بررسی تنظیمات موردنیاز جهت بوت نمودن Router از طریق فایل IOS موجود در شبکه در محیط ROMMON: فرض کنید که به دلایلی وجود مشکلات سخت‌افزاری در Flash، امکان ذخیره IOS بر روی آن وجود ندارد. همچنین نتوانسته‌اید قبل از بروز این مشکل، Router را به‌گونه‌ی پیکربندی کنید که از TFTP Server جهت لود IOS استفاده کند. با وجود چنین شرایط پیچیده راه‌حل چیست؟

خوشبختانه به منظور رفع این مشکل، می‌توانید از محیط ROMMON کمک بگیرید. بدین منظور باید در مراحل اولیه بالا آمدن Router، با فشردن ترکیب CTRL و BREAK وارد محیط ROMMON خواهید شد، به شکل زیر توجه کنید:

```
1 System Bootstrap, version 12.4 (13r) T, RELEASE SOFTWARE (fc1)  
  
Technical Support : http://www.cisco.com/techsupport  
  
Copyright (C) 2006 by cisco Systems, Inc.  
  
Initializing memory for ECC  
.....  
  
C2811 Plat form with 786432 Kbytes of main memory  
  
Main memory is configured to 64 bit mode with ECC enabled  
  
Readonly ROMMON initialized  
  
Program load complete, entry point : 0x8000f000, Size : 0xcb80  
  
Program load complete, entry point : 0x8000f000, Size : 0xcb80  
  
Monitor: command "boot" aborted due to user interrupt
```

شکل (۳-۹) محیط ROMMON

در این محیط باید چندین متغیر را تعریف کنید. توجه داشته باشید که اگر چنانچه TFTP Server مورد نظر در Subnet یکسان با Router مورد نظر قرار دارد، نیازی به مشخص کردن آن نیست. به مثال زیر نگاه کنید:

```
rommon 1 > IP_ADDRESS=192.168.1.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.254
rommon 4 > TFTP_SERVER=192.168.1.2
rommon 5 > TFTP_FILE=c2800nm-adventerprise9-mz.151-4.M12a.bin
```

هنگامی که از صحت تنظیمات نمایش داده شده در شکل فوق اطمینان حاصل کردید، باید به Router بفهمانید که IOS مشخص شده را در Flash خود ذخیره سازی نمایید. بدین منظور از دستور زیر استفاده کنید:

```
rommon 6 > tftpdnld -r
```

با اجرای دستور فوق، رویداد زیر به وقوع خواهد پیوست:

```

IP_ADDRESS : 192.168.1.1
IP_SUBNET_MASK : 255.255.255.0
DEFAULT_GATEWAY : 192.168.1.254
TFTP_SERVER : 192.168.1.2
TFTP_FAIL : c2800nm - adventerprise9-mz.151 - 4.m12a.bin
TFTP_VERBOSE : Progress
TFTP_RETRY_COUNT : 18
TFTP_TIMEOUT : 7200
TFTP_CHECKSUM : Yes
TFTP_MACADDR : 00:1d:a1:8b:36:d0
FE_PORT : Fast Ethernet 0
FE_SPEED_MODE : Auto

Receiving c2800nm-adventerprise9-mz.151-4.M12a.bin from
192.168.1.2 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Validating checksum.

loading image c2800nm-adventerprise9-mz.151-4.m12a.bin
program load complete, entry point: 0x8000f000, size: 0x40c8438
Self decompressing the image : ##### [OK]
```

شکل (۳-۱۰) نتیجه دستور tftpdnld -r

همانطور که مشاهده می کنید، تنظیمات صورت گرفته به شما نمایش داده شده و در نهایت، در صورت عدم وجود مشکل در تنظیمات، IOS نظر شروع به دانلود شدن کرده است و نهایتاً کنترل دستگاه به وی سپرده می شود.

۳.۶ تنظیمات ابتدایی روترهای سیسکو (Cisco Router Basic Configuration)

۳.۶.۱ راه‌های دسترسی به تجهیزات سیسکو

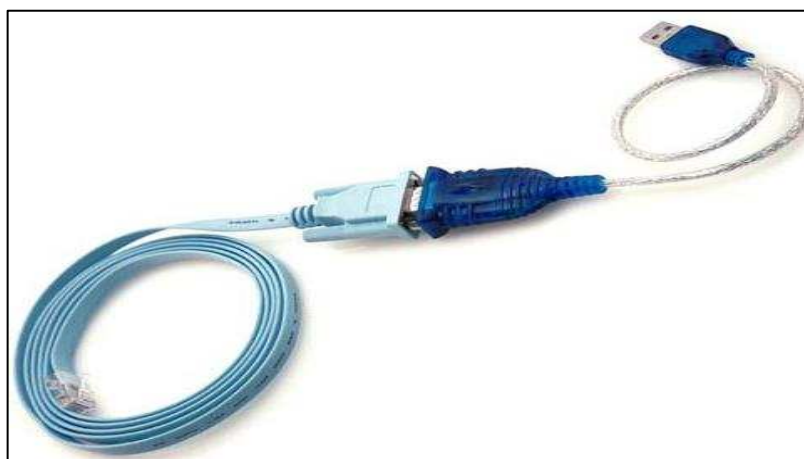
برای دسترسی به روتر و سوئیچ 5 روش وجود دارد. 3 روش جهت دسترسی به CLI و یک روش جهت ارتباط بین TFTP Server و تجهیزات سیسکو و روش آخر تنظیم کردن تجهیزات سیسکو به کمک Web Browser می‌باشد. در این بخش ما قصد داریم روش‌های اتصال به CLI را مورد بحث قرار می‌دهیم. برای اتصال به CLI شما می‌توانید از 3 روش استفاده کنید.

- Console Port
- Telnet
- Auxiliary Port

Console Port: به هنگام که یک روتر یا سوئیچ را بار اول خریداری می‌کنید، هیچ تنظیمی روی آن وجود ندارد؛ بنابراین تنها راه دسترسی به IOS و تنظیم کردن آن استفاده از پورت console می‌باشد. این پورت برای اتصال به محیط خط فرمان (CLI) استفاده می‌شود که در زیر به صورت مفصل به آن خواهیم پرداخت. اتصال به پورت Console روتر یا سوئیچ با استفاده از کیبل Rollover، کیبل Rollover کیبل است که یک سر آن دارای کانکتور RG45 جهت اتصال به پورت Console روتر و یک سر دیگر آن دارای کانکتور 9 پین جهت اتصال به Com Port کامپیوتر می‌باشد. تنها راه ارتباط با سوئیچ یا روتری که تازه تهیه کرده‌اید، استفاده از Console Port است. ابتدا با استفاده از یک کیبل Rollover که یک سرش به پورت Console روتر وصل می‌شود و طرف دیگر به پورت com کامپیوتر وصل می‌شود. در صورتی که کامپیوتر شما، پورت com نداشت، باید از تبدیل com به USB استفاده کنید و پس از نصب کردن نرم‌افزار آن در سیستم عامل، می‌توان از طریق این کیبل به روتر وصل شد. نمونه کیبل‌های کنسول Rollover و همچنین تبدیل com به USB را در زیر مشاهده می‌کنید:



شکل (۳-۱۱) کیبل Rollover



شکل (۱۲-۳) اتصال به کنسول توسط پورت USB



شکل (۱۳-۳) پورت کنسول در روتر

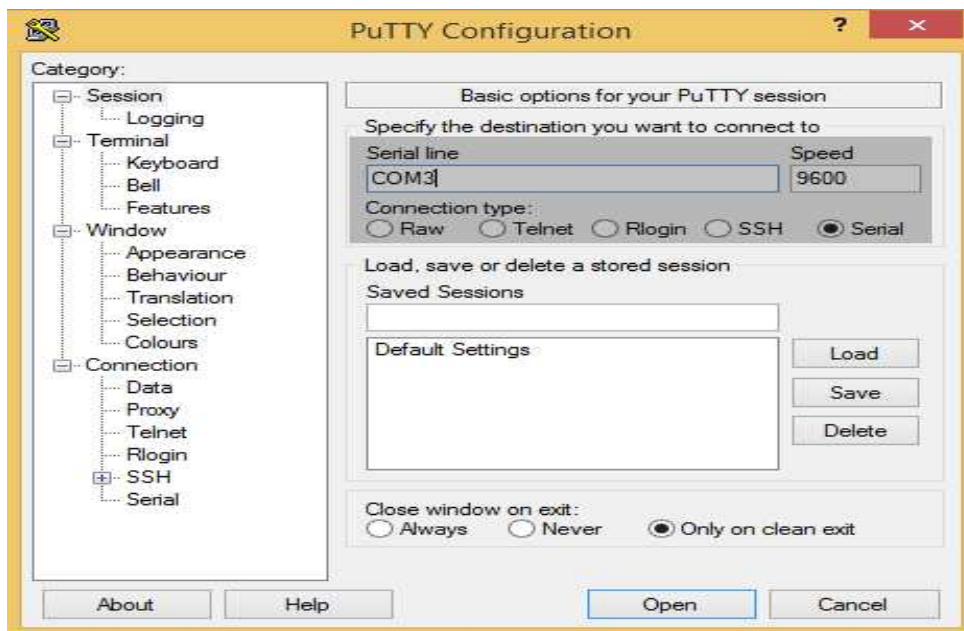
```
Router#
Router#show version | include image
System image file is "flash0:c2900-universalk9-mz.SPA.151-1.M4.bin"
Router#
```

چون، قرار است از طریق سریال به روتر وصل شویم، باید شماره پورت سریال Serial را بدانیم. برای این کار می‌توانید از طریق device manager از قسمت پورت شماره پورت serial یا com خودتان را پیدا کنید.



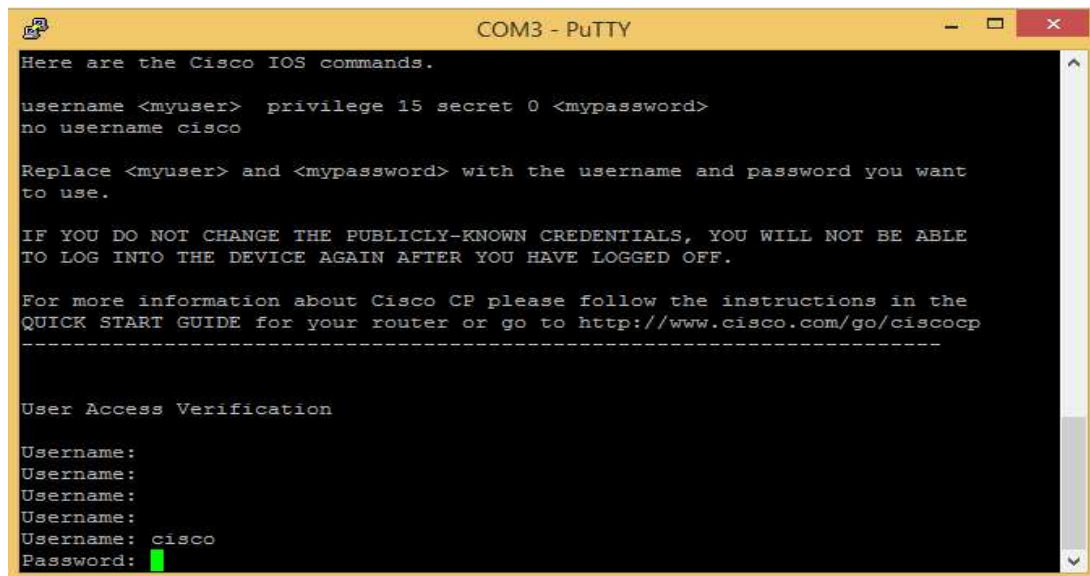
Device Manager (۱۴-۳) شکل

برنامه Putty را باز کرده، از قسمت Connection Type دکمه Serial را انتخاب کنید و از قسمت Line شماره پورت سریال خود را انتخاب نمایید. در بخش Speed هم 9600 که به صورت پیش فرض می باشد، نیاز نیست تغییر دهید و در اینجا چون پورت سریال من روی COM3 می باشد، در قسمت Serial Line شماره سریال را تغییر می دهیم.



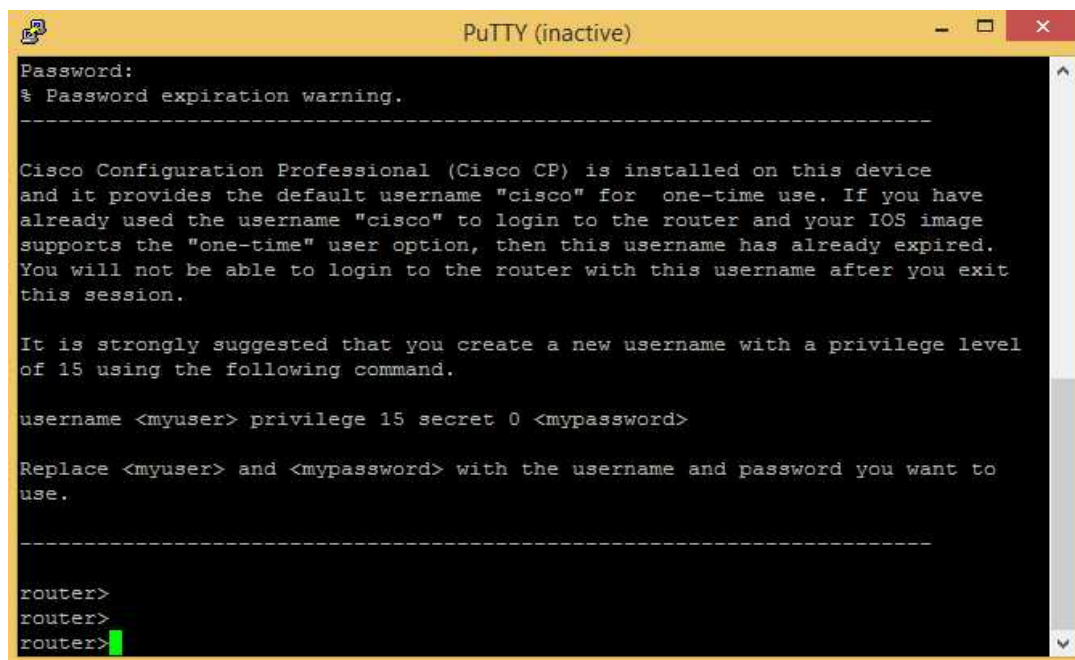
Putty نرم افزار (۱۵-۳) شکل

روی دکمه Open کلیک کنید تا به کنسول روتر وصل شوید. در صورتی که بعد از زدن open صفحه putty مشکی ماند و هیچ عکس العملی نداشت، چندین بار دکمه Enter را پشت سر هم فشار دهید که کنسول router را برای شما نمایش دهد.



شکل (۳-۱۶) صفحه اتصال به Router

یوزر و پسورد خود را جهت اتصال به command line روتر وارد کنید.



شکل (۳-۱۷) صفحه اتصال به Router توسط نرم افزار Putty

۳.۶.۲ Telnet

در صورتی که هنگام تنظیم کردن اولیه، روتر و سوئیچ IP Address را به آن نسبت داده باشید، به راحتی می توانید در یک شبکه TCP/IP به روتر یا سوئیچ دسترسی پیدا کرده، آن را تنظیم کنید. این ارتباط از طریق سرویس Telnet می باشد، بنابراین در صورت داشتن آدرس (IP Address) روتر یا سوئیچ و همچنین فعال

بودن امکان دسترسی از طریق Telnet در روتر می‌توانید به آن متصل شوید و تنظیمات موردنظرتان را انجام دهید.

۳.۶.۳ Auxiliary Port

در این روش استفاده از پورت AUX می‌باشد. شما می‌توانید از راه دور با روتر یا سوئیچ ارتباط برقرار کرده و آن‌ها را تنظیم کنید. این ارتباط از بستر مخابراتی صورت می‌پذیرد. به‌طور مثال با متصل کردن یک روتر به یک مودم و ارتباط از طریق خطوط Dial UP می‌توان به روتر دسترسی پیدا کرد و آن را تنظیم کرد.

۳.۷ انواع Mode ها در CLI

محیط خط فرمان (CLI) در IOS سیسکو دارای دو Mode اجرایی می‌باشد:

- User Mode
- Privileged Mode

این بدان معناست که برای وارد کردن تنظیمات روی روتر یا سوئیچ، باید ابتدا وارد Mode مربوطه شوید.

User Mode: در این Mode می‌توانید عملیات محدودی را انجام دهید. درواقع این Mode پایین‌ترین سطح دسترسی به روتر یا سوئیچ را نشان می‌دهد. در این Mode عملیات Monitoring قابل اجراست. درواقع افراد مختلف می‌توانند وارد این Mode شده و بدون دسترسی داشتن به تنظیمات، عملیات محدودی؛ چون چک کردن عملکرد روتر و یا سوئیچ، نمایش وضعیت حافظه و کنترل میزان ترافیک ورودی و یا خروجی به هر Interface را انجام دهند. بعد از Boot شدن IOS و Load شدن کامل تنظیمات، User Mode اولین جایگاهی است که CLI نشان می‌دهد. در این جایگاه Command Prompt به‌صورت زیر می‌باشد.

Hostname >

Privilege Mode: این Mode جایگاهی با دسترسی بالاتر برای انجام تنظیمات روی روتر و یا سوئیچ می‌باشد. به‌صورت پیش‌فرض برای وارد شدن به این Mode نیازی به وارد کردن پسورد نیست، اما برای برقراری امنیت باید قبل از وارد شدن به آن Mode، پسورد گذاشته شود تا فقط افراد خاص با داشتن پسورد به این Mode دسترسی داشته باشند. در این Mode که به آن Enable Mode هم گفته می‌شود، اجازه دسترسی کامل به تمامی فرامین جهت تنظیمات بیشتر داده می‌شود. با وارد کردن دستور Enable در User Mode وارد Privileged Mode خواهید شد.

Hostname > enable

با وارد کردن دستور بالا علامت بزرگ تر ">" در Command Prompt به علامت شارپ "#" تغییر خواهد کرد.

Hostname #

برای خارج شدن از این Mode می توانید از دستور Exit استفاده کنید.

Hostname # exit

نکته: برای خارج شدن از محیط Privilege می توانید از کلیدهای Ctrl+Z هم استفاده کنید.

کمک گرفتن از Help (علامه سوال ؟)

برای دیدن لیست فرمان ها در یک Mode می توان از علامه سوالیه "?" استفاده کرد. با وارد کردن علامه سوالیه "?"، همه دستورات قابل اجرا در هر Mode که هستیم، برای ما نمایش داده خواهد شد. در صورتی که تعداد دستورات نمایش داده شده از یک صفحه بیشتر باشد، با زدن کلید Space صفحه به صفحه و با زدن کلید Enter خط به خط دستورات را می توانید مشاهده کنید.

همچنین می توانید چند حرف اول از یک فرمان را نوشته و سپس با زدن علامت "?" فرمان هایی را که با این حرف آغاز می شوند، ببینید. به طور مثال، بعد از نوشتن حرف "e" علامت "?" را تایپ کنید. بنابراین کلماتی را که با حرف "e" آغاز شده اند، برای شما نمایش خواهد داد.

router>e?

emm enable ethernet exit

تنظیم ساعت و تاریخ در روتر و سوئیچ

در این مثال می خواهیم ساعت (Router and Switch) را با کمک گرفتن از علامت سوالیه، تنظیم کنیم.

router#clock ?

read-calendar -- Read the hardware calendar into the clock

set -- Set the time and date

update-calendar -- Update the hardware calendar from the clock

router#clock set ?

hh:mm:ss -- Current Time

router#clock set 19:06:00

<1-31> Day of the month

MONTH Month of the year

router#clock set 19:07:00 16 february 2020 ?

<cr>

router#clock set 19:07:00 16 february 2020

router#

*Feb 16 19:07:00.000: %SYS-6-

CLOCKUPDATE: System clock has been updated from 15:33:56 UTC Tue Feb16 2020 to 19:07:00 UTC Tue Feb 16 2020, configured from console by cisco on console.

نکته: <cr> مخفف Carriage Return می باشد، یعنی به آخر دستور رسیده ایم و دستور کامل می باشد. با دستور Show Clock می توانید ساعت و تاریخ روتر یا سوئیچ را مشاهده کنید.

router#show clock

19:07:15.775 UTC Tue Feb 16 2020

router#

دستور History در Router: History لیستی از آخرین دستورات را که وارد کرده اید، نشان می دهد. به کمک دستور زیر می توانید History و محتویات آن را مشاهده کنید.

router#show history

با این دستور شما می توانید 10 دستور قبلی را که اجرا کرده اید، مشاهده کنید.

در صورتی که بخواهیم بیشتر از 10 دستور را در History روتر یا سوئیچ ذخیره کنیم، از دستور زیر استفاده می کنیم. در اینجا ما تعداد دستورهای را که باید در Router یا Switch ذخیره شود، به 256 عدد می رسانیم.

router#terminal history size 256

دستور Version: این دستور برای اطلاعات پایه ای کاربرد زیادی دارد. به کمک این دستور می توان در مورد سخت افزار و ورژن IOS و میزان حافظه های RAM, NV RAM, Flash, Platform و مدت زمان up بودن روتر یا سوئیچ معلومات حاصل کنیم.

router#show version

```
Router>show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2901 uptime is 33 seconds
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.
151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this
product you
agree to comply with applicable laws and regulations. If you are
```

show version شکل (۳-۱۸) نتیجه دستور

۳.۸ پیغام‌های خطا و معنای آن‌ها

در زیر شما را با برخی پیام‌های خطا را که در روتر با آن زیاد مواجه می‌شوید، آشنا می‌کنیم، همچنین معنای هر یک از این خطاها را خواهید آموخت.

% Ambiguous Command: "e"

یعنی با کلمه "e" آپشن‌های متفاوتی داریم و فقط یک آپشن نیست.

% Unknown Command

یعنی هم‌چون آپشن وجود ندارد.

% Invalid input detected at '^' marker

یعنی با این علامت '^' نشان می‌دهد که کجای دستور مورد نظر را اشتباه نوشته‌ایم.

% Incomplete Command

یعنی دستور کامل نیست.

% Unrecognized Command

یعنی این دستور را در این Mode نمی‌شناسد.

۳.۹ تغییر Hostname در روتر و سوئیچ

برای تغییر Hostname در Router خود می‌توانید از دستور Hostname استفاده کنید.

```
router(config)#hostname TVET
```

```
TVET(config)#
```

نام مسیر یاب (Router) به (TVET) تبدیل گردید. برای ذخیره (save) کردن تغییرات دو روش وجود دارد. در Privilege mode از دستورات ذیل استفاده کنید.

```
TVET#write
```

```
TVET#copy running-config startup-config
```

درست کردن بنر (Banner) در مسیر یاب (Router): پیام روزانه، پیامی می‌باشد که در هر بار Login کردن به Router یا Switch برای کاربر نمایش داده می‌شود. بنر (banner) را توسط دو دستور ذیل ایجاد کرده می‌توانیم.

```
TVET(config)#banner motd "Message"
```

```
TVET(config)#banner login "Message"
```

```
TVET(config)#banner motd
TVET(config)#banner motd .
Enter TEXT message. End with the character '.'
.
Belongs to TVET.
TVET(config)#
```

شکل (۳-۱۹) دستور banner

تنظیمات Console Port و پسورد گذاشتن روی User Mode: تنها راه ارتباط با روتر یا سوئیچ که تازه تهیه کرده‌ایم، استفاده از Console Port می‌باشد. روش ارتباط با روتر یا سوئیچ را از طریق کابل کنسول در درس‌های قبلی تشریح گردید، اکنون تنظیمات Console Port را مورد بحث قرار می‌دهیم.

وارد شدن به کنسول: از دستور زیر برای وارد شدن به Console Port استفاده می‌کنیم تا بتوانیم تنظیمات را انجام دهیم.

```
TVET(config)#line console 0
```

```
TVET(config-line)#
```


نامحدود کردن زمان اتصال به کنسول روتر (Router): مدت زمان برقراری ارتباط کنسول با روتر یا سوئیچ به صورت پیش فرض 10 دقیقه می باشد. به کمک دستور زیر می توانیم مدت زمان برقراری این ارتباط را به صورت نامحدود تعریف کنیم. درواقع، اگر Packet هایی برای مدت زمان طولانی از این اینترفیس رد و بدل نشود، این ارتباط قطع نخواهد شد. در اینجا عدد 0 یعنی هیچ وقت ارتباط قطع نشود.

```
TVET(config-line)#exec-timeout 0 0
```

روش برداشتن خطاهای مزاحم: یکی دیگری از مشکلاتی که ممکن است با آن مواجه شوید این است که شما دستورات را که در Command Prompt روتر یا سوئیچ خود وارد می کنید، به طور مثال: دستور Show Run و منتظر نتیجه آن هستید، در این لحظه پیام جدیدی مبنی بر اینکه یکی از اینترفیس ها Up شده است، ظاهر می شود. بنابراین نمی توانید تفاوت بین نتیجه فرمان خودتان و پیام هایی را که ظاهر شده است، متوجه شوید. به کمک این دستور می توانید به Router یا Switch بگویید؛ پیام جدید را بعد از خروجی دستور شما نمایش دهد.

```
TVET(config-line)#logging synchronous
```

۳.۱۰ پسورد گذاشتن روی Console یا User Mode

Console Password پسوردی است که قبل از وارد شدن به User Mode پرسیده می شود. دو روش برای دادن پسورد وجود دارد که به صورت زیر تنظیم می شود.

روش اول:

```
TVET(config)#line console 0
```

```
TVET(config-line)#password cisco
```

```
TVET(config-line)#login
```

روش دوم:

```
TVET(config)#username cisco password cisco
```

```
TVET(config)#line console 0
```

```
TVET(config-line)#login local
```

با این روش در User Mode می توانیم افرادی را که با Username های مختلف وارد شده اند و کار کرده اند، مشاهده و کنترل کنیم.

۳.۱۱ Line VTY

شماره VTY از 0 تا 15 است. که 16 می شود؛ یعنی اگر همه را فعال کنیم، همزمان 16 استفاده کننده (user) از طریق Telnet از راه دور با این روتر یا سوئیچ متصل شده می توانند. برای فعال کردن آن از دستورات ذیل استفاده می کنیم. می خواهیم پنج line را فعال کنیم.

```
TVET(config)#line vty 0 4
```

```
TVET(config-line)#login
```

```
TVET(config-line)#password cisco
```

```
TVET(config-line)#
```

۳.۱۲ روش پسورد گذاشتن برای Enable Mode

برقراری امنیت هنگام وارد شدن به Privileged Mode استفاده می شود. برای گذاشتن پسورد روی Enable Mode می توانید مثل دستور زیر عمل کنید.

```
TVET(config)#enable password cisco1234
```

بعد از گذاشتن پسورد، هر موقع شما بخواهید وارد محیط Enable بشوید، از شما این پسورد را در خواست می کند.

۳.۱۳ امن کردن پسورد Enable Mode

پسوردی که در بالا گذاشتیم، به صورت Clear Text ذخیره می شود و به کمک دستور Show Run می توانید آن را به صورت Clear و کد نشده ببینید. برای اینکه کسی نتواند رمزهای ما را در Show Run ببیند، می توانیم از دستور زیر استفاده کنیم.

```
TVET(config)#enable secret cisco1234
```

۳.۱۴ روش پنهان کردن حروف پسورد

از دستور زیر برای پنهان کردن حروف Password استفاده می کنیم که در حقیقت پسوردها را به یک سلسله اعداد تبدیل می کند.

```
TVET(config)#service password-encryption
```

۳.۱۵ تنظیم Interface های مسیریاب

وارد شدن به یک Interface به کمک دستور زیر می توانیم وارد اینترفیس موردنظر شده و آن را تنظیم کنیم.

```
TVET(config)#interface type mod/num
```

Type: در قسمت Type نوع اینترفیس را مشخص می کنیم، مثلاً: Ethernet / Fast Ethernet یا Gigabit Ethernet و غیره...

Number: در قسمت num شماره port یا اینترفیس مورد نظر نوشته می شود.

نکته: شماره interface در switch ها از 1/0 و در روترها از 0/0 شروع می شود.

روشن و خاموش کردن یک Interface برای تنظیم کردن یک Interface همانطور که در بالا گفته شد، ابتدا باید وارد آن Interface شویم. برای این کار از دستور زیر استفاده می کنیم.

```
TVET(config)#interface GigabitEthernet 0/0
```

```
TVET(config-if)#
```

از دستور shutdown برای خاموش یا غیرفعال کردن یک انترفیس و از دستور no shutdown برای روشن یا فعال کردن یک انترفیس استفاده می شود.

```
TVET(config-if)#shutdown
```

```
TVET(config-if)#no shutdown
```

برای نشان دادن وضعیت یک پورت یا انترفیس می توانید از دستور show interfaces استفاده کنید.

```
TVET#show interfaces GigabitEthernet 0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
Hardware is PQ3_TSEC, address is 78da.6edf.5501 (bia 78da.6edf.5501)
```

```
Internet address is 172.16.16.147/25
```

```
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

Keepalive set (10 sec)
Full Duplex, 100Mbps, media type is RJ45
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:07, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 1000 bits/sec, 1 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
66774 packets input, 6350046 bytes, 0 no buffer
Received 66640 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 2769 multicast, 0 pause input
6782 packets output, 746971 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
923 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
TVET#

۳.۱۶ نمایش وضعیت خلاصه Port ها و Interface ها

با دستور Show interface brief می‌توانید وضعیت تمام انترفیس‌ها را مشاهده کنید.

```
TVET#show interface brief
```

از دستور زیر هم می‌توانید جهت مشاهده اطلاعات Interface ها به صورت خلاصه‌تر استفاده کنیم.

```
TVET#show ip interface brief
```

| Interface | IP-Address | OK? | Method | Status | Protocol |
|-----------------------------|---------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine 0/0 | unassigned | Yes | NVRAM | administratively down | |
| GigabitEthernet0/0 | 172.16.16.147 | YES | manual | administratively down | |
| GigabitEthernet0/1 | 172.16.100.17 | YES | DHCP | up | up |
| GigabitEthernet0/2 | unassigned | YES | NVRAM | administratively down | down |

۳.۱۷ نوشتن توضیحات برای Port ها

جهت مدیریت بهتر interface ها، شما می‌توانید برای آنها توضیحاتی را با استفاده از دستور description بنویسید.

```
TVET(config)#interface GigabitEthernet 0/0
```

```
TVET(config-if)#description connect to gateway data center
```

برای دیدن این توضیحات از انترفیس مورد نظرتان از دستور show استفاده کنید.

۳.۱۸ انتخاب چندین Interface هم‌زمان

برای انتخاب چندین انترفیس هم‌زمان، ما از دستور Interface Range به 2 روش زیر می‌توانیم عمل کنیم:

روش اول: در این روش، نام انترفیس را به همراه شماره پورت آن وارد کرده و میان آنها را با کامه "،" جدا می‌کنیم.

```
TVET(config)#interface range GigabitEthernet 0/0 , GigabitEthernet 0/1 , GigabitEthernet 0/2
```

```
TVET(config-if-range)#
```

روش دوم:

```
TVET(config)#interface range GigabitEthernet 0/0-2
```

```
TVET(config-if-range)#
```

۳.۱۹ طریقه دادن IP به Interface های Router

استفاده از دستور IP Address به انترفیس های روتر (Router) خود IP بدهیم. ساختار دستور به شکل زیر می باشد.

```
TVET(config)#interface GigabitEthernet 0/0
```

```
TVET(config-if)#ip address 172.16.16.147 255.255.255.0
```

بعد از نوشتن دستور IP Address و بعد از آن Subnet Mask مورد نظر را وارد می کنیم.

۳.۲۰ معرفی Shortcut های مهم در روتر (Router)

Ctrl + A: کرسر را به اول خط برمی شود.

Ctrl + E: کرسر را به آخر خط می برد.

Ctrl + F: کرسر یک حرف به پیش می رود.

Ctrl + B: کرسر یک حرف به عقب می رود.

Ctrl + D: یک حرف را پاک می کند.

Ctrl + U: از جای کرسر تا اول مود را پاک می کند.

Ctrl + R: خط فرمان (CLI) را Refresh می کند.

Ctrl + B: کرسر یک کلمه به عقب می رود.

Ctrl + F: کرسر یک کلمه به پیش می رود.

\$: یعنی قبل از این حرف نیز نوشته هست.

برای نمایش دستورهای قبلی و بعدی که قبلاً نوشته شده باشد از shortcut های ذیل استفاده کنید.

UP \$ Down or Ctrl + P & Ctrl + N

۳.۲۱ ذخیره کردن تنظیمات در روتر

دستور write memory برای ذخیره تنظیمات: تا اینجا هرچه تنظیمات انجام داده ایم، در حافظه موقت روتر وجود دارد و با قطع و وصل شدن برق روتر یا Reload کردن روتر، تمام تنظیماتی که انجام داده ایم از

بین می‌رود. برای ذخیره تغییراتی که انجام شده است، از دستور Write Memory در محیط User Mode استفاده می‌کنیم.

```
TVET#write memory
Building configuration...
[OK]
TVET#
```

۳.۲۲ **طریقه Telnet نمودن به یک Router سیسکو**

یکی از راه‌های دسترسی به سوئیچ یا روتر Telnet می‌باشد. در هر ارتباط Telnet یک Session برقرار می‌شود. بنابراین به اندازه تعداد Line‌هایی که IOS حمایت می‌کند، می‌توانید Telnet Session برقرار کنید. برای تنظیم Telnet باید 3 مرحله زیر را طی کنید:

- Setting IP Address
- User Mode Security
- Enable Mode Security

این 3 مرحله در بحث‌های قبلی به صورت مفصل تشریح شده است.

Telnet از طریق Command Prompt: Command prompt را باز کرده و همانند زیر با استفاده از دستور Telnet به روتر خود Telnet بزنید.

```
C:\Users\habili>telnet 172.16.1.47
```

بعد از وارد کردن یوزر و پسورد به روتر Login کنید و دیگر تنظیمات خود را انجام دهید.

۳.۲۳ Telnet از طریق Putty

نرم افزار Putty را باز کنید و از قسمت Connection Type دکمه Telnet را انتخاب کنید، در قسمت Hostname هم IP روتر یا سوئیچ خود را انتخاب کرده، روی دکمه Open کلیک کنید. در مرحله بعد، یوزر و پسورد خود را جهت Login کردن به روتر وارد کنید.

نکته: اگر بعد از انجام تنظیمات فوق، موفق نشدید به روتر Telnet بزنید، حتماً تنظیمات روتر را بررسی کنید. ممکن است که access list تعریف نشده باشد و روتر شما را به IP Address های خاصی محدود کرده باشد. اگر Access List داشتید، حتماً آن را تغییر داده، رنج IP Address روتر را در آن وارد کنید.



شرکت Cisco روترهای خود را در انواع و مدل‌های مختلف ارائه می‌کند که تفاوت این مدل‌ها در قابلیت‌های سخت‌افزاری آن‌ها نهفته است. انجیران و طراحان این بخش باید با این نوع تفاوت‌ها آشنایی حاصل نمایند.

سیستم عامل که با آن Routerهای سیسکو را پیکربندی می‌نمایند و Cisco IOS نامیده می‌شود. در اکثر محصولات یکسان می‌باشد و تمامی دستورات پیکربندی را پشتیبانی می‌کند. سخت‌افزار هر Router سیسکو را می‌توان به دو بخش تقسیم کرد (سخت‌افزارهای عمومی و سخت‌افزارهای ویژه)

همچنین می‌توان سخت‌افزار یک روتر را به سخت‌افزار داخلی و خارجی قابل مشاهده تقسیم کرد. بدنه Cisco به‌طور خاص تهیه می‌شود تا استفاده از آن برای انجیران و طراحان شبکه راحت باشد. بدنه در روترهای سیسکو دارای رنگ آمیزی خاص است.

پورت‌های Console و Aux از مولفه‌هایی است که پشت روترهای سیسکو قرار دارند و پورت Console اولین راه برای برقراری ارتباط با روتر سیسکو محسوب می‌شود.

خط اتصال (Interface) اتصال به شبکه‌های LAN واسط ایست، برای اتصال روترها به شبکه‌های محلی مانند: اترنت، توکن رینگ و یا شبکه‌های محلی مبتنی بر فیبر نوری FDDI استفاده می‌شود.

خط اتصال (Interface) اتصال به شبکه‌های WAN که بسیاری از روترهای سیسکو قابلیت اتصال به WAN را دارند. لذا در این روترها کارت توسعه WAN که به اختصار WIC نامیده می‌شود، از قبل در محل مربوط نصب شده است.

استفاده از روترها در شبکه به امری متداول تبدیل شده است. یکی از دلایل مهم گسترش استفاده از روتر، ضرورت اتصال یک شبکه به چندین شبکه دیگر (ایترنت و یا سایر سایت‌های از راه دور) در عصر حاضر است.

CPU و احد پردازش مرکزی مسئولیت اجرای دستورالعمل‌ها در سیستم عامل سیسکو را برعهده دارد

حافظه اصلی RAM به منظور ذخیره اطلاعات جدول مسیریابی (Routing)، بسته‌های اطلاعاتی اجرای پیکربندی و Cache سوئیچینگ سریع استفاده می‌شود.

حافظه پایدار (Non – Volatile RAM (NV RAM از جمله حافظه‌های پر سرعت است و همان گونه که از نامش پیداست، پایدار می‌باشد. یعنی با خاموش شدن یا ریستارت شدن روتر اطلاعات آن از بین نمی‌رود. از حافظه فلش (Flash) به منظور ذخیره نسخه کامل نرم‌افزار IOS استفاده می‌شود، روتر معمولاً IOS پیشفرض خود را از حافظه فلش دریافت می‌نماید.

اگر روترهای شامل یک گذرگاه (Buses) سیستم و یک گذرگاه پردازنده (processor) می‌باشند. از گذر سیستم به منظور مبادله اطلاعات بین پردازنده (processor) و انترفیس‌ها استفاده می‌شود.

از حافظه ROM به منظور ذخیره دائم کد اشکال‌زدایی راه‌انداز (ROM Monitor) استفاده می‌شود. مهم‌ترین وظیفه حافظه ROM، تست و عیب‌یابی سخت‌افزار در زمان راه‌اندازی روتر و استقرار نرم‌افزار IOS از حافظه فلش به داخل حافظه RAM می‌باشد.

همه تجهیزات برای خودشان عملیاتی دارند که از زمان روشن شدن دستگاه تا رسیدن بر سیستم‌عامل مربوطه انجام می‌شود که به این عملیات در اصطلاح روترهای سیسکو، Cisco Boot Sequence یا ترتیب بوت روترهای سیسکو گفته می‌شود.

جهت اتصال به CLI ما می‌توانیم از 3 روش مهم استفاده کنیم (console port, telnet, Auxiliary port)

CLI در IOS سیسکو دارای دو Mode اجرایی می‌باشد (user mode, privileged mode)

یکی از راه‌های دسترسی به سوئیچ یا روتر Telnet می‌باشد، برای هر ارتباط Telnet یک Session برقرار می‌شود. بنابراین به اندازه تعداد Line‌هایی که IOS حمایت می‌کند، می‌توانید Telnet Session برقرار کنید.



سوالات فصل سوم

۱. پورت‌های Console و Aux را تشریح نمایید.
۲. تفاوت بین اینترفیس‌های LAN و WAN را در روترهای سیسکو واضح سازید.
۳. عناصر داخلی Router، CPU و RAM را مختصراً توضیح دهید.
۴. حافظه پایدار (NV RAM) و حافظه فلش (Flash) را توضیح کنید.
۵. مراحل Boot شدن روتر را مختصراً شرح دهید.
۶. انتخاب IOS یک روتر به چند عامل بستگی دارد؟ توضیح کنید.
۷. تنظیمات و مراحل Boot نمودن Router از طریق فایل IOS موجود در شبکه را توضیح نمایید.
۸. راه‌های دسترسی به روتر را بر شمارید.
۹. مراحل اتصال به CLI روتر از طریق پورت Console را واضح سازید.
۱۰. مدهای CLI را توضیح نمایید.
۱۱. دستور کمک گرفتن از محیط CLI را تشریح کنید.
۱۲. پیام‌های خطا را در محیط CLI بیان کنید.
۱۳. مراحل پسورد گذاشتن روی User Mode را تشریح کنید.
۱۴. مراحل پسورد گذاشتن روی Enable Mode را توضیح دهید.
۱۵. شماره (VTY) از صفر تا 4 را یا از صفر تا 15 چه را بیان می‌کند.
۱۶. چگونه به یک Router، Telnet نماییم؟



۱. با استفاده از نرم افزار packet tracer یا GNS3 پیکربندی ابتدایی روتر را انجام دهید.
۲. پسوندهای پورت‌های مختلف روتر را فعال و غیر فعال نمایید.
۳. دو شبکه کوچک را - هر کدام دارای 5،5 کامپیوتر باشد- توسط روتر باهم وصل نمایید که موفقانه باهم ارتباط برقرار کنند.

فصل چهارم

مسیریابی (Routing)



هدف کلی: آشنایی با پروسه مسیریابی و انواع پروتوکول‌های آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. مفاهیم اولیه مسیریابی (Routing) را تشریح نمایند.
۲. با مسیریابی (Routing)، پروتوکول‌های Static، Default و Dynamic آشنا شوند.
۳. شرح عملکرد پروتوکول‌های مسیریابی Distance Vector Routing بدانند.
۴. شرح عملکرد پروتوکول‌های مسیریابی Link State Routing بدانند.
۵. شرح عملکرد پروتوکول‌های مسیریابی Hybrid Routing بدانند.

مسیریابی عبارت از پروسه انتخاب بهترین مسیر برای دسترسی به شبکه‌های غیر محلی می‌باشد.

مسیریابی (Routing) یکی از مهمترین ویژگی‌های موردنیاز در یک شبکه (Network) به منظور ارتباط با سایر شبکه Host. در صورتی که پروتوکول‌های مسیریابی وجود نداشته باشد، کامپیوترها قادر به مبادله اطلاعات (Data) نخواهند بود.

بنابراین، روتر با شناخت از شبکه‌ها، مسیرهای رسیدن به هر کدام و نگهداری این اطلاعات در یک جدول به عنوان مسیریاب ایفای وظیفه می‌کند. در این فصل مفاهیم مسیریابی، انواع مسیریابی و عملکرد پروتوکول‌های مسیریابی به صورت اساسی تشریح شده است. از مسیریابی (Routing) به منظور دریافت یک بسته اطلاعاتی (Packet) از یک دستگاه و ارسال آن از طریق شبکه به دستگاه دیگر و بر روی شبکه متفاوت استفاده می‌شود. در صورتی که شبکه شما دارای روتر نباشد، امکان مسیریابی اطلاعات بین شبکه شما و سایر شبکه‌ها وجود نخواهد داشت.

یک مسیریاب (Router) به منظور مسیریابی یک بسته اطلاعات، باید آگاهی موارد ذیل را داشته باشد.

۱. آدرس مقصد (Destination Address)
۲. روترهای مجاور (Neighbors) که با استفاده از آنان امکان اخذ اطلاعات لازم در خصوص شبکه‌های از راه دور، فراهم می‌شود.
۳. مسیرهای موجود به تمامی شبکه‌های از راه دور؛
۴. بهترین مسیر به هریک از شبکه‌ها از راه دور؛
۵. نحوه نگهداری و بررسی اطلاعات مسیریابی (Routing).

۴.۱ همگرایی (Convergence – Routing Update)

عملیه موردنیاز برای تمامی روترهای موجود در یک شبکه، به منظور به‌روز (Update) کردن جداول مسیریابی (Routing) و ایجاد یک نگرش سازگار از شبکه با استفاده از بهترین مسیرهای موجود، در زمان انجام عملیه فوق (همگرایی) اطلاعات کاربر ارسال خواهد شد.

۴.۲ مسیریابی آی پی (IP Routing)

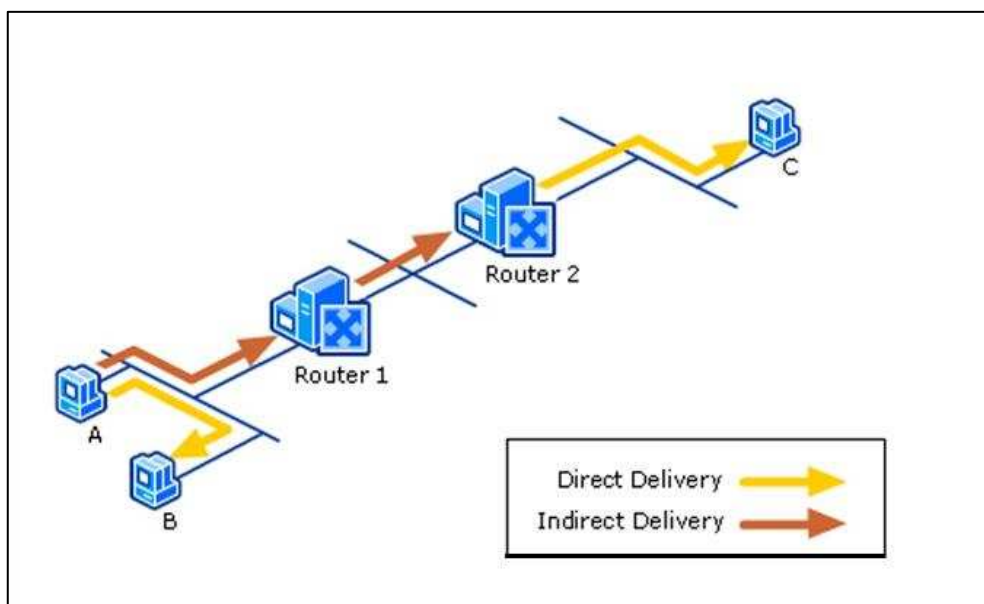
به طور عموم، روترها که اکثر اوقات Gateway هم گفته می‌شود. هم Host مبدأ و هم روتر به یک برآورد اولیه برای اینکه چطور بسته را ارسال کند، نیاز دارند. برای انجام تخمین، لایه IP که نام دیگر آن لایه شبکه است، با جدول مسیریابی (Routing Table) خود که در حافظه‌اش ذخیره شده است، مشورت می‌کند. اطلاعات جدول مسیریابی در ابتدا با آغاز مذاکرات TCP / IP ایجاد می‌شوند و در ادامه اطلاعات بعدی به‌طور خودکار از طریق ارتباط روترها با یکدیگر به جدول اضافه می‌شود.

۴.۳ تحویل مستقیم و غیر مستقیم

بسته‌های IP براساس اینکه مقصد نهایی، مستقیماً در یک شبکه متصل به شبکه خودش است یا نه؟ می‌تواند حداقل یکی از دو نوع تحویل استفاده کند. این دو نوع از تحویل، بسته به تحویل مستقیم و غیر مستقیم معروف هستند.

- تحویل مستقیم زمانی رخ می‌دهد که نود IP یک بسته را به مقصدی در شبکه فعلی مبدأ، به‌طور مستقیم ارسال می‌کند. برای این کار، نود مربوط بسته IP را در قالب یک فریم، کپسول‌بندی می‌کند و در حالی که آن را با آدرس سخت‌افزاری (آدرس مک) مقصد آدرس‌دهی می‌کند، برای لایه دوم؛ یعنی لایه Data Link مثل (اترنت یا توکن رینگ) ارسال می‌کند.
- تحویل غیر مستقیم زمانی رخ می‌دهد که نود یک بسته را به نود میانی که غالباً یک روتر است ارسال می‌کند. این قضیه به این علت رخ می‌دهد که مقصد نهایی در شبکه فعلی مبدأ قرار ندارد. برای این کار، نود مربوط بسته IP را در قالب یک فریم، کپسول‌بندی می‌کند و در حالی که آن را با آدرس سخت‌افزاری (آدرس مک) روتر میانی آدرس‌دهی می‌کند. برای لایه دوم، یعنی لایه Data Link مثل (اترنت یا توکن رینگ) ارسال می‌کند.

درواقع مسیریابی IPv4 به ترکیبی از تحویل‌های مستقیم و غیر مستقیم اطلاق می‌شود. در شکل زیر، هنگامی که بسته‌ها به نود B ارسال می‌شوند، نود A یک تحویل مستقیم انجام اطلاعات است. اما هنگامی که بسته‌ها به مقصد نود C ارسال می‌شوند، نود A درواقع یک تحویل غیر مستقیم را به روتر 1 و سپس روتر 1 یک تحویل غیر مستقیم را به روتر 2 و نهایت روتر 2 یک تحویل مستقیم را به نود C انجام می‌دهد:

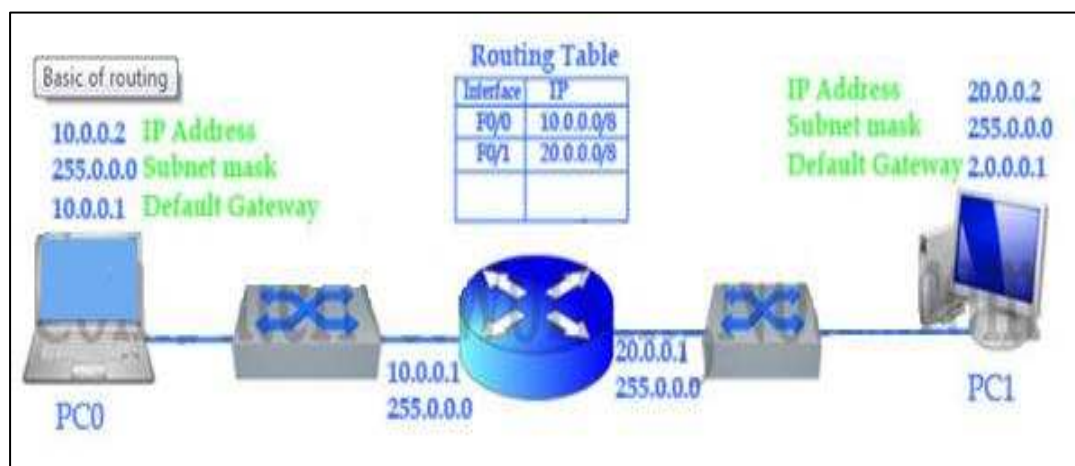


شکل (۴-۱) روش انتقال اطلاعات به شکل مستقیم و غیر مستقیم

۴.۴ جدول مسیریابی IP

یک جدول مسیریابی در تمام نودهای IP وجود دارد. این جدول اطلاعات مربوط به شبکه‌های IP و نحوه دسترسی (مستقیم و غیرمستقیم) به آن‌ها را در خود ذخیره می‌کند. به علت آن که تمام نودهای IP در حوزه فعالیت خود برخی از انواع مسیریابی را انجام می‌دهند، نمی‌توان اینطور برداشت کرد که جدول‌های مسیریابی فقط مختص روتر Host . هر نودی که از پروتوکول TCP / IP استفاده می‌کند، یک جدول مسیریابی دارد. در این جدول یک سلسله از اطلاعات‌های پیش‌فرض بر اساس پیکربندی نود وجود دارند و دیگر اطلاعات‌های ورودی می‌توانند به‌طور خودکار از طریق تعامل با روترها و یا به‌طور دستی از طریق مولفه‌های TCP / IP به جدول اضافه شوند.

در شکل زیر دو کامپیوتر داریم هر دو در شبکه‌های مختلف قرار دارند. فرض کنید PC0 یک بسته را به PC1 می‌فرستد. این مراحل زیر را طی می‌کند:



شکل (۴-۲) طی مراحل ارسال بسته‌ها در دو شبکه مختلف

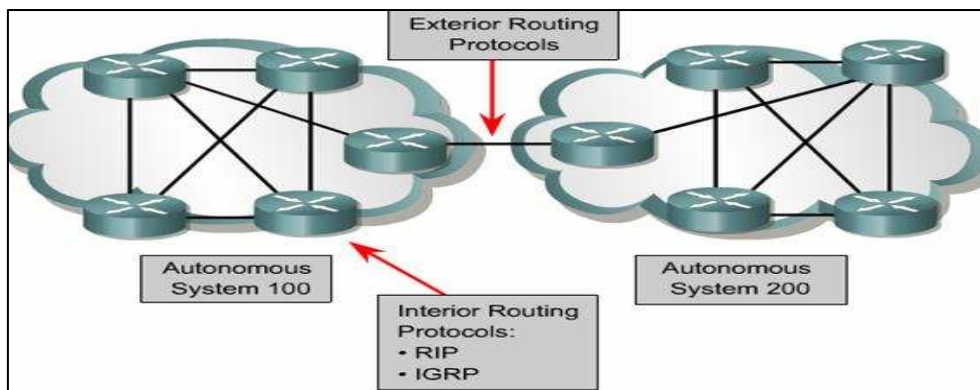
هنگام ارسال بسته (Packet) با جدول مسیریابی در موارد زیر مشورت و تخمین انجام می‌شوند:

آدرس Next - hop: در یک تحویل مستقیم، آدرس Next - hop همان IP Address مقصد نهایی است، اما در یک تحویل غیر مستقیم، آدرس Next - hop برابر با IP Address یک روتر میانی است.

Next - hop Interface: اینترفیس منطقی و یا سخت‌افزاری مثل یک کارت شبکه را که برای ارسال بسته به مقصد و یا روتر بعدی استفاده می‌شود، مشخص می‌کند.

۴.۵ پروتوکول‌های داخلی Interior Gateway Protocols

پروتوکول‌های داخلی (IGPs) برای به اشتراک گذاشتن و توزیع مسیریابی بین روترها در همان AS استفاده می‌شود. برخی از نمونه‌های IGP عبارتند از: RIPv1، RIPv2، EIGRP، IGRP و OSPF.



شکل (۳-۴) پروتوکول‌های داخلی و بیرونی

۴.۶ پروتوکول‌های بیرونی Exterior Gateway Protocol

پروتوکول‌های بیرونی (EGPs) برای به اشتراک گذاشتن و توزیع مسیریابی بین AS‌های مختلف مورد استفاده قرار می‌گیرند. مثال EGP پروتوکول (BGP) است.

۴.۷ فاصله‌اداری (Administrative Distance)

روترهای شرکت سیسکو برای انتخاب بهترین مسیر به مقصد بین چندین Routing Protocol به نام Administrative Distance استفاده می‌کنند. در این حالت برای رسیدن به یک مقصد، مسیرهای مختلفی در داخل جدول مسیریابی روترها وجود دارد که توسط پروتوکول‌های مسیریابی مختلف به دست آمده است. در این شرایط روترهای شرکت سیسکو برای انتخاب بهترین مسیر بین چندین Routing Protocol از Administrative Distance استفاده خواهند کرد و از مسیری که دارای Administrative Distance کمتری باشد استفاده خواهند کرد که Administrative Distance یک روش اختصاصی سیسکو برای رتبه بندی پروتوکول‌ها و منابع Routing می‌باشد و عدد بین 0 تا 255 است که در جدول زیر مقادیر آن را برای هر Routing Protocol مشاهده می‌کنید.

جدول (۴-۱): مقایسه Administrative Distance پروتوکول‌های مسیر یابی

| Route source | Administrative Distance (AD) |
|---------------------|------------------------------|
| Connected Interface | 0 |
| Static Route | 1 |
| EIGRP Summary Route | 5 |
| External BGP | 20 |
| EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EGP | 140 |
| External EIGRP | 170 |
| Internal BGP | 200 |
| Unknown | 255 |

۴.۸ متریک Metric

۱. اگر دو بهنگام‌سازی (Update) مسیریابی برای یک شبکه با یک مقدار AD برسد، درآنصورت متریک برای انتخاب بهترین مسیر استفاده خواهد شد. Metric یک واحد اندازه‌گیری برای محاسبه بهترین مسیر است.
۲. مسیر با کمترین متریک انتخاب خواهد شد. پروتوکول‌های مختلف مسیریابی از معیارهای مختلف استفاده می‌کنند. ممکن است از یک متریک یا چند متریک‌ها استفاده کنند.
۳. برای مثال EIGRP از پهنای باند (Bandwidth)، تأخیر (Delay)، بار (Load)، MTU و قابلیت اطمینان (Reliability) استفاده می‌کند. در حالی که RIP فقط از تعداد Hop‌ها به‌عنوان متریک استفاده می‌کند.

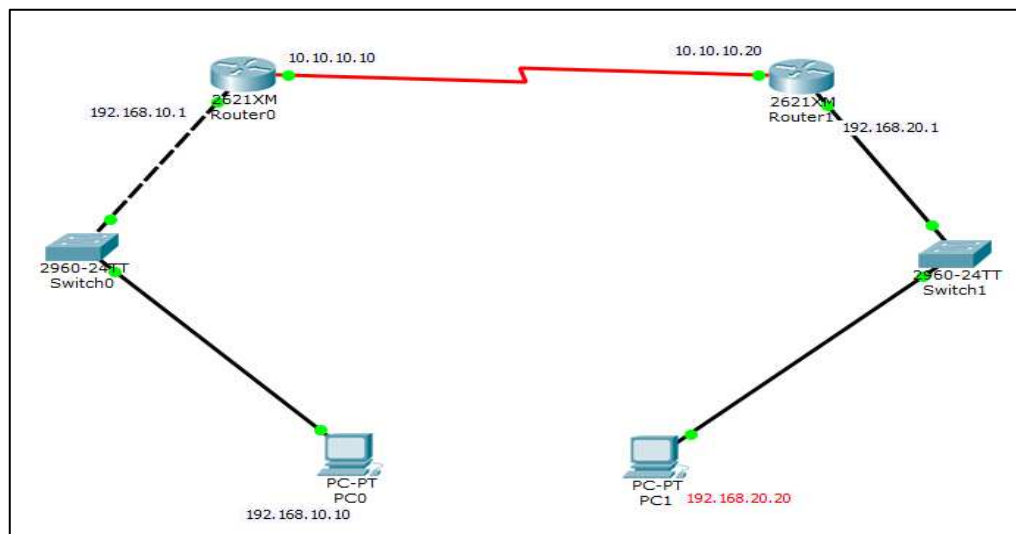
جدول (۴-۲) روتینگ Metric

| برای روشن شدن بهتر موضوع جدول ذیل را مدنظر می گیریم: | | |
|--|-------------|--|
| Routing Protocol | Metric | Description |
| EIGRP | Bandwidth | Capacity of link in Kbps |
| EIGRP | Delay | Time to reach in destination |
| EIGRP | Load | Path that is least utilize |
| EIGRP | MTU | Path that support largest frame size |
| EIGRP | Reliability | Path that have least down time |
| OSPF | Cost | Inverse of bandwidth links |
| RIP | Hop Count | Hops (Routers) in the way of destination |

۴.۹ مسیریابی ثابت (Static Routing):

Static Routing یا مسیریابی ثابت نوعی از مسیریابی است که دستگاه روتر با استفاده از Route‌هایی که در Routing Table دارد و به صورت دستی در روتر Learn یا تعریف شده است، بسته اطلاعاتی را به سمت مقصد هدایت می کند. در بسیاری از موارد Static Route‌ها به صورت دستی توسط مدیر شبکه در Routing Table مسیریاب (Router) پیکربندی می شوند. بر خلاف مسیریابی دینامیک یا Dynamic Routing مسیریابی ثابت یا Static Routing ثابت هستند و تا زمانی که تغییری در ساختار فیزیکی شبکه؛ مانند (اضافه شدن یا حذف شدن یک روتر از شبکه) به وجود نیامده است، بدون تغییرات باقی می مانند. Static Routing و Dynamic Routing نقطه مقابل هم نیستند و اینطور نیست که تنها یکی از آن دو در روتر پیاده سازی شود؛ بلکه می توان Static Routing و Dynamic Routing را در یک روتر هم زمان داشته باشیم و از خوبی های هر دو استفاده کنیم، به عنوان مثال، در صورت به مشکل افتادن پروتوکول مسیریابی از Static Routing می توان استفاده کرد و کارایی عملیاتی مسیریابی را بالا برد. از مسیریابی Static یا Static Routing بیشتر در شبکه های کوچک استفاده می شود؛ زیرا مدیریت آن در شبکه های کوچک آسانتر است.

مثال ذیل را جهت پیکربندی (Configuration) مسیریابی پیش فرض (Default) و ثابت (Static) در نظر می گیریم:



شکل (۴-۵) پیکربندی مسیریابی پیش فرض و ثابت

Router1:

```
#Interface Serial 1/0
```

```
#IP Address 10.10.10.10 255.0.0.0
```

```
#Bandwidth 64
```

```
#Clock Rate 64000
```

```
#No Shutdown
```

```
#Interface Fast Ethernet 0/1
```

```
#IP Address 192.168.10.1 255.255.255.0
```

```
#No Shutdown
```

Router2:

```
#Interface Serial 1/0
```

```
#IP Address 10.10.10.20 255.0.0.0
```

#No Shutdown

#Interface Fast Ethernet 0/1

#IP Address 192.168.20.1 255.255.255.0

#No Shutdown

ساختار مسیر ثابت برای روتر ۱

#IP Route 192.168.20.0 255.255.255.0 Serial 1/0

ساختار مسیر ثابت برای روتر ۲

#IP Route 192.168.10.0 255.255.255.0 Serial 1/0

ساختار مسیر Default برای روتر 1

#IP Route 0.0.0.0 0.0.0.0 Serial 1/1

۴.۹.۱ مزایای استفاده از مسیریابی ثابت (Static Routing)

۱. از Static Routing می‌توان برای تعیین یک مسیر پیش‌فرض خروج بسته اطلاعاتی، در صورت نبود آدرس مقصد آن بسته در Routing Table روتر استفاده کرد.
۲. از Static Routing می‌توان در شبکه‌های کوچک که نیاز به یک یا دو Route دارند، استفاده کرد.
۳. از Static Routing می‌توان در مواقعی استفاده کرد که Dynamic Routing در دسترس نباشد؛ به این معنا که می‌توان به‌عنوان یک Backup Routing یا بهتر است بگوییم؛ به‌عنوان یک مکمل در کنار Dynamic Routing از آن استفاده کرد.
۴. از Static Routing می‌توان به‌عنوان یک کمک برای انجام عملیات Routing از یک پروتوکول مسیریابی به پروتوکول مسیریابی دیگر بهره برد (Routing Redistribution).

۴.۹.۲ معایب استفاده از مسیریابی ثابت (Static routing)

۱. Human error: در بسیاری از موارد Static Route ها به‌صورت دستی در روتر تعریف می‌شود که سبب اشتباهات فردی می‌شود. اگر تنها یک Route به اشتباه در Router وارد شود، عملیات مسیریابی در کل شبکه از کار می‌افتد.
۲. Fault Tolerance: مسیریابی ثابت یا Static Routing از قابلیت Fault Tolerant یا تحمل خرابی پشتیبانی نمی‌کند. به این معنا که اگر یکی از Router ها در شبکه خراب شود یا تغییری در ساختار

فیزیکی شبکه ایجاد شود، دیگر ترافیک قابل مسیریابی در شبکه نمی‌شود. در نتیجه شبکه غیر قابل استفاده می‌شود و تا زمانی که مشکل برطرف نشده باشد کل شبکه فلج می‌شود.

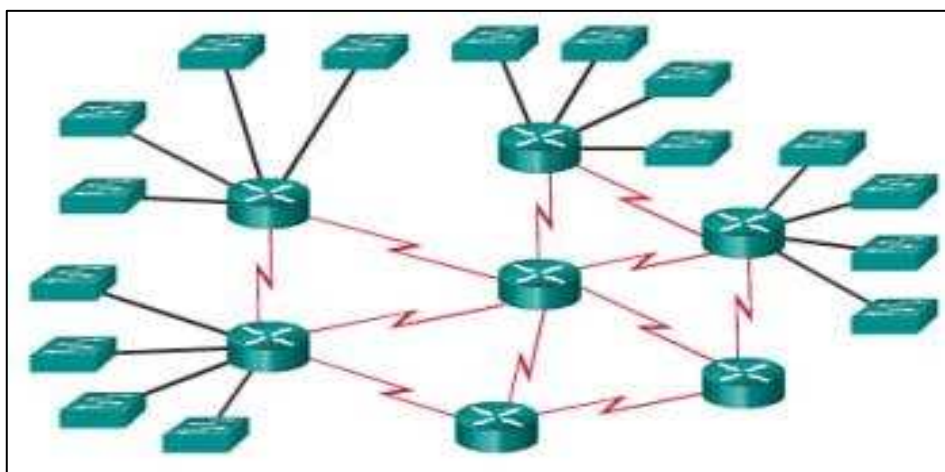
۳. Administrative Distance: مسیره‌های ثابت یا Static Route ها بر Dynamic Route ها تقدم دارند به این معناست که Static Route ها ممکن است مانع از کارکرد مناسب پروتوکول‌های مسیریابی یا Routing Protocol ها شود. که راهکار این مشکل تغییر دادن مقدار Administrative Distance پروتوکول مسیریابی است.

۴.۱۰ Dynamic Routing

Dynamic Routing از پروتوکول‌های مسیریابی (Routing Protocols) برای شناسایی شبکه‌ها و مقصدها و همچنین پیدا کردن بهترین مسیر برای رساندن بسته اطلاعاتی به مقصد استفاده می‌کنند. Dynamic Routing این قابلیت را به Routing Table می‌دهد که بتواند زمانی که یک Router خاموش است یا در دسترس نیست یا اینکه یک شبکه جدید به مجموعه اضافه می‌شود؛ این تغییرات را در Routing Table ها اضافه کند.

Dynamic Routing با استفاده از Routing Protocol ها این قابلیت را دارند که به صورت دائمی با شبکه تبادل اطلاعات داشته باشند و وضعیت هر یک از Router های شبکه را بررسی کنند و با استفاده از Broadcast و یا Multicast با هم ارتباط برقرار کنند و اطلاعات Routing Table را به روز (update) کنند. با این روش همیشه توپولوژی شبکه به روز (update) باقی می‌ماند و همه Router های شبکه از آخرین Routing Table بروز استفاده می‌کند. از پروتوکول‌های Dynamic Routing می‌توان به Routing Information Protocol یا RIP، Enhanced Interior Gateway Protocol (EIGRP) و Open Shortest Path First (OSPF) اشاره کرد.

شکل ذیل مثال از پروتوکول‌های متغیر Dynamic Routing Protocol را نشان می‌دهد.



شکل (۴-۶) مسیریابی متغیر (Dynamic routing)

۴.۱۰.۱ مزایای استفاده از مسیریابی متغیر (Dynamic routing)

۱. مناسب برای تمام انواع شبکه‌ها است.
۲. جدول مسیریابی را به‌طور خودکار می‌سازد.
۳. وقتی که یک ارتباط قطع شود، ترافیک را از شبکه احتمالی قابل دسترس ارسال می‌دارد.

۴.۱۰.۲ معایب استفاده از مسیریابی متغیر (Dynamic Routing)

۱. پیاده‌سازی (Configuration) سخت است.
۲. کمتر امن است، زیرا Update مسیریابی را با دیگر روترها به اشتراک می‌گذارد.
۳. هزینه اضافی را در منابع مانند CPU، حافظه و پهنای باند لینک قرار می‌دهد.

۴.۱۱ Default Route

Default Route یا مسیر پیش‌فرض که به Gateway of Last Resort یا آخرین محل رفت و آمد معروف است، یک نوع خاص از Static Route است. همانطوری که در Static Route شما یک مسیر را برای روتر مشخص می‌کنید تا به یک مقصد برسد، در Default Route شما یک مسیر را برای روتر مشخص می‌کنید تا زمانی که یک مقصد را شناسایی نکرد یا در Routing Table آن تعریف نشده بود، درخواست موردنظر را به مسیر پیش‌فرضی که برایش تعریف شده ارسال کند. به عبارت دیگر Default Route یک Network Route است، روتر زمانی که در IP Datagram آدرس Destination یا مقصدی را مشاهده کند که آن را شناسایی نکند، به این مسیر ارسالش می‌کند.

تمامی IP Datagram‌هایی که به‌صورت Unknown شناسایی می‌شوند، به سمت Default Route هدایت می‌شود.

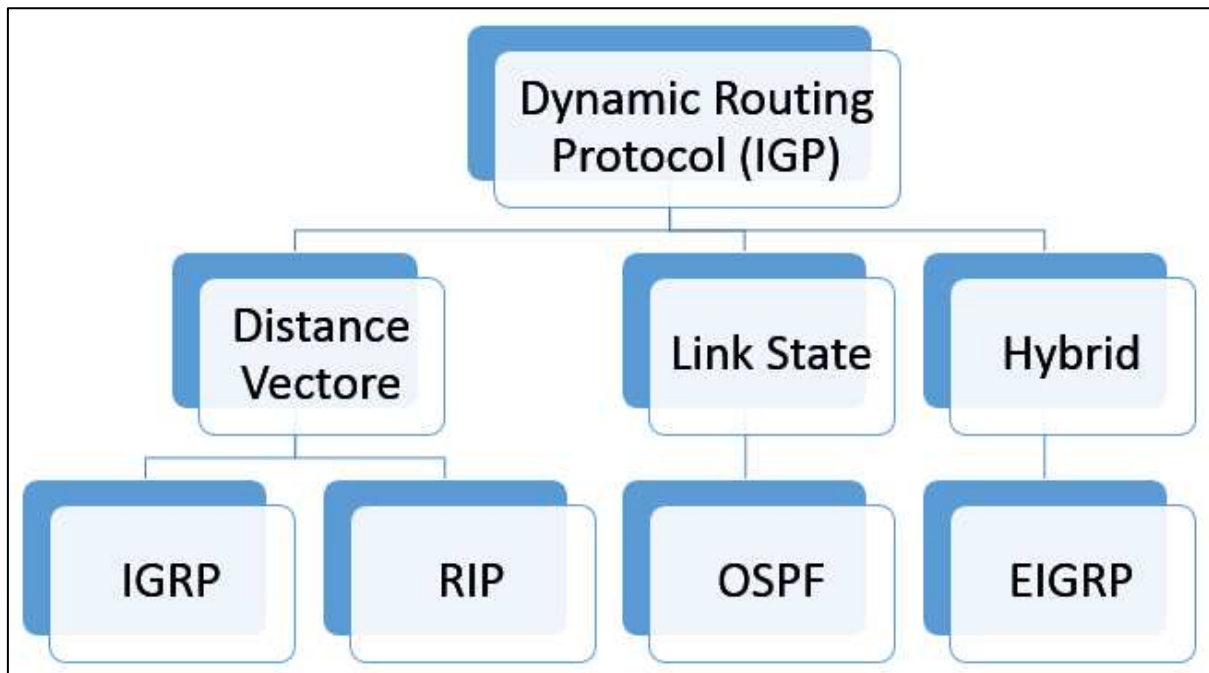
```
Router(config)# ip route 0.0.0.0 0.0.0.0 IP_address_of_next_hop_neighbor
[administrative_distance] [permanent]

Or

Router(config)# ip route 0.0.0.0 0.0.0.0 interface_to_exit
[administrative_distance] [permanent]
```

شکل (۴-۷) عیار سازی default route در روتر

به صورت کلی Routing Protocol های داخلی (IGP) به سه دسته تقسیم بندی می شود:



شکل (۴-۸) انواع پروتوکول های مسیریابی داخلی (IGP)

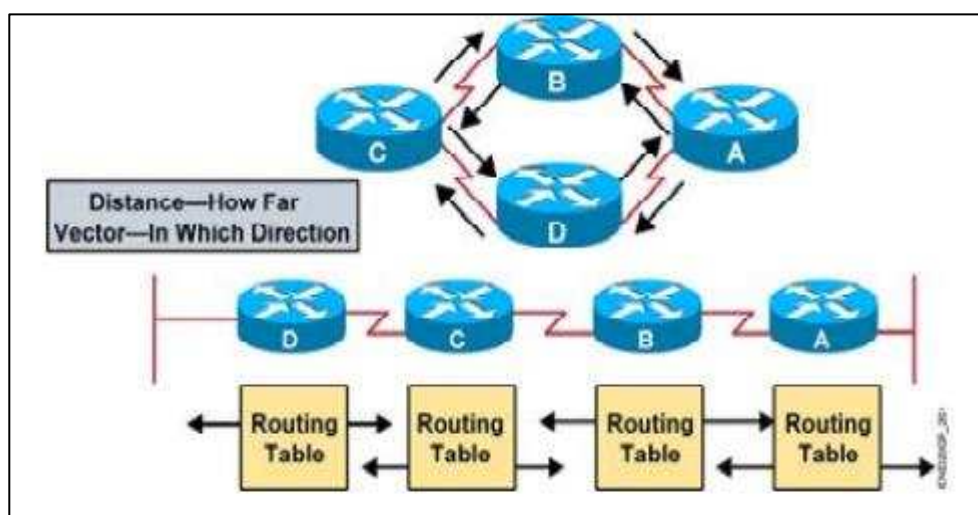
۴.۱۲ پروتوکول های Distance Vectore

همانطور که از نام اینگونه پروتوکول ها نیز پیداست از دو فاکتور، مسافت (Distance) و جهت (Vector) برای پیدا کردن مقصد استفاده می کنند. این پروتوکول ها به اساس Hop Count کار می کنند. روترهایی که از پروتوکول های مسیریابی Distance Vector استفاده می کنند به روترهای همسایه (Neighbor) های خود در خصوص توپولوژی شبکه و تغییراتی که در اوقات زمانی متفاوت انجام می شود، اطلاع رسانی می کنند، این اطلاع رسانی با استفاده از Broadcast انجام می شود و از آدرس IP ای، به شکل 255.255.255.255 برای اینکار استفاده می کند. پروتوکول های Distance Vector از الگوریتم Bellman-Ford برای پیدا کردن بهترین مسیر برای رسیدن به مقصد استفاده می کنند. روترهای مورد استفاده در توپولوژی های Distance Vector برای اینکه از اطلاعات موجود در Routing Table های روترهای همسایه خود مطلع شوند، بر روی Interface های خود، درخواست را Broadcast می کنند. این پروتوکول ها برای شریک کردن اطلاعات Routing Protocol خود نیز از ساختار Broadcasting استفاده می کنند.

الگوریتم های Distance Vector تغییراتی را که در Routing Table انجام می شود، بلافاصله برای روترهای همسایه خود در همه جهتها روی همه Interface ها ارسال می کند. با هر تبادلهایی که انجام می شود، روتر Distance Value مربوط به Route دریافت شده را افزایش می دهد و Distance Value خودش را نیز بر روی Route های جدید قرار می دهد. روتری که این تغییرات یا Update ها را دریافت می کند، نیز به

همین ترتیب Route های خودشان را بر روی این Table قرار می‌دهند و برای روترهای باقی‌مانده، ارسال می‌کنند. این پروسه به همین شکل ادامه پیدا می‌کند. پروتوکول‌های Distance Vector به این موضوع توجه نمی‌کنند که چه کسی به Update هایی که ارسال می‌شوند، گوش می‌کند. جالب اینجاست که بدانید پروتوکول‌های Distance Vector حتی در صورتی که هیچ تغییری در Routing Protocol خود نداشته باشند، هم بصورت متناوب Routing Table خود را Broadcast می‌کنند، یعنی حتی اگر توپولوژی شبکه شما تغییر هم نکرده باشد، Broadcasting انجام می‌شود.

پروتوکول‌های Distance Vector ساده‌ترین نوع از پروتوکول‌های مسیریابی یا Dynamic Routing می‌باشد، پیاده‌سازی و رفع مشکل این نوع از پروتوکول‌ها بسیار ساده است، همچنان روتر برای انجام پروسه‌های پروسس، نیاز به منابع بسیار کمتری دارد. منطق کاری Distance Vector ها ساده است، آنها Routing Update ها را دریافت می‌کنند، مقدار Metric را افزایش می‌دهند، نتایج را با مقادیر موجود در Routing Table خود مقایسه می‌کنند و در صورت نیاز Routing Table را Update می‌کنند. پروتوکول‌هایی مثل RIPv1 و IGRP از پروتوکول‌های Distance Vector می‌باشد.



شکل (۴-۹) کارکرد پروتوکول Distance Vector

۴.۱۳ Link State Routing Protocol های

الگوریتم‌های مورد استفاده در این نوع پروتوکول‌ها نسبت به Distance Vector ها کاملاً متفاوت عمل می‌کند و دارای پیچیدگی‌های خاص خود می‌باشد. در این الگوریتم‌ها از فاکتورهای مثل Hop Count، فاصله، سرعت، لینک و ترافیک به صورت هم‌زمان برای تعیین بهترین مسیر و بهترین Cost برای انجام عملیات Routing استفاده می‌شود. روترهایی که از پروتوکول‌های Link State استفاده می‌کنند، فقط زمانی معلومات Routing Table های خود را به همدیگر ارسال می‌کند که چیز جدید به Routing Table یکی از Router ها اضافه شده باشد. به همین دلیل کمترین ترافیک را در هنگام یکسان سازی Routing Table با همدیگر ایجاد می‌کنند. الگوریتم‌های مسیریابی مثل OSPF از نوع پروتوکول‌های Link State هستند.

در پروتوکول‌های Link State هر یک از روترهایی که از یکی از پروتوکول‌های Link State استفاده می‌کند، اطلاعات کاملی در مورد خود روتر، لینک‌های مستقیم متصل شده به آن و وضعیت آن لینک‌ها را در اختیار شبکه قرار می‌دهد. این اطلاعات توسط پیام‌های Multicast به همه روترهای موجود در شبکه ارسال می‌شود، دقیقاً بر خلاف پروتوکول‌های مسیریابی Distance Vector که اینکار را به وسیله استفاده از Broadcast انجام می‌دهند.

پروسه مسیریابی Link State به گونه ای است که با ایجاد شدن کوچکترین تغییری در توپولوژی شبکه‌های موجود، بلافاصله این تغییر به صورت Incremental برای سایر روترها هم ارسال می‌شود تا توپولوژی شبکه روی همه روترها همیشه به‌روز (update) باشد. هر کدام از روترهای موجود در شبکه‌های Link State، یک کاپی از این توپولوژی شبکه را در خود دارند و آن را تغییر نمی‌دهند. بعد از اینکه آخرین تغییرات شبکه‌ها را دریافت کردند، هر روتر به صورت کاملاً مستقل به محاسبه بهترین مسیرها برای رسیدن به شبکه‌های مقصد می‌پردازد.

پروتوکول‌های مسیریابی Link State بر اساس الگوریتم SPF (shortest path first) برای پیدا کردن بهترین مسیر برای رسیدن به مقصد پایه‌ریزی شده اند. نام دیگر این الگوریتم Dijkstra است. در الگوریتم SPF، زمانی که وضعیت یک لینک ارتباطی تغییر می‌کند، یک Routing Update که به عنوان Link-State Advertisement یا LSA شناخته می‌شود ایجاد شده، بین تمامی روترهای موجود تبادل می‌شود.

زمانی که یک روتر LSA Routing Update را دریافت می‌کند، الگوریتم Link-State با استفاده از آن کوتاه‌ترین مسیر را برای رسیدن به مقصد مورد نظر محاسبه می‌کند. هر روتر برای خود یک نقشه کامل از شبکه‌ها ایجاد می‌کند. چند نکته مهم در مورد پروتوکول‌های Link State وجود دارد که قرار ذیل بیان می‌شود.

- Link-State Advertisement یا LSA: یک Packet کوچک اطلاعاتی است که در آن اطلاعات مربوط به Routing بین روترها رد و بدل می‌شود
- Topological Database : مجموعه اطلاعاتی که از LSA ها دریافت می‌شود.
- الگوریتم SPF یا Dijkstra : الگوریتمی است که محاسبات بر روی database های موجود در SPF Tree را انجام می‌دهد.
- Routing Table: یک لیست از مسیرها و Interface های شناسایی شده است.

پروتوکول‌های مسیریابی Link State در عین این که به مدت زمان کمتری برای Converge شدن نسبت به پروتوکول‌های مسیریابی Distance Vector برخورد دارند، در مقابل به وجود آمدن Routing Loop هم نسبت به Distance Vector ها مقاوم‌تر هستند و کمتر موردی پیش می‌آید که Routing Loop در پروتوکول‌های Link State ایجاد شود. اما از طرفی دیگر الگوریتم‌های مورد استفاده در پروتوکول‌های Link State به قدرت پروسس CPU و حافظه RAM به نسبت پروتوکول‌های Distance Vector نیاز دارند.

پروتوکول‌های Link State از یک ساختار سلسله مراتبی و موروثی استفاده می‌کنند که این ساختار باعث کاهش فاصله‌ها و نیاز کمتر به انتقال LSA ها می‌شود. پروتوکول‌های Link State از مکانیزم Multicast برای اشتراک‌گذاری اطلاعات مسیریابی استفاده می‌کنند، فقط روترهایی که از پروتوکول‌های مسیریابی Link State استفاده می‌کنند، این Routing Update ها را پروسس می‌کنند. Link State ها فقط زمانی اطلاعات روتر را ارسال می‌کنند که در شبکه تغییری ایجاد شده باشد و صرفاً همان تغییر را برای سایر روترها ارسال می‌کنند. پیاده‌سازی پروتوکول‌های مسیریابی Link-State پیچیده‌تر و پرهزینه‌تر از پیاده‌سازی پروتوکول‌های Distance Vector می‌باشد و هزینه نگهداری پروتوکول‌های Link-State نسبت به پروتوکول‌های Distance Vector بیشتر می‌باشد.

۴.۱۴ Hybrid Routing Protocol های:

همانطوری که از نام این پروتوکول ها نیز مشخص است، این پروتوکول ها از ترکیب شدن پروتوکول های مسیریابی Distance Vector و پروتوکول های مسیریابی Link State تشکیل شده اند.

در حقیقت این نوع پروتوکول های مسیریابی از نقاط قوت هر دو نوع پروتوکول Distance Vector و Link State را در یک پروتوکول جمع کرده اند. اما حقیقت امر این است که در واقع پروتوکول های مسیریابی Hybrid یک نوع پروتوکول مسیریابی Distance Vector هستند که بسیاری از مزایا و امکانات پروتوکول های Link State به داخل آنها اضافه شده است. مانند پروتوکول مسیریابی EIGRP که مخفف کلمات Enhanced Interior Gateway Routing Protocol است به عنوان یک پروتوکول مسیریابی Hybrid معرفی می شود که ویژگی های پروتوکول های Distance Vector و Link State را در خود دارد. یعنی زمانی که صحبت از قدرت پردازشی (Process) روترها می شود، از قابلیت های Distance Vector و زمانی که صحبت از تبادل Routing Table در شبکه باشد، از قابلیت Link State استفاده می کند.

EIGRP برخلاف OSPF که Link State Advertisement یا LSA ارسال می کند، به عوض آن به صورت قدیمی از طریق شیوهی که در پروتوکول های Distance Vector مورد استفاده قرار می گیرد، از طریق Update کردن اطلاعات مربوط به شبکه ها، به علاوه Cost مربوط به دسترسی به هر یک از مسیرها پروسه شبیه به همان LSA را انجام می دهد. EIGRP همچنین ویژگی های پروتوکول های Link State را نیز دارد. EIGRP در زمان startup محتویات routing table خود را با سایر شبکه های همسایه (neighbor) خود یکپارچه سازی و synchronize می کند. هر زمان که احساس کند تغییری در توپولوژی شبکه ایجاد شده است، بلافاصله این تغییرات را اعلام می کند.



خلاصه فصل چهارم

روتینگ (Routing) یکی از مجهزترین ویژگی‌های موردنیاز در یک شبکه (Network) به منظور ارتباط با سایر شبکه Host. از Routing به منظور دریافت یک بسته اطلاعاتی (Packet) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاه دیگر بر روی شبکه استفاده می‌شود.

برای پیکربندی جدول مسیریابی روتر، به صورت Static مدیر شبکه باید از اطلاعات مربوط به شبکه‌های موجود و مسیر یابی آنها آگاهی داشته باشد و به صورت دستی مسیرها و شبکه‌ها را درون این جدول اضافه نماید. در مسیریابی (Dynamic) از پروتوکول‌های مسیریابی (Routing Protocol) برای شناسایی شبکه‌ها و مقصدها و همچنین پیدا کردن بهترین مسیر برای رساندن بسته اطلاعاتی به مقصد استفاده می‌کند. به روترها غالباً Gateway هم گفته می‌شود، هم Host مبدأ و هم Router به یک برآورد اولیه برای اینکه چگونه بسته را ارسال کند، نیاز دارد. بسته‌های IP براساس اینکه مقصد نهایی مستقیماً در یک شبکه متصل به شبکه خودش است یا نه؟ می‌تواند حداقل از یکی و یا از دو نوع تحویل استفاده کند که به تحویل مستقیم و غیر مستقیم معروف هستند.

به صورت کلی Routing Protocols به سه دسته تقسیم می‌شوند:

۱. Routing Protocol های Distance Vector که از معیارهای Hop Count یا تعداد روترهای مسیر برای Metric در Routing Table های خود استفاده می‌کنند.
۲. پروتوکول‌های Link State نسبت به Distance Vector کاملاً متفاوت عمل می‌کند و دارای پیچیدگی‌های خاص خود می‌باشد. در این الگوریتم‌ها از فاکتورهای مثل Hop Count، فاصله، سرعت، لینک و ترافیک به صورت هم‌زمان برای تعیین بهترین مسیر استفاده می‌کند و از الگوریتم Dijkstra استفاده می‌کند.
۳. روتینگ پروتوکول‌های Hybrid، همانطوریکه از نام این پروتوکول معلوم است، پروتوکول ترکیبی است که از خوبی‌های پروتوکول‌های Distance Vector و Link State استفاده می‌کند.



۱. موارد استفاده از روتینگ را خلاص توضیح دهید.
۲. یک روتر به منظور مسیریابی یک بسته اطلاعات، به کدام اطلاعات آگاهی داشته باشد؟
۳. مسیریابی IP، ثابت و متغیر را توضیح دهید.
۴. Default Route چیست؟ توضیح دهید.
۵. دستور ساختار Default Route را در یک Router توضیح دهید.
۶. جدول مسیریابی (IP Routing Table) چیست؟ توضیح دهید.
۷. مزایا و معایب Static Route را برشمارید.
۸. مزایا و معایب Default Route را برشمارید.
۹. Autonomous System چیست؟ توضیح دهید.
۱۰. تفاوت میان IGP و EGP را واضح سازید.
۱۱. Administrative Distance و Metric چیست؟ واضح سازید.
۱۲. Routing Protocol های Distance Vector را توضیح و نام ببرید.
۱۳. Routing protocol های Link State را شرح و نام ببرید.
۱۴. Routing Protocol های Hybrid را توضیح نموده و نام ببرید.



فعالیت‌های فصل چهارم

- در نرم افزار packet tracer توپولوژی را رسم نمایید که دارای سه روتر باشد، با استفاده از (static route و default route) مسیریابی را بین آنها فعال نمایید.
- در باره تفاوت پروتوکول‌های Dynamic را بین گروپ‌ها بحث نمایید.

فصل پنجم

سوئیچ سیسکو (Cisco Switch)



هدف کلی: آشنایی با سوئیچ‌های سیسکو و تنظیمات اولیه آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. اجزای داخلی سوئیچ را تشریح نمایند.
۲. تنظیمات ابتدایی سوئیچ را انجام دهند.
۳. محیط CLI سوئیچ و مدهای آن را شرح نمایند.
۴. تنظیمات انواع پسورد را انجام دهند.
۵. انترفیس VLAN1 را تنظیم نمایند.
۶. وظایف سوئیچ‌های لایه دوم را توضیح دهند.
۷. میتودهای انتقال فریم در شبکه LAN را توضیح نمایند.

سوئیچ‌های سیسکو (Cisco switches) جزو پر مصرف‌ترین و پرتعدادترین وسیله‌هایی به حساب می‌رود که در شبکه‌ها، دیتاسنترها، سازمان‌ها، موسسات و شرکت‌ها مورد استفاده قرار می‌گیرد. سوئیچ‌های سیسکو (Cisco switches) اولین لایه برای متصل شدن دستگاه‌ها، کامپیوترها، سرورها، کامره‌های امنیتی و ... به شبکه می‌باشد. به همین خاطر از اهمیت بسیار زیادی برخوردار هستند. بیشتر سوئیچ‌های سیسکو (Cisco switches) در لایه 2 مدل OSI یا Data Link عمل کرده و وظیفه (Forward) کردن یا سوئیچینگ فریم‌های دریافت شده به پورت‌های خود و انتقال آن‌ها به پورت‌های دیگر را بر عهده دارد. سوئیچ‌های شرکت سیسکو (Cisco) پایداری خوبی دارند و با امکانات و ویژگی‌های خاص که دارند، مسئول شبکه به راحتی می‌تواند پورت‌ها و نودهای شبکه را مدیریت کرده، از قابلیت‌های امنیتی سوئیچ در افزایش سطح امنیتی شبکه استفاده کند. در این فصل به اجزای داخلی سوئیچ سیسکو پرداخته شده است. با استفاده از محیط خط فرمان (CLI) تنظیمات ابتدایی سوئیچ و نحوه تنظیم انواع پسوردها تشریح شده است. نحوه تنظیم انترفیس VLAN1 و وظایف سوئیچ‌های لایه دوم به صورت اساسی تشریح شده است و هم‌چنان در اخیر میتودهای انتقال فریم در شبکه LAN توضیح داده شده است.

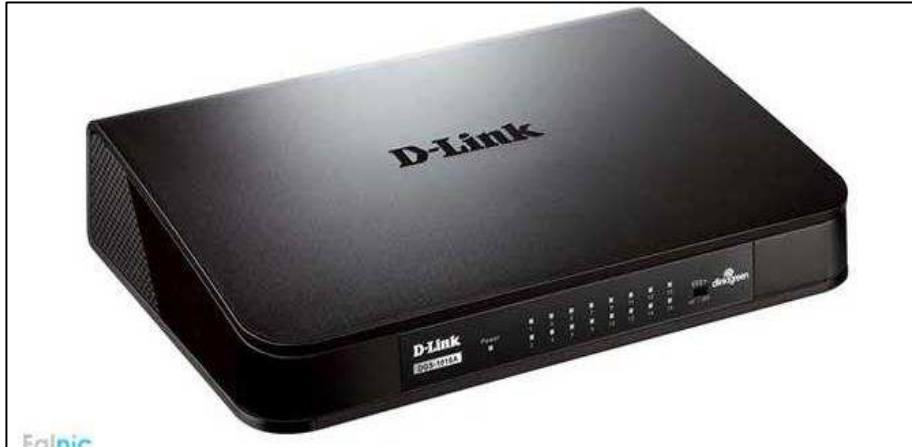
۵.۱ سوئیچ (Switch)

سوئیچ یکی از سخت‌افزارهای شبکه است که در عین شباهت به (Hub)، بسیار هوشمندتر از آن است. براساس مدل OSI سوئیچ‌ها در لایه 2 یا همان لایه Data Link کار می‌کنند. وظیفه این سخت‌افزارها، انتقال بسته‌های دیتا از یک دستگاه به دستگاه دیگر از طریق شبکه و براساس آدرس سخت‌افزاری MAC Address است. در یک شبکه که کامپیوترها توسط Switch به هم متصل هستند، چندین کاربر می‌توانند در یک لحظه اطلاعات را از طریق شبکه ارسال نمایند و در این حالت سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تأثیر نخواهد کرد. تصادمی میان بسته‌های اطلاعاتی صورت نمی‌گیرد و ارتباط کاملاً دو طرفه می‌باشد. یکی از خوبی‌های موجود در سوئیچ‌ها این است که در هر لحظه، یک سرعت ارتباطات دو طرفه مابین دو Device موجود در شبکه ایجاد می‌کنند، همین امر باعث بلند بردن سرعت این شبکه می‌شود.

۵.۲ انواع Switch ها

۵.۲.۱ سوئیچ های غیر قابل کنترل Unmanageable Switches:

این نوع سوئیچ ها طبق آن معیارهایی که کمپنی سازنده تعیین کرده کار می کند و نمی توان آن ها را مدیریت کرد.



شکل (۵-۱) سوئیچ غیر قابل کنترل

۵.۲.۲ سوئیچ های قابل کنترل Manageable Switches:

یک سوئیچ را در نظر بگیرید: می دانیم که همه سوئیچ ها Mac Address Table دارند، اما گاهی قصد داریم تعیین کنیم که سوئیچ به چه صورت روی این جدول کار کند. برای کارهای این چینی، باید سوئیچ راهی داشته باشد که بتوانیم آن را مدیریت کنیم، یعنی باید یک خروجی داشته باشد که از طریق آن بتوانیم به سیستم عاملی که درون سوئیچ وجود دارد، دستور بدهیم که چه کارهایی را انجام دهد و چه کارهایی را انجام ندهد، در نتیجه باید از سوئیچ های Manageable استفاده کنیم.



شکل (۵-۲) سوئیچ قابل کنترل

به طور دقیق زمانی می توانیم روی یک دستگاه پیکربندی (Configuration) انجام دهیم که بتوانیم با آن ارتباط برقرار کنیم، پس داخل دستگاه سیستم عامل گنجانیده شده و سیستم عامل داخل دستگاه های Cisco و IOS است.

۵.۳ عناصر داخلی سوئیچ ها

۵.۳.۱ پردازنده مرکزی (CPU)

ترافیک ورودی را با جداول بالاتر مقایسه می نماید و تصمیم می گیرد که به یک پورت خاص ارسال بدارد یا اینکه به صورت عمومی به همه پورت ها بجز از پورت ورودی ارسال بدارد.

۵.۳.۲ RAM

در دستگاه های کمپیوتر، حافظه موقتی است. یقیناً (Running Config) که در حافظه RAM گنجانیده می شود، چیزی است که می تواند فرار کند.



شکل (۳-۵) حافظه RAM

۵.۳.۳ NV RAM

حافظه غیر فرار و ماندگار است. خودش در قالب فایل Config.text داخل Flash ذخیره می شود، فقط چون در قالب یک حافظه جداگانه در حافظه RAM بالا می آید، به آن NV RAM گفته می شود. یعنی یک Process حافظه بی می گیرد.



شکل (۴-۵) NV RAM

ROM ۵.۳.۴

حافظه ROM در دستگاه‌های Cisco، بوت (Boot) شدن دستگاه را برعهده دارد و مشخصات دستگاه و پارامترهای Boot دستگاه را نشان می‌دهد. درواقع نشان می‌دهد که IOS دستگاه چیست و از کجا باید شروع به Load شدن کند.



شکل (۵-۵) ROM

:Flash ۵.۳.۵

مثل فلش‌های معمولی است که داخل دستگاه قرار داده شده است. سیستم عامل روتر در آن قرار دارد. در Routerهای Cisco می‌توانیم این فلش را بیرون بیاوریم که با این کار، سیستم بدون سیستم‌عامل (IOS) می‌شود.



شکل (۵-۶) ساختمان ظاهری فلش Flash

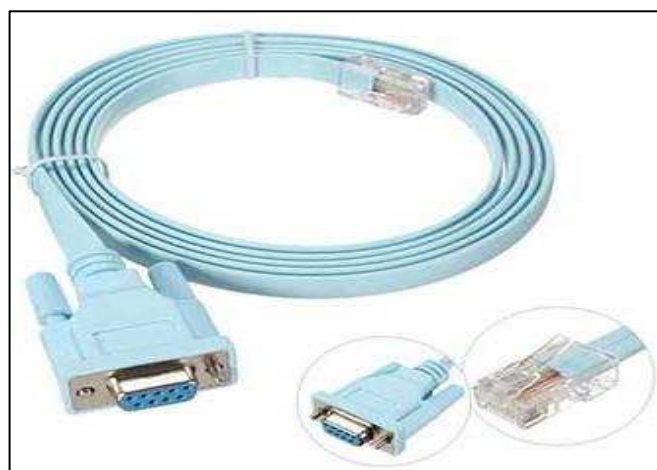
وقتی که به دستگاه وصل می‌شویم و می‌خواهیم شروع به کارکردن با IOS کنیم، صفحه‌ی مقابل ما قرار می‌گیرد که به نام CLI یاد می‌شود. از طریق آن می‌توانیم دستورهای مربوط به دستگاه را بنویسیم، هرکاری که در این محیط انجام می‌دهیم، داخل Running Config اتفاق می‌افتد که دستورات را اجرا می‌کند.

اما اگر دستگاه را خاموش و روشن کنیم، این حافظه از بین می‌رود، مگر اینکه دستورات را در قالب فایل به نام Config.text ذخیره کنیم. این فایل داخل Flash ذخیره می‌شود، هر بار که دستگاه بالا می‌آید، محتویات این فایل را داخل حافظه RAM، Load می‌کند و در قالب Running config به محتویاتی که مقابل چشم ماست، اضافه می‌کند.

۵.۴ تنظیمات اولیه سوئیچ‌های سیسکو Cisco Switch Basic Configuration

چگونه می‌توان با یک سوئیچ ارتباط برقرار کرد؟ سوئیچ دارای یک Port است که بر روی آن Console نوشته شده است. یک کیبل آبی فیروزه‌یی یا مشکی داریم به نام کیبل Console که یک سر آن ساکت RJ45 است و سر دیگر آن RS232 است.

قسمت RJ45 به Port Console متصل می‌شود و طرف RS232 به PC که قرار است با استفاده از آن سوئیچ را Configure کنیم، متصل می‌شود. کیبل کنسول در شکل زیر نشان داده می‌شود:



شکل (۷-۵) ساختمان کیبل کنسول

کیبل Console کیبل Ethernet به حساب نمی‌آید. کیبل Serial است و برای Config و تنظیم دستگاه استفاده می‌شود.

نکته: برای Configure دستگاه نیاز به لپ‌تاپ داریم. لپ‌تاپ‌های امروزه پورت RS232 را ندارند، در اینجا ما به یک تبدیل نیاز داریم که به آن تبدیل RS232 به USB گفته می‌شود که به شکل زیر است:



شکل (۷-۵) تبدیل USB به RS232

عملکرد این کیبل به اینگونه است که RS232 را می‌گیرد و به USB تبدیل می‌کند تا بتوانیم آن را به لپ‌تاپ وصل کنیم. حال برای اینکه بتوانیم در لپ‌تاپ خودمان محیط Config را ببینیم، احتیاج به یک نرم‌افزار (ترمینال) داریم؛ مانند HyperTerminal، Putty، Secure CRT و...

RS232 یک کیبل Serial است، با این کیبل باید از طریق نرم‌افزارهای Terminal با دستگاه ارتباط برقرار کنیم.

سوئیچ را روشن می‌کنیم، همان‌طور که می‌دانیم، سوئیچ یک دستگاه Active است و چون به Power متصل است، کیبل کنسول را برداشته و سر RJ45 آن را به سوئیچ و سر RS232 آن را به کامپیوتر وصل می‌کنیم. سپس داخل Desktop به دنبال یک نرم‌افزار Terminal می‌گردیم، مانند Putty.

این نرم‌افزار کارهای مختلفی می‌تواند انجام دهد. از جمله اینکه می‌تواند به کیبل Serial وصل شود. در قسمت Session Type، Connection Type را بر روی Serial گذاشته و قسمت Bit Per Second را روی 9600 قرار می‌دهیم، با این مقدار Bandwidth، ارتباط برقرار است و OK می‌کنیم. با این کار به محیط CLI وارد شده‌ایم.

۵.۵ پیکربندی ابتدایی سوئیچ Switch Basic Configuration:

فرض کنید یک سوئیچ سیسکو 2960 خریداری کرده‌اید و نیاز دارید که ابتدا تنظیمات اولیه را بالای آن اجرا نمایید، برای شروع، ابتدا سوئیچ سیسکو را با کیبل کنسول سیسکو به یک PC با پورت سریال متصل و با یک برنامه ترمینال مثل Putty به آن متصل شوید.

پس از اینکه موفق به ارتباط با سوئیچ یا روتر سیسکو خود شدید، حال قادر خواهید بود تنظیمات مقدماتی را روی آن انجام دهید. این تنظیمات عبارتند از:

- انتخاب یک نام برای سوئیچ خود (hostname)

- تخصیص (Privileged Level)
- امن نمودن (VTY Lines)
- Encrypt نمودن Passwordها

انتخاب نام مناسب برای سوئیچ یا روتر خود روی شبکه بسیار مفید خواهد بود و در صورتی که تعداد آن‌ها در مجموعه بیشتر شود. شناسایی آن‌ها تنها با نام به راحتی قابل انجام است. در صورتی که در شبکه، بخش‌های متعددی وجود دارد، انتخاب این اسم‌ها را می‌توانید با توجه به نام آن بخش انجام دهید. برای تنظیم نام، ابتدا باید حق دسترسی Administrator به دستگاه خود بدهید و سپس به حالت تنظیم دستگاه بروید.

دستورات زیر برای این منظور استفاده می‌شوند. برای بازگشت به مود اولیه از دستور disable می‌توانید استفاده کنید.

Enable administrative privilege

Switch>enable

Enter the configurationmode:

Switch #configure terminal

Hostname: حال برای اینکه نام سوئیچ خود را به‌طور مثال به "نام دلخواه" تغییر دهید، از دستور ذیل استفاده کنید:

Switch(config)#hostname TVET

TVET(config)#

همانطور که مشاهده می کنید نام سوئیچ در خط های دستور به TVE تغییر کرد. حال نوبت آن است که Privileged Level Secret را تنظیم کرده، برای آن کلمه عبوری (پسورد) تعیین کنید. فایده این کار این است که اعمال تغییرات در سیستم سیسکو را محدود کرده و هر شخصی امکان Enable کردن سیسکو و اعمال تغییرات را نخواهد داشت. برای انجام این منظور از دستورات زیر استفاده کنید:

```
Enable administrativeprivilege
```

```
TVET >enable
```

```
configuration mode: Enter the
```

```
TVET #configureterminal
```

```
TVET (config)#enable secret cisco
```

حال باید برای امن کردن بیشتر کنسول Administrator را نیز امن کنید. لذا مراحل زیر را انجام دهید تا برای کنسول نیز کلمه عبور (پسورد) تنظیم کنید.

```
TVET >enable
```

```
TVET #configure terminal
```

```
TVET (config)#line console 0
```

```
TVET (config-line)#password 123456
```

```
TVET (config-line)#login
```

Use the “logging synchronous” command, so the messages appear only after you press Return

```
TVET (config-line)#logging synchronous
```


دستور آخر درواقع به معنی Apply کردن تنظیمات شما است.

همانطور که می دانید برای ارتباط از راه دور با سوئیچ یا روتر سیسکو از دستورات زیادی مانند Telnet, SSH استفاده می شود. این روش یک ارتباط را از طریق خطوط VTY برقرار می سازند. با توجه به این مطلب این خطوط نیز باید ایمن شوند و از کلمه عبور (پسورد) استفاده شود. برای تنظیم کلمه عبور (پسورد) بر روی این خطوط از دستور زیر استفاده می شود:

```
TVET >enable
```

```
TVET #configureterminal
```

```
TVET (config)#line vty 0 4
```

```
TVET (config-line)#password 123456
```

```
config-line)#login(TVET
```

```
TVET (config-line)#logging synchronous
```

باید توجه داشته باشید که کلمه های عبوری که در Running – Config ذخیره شده اند. به صورت (واضح) Plain Text استفاده کرده اید و قبل از ذخیره نمودن نهایی آن ها باید رمزگذاری یا Encrypt شوند. برای انجام این کار از دستورهای زیر استفاده کنید.

```
TVET >enable
```

```
TVET #configure terminal
```

```
TVET (config)#service password-encryption
```

حال برای نمایش پسورد که آیا به رمز تبدیل شده یا نه، از دستور ذیل استفاده کنید:

```
TVET #show running-config
```

دیده می شود که پسوردهای خطوط کنسول و VTY به رمز تبدیل شده و از حالت متن واضح (plain text) خارج شده است.

line con 0

password 7 08701E1D5D4C53

logging synchronous

!

line vty 0 4

password 7 08701E1D5D

logging synchronous

فراموش نکنید که تغییرات شما در Running – Config هستند و هنوز ذخیره نهایی نشده است. برای اینکه آن را در حافظه دائمی ذخیره کنید، از دستور زیر استفاده کنید.

TVET#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

TVET#

۵.۶ تنظیم انترفیس VLAN ۱

تا حال یاد گرفتیم که چطور باید به یک سوئیچ سیسکو وصل شویم و چطور باید تنظیمات اولیه را انجام دهیم. اما باید به یاد داشته باشید که همیشه نمی‌توان به صورت مستقیم و با کیبل به دستگاه سیسکو خود وصل شویم و نیاز به ارتباط از راه دور روی شبکه همیشه وجود خواهد داشت. شما باید قادر باشید از راه دور و از طریق کامپیوترتان به دستگاه وصل شوید، آن را چک کنید، تغییرات وارد کنید و یا تنظیم کنید. برای انجام این کار باید به دستگاه خود IP بدهید. شما باید یک IP از رنج شبکه برای این کار اختصاص دهید. برای تنظیم IP دستگاه خود، مراحل زیر را باید انجام دهید:

در ابتدا باید به دستگاه خود Login کنید دستور زیر را اجرا کنید.

```
TVET > enable
```

رمز عبور (پسورد) را وارد کنید (در صورتی که در مرحله قبل تنظیم نکرده‌اید، تنها دکمه انتر را بزنید)

```
TVET # Config Terminal
```

```
TVET (config)# interface vlan 1
```

```
TVET (config-if) #
```

```
TVET (config-if) #ip address 192.168.1.100 255.255.255.0
```

```
TVET (config-if) # no shutdown
```

```
TVET (config-if) #end
```

فراموش نکنید که تغییرات و تنظیمات خود را حتماً باید در آخر ذخیره کنید. برای این کار – Running Config را که حکم حافظه موقت برای دستگاه دارد، باید به Startup-Config - که مانند هاردیسک دستگاه شما است - کپی کنید.

```
TVET#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
TVET#
```

چند نکته مهم

- سوئیچ‌های سیستم یک VLAN Database دارند که اطلاعات هر VLAN در آن ذخیره با سایر سوئیچ‌های سیستم به اشتراک گذاشته می‌شود، برای ایجاد هر VLAN، حتماً باید آن VLAN در VLAN database موجود باشد.
- سوئیچ‌های لایه 2 سیستم قابلیت IP Routing نداشته و برای Routing باید از یک روتر برای Inter VLAN Routing استفاده کرد.
- سوئیچ‌های سیستم به صورت پیش فرض به صورت یک سوئیچ معمولی عمل می‌کنند و تمامی پورت‌های آن‌ها در حالت فعال و به صورت پیش فرض عضو VLAN 1 هستند، پس می‌توانید از باکس خارج کنید و با وصل کردن به برق، استفاده کنید.

۵.۷ عملکرد سوئیچ و اصطلاحات رایج سوئیچینگ

سوئیچ (switch) یکی از عناصر اصلی و مهم در شبکه‌های کمپیوتری است. در این دستگاه علاوه بر دریافت و ارسال سیگنال، کارهای دیگری نیز انجام می‌شود. در حقیقت حدود عملیاتی که در Switch انجام می‌شود، لایه datalink می‌باشد. در واقع switch در دو لایه پایینی OSI کار می‌کند.

در یک شبکه که کمپیوترها توسط سوئیچ به هم متصل هستند، چندین کاربر می‌توانند در یک لحظه اطلاعات را از طریق شبکه ارسال نمایند. در این حالت سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تأثیر نخواهد گذاشت. در این صورت برخوردی میان بسته‌های اطلاعاتی صورت نمی‌گیرد و ارتباط کاملاً دو طرفه می‌باشد. در واقع یکی از خوبی‌های موجود در سوئیچ‌ها این است که در هر لحظه یک ارتباطات دو طرفه مابین دو device موجود در شبکه ایجاد می‌کنند. همین امر باعث افزایش سرعت شبکه می‌شود.

۵.۸ سوئیچ در لایه دوم (Data Link Layer) مدل OSI

سوئیچ در لایه دوم مدل OSI وظیفه انجام می‌دهد. بدین معناست که به صورت هوشمند مسیر اطلاعات را مشخص می‌کند. به طور مثال اگر یک بسته اطلاعاتی مقصدش کمپیوتر شماره ۱ باشد، سوئیچ، آن بسته را فقط برای همان کمپیوتر ارسال می‌کند. سوئیچ در یک لیست، آدرس پورت‌های خود و آدرس کمپیوترهای متصل به آن پورت‌ها را ذخیره کرده، با استفاده از آن می‌تواند مسیر اطلاعات را مشخص کند.

برای اطمینان از سالم دریافت شدن اطلاعات در کمپیوتر مقصد، نیاز به یک راهکار مناسب می‌باشد. در ساختار FRAME قسمتی تحت عنوان Cyclic redundancy check وجود دارد که به وسیله آن کمپیوتر

مقصد در می‌باید که آیا اطلاعات دریافتی را صحیح و سالم گرفته است یا نه! به این فعالیت CRC گفته می‌شود.

سوئیچ سیگنال‌ها را دریافت کرده، پس از دریافت سیگنال‌ها یک Frame به صورت کامل، ابتدا اقدام به کنترل crc می‌نماید. در صورتی که crc نشان‌دهنده سالم بودن Frame باشد. در مرحله بعدی آدرس مبدأ و مقصد mac address را کنترل می‌کند. با کنترل آدرس مبدأ و شماره پورت و address mac مربوط به کامپیوتر ارسال کننده، در جدول Filter/Forward Table ثبت می‌شود. سپس در صورتی که مقصد نیز در جدول مذکور شناخته شده بود، اطلاعات صرفاً به همان پورتی که مقصد به آن متصل است، ارسال می‌شود.

در صورت وجود نداشتن آدرس کامپیوتر مقصد در جدول مذکور، با توجه به اینکه معلوم نیست مقصد بر روی کدام پورت است؟ Frame دریافت شده توسط Switch به تمام پورت‌ها ارسال شده یا اصطلاحات Flood می‌شود. ضمناً در صورتی که یک Frame از نوع Broadcast به Switch برسد، به تمام پورت‌ها Flood می‌شود.

تعداد پورت‌های Switch در برخی مدل‌ها بیش از ۴۸ عدد می‌باشد و دارای کاربردها و مدل‌های بسیار متفاوتی می‌باشد. قابل ذکر است: با توجه به کاربردهای متفاوت از سوئیچ‌های متفاوت با ابعاد و توانایی‌های گوناگون استفاده می‌شود. سوئیچ‌هایی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می‌شوند، سوئیچ‌های LAN نامیده می‌شوند.

۵.۹ مهم‌ترین روش‌های مسیریابی سوئیچ

۵.۹.۱ Packet – Switching

سوئیچ‌ها بر مبنای Packet-Switching کار می‌کنند و بین سگمنت‌هایی که از نظر بُعد مکانی از هم به حد کافی دور می‌باشند، ارتباط برقرار می‌سازد. بسته‌های اطلاعاتی وارده در Buffer نگهداری می‌شوند. آدرس‌های Mac در قسمت Header فریم نگهداری می‌شوند. آدرس‌های مذکور که در این قسمت قرار دارد، خوانده می‌شوند و با جدول Mac سوئیچ (MAC Table) مقایسه می‌شوند. همچنین فریم اینترنت در یک شبکه LAN قسمتی به نام Payload دارد که شامل MAC Address مبدأ و مقصد می‌باشد. همانطور که قبلاً گفته شد، سوئیچ MAC Address مبدأ و مقصد را چک کنید، در صورتی که آدرس مقصد را در جدول مک آدرس‌های خود داشت، برای مقصد ارسال می‌کند.

منظور از حافظه بافر (Buffer Memory) در رابطه با سوئیچ چیست؟

حافظه بافر، یک ناحیه ذخیره‌سازی برای رسیدگی به دیتاهای عبوری می‌باشد. بافرها معمولاً برای دریافت و ذخیره‌سازی اطلاعات پراکنده را که پشت سر هم توسط دستگاه‌های سریع‌تر، ارسال می‌شود، دریافت می‌کنند و تفاوت سرعت را جبران می‌نمایند. اطلاعات ورودی ذخیره می‌شوند تا هنگامی که تمام دیتاهای گرفته‌شده قبلی فرستاده شوند. این حافظه در سوئیچ به اشتراک گذاشته می‌شود.

۵.۱۰ میتودهای انتقال فریم در شبکه

سوئیچ‌ها از سه روش برای انتقال فریم (اطلاعات) در شبکه استفاده می‌کند:

- Cut – through
- Store – and – Forward
- Fragment – Free

Cut – through ۵.۱۰.۱

در این روش، سوئیچ آدرس‌های Mac را به محض دریافت بسته می‌خواند و سپس ۶ بایت Mac اطلاعات مربوط به آدرس را ذخیره می‌کند. با وجود این که ما بقی بسته‌ها در حال رسیدن به سوئیچ می‌باشند، اقدام به ارسال بسته مذکور به سمت نود مقصد می‌نماید.

:Store – and – Forward ۵.۱۰.۲

سوئیچی که از این روش استفاده می‌کند، ابتدا تمام اطلاعات داخل بسته را دریافت و نگهداری می‌کند و قبل از ارسال بسته مورد نظر به دنبال خطای CRC و یا مشکلات دیگر می‌شود. در صورتی که بسته دارای خطایی باشد، آن بسته را کنار می‌گذارد. در غیر این صورت، سوئیچ آدرس کارت شبکه گیرنده را جستجو کرده، سپس آن را برای نود مقصد ارسال می‌دارد.

بیشتر سوئیچ‌ها هم‌زمان از دو روش فوق استفاده می‌کنند؛ مثلاً: ابتدا از روش Cut – through استفاده می‌کند، ولی به محض برخورد با یک خطا، روش خود را تغییر می‌دهد و به شیوه Store – and – Forward عمل می‌کند، از آنجایی که روش Cut – through قادر به اصلاح خطا نمی‌باشد، در نتیجه سوئیچ‌های کمتری از این روش استفاده می‌کنند؛ ولی از سرعت بالاتری برخوردار است.

Fragment – Free ۵.۱۰.۳

سوئیچ‌ها از این روش کمتر استفاده می‌کند. این روش مانند روش اول می‌باشد؛ با این تفاوت که در این شیوه، سوئیچ قبل از ارسال بسته، ۶۴ بایت اول آن را نگه می‌دارد. این کار به خاطر آن است که بیشتر خطاها و برخوردها در طول اولین ۶۴ بایت بسته اطلاعاتی، اتفاق می‌افتد.

Switch Configuration ۵.۱۱

سوئیچ‌های LAN از نظر شکل فیزیکی با هم متفاوت‌اند، در حال حاضر سوئیچ‌ها دارای سه شکل عمده می‌باشند:

۱. Shared Memory: این نوع از سوئیچ‌ها، بسته رسیده را در یک حافظه مشترک یا بافر که این بافر در بین تمامی دستگاه‌های سوئیچ تقسیم می‌شود، نگهداری می‌کنند. سپس پکت (Packet) را از طریق دستگاه مناسب برای سمت نود مقصد ارسال می‌کنند.
۲. Bus Architecture: در این دسته از سوئیچ‌ها، یک بافر (Buffer) برای هر یک از دستگاه‌ها در نظر گرفته شده است- که گذرگاه اطلاعات را کنترل می‌کند.
۳. Matrix: این نوع سوئیچ‌ها دارای یک شبکه خطوط داخلی (ماتریکس) با پورت‌های ورودی و خروجی می‌باشند. زمانی که وجود یک بسته اطلاعاتی در پورت ورودی تشخیص داده شود، آدرس کارت شبکه (Mac) با جدول جستجوی موجود در سوئیچ (Mac Table)، مقایسه می‌شود تا در نهایت بسته مذکور به پورت خروجی موردنظر هدایت شود. بنابراین سوئیچ در حد فاصل بین این دو پورت یک خط ارتباطی ایجاد کرده، آن دو پورت را به هم متصل می‌کند.

۵.۱۲ جدول آدرس‌های Mac در سوئیچ

سوئیچ‌های لایه ۲، کارهای متفاوتی مانند: یاد گرفتن آدرس Mac، فرستادن و فیلترکردن تصمیمات و غیره را انجام می‌دهند. وقتی یک سوئیچ روشن می‌شود، جدول آدرس‌های Mac آن خالی است. وقتی دستگاه، فریم می‌فرستد و توسط واسط (Interface) دریافت می‌شود، سوئیچ آدرس مبدأ را در جدول آدرس‌های Mac ذخیره می‌کند. بعد از این مرحله، سوئیچ جدول آدرس‌های Mac را برای فرستادن و فیلترکردن فریم‌های دریافتی استفاده می‌کند و سوئیچ مشخص می‌کند که فریم‌ها باید از پورت مشخص شده عبور کنند یا خیر؟ به همین دلیل جدول آدرس‌های Mac، جدول فیلتر Mac، یا فیلتر کننده نیز گفته می‌شود.

۵.۱۳ Transparent Bridging

اکثر سوئیچ‌ها از سیستمی موسوم به Transparent Bridging استفاده می‌کنند تا جداولی جهت جستجوی آدرس بسازند. سیستم مذکور یک تکنالوژی می‌باشد که امکان می‌دهد تا سوئیچ همه آنچه را که در مورد موقعیت نودها در شبکه باید بداند، بدون دخالت مدیر شبکه (Network Administrator) می‌آموزد. این سیستم دارای پنج قسمت زیر می‌باشد:

- Learning
- Flooding
- Forwarding
- Filtering
- Aging

Learning: اگر کمپیوتر a که در سگمنت a قرار دارد، دیتایی برای کمپیوتر b واقع در سگمنت c ارسال می‌کند. پس سوئیچ اولین بسته اطلاعاتی را از روی نود a دریافت می‌کند. آدرس کارت شبکه یا Mac Address آن را می‌خواند و آن را در جدول Mac خود به ثبت می‌رساند. پس از این، سوئیچ به محض دریافت یک بسته اطلاعاتی که آدرس مقصد دستگاه، نود a آدرس دهی شده باشد، می‌تواند نود a را با توجه به آدرس موجود بیابد. به این عملیات Learning می‌گویند. یعنی به محض دیدن یک Mac Address جدید، سوئیچ آن را یادداشت و آن را یاد می‌گیرد.

Flooding: با توجه به اینکه سوئیچ، Mac Address نود b را نمی‌شناسد، بسته را به تمامی سگمنت‌ها به استثنای سگمنت a می‌فرستد. هرگاه سوئیچ برای یافتن یک نود مشخص بسته را به تمامی سگمنت‌ها بفرستد. در اصطلاح به این عمل Flooding می‌گویند.

Forwarding: نود b بسته را دریافت کرده، بسته‌یی را برای شناسایی به سمت نود a می‌فرستد. بسته‌ی ارسالی از سوی نود b به سوئیچ می‌رسد و سوئیچ نیز آدرس کارت شبکه‌ی نود b را به لیست Mac Table خود در سگمنت c اضافه می‌کند. از آنجایی که سوئیچ، آدرس نود a را از قبل می‌داند، در نتیجه بسته را مستقیماً به نود a می‌فرستد. چون سگمنتی که نود a متعلق به آن است با سگمنتی که نود b به آن تعلق دارد با هم متفاوت می‌باشند. در نتیجه، سوئیچ باید این دو سگمنت را با هم مربوط سازد و سپس اقدام به ارسال بسته نماید که به این عمل Forwarding می‌گویند. بسته‌ی دیگری از سوی a به سمت نود b ارسال می‌شود. بسته ابتدا به سوئیچ می‌رسد، سوئیچ نیز آدرس نود b را می‌داند و بسته را مستقیماً به نود b می‌فرستد.

Filtering: نود c اطلاعاتی را برای نود a می‌فرستد. آدرس نود c به سوئیچ نیز از طریق Hub، ارسال می‌شود و سوئیچ آدرس نود c را نیز به لیست آدرس‌های خود در سگمنت a اضافه می‌کند. پیش از این، سوئیچ آدرس مربوط به نود a را می‌دانست و مشخص می‌ساخت که این نودها (a و c) هر دو در یک سگمنت مشابه قرار دارند، پس برای ارسال اطلاعات از نود c به نود a، دیگر نیازی نیست تا سوئیچ سگمنت a را با سگمنت دیگری مرتبط سازد. بنابراین، سوئیچ در حین انتقال اطلاعات بین نودهای درون یک سگمنت عکس‌العملی از خود نشان نمی‌دهد که به این عمل Filtering می‌گویند.

مراحل Learning و Flooding ادامه می‌یابد تا اینکه سوئیچ، مک آدرس تمامی نودها را به لیست خود اضافه کند. بیشتر سوئیچ‌ها برای نگهداری لیست آدرس‌ها از حافظه‌ی زیادی برخوردارند. اما برای استفاده بهتر از این حافظه، سوئیچ آدرس‌های قدیمی را از جدول پاک می‌کند و برای جلوگیری از ضایع شدن وقت، در آدرس‌های قدیمی به دنبال آدرسی نمی‌شود. برای انجام این کار از تکنیکی موسوم به aging بهره می‌گیرد. اساساً وقتی اطلاعات یک نود وارد جدول سوئیچ می‌شود یک Timestamp در مقابل آن اطلاعات نوشته می‌شود و با دریافت هر بسته‌ی اطلاعاتی دیگر، آن بر حسب زمان (Timestamp) به روز (Update) می‌شود.

سوئیچ دارای قابلیت است که پس از مدتی در صورت عدم فعالیت نود، اطلاعات مربوط به آن را پاک می‌کند. این قابلیت باعث می‌شود تا فضای قابل توجهی از حافظه برای اطلاعات و پکت‌های دیگر اختصاص داده شود. در نمونه‌ای که ملاحظه کردید، دو نود (a و c) یک سگمنت را بین خود تقسیم می‌کنند حال آنکه سوئیچ برای هر یک از نودهای b و d یک سگمنت مستقل می‌سازد. در یک شبکه LAN – Switched هر یک از نودها دارای یک سگمنت جداگانه می‌باشد که خصوصیت مذکور، احتمال برخورد بین بسته‌های اطلاعاتی و همچنین نیاز به فیلترینگ را حذف می‌کند.

۵.۱۴ روش‌های انتقال دیتا در شبکه

پروسه ارسال اطلاعات، شامل مراحل متعددی است. این مراحل شامل سازماندهی دیتا درون بسته‌های اطلاعاتی در کمپیوتر مبدأ و بهم بستن آنان در کمپیوتر مقصد می‌باشد- بگونه‌یی که شکل اولیه مجدداً ایجاد شود. هر لایه از پروتوکول TCP/IP، دارای نقشی موثر در کمپیوترهای مبدأ و مقصد است.

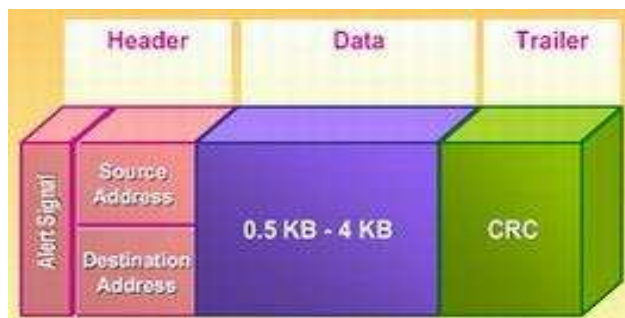
۵.۱۵ واژه‌های بسته‌های اطلاعاتی (Packets)

در هر یک از لایه‌های TCP/IP از بسته‌های اطلاعاتی (packet) با اسامی متفاوتی نام برده می‌شود. همزمان با حرکت یک بسته‌های اطلاعاتی از یک لایه به لایه دیگر، در پروتوکول TCP/IP هر یک از پروتوکول‌های مربوطه، اطلاعات اختصاصی خود را به آن اضافه می‌نمایند. از بسته‌های اطلاعاتی خود با اطلاعات اضافه شده به آن، با نام‌های فنی دیگر، یاد می‌گردد که عبارتند از: Segment (سگمنت)، message (پیام)، datagram (دیتاگرام) و frame (فریم)، می‌باشند.

- سگمنت: سگمنت واحد انتقال اطلاعات در TCP بوده و شامل یک TCP header است که توسط Application data، همراهی شده است.
- پیام: واحد انتقال اطلاعات در پروتوکول‌های ICMP, UDP, ARP و است. پیام شامل یک Protocol header بوده که توسط Application و یا protocol data، اضافه شده است.
- دیتاگرام: دیتاگرام، واحد انتقال اطلاعات در سطح لایه IP است. دیتاگرام شامل یک IP header است که توسط لایه transport، اضافه شده است.
- فریم: واحد انتقال اطلاعات در سطح لایه اینترنتی شبکه است. فریم شامل یک header است که در لایه network به آن اضافه شده است که توسط دیتای لایه IP، اضافه شده است.

۵.۱۶ اجزای یک فریم

یک فریم (اصطلاحی برای یک بسته اطلاعاتی در سطح لایه شبکه) شامل سه بخش اساسی (header، data، و trailer) است.



شکل (۵-۸) اجزای یک فریم

Header. اطلاعات موجود در این بخش شامل موارد زیر می باشد:

- یک سیگنال هشداردهنده، مبنی بر ارسال یک بسته اطلاعاتی؛
- آدرس مبدأ؛
- آدرس مقصد.

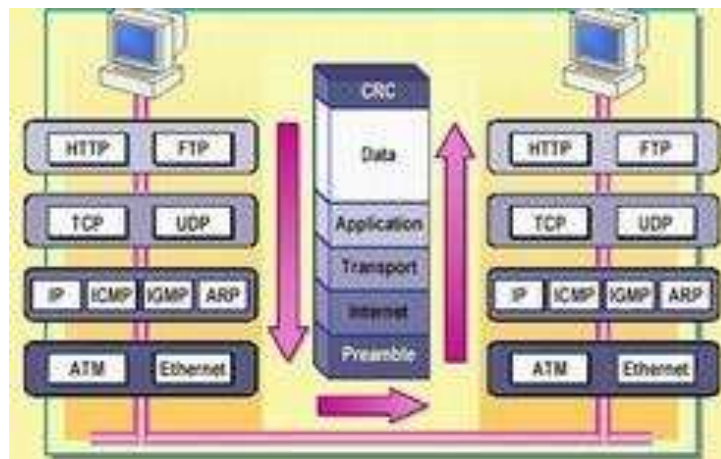
Data: در این بخش، اطلاعات واقعی ارسال شده توسط برنامه، قرار می گیرد. این بخش از بسته اطلاعاتی دارای اندازه های متفاوتی است. (بستگی به محدودیت اندازه تنظیم شده توسط شبکه دارد). بخش Data، در اکثر شبکه ها از نیم کیلوبایت تا چهار کیلوبایت را می تواند شامل شود. در شبکه های اینترنت، اندازه دیتا تقریباً معادل یک و نیم کیلو بایت است. با توجه به اینکه اکثر تنظیمات دیتاهای اولیه، بیش از چهار کیلوبایت می باشند، باید دیتا به بخش های کوچکتری به نام بسته های اطلاعاتی (packet)، تقسیم شود. در زمان انتقال یک فایل با ظرفیت بالا، بسته های اطلاعاتی زیادی در طول شبکه منتقل خواهند شد.

Trailer: محتویات trailer، ارتباط مستقیم به پروتوکول استفاده شده در لایه انترفیس شبکه دارد. trailer، معمولاً شامل بخشی به منظور بررسی خطا بوده که CRC (Cyclical redundancy check)، نامیده می شود. CRC، عددی است که توسط یک محاسبه ریاضی بر روی بسته اطلاعاتی در مبدأ (فرستنده)، تولید می شود. زمانی که بسته اطلاعاتی به مقصد خود می رسد، مجدداً محاسبه مربوطه انجام خواهد شد. در صورتی که نتایج به دست آمده یکسان باشد، نشان دهنده صحت ارسال یک بسته اطلاعاتی خواهد بود. در صورتی که حاصل محاسبه در مقصد با نتیجه محاسبه شده در مبدأ، مغایرت داشته باشد، به این مفهوم خواهد بود که دیتا در زمان انتقال، تغییر نموده است. در چنین حالتی، کمپیوتر مبدأ، دوباره دیتا را ارسال خواهد کرد.

۵.۱۷ جریان انتقال اطلاعات (از کمپیوتر مبدأ تا کمپیوتر مقصد)

بسته‌های اطلاعاتی ارسال شده از یک کمپیوتر برای کمپیوتر دیگر، از بین لایه‌های متعدد پروتوکول TCP/IP عبور خواهد کرد. زمان رسیدن یک بسته اطلاعاتی به یک لایه، پروتوکول‌های موجود در آن، اطلاعات خاصی را به آن اضافه خواهند کرد. اطلاعات اضافه شده، توسط هر پروتوکول، شامل اطلاعاتی در رابطه با بررسی خطا بوده که Checksum، نامیده می‌شود. از Checksum، به منظور بررسی صحت ارسال اطلاعات اضافه شده در header توسط پروتوکول مربوطه، در پروتوکول مقصد استفاده می‌شود (اطلاعات باید بدون کم و کاست در اختیار پروتوکول مقصد قرار بگیرند).

فراموش نکنیم که CRC (Cyclical redundancy check)، صحت انتقال یک بسته را به طور کامل بررسی می‌نماید. اطلاعات اضافه شده در هر لایه، به عنوان دیتا توسط پروتوکول‌های لایه زیرین، بسته‌بندی خواهد شد. زمانی که بسته اطلاعاتی به مقصد مورد نظر می‌رسد، لایه مربوطه (متناظر) یک بخش از header را برداشته و به بسته اطلاعاتی باقی، به عنوان دیتا برخورد خواهد کرد. بسته اطلاعاتی در ادامه به سمت پروتوکول‌های موجود در لایه بالاتر ارسال و در اختیار پروتوکول مربوطه قرار خواهد گرفت. در ادامه، عملکرد هر یک از لایه‌ها را در پروسه انتقال اطلاعات بررسی و این موضوع را از نظر کمپیوتر مبدأ و مقصد دنبال خواهیم کرد.



شکل (۵-۹) نحوه انتقال دیتا در شبکه

۵.۱۷.۱ لایه Application

پروسه انتقال اطلاعات از لایه application آغاز می‌شود. یک پروتوکول مانند FTP، پروسس را در کمپیوتر مبدأ مقداردهی اولیه می‌نماید؛ یعنی آماده نمودن دیتا به فارمتی که پروتوکول در کمپیوتر مقصد، قادر به تشخیص آن باشد). پروتوکول موجود در کمپیوتر مبدأ، کنترل تمام پروسه را برعهده خواهد داشت.

۵.۱۷.۲ لایه Transport

از لایه Application، دیتا به لایه transport منتقل می‌شود. این لایه شامل پروتوکول‌های TCP و UDP است. برنامه مورد نظر نوع پروتوکول "انتقال" را مشخص می‌نماید (TCP یا UDP). در هر دو حالت

Checksum برای TCP و UDP اضافه خواهد شد.

در صورتی که پروتوکول TCP، انتخاب شود:

- یک عدد مسلسل (Sequence number) به هر سگمنت منتقل شده، اضافه خواهد شد.
- اطلاعات مربوط به Acknowledgment برای یک ارتباط، به هر سگمنت اضافه می‌شود.
- شماره پورت TCP در رابطه با برنامه‌های مبدأ و مقصد، اضافه خواهد شد.

در صورتی که پروتوکول UDP، انتخاب گردد:

- شماره پورت UDP در رابطه با برنامه‌های مبدأ و مقصد، اضافه خواهد شد.

۵.۱۷.۳ لایه اینترنت (Internet)

پس از این که اطلاعات اضافه شد، بسته اطلاعاتی در اختیار لایه اینترنت قرار داده می‌شود. در این لایه، اطلاعات زیر به header اضافه می‌شود:

- آدرس IP مبدأ
- آدرس IP مقصد
- نوع پروتوکول انتقال
- مقدار checksum
- اطلاعات (Time to Live (TTL

علاوه بر اطلاعات فوق، لایه اینترنت مسئولیت برطرف نمودن آدرس‌های IP مقصد به یک آدرس MAC را نیز برعهده دارد. پروتوکول ARP، مسئول انجام عملیات فوق است. آدرس MAC به header بسته اطلاعاتی اضافه و در ادامه، بسته اطلاعاتی در اختیار لایه انترفیس شبکه، قرار داده می‌شود.

لایه انترفیس شبکه (Network Interface)

این لایه، پس از دریافت یک بسته اطلاعاتی از لایه IP، اطلاعات زیر را به آن اضافه خواهد کرد:

- مقدمه (Preamble): تعدادی از بایتهایی است که ابتدای یک "فریم" را مشخص می‌نماید.
- CRC: حاصل یک محاسبه ریاضی است که به انتهای فریم اضافه و از آن به منظور صحت ارسال فریم، استفاده می‌شود.

پس از افزودن اطلاعات مورد نظر به فریم‌ها در لایهٔ انترفیس شبکه، در ادامهٔ فریم‌ها بر روی شبکه ارسال خواهند شد.

۵.۱۸ عملیات در کمپیوتر مقصد

زمانی که فریم‌ها به کمپیوتر مقصد می‌رسند، لایهٔ انترفیس شبکه، مقدمهٔ (Preamble) را حذف و مقدار CRC را مجدداً محاسبه می‌نماید. در صورتی که مقدار به دست آمده با مقدار محاسبه شده در مبدأ، یکسان باشد، در ادامه آدرس MAC مقصد، موجود بر روی فریم، بررسی می‌شود. در صورتی که آدرس MAC، یک آدرس Broadcast و یا آدرس MAC با کمپیوتر مقصد مطابقت نماید، فریم به لایهٔ "انترنت"، ارسال خواهد شد. در غیر این صورت فریم نادیده گرفته می‌شود. در لایهٔ IP، مجدداً Checksum محاسبه و با مقدار محاسبه شده قبل از انتقال، مقایسه می‌شود تا این اطمینان حاصل شود که بستهٔ اطلاعاتی در طول مسیر تغییر ننموده است. در ادامه، IP بستهٔ اطلاعاتی را در اختیار پروتوکول "انتقال"، قرار می‌دهد (TCP یا UDP) به منظور تصمیم‌گیری در رابطه با نوع پروتوکول "انتقال"، از اطلاعات موجود در IP header استفاده می‌شود. در لایهٔ "انتقال"، در صورتی که بستهٔ اطلاعاتی از TCP دریافت شده باشد، عددی مسلسل (sequence number) بر روی بستهٔ اطلاعاتی بررسی و یک acknowledgement برای TCP کمپیوتر مبدأ ارسال می‌شود. در ادامه از اطلاعات پورت TCP موجود، در بستهٔ اطلاعاتی استفاده تا بستهٔ اطلاعاتی برای برنامهٔ مربوطه در لایهٔ Application، ارسال شود.

در صورتی که UDP بستهٔ اطلاعاتی را از لایهٔ "انترنت" دریافت نماید، از اطلاعات پورت UDP موجود در بستهٔ اطلاعاتی استفاده می‌شود تا آن را برای برنامهٔ مربوطه در لایهٔ Application ارسال نماید. (بدون ارسال یک acknowledgement برای کمپیوتر مبدأ).

پس از دریافت اطلاعات توسط Appliaction، پروسس‌های لازم و ضروری در مورد آنها انجام خواهد شد.



سوئیچ (Switch) یکی از سخت‌افزارهای شبکه بوده که در عین شباهت با (Hub)، بسیار هوشمندتر از آن‌ها می‌باشد. براساس مدل OSI سوئیچ‌ها در لایه 2 یا لایه Data Link کار می‌کند. وظیفه این سخت‌افزارها، انتقال بسته‌های دیتا از یک دستگاه به دستگاه دیگر می‌باشد. تعداد پورت‌های Switch متفاوت بوده که در برخی مدل‌ها به بیش از 48 عدد می‌رسد و دارای کاربردها و مدل‌های متفاوتی می‌باشد. Switch‌ها به دو نوع غیر قابل کنترل و قابل کنترل تقسیم می‌شوند. نوع اول طبق هر آن چیزی که کمپنی سازنده تعیین کرده است، کار می‌کند و نمی‌توان آن‌ها را مدیریت کرد. switch‌های قابل کنترل را می‌توان نظر به ضرورت سازمان خود تنظیم و پیکربندی کرد. برای امنیت سوئیچ از پسورد استفاده می‌شود که به پورت‌های کنسول و خط VTY داده می‌شود.

عناصر مهم داخلی سوئیچ‌ها: عبارت از CPU، RAM، NVRAM، ROM، Flash می‌باشد. سوئیچ دارای یک Port است که بر روی آن Console نوشته شده است، یک کیبل آبی فیروزی یا مشکی به نام کیبل Console که یک سر آن ساکت RJ45 است و سر دیگر آن RS232 است. قسمت RJ45 به پورت کنسول متصل می‌شود و طرف دیگر آن به PC که قرار است با استفاده از آن سوئیچ را Configuration کنیم، متصل می‌شود. باید به خاطر داشت که همیشه نمی‌توان به صورت مستقیم و با کیبل به دستگاه سیسکو وصل شویم. باید قادر بود تا از راه دور و از طریق کامپیوتر به دستگاه وصل شود و آن را چک و پیکربندی کرد، برای انجام این کار باید به انترنس VLAN1 دستگاه خود IP بدهیم.

سوئیچ‌ها از سه روش برای انتقال اطلاعات در شبکه استفاده می‌کند که به نام‌های (Cut-through، Store and Forward و Fragment free) یاد می‌شود. اکثر سوئیچ‌ها از سیستمی موسوم به Transparent Bridging استفاده می‌کنند تا جدول‌های جهت جستجوی آدرس بسازند. سیستم مذکور یک تکنالوژی می‌باشد که امکان می‌دهد تا سوئیچ همه آنچه که در مورد موقعیت نودها در شبکه باید بداند، را بدون دخالت مدیر شبکه (Network Administrator) می‌آموزند. این سیستم دارای پنج قسمت (Learning, Flooding, Forwarding, Filtering, Aging) می‌باشد.

ارسال اطلاعات از یک کامپیوتر به کامپیوتر در شبکه، شامل مراحل متعددی است (سازماندهی دیتا درون بسته‌های اطلاعاتی در کامپیوتر مبدأ و بهم بستن آنان در کامپیوتر مقصد بگونه‌یی که شکل اولیه مجدداً ایجاد شود). هر لایه از پروتوکول TCP/IP، دارای نقشی موثر در کامپیوترهای مبدأ و مقصد است.



سوالات فصل پنجم

۱. سوئیچ را تعریف کرده و انواع آنرا توضیح دهید.
۲. اجزای داخلی سوئیچ را نام برده و وظیفه فلش را شرح دهید.
۳. فرق بین حافظه‌های RAM و NVRAM را توضیح دهید.
۴. سوئیچ‌های قابل کنترل و غیر قابل کنترل چه فرق دارد؟ توضیح دهید.
۵. جهت تنظیمات اولیه سوئیچ از کدام پورت و کدام نوع کیبل استفاده می‌شود؟ توضیح دهید.
۶. اهمیت انواع پسوردها در سوئیچ‌های سیسکو را تشریح نمایید.
۷. دستورات دادن نام به یک سوئیچ سیسکو را توضیح دهید.
۸. مراحل دادن پسورد برای Privileged Level Secret را تشریح نمایید.
۹. مراحل خط VTY و امن نمودن آن را با دستورات خاص آن بنویسید.
۱۰. تنظیم اینترفیس VLAN 1 را با دستورات آن بنویسید.
۱۱. Packet Switching را شرح دهید.
۱۲. مراحل کار سیستم Transparent Bridging را توضیح دهید.
۱۳. مراحل انتقال اطلاعات در مدل TCP/IP را توضیح نمایید.



۱. با استفاده از نرم افزار packet tracer پیکربندی ابتدایی سوئیچ را انجام دهید.
۲. پسوندهای مختلف پورتهای سوئیچ را انجام دهید.
۳. انترفیس VLAN1، پورت کنسول و پورت VTY را تنظیم نمایید.

پروتوکول STP (Spanning Tree Protocol)



هدف کلی: آشنایی با پروتوکول STP و عمل کردن آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. عوامل وقوع Loop در شبکه را توضیح دهند.
۲. پروتوکول STP را تشریح نمایند.
۳. پروتوکول STP را در شبکه راه اندازی نمایند.

Spanning-tree Protocol عبارت از پروتوکول است که ابتدا توسط شرکت DEC و بعداً توسط IEEE تحت عنوان 802.1D استاندارد شد. تمام سوئیچ‌های سیسکو با ورژن 802.1D کار می‌کند. وظیفه اصلی STP جلوگیری از رخ دادن Loop و متوقف کردن Loop واقع شده در لایه 2 می‌باشد. در حقیقت این کار را با Shutdown کردن link‌های اضافه انجام می‌دهد.

STP با به کار بردن Spanning-tree Algorithm توپولوژی شبکه را به صورت درخت قرار می‌دهد و سپس با غیر فعال کردن مسیرهای اضافی که منجر به رخ دادن حلقه (Loop) در شبکه شده اند، Loop واقع شده را مهار می‌کند.

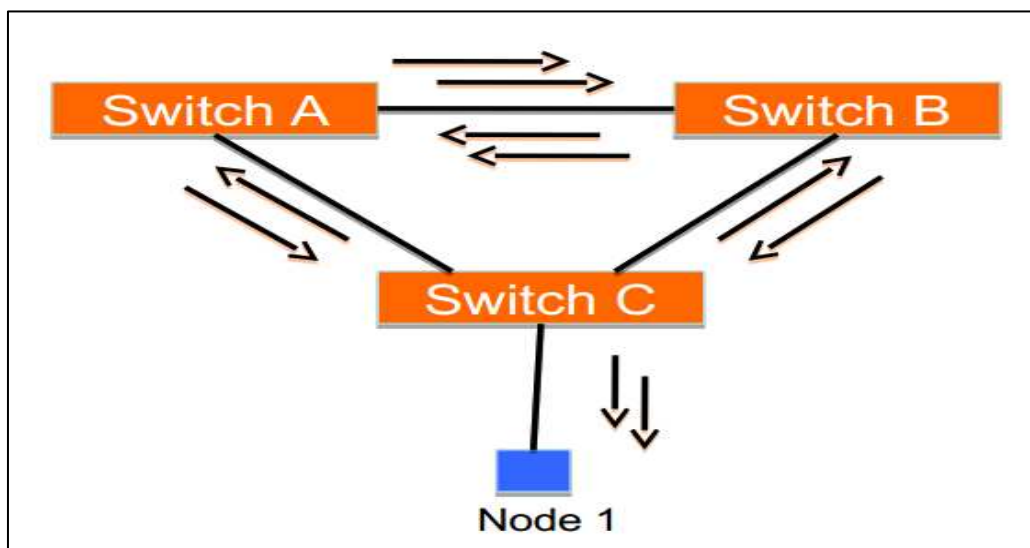
۶.۱ حلقه (Loop)

حلقه زمانی به وجود می‌آید که شما در ارتباطات شبکه‌یی خود، ارتباطات چندگانه (redundant) داشته باشید. این مسیرهای اضافی سبب به وجود آمدن حلقه (loop) در شبکه می‌شود. به این معنا که یک فریم برای رسیدن به مقصد، بین سوئیچ‌ها مکرراً به حرکت خود ادامه می‌دهد و گاه منجر به از بین رفتن فریم می‌شود.

حال این چرخه می‌تواند چه تاثیری روی شبکه داشته باشد:

۱. Broadcast Storms (طوفان ارسال اطلاعات)
۲. Duplicate Frame Copies (ارسال کپی فریم‌ها)
۳. Unstable MAC Table (جدول MAC غیر ثابت)

یکی از تاثیرات این حلقه در شبکه اشغال پهنای باند Bandwidth می‌باشد. گاهی ممکن است این حلقه پهنای باند شبکه شما را تا ۱۰۰٪ اشغال کند. در این حالت فریم‌هایی که به عنوان Broadcast به سوئیچ ارسال می‌شود که سوئیچ مجدداً این فریم‌ها را بر روی تمامی پورت‌های خود ارسال می‌کند. با ادامه این کار، حجم عظیمی از ترافیک در شبکه ایجاد می‌شود. هنگامی که این اتفاق می‌افتد، هر سیستم توانایی برقراری ارتباط را در شبکه از دست می‌دهد و چراغ‌های روی سوئیچ شما از حالت چشمک‌زدن به حالت روشن دوام‌دار تغییر خواهند کرد. البته اگر حلقه ایجاد شده در شبکه شکسته شود، ظرف چند دقیقه چراغ‌ها به حالت اولیه باز می‌گردند.



شکل (۶-۱) حلقه (Loop) در شبکه

یکی دیگر از تاثیرهای ایجاد حلقه در شبکه، بالابردن کار CPU سوئیچ شما است. سوئیچ شما در این زمان به علت ارسال و دریافت‌های حجم زیاد، از فریم‌ها و بالابودن میزان پروسس اطلاعات با بالا رفتن میزان کار CPU و RAM مواجه می‌شود. دلایل زیادی برای ایجاد Loop در شبکه وجود دارد. مثل اشتباه در کیبل کشی، اشتباه در پیکربندی (Configuration) سوئیچ و یک سلسله دلایل دیگر؛ اما یکی از نکات قابل توجه این است که حلقه ایجاد شده در لایه دوم است. یکی از راهکارهای شرکت سیسکو برای رفع این مشکل، پروتوکول STP است. این پروتوکول به صورت پیش فرض بر روی سوئیچ‌های سیسکو فعال است. به صورت پیش فرض از امکان ایجاد حلقه در شبکه شما جلوگیری می‌کند، اما چنانچه قصد دارید، ایجاد Loop را در شبکه امتحان کنید، باید این پروتوکول را غیر فعال کنید.

۶.۲ Spanning Tree Protocol (STP)

سوئیچ‌های سیسکو با استفاده از پروتوکول STP، از به وجود آمدن Loop در شبکه جلوگیری می‌کنند. اگر در یک LAN که دارای مسیرهای زیاد (Redundant) می‌باشد، پروتوکول STP فعال نباشد، Loop‌های نامحدود در شبکه به وجود می‌آید که این امر می‌تواند باعث توقف (Down) شدن شبکه شود. در حالی که اگر در همان LAN پروتوکول STP فعال باشد، سوئیچ‌ها برخی از پورت‌ها را بلاک می‌کنند و اجازه عبور اطلاعات از آن پورت‌ها را نمی‌دهند تا در شبکه، حلقه (Loop) ایجاد نشود.

تمامی Device‌های موجود در LAN باید بتوانند با هم ارتباط برقرار کنند. درواقع STP حداقل تعداد پورت‌ها را بلاک می‌کند تا LAN به چند بخش مستقل از هم که نمی‌توانند با هم ارتباط برقرار کنند، تقسیم نشود. Frame‌ها بعد از مدتی Drop می‌شوند و به طور نامحدود در Loop قرار نمی‌گیرند.

پروتوکول STP شبکه‌ها را متعادل می‌کند؛ به طوری که Frame‌ها به هر کدام از Device‌ها می‌توانند ارسال شوند؛ بدون این که مشکل Loop به وجود آید.

پروتوکول STP با چک کردن هر پورت قبل از این که از طریق آن اطلاعات ارسال کند، از به وجود آمدن Loop در شبکه جلوگیری می‌کند. در روند چک کردن، اگر آن پورت در یک VLAN، در وضعیت STP Forwarding باشد، از آن پورت داخل همان VLAN در حالت عادی استفاده می‌شود، اما اگر در وضعیت STP Blocking باشد، در آن VLAN، ترافیک تمام کاربران بلاک می‌شود و ترافیکی از آن پورت عبور نخواهد کرد.

توجه کنید که وضعیت STP یک پورت، دیگر اطلاعات مربوط به پورت را تغییر نمی‌دهد. برای مثال با تغییر وضعیت خود تغییری در وضعیت‌های trunk/access و connected/not-connected ایجاد نمی‌کند. وضعیت STP یک مقدار جدا از وضعیت‌های قبلی دارد و اگر در حالت بلاک باشد، پورت را از پایه غیر فعال می‌کند.

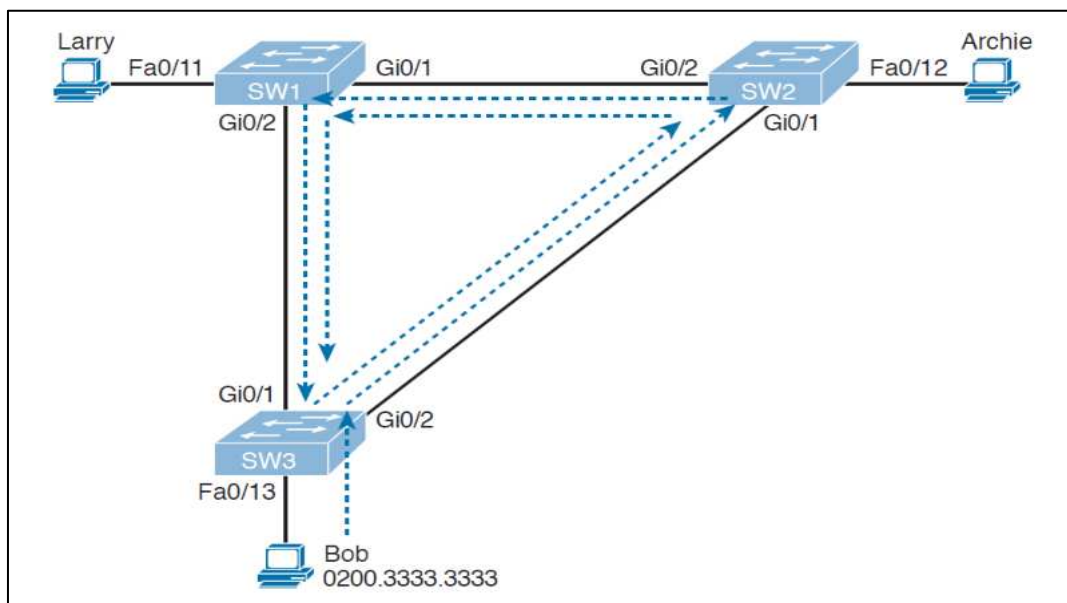
۶.۲.۱ نیاز به پروتوکول STP

پروتوکول STP از وقوع سه مشکل رایج در Ethernet LAN‌ها جلوگیری می‌کند. در نبود پروتوکول STP، بعضی از Frame‌های Ethernet برای مدت زیادی (ساعت‌ها، روزها و حتی برای همیشه، اگر Device‌های LAN و لینک‌ها از کار نیافتند) در یک Loop داخل شبکه قرار می‌گیرند. سوئیچ‌های سیسکو به طور پیش فرض پروتوکول STP را اجرا می‌کند. توصیه می‌کنیم پروتوکول STP را تا زمانی که تسلط کامل به آن ندارید، غیر فعال نکنید.

اگر یک Frame در Loop قرار بگیرد، Broadcast Storm به وجود می‌آید، Broadcast Storm زمانی به وجود می‌آید که هر نوعی از Frame‌های Ethernet مانند Multicast Frame، Broadcast Frame و Unicast Storm‌های که مقصدشان مشخص نیست در Loop بی‌نهایت داخل LAN قرار بگیرند.

Broadcast Storm‌ها می‌توانند لینک‌های شبکه را با کاپی‌های به وجود آمده از یک Frame اشباع کنند و باعث از بین رفتن بعضی از Frame‌ها شوند. از سوی دیگر با توجه به بار پردازشی (process) مورد نیاز برای پروسس Broadcast Frame‌ها، تأثیر قابل ملاحظه‌ای روی عملکرد Device‌های کاربران دارند.

تصویر ذیل مثال ساده از Broadcast Storm را نشان می‌دهد که در آن سیستمی که Bob نام دارد، یک Broadcast Frame ارسال می‌کند. خط چین‌ها نحوه ارسال Frame‌ها توسط سوئیچ‌ها را در نبود STP نمایش می‌دهند.



شکل (۶-۲) Broadcast Storm

در تصویر فوق frame‌ها در جهت‌های مختلفی می‌چرخند، برای ساده‌تر شدن مثال فقط در یک جهت آن‌ها را نمایش داده‌ایم.

سوئیچ‌ها Broadcast Frame‌ها را به تمام پورت‌ها به جز پورت فرستنده آن Frame، ارسال می‌کنند. در شکل فوق سوئیچ سوم Frame دریافتی از Bob را به سوئیچ SW2 ارسال می‌کند، سوئیچ SW2 آن را برای سوئیچ SW1 ارسال می‌کند و سوئیچ SW1 نیز آن را برای SW3 ارسال می‌کند و به همین ترتیب این Frame داخل یک حلقه (Loop) قرار می‌گیرد. زمانی که یک Broadcast Storm اتفاق می‌افتد، Frame‌ها مانند مثال بالا به چرخیدن ادامه می‌دهند تا زمانی که تغییری به وجود آید؛ مثلاً: شخصی یکی از پورت‌ها را خاموش کند، سوئیچ را Reload کند یا کاری کند که loop از بین برود).

Broadcast Storm همچنان باعث به وجود آمدن مشکل نا محسوسی به نام MAC Table Instability یا به نام ناپیوستگی جدول مک می‌شود. در این مشکل Frame‌هایی که مک‌آدرس مبدأ یکسانی دارند، از پورت‌های مختلفی وارد سوئیچ می‌شوند که منجر به تغییر دائمی جدول مک‌آدرس می‌شود. به مثال زیر توجه کنید:

در شکل فوق در ابتدا سوئیچ SW3 مک‌آدرس Bob را که از طریق پورت Fa0/13 وارد سوئیچ می‌شود، به جدول مک‌آدرس خود اضافه می‌کند:

0200.3333.3333 Fa0/13 VLAN 1

حالا پروسه Switch Learning را در نظر بگیرید، Frame ارسالی پس از یک دور چرخیدن از طریق پورت Gi0/1، مک آدرس مبدأ 0200.3333.3333 را دارد، بنابراین جدول مک آدرس خود را به روز (Update) می کند:

0200.3333.3333 Gi0/1 VLAN 1

پس از به روز (Update) کردن جدول مک آدرس، سوئیچ SW3 هم دیگر نمی تواند به درستی Frame را به سیستم Bob برساند، برای مثال در این حالت، اگر یک Frame که مقصد آن Bob باشد به سوئیچ SW3 برسد (خارج از Frame های که در داخل Loop افتاده اند)، سوئیچ SW3 به اشتباه Frame را روی پورت Gi0/1 به سوئیچ SW1 ارسال می کند. نتیجه این اشتباه یک Loop است که ترافیک زیادی را در شبکه ایجاد می کند.

سومین مشکلی که Frame های موجود در یک Broadcast Storm ایجاد می کند، رسیدن کاپی های مختلف از یک Frame به دست گیرنده است. در شکل فوق فرض کنید که باب یک Frame را برای لاره ارسال کند، در حالی که هیچ کدام از سوئیچ ها مک آدرس لاره را نمی دانند. سوئیچ ها، Frame ها را به صورت Unicast هایی که مک آدرس مقصدشان مشخص نیست، ارسال می کنند. زمانی که باب یک Frame را که مک آدرس مقصدش لاره است، ارسال می کنند، سوئیچ SW3 آن را به سوئیچ های SW1 و SW2 ارسال می کند. سوئیچ های SW1 و SW2 نیز Frame را Broadcast می کنند، این Broadcast ها منجر به قرار گرفتن آن Frame در داخل یک Loop می شوند. سوئیچ SW1 نیز کاپی های متعددی از آن Frame را به پورت Fa0/11 برای لاره ارسال می کند. در نتیجه لاره کاپی های مختلفی از آن Frame را دریافت می کند که می تواند باعث از کار افتادن برنامه یی در سیستم لاره و یا مشکلات شبکه یی شود.

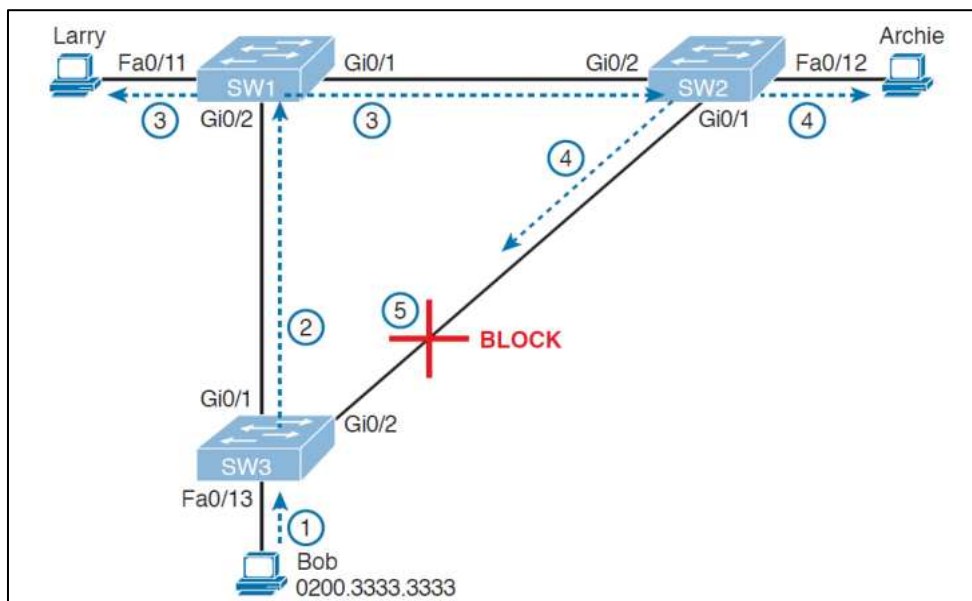
جدول (۶-۱) مشکل های اساسی در شبکه

| جدول ذیل خلاصه یی از سه مشکل اساسی در شبکه یی است که دارای Redundancy است و STP در آن اجرا نمی شود: | | |
|---|-----------------------------|---|
| شماره | مشکل | توضیحات |
| 1 | Broadcast Storm | ارسال مکرر یک Frame بر روی یک لینک، ظرفیت قابل ملاحظه یی از لینک را اشغال می کند. |
| 2 | MAC Table Instability | به روز رسانی مکرر جدول مک آدرس سوئیچ ها با ورودی های اشتباه بر اثر چرخش Frame ها- که باعث ارسال Frame ها به مقصد اشتباه می شود. |
| 3 | Multiple Frame Transmission | یکی از جنبه های تاثیرات چرخش Frame ها که باعث می شود کاپی های مختلفی از Frame به مقصد برسد و آن Device را گیج کند |

۶.۳ نحوه کار پروتوکول STP

پروتوکول STP با قرار دادن هر یک از پورت‌های سوئیچ در وضعیت‌های Forwarding و Blocking از به وجود آمدن Loop جلوگیری می‌کند. پورت‌هایی که در وضعیت Forwarding هستند به‌صورت عادی فعالیت می‌کنند. Frame‌ها را ارسال و دریافت می‌کنند. اما پورت‌هایی که در وضعیت Blocking قرار دارند به جز پیام‌های مربوط به پروتوکول STP و برخی دیگر از پیام‌های که برای پروتوکول‌ها استفاده می‌شوند، هیچ Frame دیگری را پروسس نمی‌کنند. درحقیقت این پورت‌ها Frame‌های کاربران را ارسال نمی‌کنند، مک آدرس Frame‌های ورودی را ذخیره نمی‌کنند و Frame‌های دریافتی از کاربران را نیز پروسس نمی‌کنند.

تصویر ذیل راه‌حل استفاده از پروتوکول STP (قرار دادن یکی از پورت‌های سوئیچ SW3 در وضعیت Blocking) در مثال پیشین را نمایش می‌دهد:



شکل (۶-۳) (قرار دادن یکی از پورت سوئیچ‌های SW3 در وضعیت Blocking)

همانطور که در مراحل زیر نشان داده‌شده، زمانی که باب یک Broadcast را ارسال می‌کند، دیگر Loop به وجود نمی‌آید:

مرحله اول: باب Frame را به سوئیچ SW3 ارسال می‌کند.

مرحله دوم: سوئیچ SW3 این Frame را فقط به سوئیچ SW1 ارسال می‌کند، دیگر به سوئیچ SW2 ارسال نمی‌کند، چون پورت Gi0/2 در وضعیت Blocking قرار دارد.

مرحله سوم: سوئیچ SW1 این Frame را روی پورت‌های Fa0/11 و Gi0/1 ارسال می‌کند.

مرحله چهارم: سوئیچ SW2 این Frame را روی پورت‌های Fa0/12 و Gi0/1 ارسال می‌کند.

مرحله پنجم: سوئیچ SW3 به صورت فیزیکی یک Frame را دریافت می کند، اما Frame دریافتی از SW2 به دلیل اینکه پورت Gi0/2 در سوئیچ SW3 در وضعیت Blocking قرار دارد، نادیده گرفته می شود.

با استفاده از توپولوژی STP در تصویر فوق، سوئیچ ها از لینک موجود بین SW2 و SW3 برای انتقال ترافیک استفاده نمی کنند. با این حال، اگر لینک بین SW3 و SW1 دچار مشکل شود، پروتوکول STP وضعیت پورت Gi0/2 را از Blocking به Forwarding تغییر می دهد و سوئیچ ها می توانند از آن لینک Redundant استفاده کنند. در این موقعیت ها پروتوکول STP با انجام این پروسه، متوجه تغییرات در توپولوژی شبکه می شود و تشخیص می دهد که پورت ها نیاز به تغییر در وضعیت شان دارند و وضعیت آن ها را تغییر می دهد.

سوالاتی در ذهن ما خطور می کند: پروتوکول STP چگونه پورت ها را برای تغییر وضعیت انتخاب می کند و چرا این کار را می کند؟ چگونه وضعیت Blocking را برای بهره مندی از مزایای لینک های اضافی Redundant، به وضعیت Forwarding تغییر می دهد؟ در ادامه به این سؤالات پاسخ خواهیم داد.

۶.۴ پروتوکول STP چگونه کار می کند؟

الگوریتم STA از پورت هایی که در جابجایی Frame ها مشارکت می کنند، یک درخت پوشا (Spanning Tree) تشکیل می دهد. این ساختار درختی، مسیریابی را که برای رساندن لینک های Ethernet به هم مشخص می کنند. (مانند: پیمودن یک درخت واقعی که از ریشه درخت شروع می شود و تا برگ ها ادامه دارد).

توجه: STP قبل از اینکه در سوئیچ های LAN استفاده شود، در Ethernet Bridge ها به کار رفته بود.

STP از عملیه که بعضاً (Spanning – Tree Algorithm – STA) نامیده می شود، استفاده می کند تا پورت هایی که باید در وضعیت Forwarding قرار بگیرند را انتخاب کند، سپس STP پورت هایی که برای Forwarding انتخاب نشدند را در وضعیت Blocking قرار می دهد. در واقع پروتوکول STP پورت هایی که در ارسال کردن اطلاعات باید فعال باشند را انتخاب می کند و پورت های باقی مانده را در وضعیت Blocking قرار می دهد. پروتوکول STP برای قرار دادن پورت ها در حالت Forwarding از سه مرحله استفاده می کند:

۱. پروتوکول STP یک سوئیچ را به عنوان اساس (Root) انتخاب می کند و تمام پورت های فعال در آن سوئیچ را در وضعیت Forwarding قرار می دهد.

۲. در هر کدام از سوئیچ های (Non – Root) همه سوئیچ ها به جز Root، پورتی که کمترین هزینه را برای رسیدن به سوئیچ Root دارد (Root Cost)، به عنوان Root Port انتخاب می کند و آن ها را در وضعیت Forwarding قرار می دهد.

۳. تعداد زیادی سوئیچ ها می توانند به یک بخش از Ethernet متصل شوند، اما در شبکه های مدرن، معمولاً دو سوئیچ به هر لینک (بخش) متصل می شوند. در بین سوئیچ هایی که به یک لینک مشترک

متصل هستند، پورت سوئیچی که Root Cost کمتری دارد در وضعیت Forwarding قرار می گیرد. این سوئیچ ها را Designated Switch می نامند و پورت هایی که در وضعیت Forwarding قرار گرفته را Designated Port (DP) می نامند.

باقی پورت ها در وضعیت Blocking قرار می گیرند.

خلاصه ای از علت قرار گرفتن پورت ها در وضعیت های Blocking و Forwarding توسط پروتوکول STP قرار ذیل بیان می شود:

جدول (2-6) وضعیت قرار گرفتن پورت ها

| پورت | وضعیت | توضیح |
|--|------------|---|
| تمام پورت های سوئیچ Root | Forwarding | سوئیچ Root همیشه در بخش هایی که به آن متصل هستند، Designated Switch است. |
| Root Port سوئیچ ها به جز سوئیچ Root | Forwarding | پورتهای که کمترین هزینه را برای رسیدن به Root دارد. |
| Designated Port های مربوط به هر LAN | Forwarding | سوئیچ که کمترین Root Cost را دارد. |
| باقی پورت ها | Blocking | این پورت های برای ارسال Frame های کاربران استفاده نمی شوند یا حتی Frame هایی که از این پورت ها دریافت شوند، برای ارسال در نظر گرفته نمی شوند. |

۶.۵ Hello BPDUs و Bridge

پروسه STA با انتخاب یک سوئیچ به عنوان Root شروع می شود. برای اینکه روند انتخاب را بهتر متوجه شوید، شما باید با مفهوم پیام هایی که بین سوئیچ ها تبادل می شود و فرمت شناساگری که برای شناسایی هر سوئیچ استفاده می شود آشنا شوید.

STP Bridge ID (BID) یک مقدار 8 بیتی برای شناسایی هر سوئیچ می باشد. Bridge ID به دو بخش 2 بیتی که مشخص کننده اولویت و حق تقدم است و 6 بیتی که System ID نامیده می شود و همان مک آدرس هر سوئیچ است، تقسیم می شود. استفاده از مک آدرس این اطمینان را می دهد که Bridge ID هر سوئیچ یکتا خواهد بود.

پیام‌هایی که برای تبادله اطلاعات مربوط به پروتوکول STP بین سوئیچ‌ها استفاده می‌شود، BPDUs یا Bridge Protocol Data Unit نام دارد. رایج‌ترین BPDUs، که Hello BPDUs نام دارد، تعدادی از اطلاعات که شامل BID سوئیچ‌ها نیز می‌شود را لیست و ارسال می‌کند. با استفاده از BID درج شده روی هر پیام، سوئیچ‌ها می‌توانند تشخیص دهند که هر پیام Hello BPDUs از طرف کدام سوئیچ است.

جدول زیر اطلاعات کلیدی مربوط به Hello BPDUs را نشان می‌دهد:

| جدول (۳-۶) اطلاعات کلیدی Hello BPDUs | |
|--------------------------------------|--|
| عنوان | توضیح |
| Root Bridge ID | در ابتدا تمام سوئیچ‌ها در پیام خود می‌گویند که من Root هستم تا زمانی که سوئیچ Root مشخص شود. |
| Bridge ID ارسال کننده | Bridge ID سوئیچ که پیام Hello BPDUs را ارسال می‌کند. |
| Root Cost ارسال کننده | هزینه رسیدن اطلاعات از سوئیچ ارسال کننده به سوئیچ که در آن لحظه Root است. |

۶.۶ انتخاب سوئیچ Root:

سوئیچ‌ها با استفاده از BIDهای موجود در پیام‌های BPDUs، سوئیچ Root را انتخاب می‌کنند. سوئیچی که عدد BID آن مقدار کمتری را داشته باشد به عنوان سوئیچ Root انتخاب می‌شود. با توجه به اینکه بخش اول عدد BID مقدار اولویت می‌باشد، سوئیچی که مقدار اولویت پایین‌تری داشته باشد به عنوان سوئیچ Root انتخاب می‌شود. برای مثال اگر سوئیچ‌های اول و دوم به ترتیب دارای اولویت‌های 4096 و 8192 باشند، بدون در نظر گرفتن مک آدرس سوئیچ‌ها که در به وجود آمدن BID هر سوئیچ مؤثر است، سوئیچ اول به عنوان سوئیچ Root انتخاب خواهد شد.

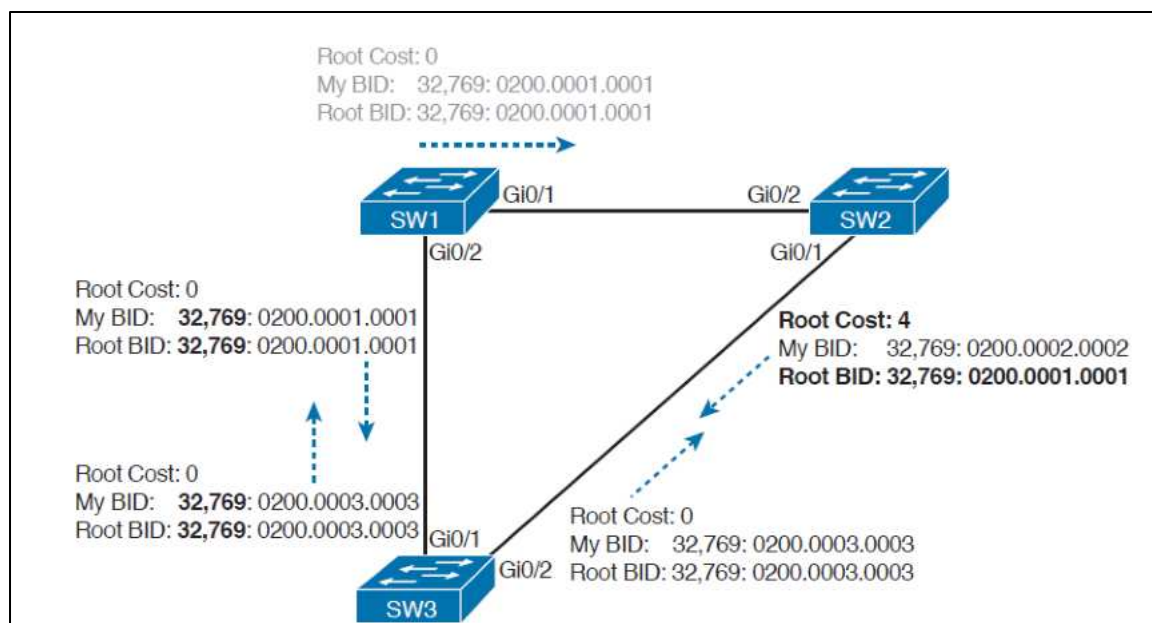
اگر مقدار اولویت دو سوئیچ برابر شد، سوئیچی که مک آدرس آن مقدار کمتری را داشته باشد به عنوان سوئیچ Root انتخاب می‌شود. در این حالت به علت یکتا بودن مک آدرس، حتماً یک سوئیچ انتخاب خواهد شد. پس اگر مقدار اولویت دو سوئیچ برابر باشد و مک آدرس آنها 0200.0000.0000 و 0911.1111.1111 باشد، سوئیچی که دارای مک آدرس 0200.0000.0000 است، به عنوان سوئیچ Root انتخاب می‌شود.

مقدار اولویت مضربی از 4096 است و به صورت پیش فرض برای همه سوئیچ‌ها مقدار 32768 را دارد. از آنجایی که مک آدرس سوئیچ‌ها معیار مناسبی برای انتخاب سوئیچ root نمی‌باشد بهتر است به صورت دستی مقدار اولویت را تغییر دهیم تا سوئیچی که می‌خواهیم، به عنوان سوئیچ root انتخاب شود.

در پروسه انتخاب سوئیچ Root، سوئیچ‌ها از طریق فرستادن پیام‌های Hello BPDUs که BID خود را در این پیام‌ها به عنوان Root BID قرار داده‌اند، سعی می‌کنند خود را به عنوان سوئیچ Root به سوئیچ‌های مجاور خود معرفی کنند. اگر یک سوئیچ پیامی را دریافت کند که BID کمتری نسبت به BID خودش داشته

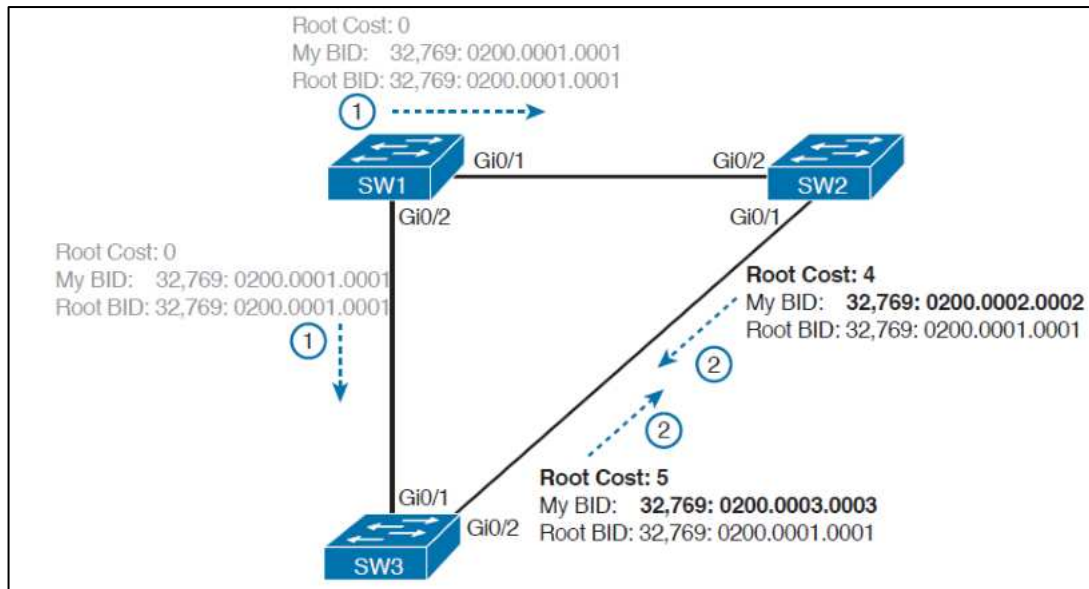
باشد، آن سوئیچ دیگر خود را به عنوان سوئیچ Root معرفی نمی کند، به جای آن شروع به ارسال BPDUs دریافتی که دارای BID بهتری است، می کند. (مانند رقابت های انتخاباتی که یک نامزد به نفع نامزد دیگر که موقعیت بهتری دارد از رقابت در انتخابات خارج می شود). در نهایت تمامی سوئیچ ها به یک نظر نهایی می رسند که کدام سوئیچ BID کمتری دارد و همه، آن سوئیچ را به عنوان سوئیچ Root انتخاب می کنند.

توجه: در مقایسه دو پیام Hello، پیامی که BID کمتری دارد، Superior Hello و پیامی که BID بیشتری دارد، Inferior Hello نام دارد.



شکل (۴-۶) چگونگی انتخاب سوئیچ Root

شکل فوق آغاز پروسه انتخاب سوئیچ Root را نشان می دهد، در ابتدای این پروسه SW2 همانند باقی سوئیچ ها خود را به عنوان سوئیچ Root معرفی می کنید. SW2 پس از دریافت Hello مربوط به SW1 متوجه می شود که SW1 شرایط بهتری را برای Root بودن دارد، پس شروع به ارسال Hello دریافت از SW1 می کند. در این حالت سوئیچ SW1 خود را عنوان Root معرفی می کند و SW2 نیز با آن موافقت می کند. اما سوئیچ SW3 هنوز سعی می کند که خود را به عنوان سوئیچ Root معرفی کند و BPDUs Hello های خود را ارسال می کند.



شکل (۵-۶) پروسه انتخاب Root

دو نامزد هنوز باقی می‌مانند: SW1 و SW3 از آنجایی که SW1 مقدار BID کمتری دارد، پس از دریافت BPDU مربوط به SW1، SW1 را به عنوان سوئیچ Root می‌پذیرد و به جای BPDU خود، دریافتی از SW1 را به سوئیچ‌های مجاور ارسال می‌کند.

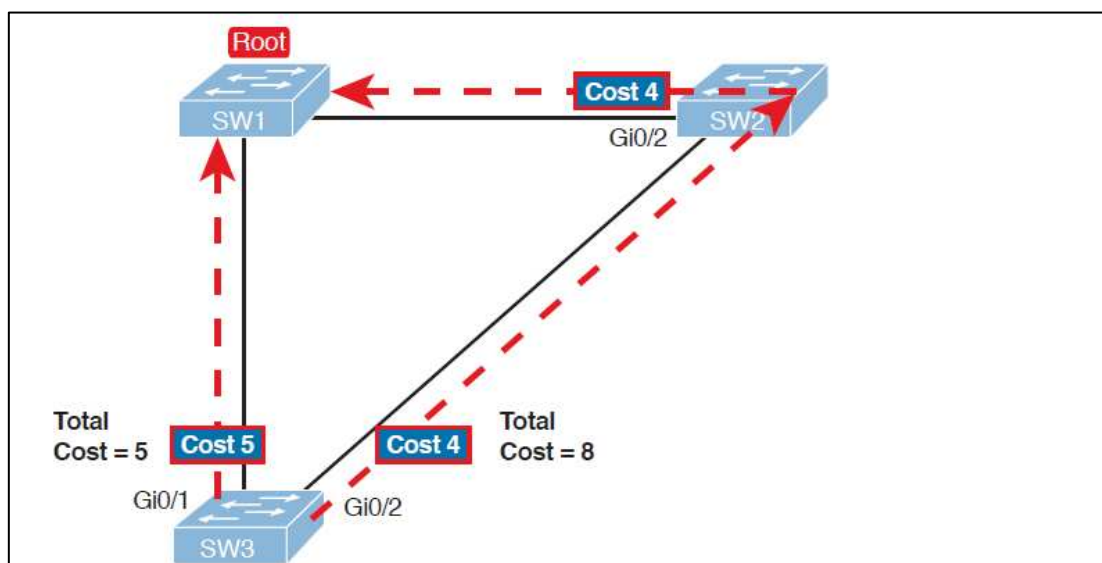
پس از اینکه پروسه انتخاب تکمیل شد، فقط سوئیچ Root به تولید پیام‌های Hello BPDU ادامه می‌دهد. سوئیچ‌های دیگر این پیام‌ها را دریافت می‌کنند و BID فرستنده و Root Cost را تغییر می‌دهد و به باقی پورت‌ها ارسال می‌کند. در شکل فوق، در قدم اول سوئیچ SW1 پیام‌های Hello را ارسال می‌کند، در قدم دوم سوئیچ‌هایی SW2 و SW3 به صورت مستقل تغییرات را روی پیام‌های دریافتی اعمال می‌کنند و آن‌ها را روی پورت‌های خود ارسال می‌کنند.

۶.۷ انتخاب Root Port برای هر سوئیچ

پس از انتخاب سوئیچ Root، در مرحله بعدی، پروتوکول STP برای سوئیچ‌های Non - Root همه سوئیچ‌ها به جز سوئیچ Root یک Root Port (انتخاب می‌کند. RP هر سوئیچ، پورتهی است که کمترین هزینه را برای رسیدن به سوئیچ Root دارد.

احتمالاً عبارت هزینه برای همه ما در انتخاب مسیر بهتر، روشن و مشخص باشد. اگر به دیاگرام شبکه‌یی که در آن سوئیچ Root و هزینه ارسال اطلاعات روی هر پورت مشخص باشد، توجه کنید، می‌توانید هزینه برقراری ارتباط با سوئیچ Root را برای هر پورت به دست آورید. توجه کنید که سوئیچ‌ها برای به دست آوردن هزینه برقراری ارتباط با سوئیچ Root، از دیاگرام شبکه استفاده نمی‌کند، صرفاً استفاده از آن برای درک این موضوع به ما کمک می‌کند.

شکل پایین همین سوئیچ‌های مثال قبلی که در آن سوئیچ Root و هزینه رسیدن به سوئیچ Root را برای پورت‌های سوئیچ SW3 نشان می‌دهد.

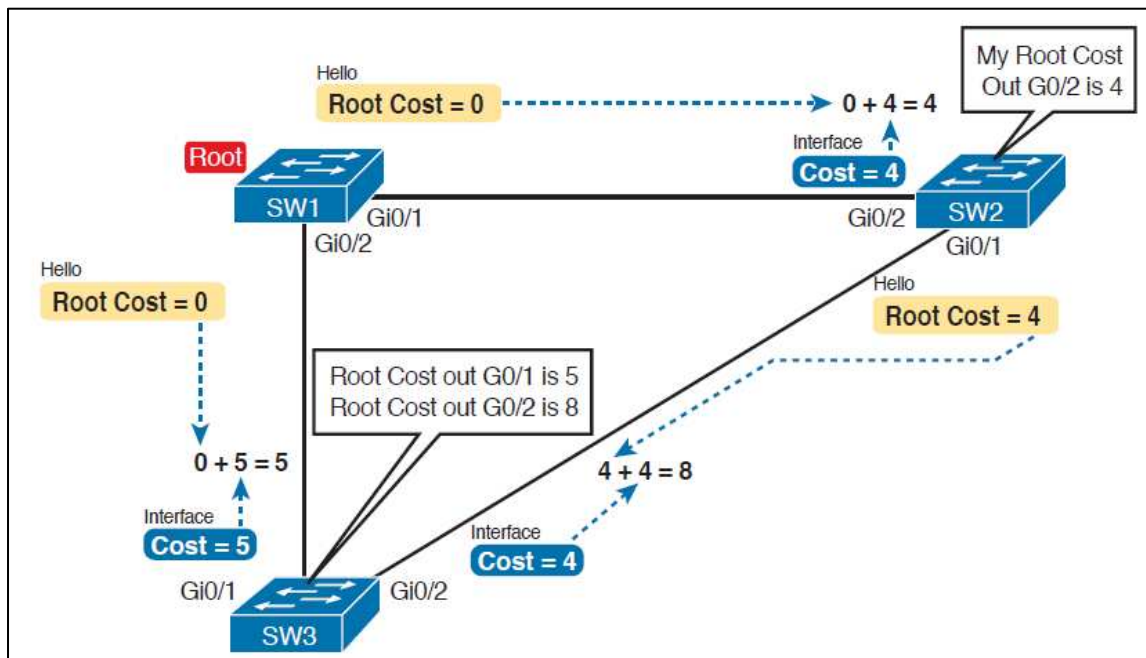


شکل (۶-۶) هزینه رسیدن به سوئیچ Root برای پورت‌های SW3

سوئیچ SW3 برای ارسال Frame‌ها به سوئیچ Root، می‌تواند از دو مسیر استفاده کند: مسیری که از پورت Gi0/1 خارج می‌شود و به سوئیچ Root می‌رسد و مسیر غیر مستقیمی که از پورت Gi0/2 خارج می‌شود و از طریق SW2 به سوئیچ Root می‌رسد. برای هر یک از پورت‌ها، هزینه رسیدن به سوئیچ Root برابر است با مجموع هزینه خروج از پورت‌هایی که Frame ارسالی، برای رسیدن به سوئیچ Root از آن‌ها عبور می‌کند (در این محاسبه، هزینه ورود به پورت‌ها حساب نمی‌شود). همانطور که مشاهده می‌کنید، مجموع هزینه مسیر مستقیم که از پورت Gi0/1 سوئیچ SW3 خارج می‌شود برابر 5 است، و مسیر دیگر دارای مجموع هزینه 8 می‌باشد. از آنجاییکه مسیری که دارای هزینه کمتری برای رسیدن به سوئیچ Root می‌باشد از پورت Gi0/1 خارج می‌شود، سوئیچ SW3 این پورت را به‌عنوان Root Port انتخاب می‌کند.

سوئیچ‌ها با سپری کردن عملیه متفاوت به همین نتیجه می‌رسند. آن‌ها هزینه خروج از پورت خود را به Root Cost موجود در Hello BPDUs ورودی از همان پورت اضافه می‌کنند و هزینه رسیدن به سوئیچ Root از طریق آن پورت را به دست می‌آورند. هزینه خروج از هر پورت در پروتوکول STP یک عدد صحیح (Integer) می‌باشد که به هر پورت در هر VLAN اختصاص می‌یابد، تا پروتوکول STP با استفاده از این مقیاس اندازه‌گیری بتواند و تصمیم بگیرد که کدام پورت را به توپولوژی خود اضافه کند.

سوئیچ‌ها در این پروسه Root Cost سوئیچ‌های مجاوری را که از طریق Hello BPDUs دریافتی به دست می‌آورند، بررسی می‌کنند.



شکل (۷-۶) محاسبه بهترین Root Cost و انتخاب Root Port

شکل (۷-۶) یک مثالی از چگونگی محاسبه بهترین Root Cost و سپس انتخاب آن به عنوان Root Port را نشان می‌دهد. اگر به شکل توجه کنید، خواهید دید که سوئیچ Root پیام‌هایی را که Root Cost آن‌ها برابر صفر می‌باشد، ارسال می‌کند. هزینه رسیدن به سوئیچ Root از طریق پورت‌های سوئیچ Root برابر با صفر است.

در ادامه به سمت چپ شکل توجه کنید که سوئیچ سوم، Root Cost دریافتی از طریق SW1 را که برابر (صفر) می‌باشد، با هزینه خروج از پورت Gi0/1 که آن Hello را دریافت کرده است. مقدار آن برابر (5) می‌باشد، جمع می‌کند و هزینه ارسال اطلاعات از طریق این پورت را به دست می‌آورد.

در سمت راست شکل، سوئیچ SW2 متوجه شده که Root Cost آن برابر با (4) است. پس زمانی که SW2 یک Hello برای SW3 ارسال می‌کند، مقدار Root Cost آن را (4) قرار می‌دهد. در سمت دیگر، هزینه ارسال اطلاعات از طریق پورت Gi0/2 در سوئیچ SW3 برابر (4) می‌باشد. از این سوئیچ SW3 این دو مقدار را با هم جمع می‌کند و به این نتیجه می‌رسد که هزینه رسیدن به سوئیچ Root از طریق پورت Gi0/2 برابر (8) است.

با توجه به نتایج به دست آمده، از آنجایی که پورت Gi0/1 نسبت به پورت Gi0/2 هزینه کمتری برای رسیدن به سوئیچ Root دارد، پس سوئیچ SW3 پورت Gi0/1 را به عنوان RP انتخاب می‌کند. سوئیچ SW2 نیز با گذراندن همین پروسه پورت Gi0/2 را به عنوان RP انتخاب می‌کند. سپس تمام سوئیچ‌ها، Root Port‌های خود را در وضعیت Forwarding قرار می‌دهند.

۶.۸ انتخاب Designated Port در هر LAN Segment

پس از انتخاب سوئیچ Root، در سوئیچ‌های Non – Root، تمام Root Port ها مشخص شدند و در وضعیت Forwarding قرار گرفتند. مرحله نهایی پروتوکول STP برای تکمیل توپولوژی STP، انتخاب Designated Port در هر LAN Segment است. در هر بخش (Segment) از LAN، پورت سوئیچ که کمترین Root Cost را دارد و به آن بخش از LAN متصل است DP (Designated Port) نامیده می‌شود. زمانی که یک سوئیچ Non – Root می‌خواهد که یک Hello را ارسال کند، هزینه رسیدن به سوئیچ Root را در Root Cost آن پیام قرار می‌دهد و ارسال می‌کند. در این صورت پورت سوئیچی که کمترین هزینه را برای رسیدن به Root دارد، در میان تمام سوئیچ‌هایی که به آن بخش متصل هستند، به عنوان DP در آن بخش شناخته می‌شود. در این مرحله اگر هزینه سوئیچ‌ها برای رسیدن به سوئیچ Root برابر بود، پورت سوئیچ را که BID کمتری دارد، به عنوان DP انتخاب می‌کند.

| جدول (۶-۳) وضعیت نهایی پورت‌ها و عوامل آن | | |
|---|------------|--|
| پورت | وضعیت | علت قرار گرفتن در وضعیت |
| SW1, G0/1 | Forwarding | از پورت‌های سوئیچ Root می‌باشد، پس به عنوان DP در آن لینک انتخاب می‌شود. |
| SW1, G0/2 | Forwarding | از پورت‌های سوئیچ Root می‌باشد، پس به عنوان DP در آن لینک انتخاب می‌شود. |
| SW2, G0/2 | Forwarding | Root Port مربوط به سوئیچ SW2 |
| SW2, G0/1 | Forwarding | پورت DP در LAN Segment متصل به SW3 |
| SW3, G0/1 | Forwarding | Root Port مربوط به سوئیچ SW3 |
| SW3, G0/1 | Blocking | این پورت به عنوان RP یا DP انتخاب شد. |

به صورت خلاصه اگر بخواهیم توضیح دهیم، در پروسه اجرای پروتوکول STP:

- در قدم اول سوئیچ Root انتخاب می‌شود که ابتدا تمام سوئیچ‌ها سعی می‌کنند که خود را به عنوان Root معرفی کنند، سپس سوئیچ که رقم BID آن مقدار کمتری را داشته باشد؛ به عنوان سوئیچ Root انتخاب خواهد شد.
- در قدم دوم برای هر سوئیچ، پورتی که کمترین هزینه (cost) برای رسیدن به سوئیچ Root را دارد، به عنوان Root Port انتخاب می‌شود. سپس همه Root Port ها را در وضعیت Forwarding قرار می‌گیرند.
- در قدم سوم، پورت‌های کاندید انتخاب می‌شوند و در وضعیت Forwarding قرار می‌گیرند. در نهایت پورت‌هایی که وضعیت‌شان مشخص نشده است، در حالت Blocking قرار می‌گیرند.

۶.۹ تبدیل کردن یک سوئیچ به Root

با دستور ذیل می‌توانیم یک سوئیچ را به Root تبدیل کنیم.

اگر عدد اولویت (Priority) از سوئیچ‌های دیگر کوچکتر داده شود، سوئیچ به Root تبدیل می‌شود.

```
Switch(config)#spanning-tree vlan 1 priority ?
```

```
<0-61440> bridge priority in increments of 4096
```

```
Switch(config)#spanning-tree vlan 1 priority 4096
```

```
Switch(config)#
```

۶.۱۰ غیر فعال کردن STP

پروتوکول STP به صورت پیش فرض در تمام سوئیچ‌های سیسکو فعال می‌باشد. هیچگاه کوشش نکنید که STP را در شبکه واقعی تان غیر فعال کنید؛ به خاطری که شبکه تان متوقف (Down) خواهد شد. اگر بخواهید آن را غیر فعال کنید، از دستور ذیل استفاده کنید

```
Switch(config)#no spanning-tree vlan 1
```

```
Switch(config)#
```

و اگر بخواهید آن را دوباره فعال کنید، از دستور ذیل استفاده کنید.

```
Switch(config)#spanning-tree vlan 1
```




یکی از مشکلات شبکه از دیدگاه لایه دوم (Data Link) مشکل وقوع حلقه (Loop) می‌باشد. STP پروتوکولی است که با به کار بردن الگوریتم STA توپولوژی را به صورت درختی و بدون حلقه (Loop) به وجود می‌آورد.

در این حالت یک سوئیچ نقش گره اصلی درخت را بازی می‌کند و بقیه سوئیچ‌ها با توجه به گره از بالا به پایین قرار می‌گیرد. الگوریتم STA در مورد وضعیت پورت‌ها و این که کدام پورت ارسال و دریافت فریم را به عهده داشته باشد و یا کدام پورت غیر فعال باشد، تصمیم‌گیری می‌کند.

بعد از اینکه کار الگوریتم STA به پایان رسد تمام پورت‌ها در دو State پایدار قرار می‌گیرد، Forwarding و Blocking. در صورتیکه تغییری در شبکه رخ دهد و توپولوژی شبکه تغییر کند الگوریتم STA دوباره روی تمام سوئیچ‌ها اجرا می‌شود. هر سوئیچ که BID کمتر داشته باشد، به حیث اساس (Root) انتخاب می‌شود. پروتوکول STP به صورت پیش‌فرض در تمام سوئیچ‌های سیسکو فعال می‌باشد. قابل یادآوری است، هیچ‌گاه کوشش نکنید که پروتوکول STP را در شبکه واقعی تان غیر فعال کنید، زیرا با این کار شبکه تان متوقف (Down) خواهد شد.



سوالات فصل ششم

۱. Loop در شبکه چه زمانی اتفاق می افتد؟
۲. تاثیرات بارز Loop در شبکه را توضیح دهید.
۳. کدام پروتوکول از وقوع Loop می تواند جلوگیری نماید.
۴. ضرورت استفاده از پروتوکول STP را توضیح کنید.
۵. Broadcast Storm چیست؟ توضیح دهید.
۶. چه باعث بی ثباتی MAC Table در سوئیچ می شود؟
۷. نحوه کار پروتوکول STP را توضیح دهید.
۸. مراحل انتخاب سوئیچ Root را در پروتوکول STP شرح دهید.
۹. انتخاب Root Port را در پروتوکول STP توضیح دهید.
۱۰. حالت پورت سوئیچ در Forwarding و Blocking را توضیح نمایید.
۱۱. با غیر فعال کردن STP در شبکه، چه واقع می شود؟ شرح دهید.
۱۲. دستور تبدیل یک سوئیچ عادی به سوئیچ Root را توضیح دهید.
۱۳. چگونه می توان STP را غیر فعال کرد؟ توضیح نمایید.



۱. کارکرد پروتوکول STP را در گروپ‌ها بحث نمایید.
۲. در نرم افزار packet tracer شبکه‌یی را دیزاین کنید که دارای چهار سوئیچ باشد. کارکرد پروتوکول STP را بررسی کنید و سپس، سوئیچ دلخواه تان را به Root تبدیل نمایید.
۳. در شبکه که دیزاین کرده‌اید، پروتوکول STP را غیر فعال کنید. ببینید که چه واقع می‌شود. با همصنفی‌ها تان بحث نمایید.

فصل هفتم

شبکه محلی مجازی (VLAN) Virtual Local Area Network



هدف کلی: آشنایی با VLAN و ساختار آن.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. VLAN و ویژگی‌های آن را توضیح نمایند.
۲. نحوه تنظیم VLAN را روی سوئیچ تشریح نمایند.
۳. رابطه Trunk را توضیح نمایند.

هرگاه یک شبکه محلی (LAN) را به صورت مجازی به چندین شبکه کوچک تقسیم نماییم، به نام (VLAN) یاد می‌شود. شبکه را به خاطری تقسیم می‌کنیم که آسان مدیریت شود و امنیت آن بالا برود، همچنان ساحه Broadcast Domain آن کوچک شود. با انجام دادن این کار ازدهام ترافیک در شبکه کم می‌شود و سرعت ارسال و دریافت دیتا زیاد می‌شود. به صورت عموم ارتباط پورت‌ها در VLAN به دو نوع است Trunk link و access link.

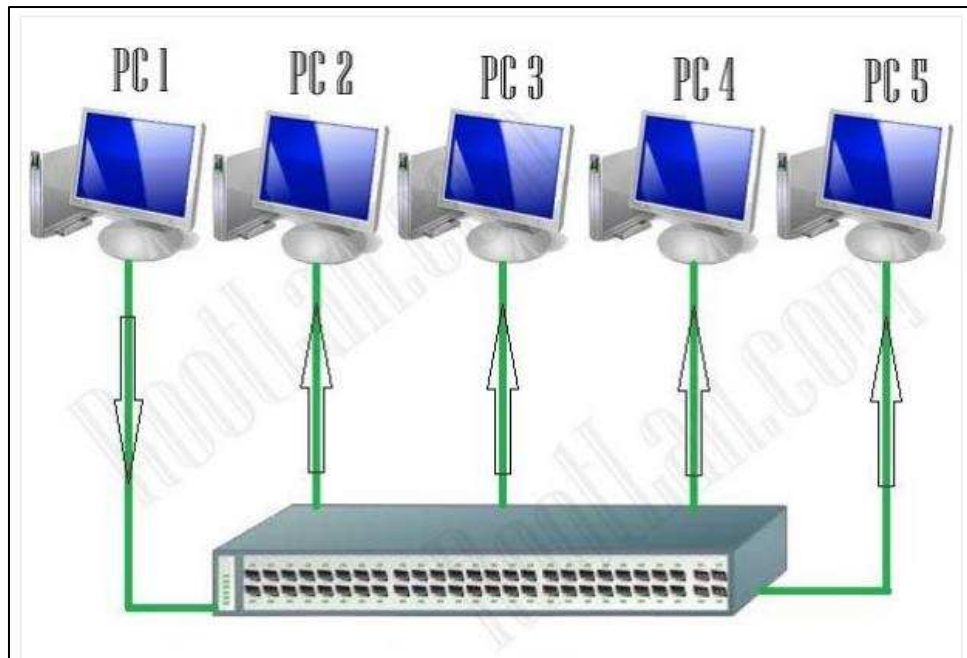
پورت‌های Trunk عبور دیتاهای VLAN‌های مختلف را از خود اجازه می‌دهد. از دو نوع پروتوکول برای بسته‌بندی فریم‌ها استفاده می‌کند که عبارت از 802.1Q و Inter-Switch Link می‌باشد.

۷.۱ شبکه محلی مجازی (VLAN)

شبکه‌یی که به صورت مجازی یک LAN را به چندین شبکه کوچک تقسیم کند، به نام VLAN یاد می‌شود. شبکه محلی مجازی (VLAN)، یکی از جدیدترین و جالب‌ترین تکنالوژی‌های شبکه است که اخیراً مورد توجه بیشتری قرار گرفته است. رشد بدون وقفه شبکه‌های LAN و ضرورت کاهش هزینه‌ها برای تجهیزات گران‌قیمت بدون از دست دادن کارایی و امنیت، اهمیت و ضرورت، توجه بیشتر به VLAN را جلب نموده است.

۷.۲ دلیل استفاده از VLAN

در ابتدا حالتی را در نظر بگیرید که VLAN نداریم، در حالت معمول در یک LAN تمام پورت‌های یک سوئیچ عضو Broadcast Domain مشابهی اند. به این ترتیب اگر یک کامپیوتر پیامی را به صورت Broadcast ارسال کند، تمام کامپیوترهایی که در آن Broadcast Domain هستند، دریافت خواهد کرد. مثلاً: در شکل زیر کامپیوتر PC1 پیامی را به صورت Broadcast ارسال می‌کند و همان طور که در شکل مشخص است، این پیام به تمام کامپیوترهایی که در آن Broadcast Domain قرار دارد، می‌رسد. این کار سبب ازدهام ترافیک در شبکه خواهد شد. به نظر شما این روش از لحاظ کارایی معقول می‌باشد؟



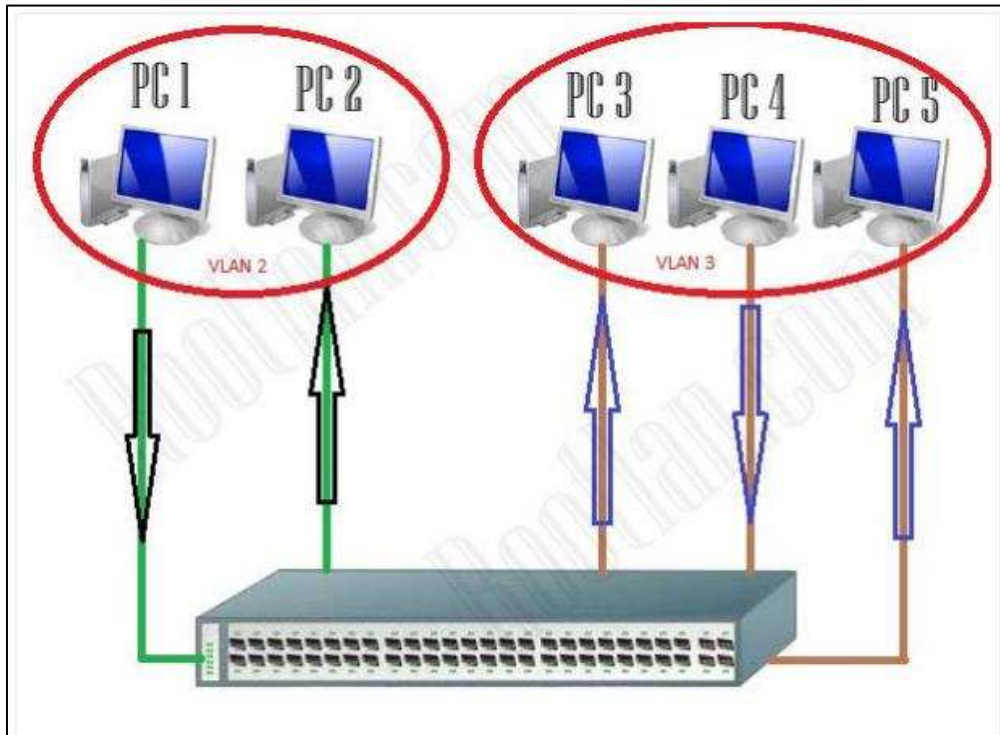
شکل (۷-۱) LAN

در حالت کلی این روش معقول نمی‌باشد؛ زیرا اگر PC1 بخواهد که این پیام را تنها به PC 2 برساند، اما از این طریق سایر کامپیوترها نیز این پیام را دریافت می‌کنند، شاید به نظر تان برسد که برای این کار به جای ارسال Broadcast می‌تواند از ارسال مستقیم به PC 2 استفاده کند، این فکر درست است، اما باید بدانیم که این شکل تنها یک مثال ساده برای بیان چیزی است که می‌خواهیم در موردش بیشتر بدانیم.

به عبارت بهتر، اگر فرض کنید که هر کدام از این کامپیوترها نماد ۱۰۰۰ کامپیوتر باشد، قضیه به چه شکل خواهد بود؟ اینجاست که ارسال Broadcast کاملاً مفید به نظر می‌رسد؛ اما همان طور که گفتیم هنوز این مشکل وجود دارد که علاوه بر PC 2 سایر کامپیوترها هم این پیام را دریافت می‌کنند. این کار پهنای باند زیادی را هدر می‌دهد. اگر از بحث پهنای باند صرف نظر کنیم، از نظر امنیتی به مشکل بر می‌خوریم.

برای رفع این مشکل می‌توان PC 1 و PC 2 را عضو یک VLAN قرار داد و سایر کامپیوترها را را عضو یک LAN دیگر، تا به این شکل هر کدام از این LAN ها Broadcast Domain خودشان را داشته باشند. اما برای این راه حل نیاز است که یک سوئیچ دیگر خریداری کنیم و این هزینه زیادی برای ما در برخواهد داشت. اما اگر از VLAN استفاده کنیم، می‌توانیم همین دو شبکه مجزا را روی یک سوئیچ پیاده‌سازی کنیم و دو VLAN مجزا داشته باشیم.

به این ترتیب، برخی از پورت‌های سوئیچ را- مثلاً به VLAN شماره ۲ و برخی دیگر را به VLAN شماره ۳ نسبت می‌دهیم و هر کدام از VLAN ها Broadcast Domain خاص خود را خواهند داشت که از دسترس سایر کامپیوترهای VLAN دیگر دور خواهد ماند. شکل زیر این موضوع را بهتر نشان می‌دهد.



شکل (۲-۷) VLAN

۷.۳ مزایای VLAN

شبکه محلی مجازی دارای مزایای ذیل می باشد:

۱. امنیت: بخش‌هایی از شبکه بزرگ که دارای اطلاعات حساس‌تری می باشد، با جداسدن از بخش‌های معمولی احتمال آسیب دیدن و یا هرگونه مشکلی برای دیتاهای حساس را کم می کند.
۲. کاهش قیمت‌ها: با استفاده از امکانات VLAN، استفاده بهتر از تمامی منابع شبکه موجود به عمل آمده، دیگر نیازی به ارتقای سخت افزاری در شبکه‌های بزرگ با قیمت بالا نخواهد بود.
۳. عملکرد بهتر: با تبدیل شبکه‌های layer2 به شبکه‌های کوچک مجازی، ترافیک‌های غیر ضروری شبکه کم و در نتیجه، عملکرد بهتر به همراه خواهد داشت.
۴. بهتر شدن کارکرد مدیران آی. تی و شبکه: همانطور که در ابتدا اشاره شد، یکی از اهداف ذاتی از استفاده VLAN ها تبدیل آنها به بخش‌های کوچک‌تر برای مدیریت راحت شبکه‌های بزرگ یاد کردیم. این موضوع در تمامی بخش‌ها از نصب تا اشکال‌یابی، به راحتی به مدیر شبکه کمک خواهد کرد تا در اسرع وقت بتواند بخش مشکل دار شبکه را یافته و رفع کند. حال آنکه در صورت دسته‌بندی نشدن، شاید این موضوع ساعت‌ها به طول انجامد.

۷.۴ انواع VLAN

۱. Default VLAN : وی لن پیش فرض نوعی از VLAN است که تمامی پورت‌های سوئیچ‌ها در وقت راه‌اندازی و تنظیمات، عضو این VLAN خواهند بود.
۲. Data VLAN : نوعی از VLAN است که صرف برای حمل دیتاهای کاربر استفاده می‌شود.
۳. Native VLAN: نوعی از VLAN است که خاص برای پورت‌های ترنک (Trunk) برای انتقال دیتا بین VLAN های مختلف استفاده می‌شود.
۴. Management VLAN: نوعی از VLAN است که برای دسترسی مدیریتی به تنظیمات سوئیچ‌ها طراحی شده است.
۵. Voice VLAN: نوعی از VLAN است که برای voice over ip استفاده می‌شود.

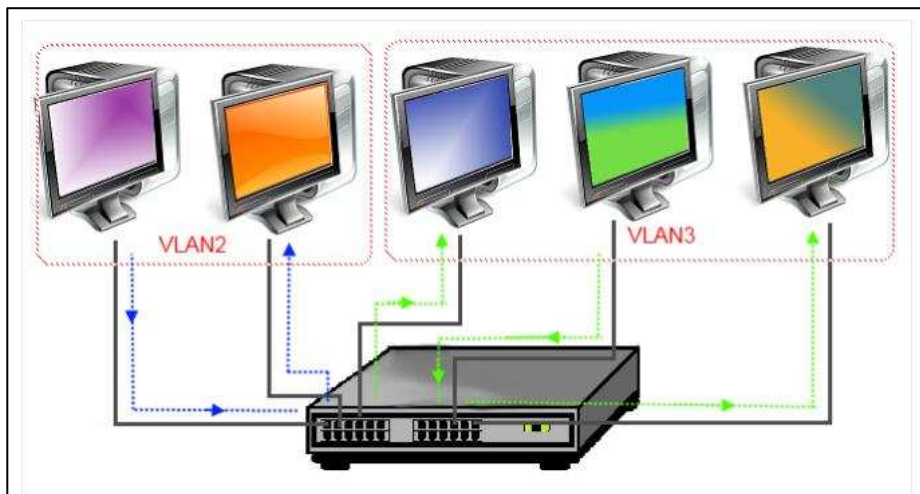
عضویت در VLAN (VLAN Membership)

- ثابت (Static)
- متغیر (Dynamic)

۷.۴.۱ عضویت ثابت (Static)

اختصاص VLAN ها به صورت ثابت، شایع‌ترین و مطمئن‌ترین روش است. تنظیم و نظارت آن بسیار آسان است. در این روش ما VLAN را به صورت دستی اختصاص می‌دهیم تا پورت را تغییر دهیم. VLAN هایی که معمولاً به این ترتیب پیکربندی شده‌اند، به عنوان VLAN های مبتنی بر پورت (Port – Based) شناخته می‌شوند.

روش ثابت (Static) امن‌ترین روش است. همانطور که هر پورت سوئیچ که ما به یک VLAN اختصاص داده‌ایم، این اتصال همیشه حفظ خواهد شد، مگر اینکه ما آن را دستی تغییر دهیم. این روش کارکرد بسیار عالی در محیط شبکه دارد که در آن هر حرکت استفاده کننده (User) داخل شبکه کنترل می‌شود.



شکل (۷-۳) نمایش VLAN ها

۷.۵ حالت ارتباط پورت در VLAN

به صورت کلی یک پورت در VLAN دارای دو نوع ارتباط می‌باشد. در جریان پیکربندی VLAN برای یک پورت، ما باید بدانیم که پورت چه نوع ارتباط را دارد. سوئیچ از دو نوع ارتباط پشتیبانی می‌کند.

۱. Access Link

۲. Trunk Link

۷.۵.۱ Access Link

NIC های استاندارد تنها فریم‌های IEEE 802.3 یا Ethernet II را درک می‌کند، اتصال دسترسی (Access Link) فقط می‌تواند به یک VLAN اختصاص داده شود. به این معناست که تمام دستگاه‌های متصل به این پورت، در یک دامنه پخش (Broadcast Domain) قرار می‌گیرند.

۷.۵.۲ Trunk Link

Trunk ارتباطی است که پورت سوئیچ با یک دستگاه که قادر به درک چندین VLAN است، متصل شود. معمولاً (Trunk Link) برای ارتباط دو سوئیچ یا سوئیچ به روتر استفاده می‌شود. با استفاده از این نوع ارتباط، VLAN می‌تواند در هر نقطه شبکه قرار بگیرد.

(Trunk Link) به ما اجازه می‌دهد تا اطلاعات VLAN های مختلف را در سراسر شبکه ارسال یا دریافت کنیم. برای پشتیبانی از Trunking، فریم اصلی اترنت (Ethernet) برای انتقال اطلاعات VLAN اصلاح شده است.

۷.۶ ایجاد VLAN

با دستورات ذیل VLAN را ایجاد کرده می‌توانیم

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#vlan 100
```

```
Switch(config-vlan)#name TVET_A
```

با دستورات بالا VLAN با شماره 100 ساخته شد حال می‌خواهیم یک پورت را به آن اختصاص دهیم.

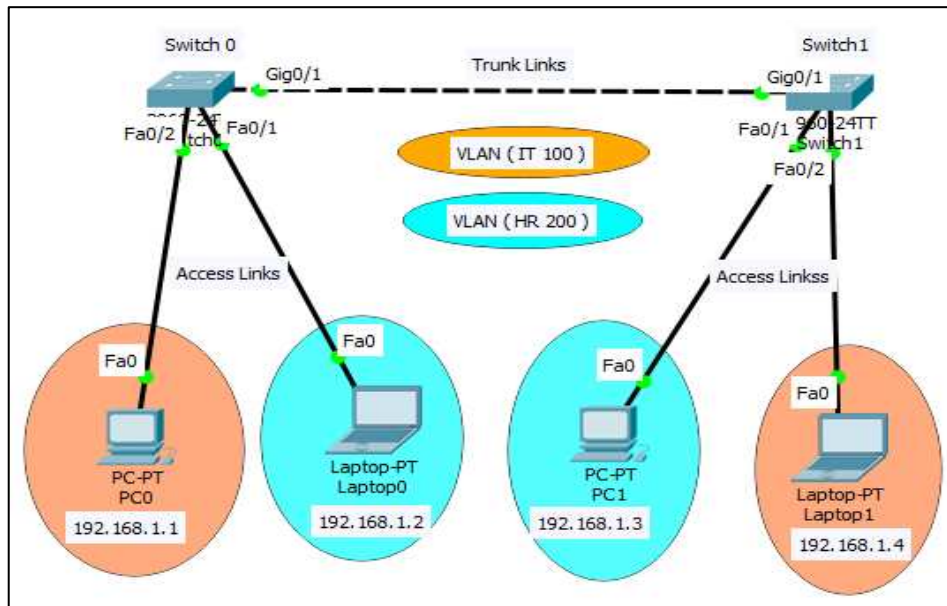
```
Switch(config)#interface fastEthernet 0/5
```

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

```
Switch(config-if)#switchport access vlan 100
```

```
Switch(config-if)#
```

۷.۷ پیکربندی VLAN (VLAN Configuration)



شکل (۷-۴) مثال پیکربندی VLAN

در شکل (۷-۴) دو سوئیچ داریم که به هرسوئیچ دو کامپیوتر وصل شده است، می‌خواهیم در هرسوئیچ دو VLAN ایجاد کنیم، به نام‌های (IT-100 و HR-200). در قدم اول وارد switch0 می‌شویم و تنظیمات ذیل را انجام می‌دهیم.

نوت: به هر vlan صرف یک شماره از (2 الی 4094) داده می‌شود و هرنام که خواسته باشید، به vlan خود داده می‌توانید.

```
Switch0>
```

```
Switch0>enable
```

```
Switch0#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch0(config)#vlan 100
```

```
Switch0(config-vlan)#name IT
```

```
Switch0(config-vlan)#exit
```

```
Switch0(config)#
```

```
Switch0(config)#vlan
```

```
Switch0(config)#vlan 200
```

```
Switch0(config-vlan)#name HR
```

```
Switch0(config-vlan)#exit
```

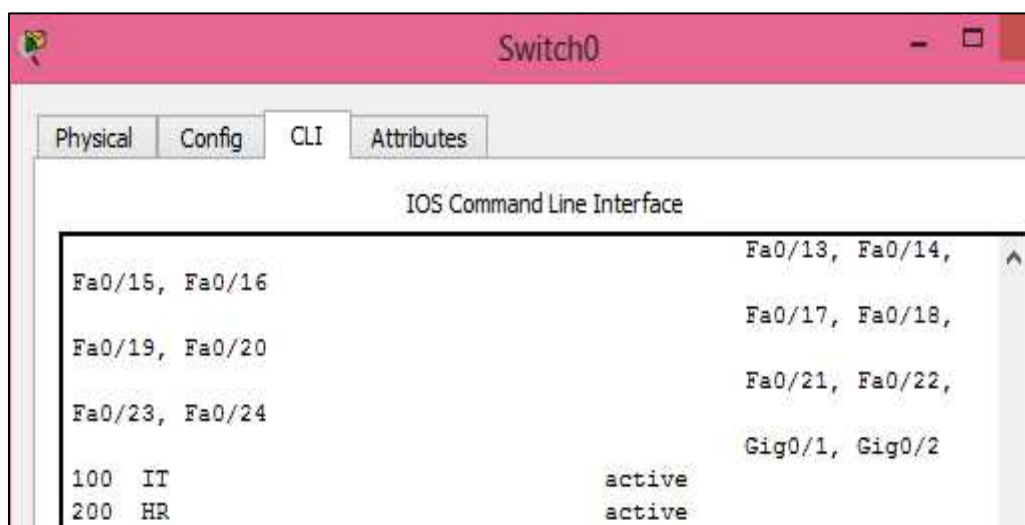
```
Switch0(config)#exit
```

```
Switch#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch0#
```

طوری که دیده می‌شود در switch0 دو Vlan (IT با شماره 100 و HR با شماره 200) ایجاد شده است. که در شکل ذیل دیده می‌شود؛ اما تا حال کدام پورت برایش اختصاص داده نشده است.



شکل (۷-۵) VLAN های ایجاد شده در switch0

به همین طور وارد switch1 می‌شویم و عین تنظیمات را انجام می‌دهیم

```
Switch1>
```

```
Switch1>enable
```

```
Switch1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch1(config)#vlan 100
```

```
Switch1(config-vlan)#name IT
```

```
Switch1(config-vlan)#exit
```

```
Switch1(config)#vlan 200
```

```
Switch1(config-vlan)#name HR
```

```
Switch1(config-vlan)#exit
```

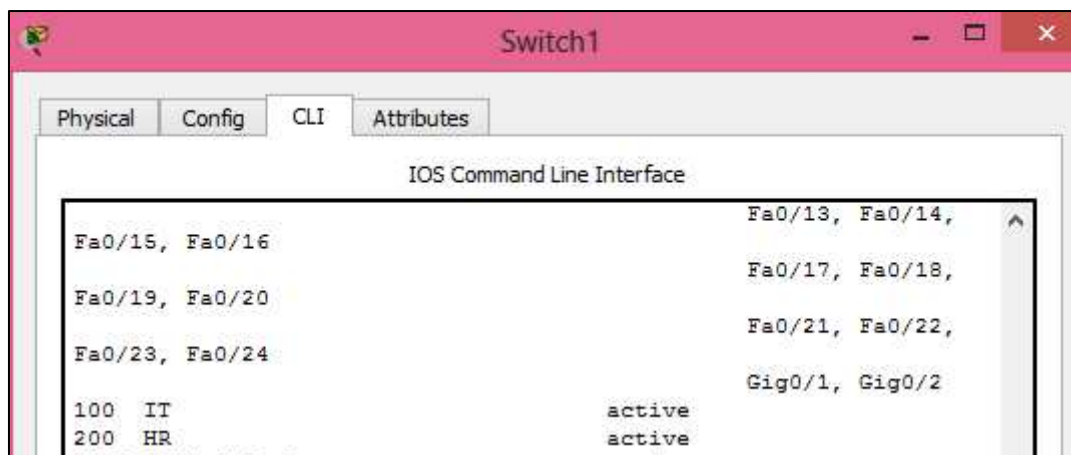
```
Switch1(config)#exit
```

```
Switch1#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch1#
```

در switch1 هم دو Vlan (IT با شماره 100 و HR با شماره 200) ایجاد شده است که در شکل ذیل دیده می شود؛ اما تا حال کدام پورت برایش اختصاص داده نشده است.



شکل (۶-۷) VLAN های ایجاد شده در switch1

به کامپیوترها آدرس های آی پی می دهیم، همه کامپیوترها موفقانه یکدیگر را ping می کند.

نوت: دستور Ping برای تست اتصال بین دو کامپیوتر استفاده می شود.

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

شکل (۷-۷) ping مؤفقا

وقتی که کمپیوترها در vlan های جداگانه انداخته شود، در آن وقت کمپیوترهای یک vlan کمپیوترهای vlan دیگر را ping نخواهد کرد.

حال در switch1 توسط دستور ذیل پورت ها را به vlan های جداگانه اختصاص می دهیم.

Switch1>

Switch1>enable

Switch1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch1(config)#

Switch1(config)#interface fastEthernet 0/1

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 100

Switch1(config-if)#exit

```
Switch1(config)#interface fastEthernet 0/2

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 200

Switch1(config)#exit

Switch1#

%SYS-5-CONFIG_I: Configured from console by console

Switch1#write

Building configuration...

[OK]

Switch1#
```

عین پیکربندی را در switch0 هم انجام می‌دهیم.

```
Switch0>

Switch0>enable

Switch0#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch0(config)#

Switch0(config)#interface fastEthernet 0/1

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 100

Switch0(config-if)#exit

Switch0(config)#interface fastEthernet 0/2

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 200
```

```
Switch0(config)#exit
```

```
Switch0#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

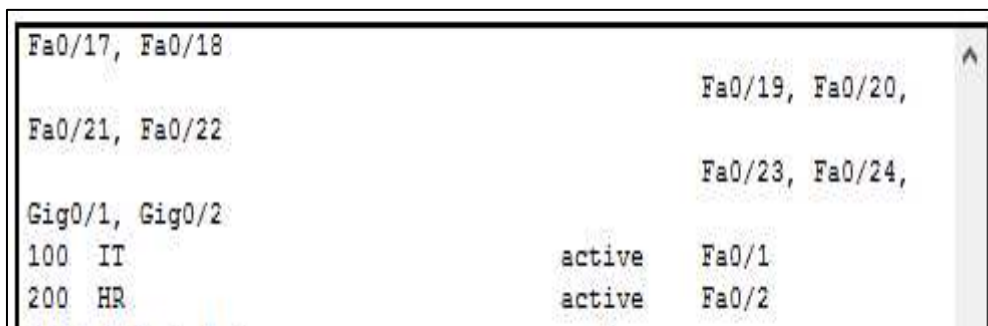
```
Switch0#write
```

```
Building configuration...
```

```
[OK]
```

```
Switch0#
```

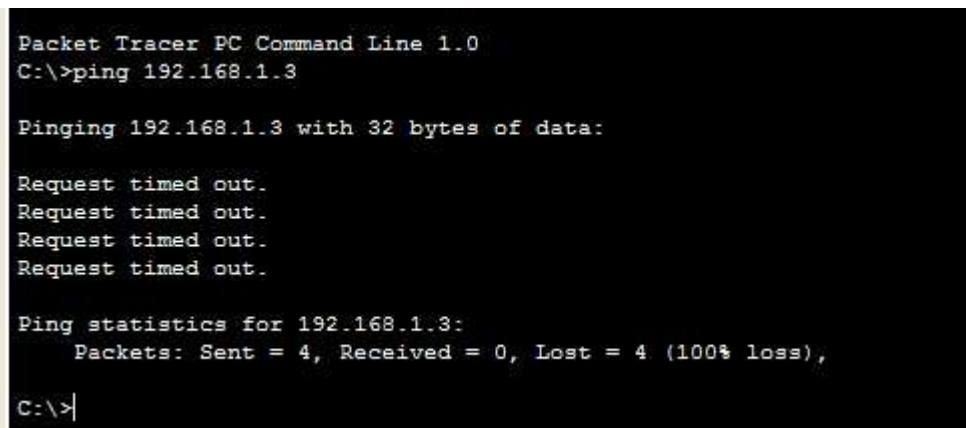
حال در هر دو سوئیچ دیده می‌شود که پورت fa0/1 به vlan-100 و پورت fa0/2 به vlan-200 اختصاص داده شده است. که در شکل ذیل نمایش داده می‌شود.



| | | |
|----------------|--------|-----------------|
| Fa0/17, Fa0/18 | | Fa0/19, Fa0/20, |
| Fa0/21, Fa0/22 | | Fa0/23, Fa0/24, |
| Gig0/1, Gig0/2 | | |
| 100 IT | active | Fa0/1 |
| 200 HR | active | Fa0/2 |

شکل (۷-۸) اختصاص پورت به vlan

حال وقتی از یک کامپیوتر، کامپیوتری را که در vlan مخالف قرار دارد، ping کنیم، جواب نمی‌دهد؛ زیرا یک سوئیچ به صورت مجازی به دو سوئیچ تقسیم گردید.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

شکل (۷-۹) Ping کردن کامپیوتر vlan مخالف

اما کمپیوترهایی که در عین vlan قرار دارد را موفقانه ping می کند.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms

C:\>|
```

شکل (۷-۱۰) ping کردن کمپیوتر در عین vlan

۷.۸ بررسی VLANها

به کمک دستور show vlan می توان تعداد و نام vlan ها و وضعیت هرکدام از آنها و پورت هایی را که در هریک از آنها قرار دارد، مشاهده کرد.

```
Switch#show vlan
```

| VLAN | Name | Status | Ports |
|------|--------------------|-----------|---|
| 1 | default | 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, Gig0/2 |
| 100 | IT | active | Fa0/1 |
| 200 | HR | active | Fa0/2 |
| 1002 | fddi-default | act/unsup | |
| 1003 | token-ring-default | act/unsup | |
| 1004 | fddinet-default | act/unsup | |
| 1005 | trnet-default | act/unsup | |

| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|------|--------|------|--------|--------|----------|-----|----------|--------|--------|
| 1 | enet | 100001 | 1500 | - | - | - | - | - | 0 | 0 |
| 100 | enet | 100100 | 1500 | - | - | - | - | - | 0 | 0 |
| 200 | enet | 100200 | 1500 | - | - | - | - | - | 0 | 0 |
| 1002 | fddi | 101002 | 1500 | - | - | - | - | - | 0 | 0 |
| 1003 | tr | 101003 | 1500 | - | - | - | - | - | 0 | 0 |

شکل (۷-۱۱) نتیجه دستور show

۷.۹ حذف کردن VLAN

در تمام سوئیچ‌ها VLAN1 به صورت پیش فرض تعریف شده است و تمامی پورت‌ها در داخل آن قرار دارد. بنابراین امکان حذف آن وجود ندارد. VLAN‌هایی را که ایجاد کرده‌ایم، می‌توان حذف کرد با این کار تمام پورهای که مربوط آن است، نیز حذف خواهد شد. اگر بخواهیم که پورت حذف نشود، اول وارد انترفیس مربوطه شده و دستور ذیل را وارد کنید تا انترفیس دوباره عضو VLAN1 شود.

```
Switch#configure terminal
```

```
Switch(config)#interface fastEthernet 0/1
```

```
Switch(config-if)#no switchport access vlan 100
```

سپس با وارد کردن دستور ذیل VLAN را حذف کنید.

```
Switch#configure terminal
```

```
Switch(config)#no vlan 100
```

```
Switch(config)#end
```

```
Switch#
```

۷.۹.۱ عضویت متغیر (Dynamic)

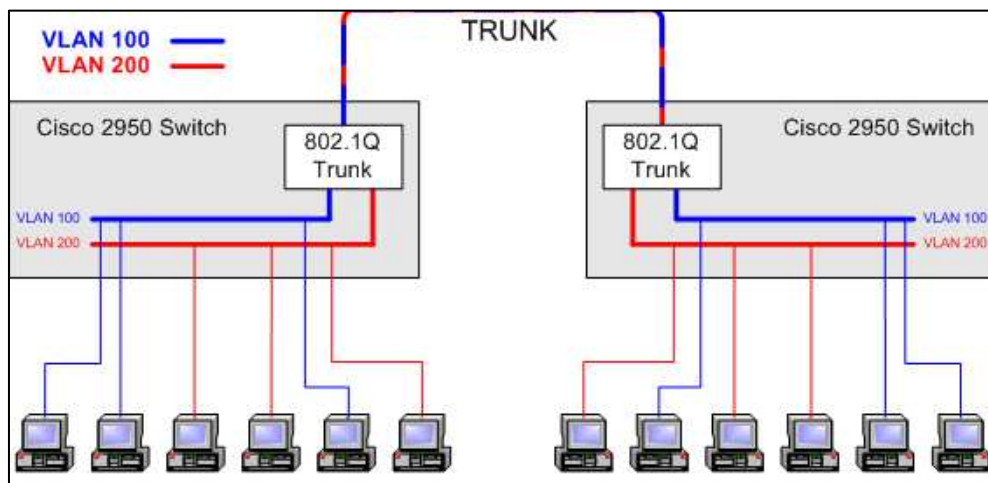
در روش متغیر، VLAN‌ها به طور خودکار به پورت اختصاص داده می‌شوند، البته وابسته به دستگاه‌های متصل. در این روش ما یک سوئیچ را از شبکه به عنوان یک سرور پیکربندی می‌کنیم، سرور شامل اطلاعات خاص دستگاه؛ مانند آدرس MAC، آدرس IP و غیره می‌باشد. این اطلاعات با VLAN هم‌نوا می‌شوند. سوئیچ به عنوان سرور عمل نموده، به عنوان (VMPS – VLAN Membership Policy Server) شناخته می‌شود (سرور خط مشی عضویت VLAN). فقط بالاترین سوئیچ می‌تواند به عنوان VMPS پیکربندی شود. پایان‌ترین سوئیچ به عنوان سرویس گیرنده عمل می‌کند و اطلاعات VLAN را از VMPS دریافت می‌نماید.

VLAN‌های متغیر از قابلیت انتقال (Plug and Play) پشتیبانی می‌کنند، برای مثال اگر ما یک کامپیوتر را از یک پورت به پورت دیگر منتقل کنیم، پورت سوئیچ جدید به طور خودکار به VLAN کاربر (User) که تعلق دارد، پیکربندی می‌شود. در روش ثابت، ما باید این روند را به صورت دستی انجام دهیم.

| Entry | VLAN Membership | MAC Address |
|-------|-----------------|-------------------|
| 1 | 2 | 5D:FF:68:DE:22:0A |
| 2 | 4 | 5A:09:DF:FF:41:12 |
| 3 | 4 | 1A:B4:4F:CC:35:32 |
| 4 | 12 | 8E:E3:FA:C8:B2:63 |
| 5 | 4 | F2:3D:A9:00:37:42 |
| 6 | 4 | C4:72:36:FF:A2:61 |
| 7 | 12 | 5B:90:03:BB:BC:25 |
| 8 | 12 | B9:42:27:A3:7F:1F |
| 9 | 2 | DD:0D:26:52:78:35 |
| 10 | 2 | C4:42:25:1F:DA:94 |

شکل (۷-۱۲) نمایش VLAN های متغیر

۷.۱۰ Trunk Port



شکل (۷-۱۳) ارتباط Trunk

Trunk عبارت از انترفیس است که اطلاعات تمام VLAN ها را از خود عبور می دهد و انترفیس های Trunk عضو هیچ VLAN نمی باشد.

تبدیل پورت به Trunk

```
Switch(config)#interface gigabitEthernet 0/1
```

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

```
Switch(config-if)#
```

```
Switch>
Switch>
Switch>ena
Switch>enable
Switch#
Switch#confi
Switch#configure
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inte
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

Switch(config-if)#
```

شکل (۷-۱۴) تبدیل پورت به Trunk

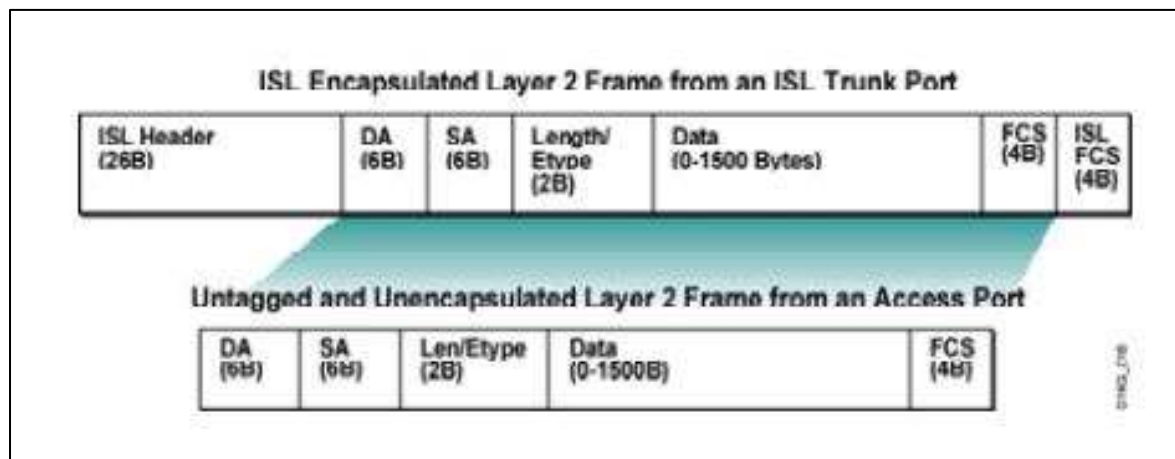
۷.۱۰.۱ Tag زدن به هر فریم جهت انتقال در Trunk

در صورتی که هر کدام از فریم‌های ارسالی از یک سوئیچ دارای برچسب (tag) باشد، به راحتی می‌توان تشخیص داد که فریم از کدام VLAN آمده است و سوئیچ دریافت کننده آن را تحویل VLAN مربوطه می‌کند. بنابراین Trunk وظیفه انتقال فریم‌هایی را که دارای Tag مربوطه هستند، به عهده دارند. برای Tag زدن به یک فریم در یک شبکه Ethernet دو استاندارد زیر وجود دارد:

1. Inter-Switch Link (ISL)
2. 802.1Q

۷.۱۰.۲ پروتوکول (ISL)

ISL به عنوان یک استاندارد لایه دوم به منظور بسته‌بندی کردن یک فریم جهت انتقال در یک کانال ارتباطی مشترک (Trunk) می‌باشد. این پروتوکول مختص به شرکت سیسکو بوده و در Device‌های لایه دوم به صورت پیش فرض فعال می‌باشد. در این استاندارد ساختار فریم اولیه Ethernet تغییر نمی‌کند؛ بلکه فقط فیلدهای ISL Header و ISL FCS به آن اضافه می‌شود.



شکل (۷-۱۵) بسته‌بندی پروتوکول ISL

این پروتوکول توسط دستورهای ذیل پیکربندی می‌شود.

```
Switch>
```

```
Switch>enable
```

```
Switch#configure terminal
```

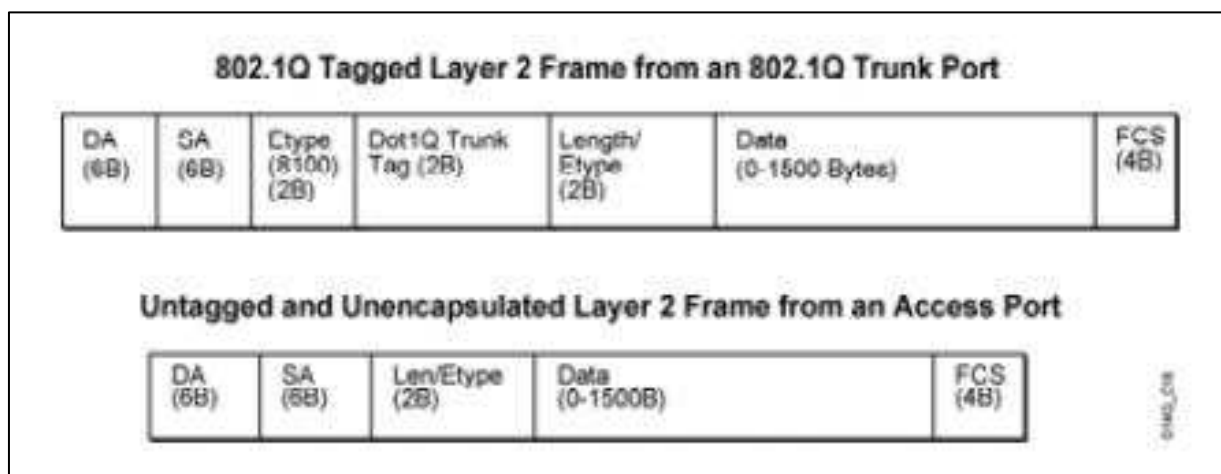
```
Switch(config)#interface fastEthernet 0/1
```

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

```
Switch(config-if)#switchport trunk encapsulation isl
```

۷.۱۰.۳ پروتوکول 802.1Q

802.1Q به عنوان یک استاندارد باز (Open) در لایه دوم جهت برچسب زدن (Tag) به فریم‌هایی که باید در داخل Trunk منتقل شوند، به کار می‌رود. بنابراین سوئیچ‌هایی از شرکت‌های مختلف این پروتوکول را پشتیبانی می‌کند که در یک شبکه، سوئیچ‌های شرکت‌های مختلف وجود داشته باشد. از این پروتوکول برای Tag زدن به فریم‌ها استفاده می‌شود. به اساس این پروتوکول، ساختار فریم Ethernet تغییر می‌کند و منجر به ایجاد یک فریم جدید می‌شود.



شکل (۷-۱۶) بسته بندی پروتوکول 802.1Q

این پروتوکول توسط دستورهای ذیل پیکربندی می‌شود.

```
Switch>
```

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface fastEthernet 0/1
```

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

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



هر شبکه محلی (LAN) دارای یک دامنه پخش (Broadcast Domain) می باشد که سبب ازدهام ترافیک، ضعف مدیریت و ضعف امنیت در شبکه می شود. برای اینکه Broadcast Domain شبکه را کوچک کرده باشیم، لازم است تا شبکه محلی را به بخش های کوچک تقسیم نماییم. بهترین و آسان ترین راه ایجاد شبکه محلی مجازی (VLAN) می باشد. VLAN به دو روش ثابت و متغیر (static و dynamic) ساخته می توانیم که امنیت روش static بیشتر می باشد.

در روش متغیر (dynamic)، VLAN ها به طور خودکار به پورت اختصاص داده می شوند. در این روش ما یک سوئیچ را از شبکه به عنوان یک سرور پیکربندی می کنیم. سرور شامل اطلاعات خاص دستگاه مانند: MAC Address، IP Address و غیره می باشد. VLAN های متغیر از قابلیت انتقال Plug and Play پشتیبانی می کنند.

سوئیچ از دو نوع ارتباط VLAN ها پشتیبانی می کند:

۱. ارتباط دسترسی (Access link)

۲. اتصال بدنه (Trunk link)

ارتباط لینک بدنه (Trunk Link) برای اتصال چندین سوئیچ و به اشتراک گذاری یکسان اطلاعات VLAN ها استفاده می شود. Trunk برای برچسب زدن فریم ها از دو نوع پروتوکول ها استفاده می کند که عبارت از ۸۰۲.۱Q و Inter-Switch Link (ISL) می باشد.



۱. VLAN را تشریح نمایید.
۲. مزایای VLAN برشمارید.
۳. سوئیچ‌ها به‌طور پیش‌فرض به کدام VLAN قرار دارد؟
۴. انواع VLAN‌ها را بیان نمایید؟
۵. فرق میان عضویت در VLAN به شکل Static و Dynamic را توضیح نمایید.
۶. Access Link را توضیح کنید.
۷. Trunk Link را تشریح نمایید.
۸. Trunk Tagging چند نوع است توضیح نمایید.
۹. دستورات ایجاد یک VLAN را تحریر دارید.
۱۰. دستور عضویت یک انترفیس را در یک VLAN تحریر دارید.
۱۱. دستورات تخصیص یک پورت مشخص به یک VLAN را تحریر دارد.
۱۲. دستورات بررسی وضعیت VLAN را توضیح نمایید.
۱۳. دستورات حذف یک VLAN مشخص را تشریح نمایید.



با استفاده از نرم افزار packet tracer یک توپولوژی را دیزاین نمایید که دارای دو سوئیچ باشد و به هر سوئیچ 8 کامپیوتر وصل باشد.

۱. در هر سوئیچ دو VLAN به نام های دلخواه تان بسازید.
۲. پورت هایی که به کامپیوترها وصل است، به حالت access link پیکربندی نمایید.
۳. پورت های بین سوئیچ را به حالت Trunk link پیکربندی نمایید.
۴. پروتوکول 802.1Q را فعال نمایید.

فصل هشتم

پروتوکول معلومات مسیریابی RIP (Routing Information Protocol)



هدف کلی: آشنایی با پروتوکول معلومات مسیریابی یا RIP.

اهداف آموزشی: در پایان این فصل محصلان قادر خواهند شد تا:

۱. پروتوکول RIP را توضیح دهند.
۲. عملکرد پروتوکول RIP را تشریح نمایند.
۳. طریقه تطبیق و تنظیم RIP را توضیح نمایند.

یکی از مباحث مهم در شبکه و زیرساخت، نحوه ایجاد ارتباط بین شبکه‌ها و هدایت بسته‌ها از یک شبکه به شبکه دیگر و تحویل آن به مقصد می‌باشد که به آن مسیریابی گفته می‌شود. مسیریابی به روش‌هایی؛ مانند Static و Dynamic صورت می‌گیرد. در این فصل می‌خواهیم با یکی از پروتوکول‌های Dynamic مسیریابی آشنا شویم.

پروتوکول مسیریابی RIP که دارای نسخه‌های (RIPv1, RIPv2, RIPv6) می‌باشد، برای انتخاب بهترین مسیر در شبکه‌های کمپیوتری استفاده می‌شود. این پروتوکول می‌تواند تا 15 روتر را پشتیبانی کند. به همین لحاظ در شبکه‌هایی که بیشتر از 15 روتر داشته باشد استفاده نمی‌شود.

۸.۱ Routing Information Protocol (RIP)

پروتوکول معلومات مسیریابی (Routing Information Protocol) یا به اختصار RIP قدیمی‌ترین پروتوکول مسیریابی است که در سال 1988 ارائه شد و به عنوان یک پروتوکول IGP، هنوز هم برای شبکه‌های کوچک مورد استفاده قرار می‌گیرد. پروتوکول RIP جزء دسته Distance Vector پروتوکول‌ها می‌باشد. این پروتوکول برای دریافت بهترین مسیر بین شبکه‌های مختلف کمپیوتری استفاده می‌شود. حداکثر تعداد Hop‌ها در پروتکل RIP فقط 15 می‌باشد، یعنی 15 روتر را می‌توان در پروتکل RIP به هم متصل کرد. پروتوکول RIP در هر 30 ثانیه یک بار تمام اطلاعات Routing Table خود را به آدرس 255.255.255.255 (Broadcast) ارسال می‌کند. پروتوکول RIP دارای سه نسخه می‌باشد. Version1 (RFC1058), RIP Version2 (RFC1721 & RFC1722) و RIPv6.

۸.۲ اصطلاحات مهم پروتوکول RIP

۱. همسایگی (Neighbors): دو روتر برای اینکه بتواند اطلاعات جدول مسیریابی خود را بین هم رد و بدل کند، باید یک سلسله شرایط را داشته باشد. در صورت داشتن این شرایط، گفته می‌شود که دو روتر با یکدیگر همسایه شده‌اند.
۲. Update: بسته حاوی اطلاعات مربوط به جدول مسیریابی
۳. Advertisement: عمل ارسال بسته Update توسط روتر روی اینترفیس‌های خود
۴. Metric: عددی که بر اساس فورمول مخصوص پروتوکول مسیریابی به دست می‌آید و جهت انتخاب بهترین مسیر کاربرد دارد.

۸.۳ ویژه گی‌های پروتوکول RIP

۱. RIP یک پروتوکول Distance-Vector می‌باشد.
۲. متریک یا معیار انتخاب بهترین مسیر در این پروتوکول تعداد گام (hop count) می‌باشد.
۳. بلندترین (Maximum) مقداری که برای متریک در این پروتوکول در نظر گرفته شده است، 15 می‌باشد و در صورتی که متریک از این مقدار بیشتر شود، مسیر غیر قابل دسترس خواهد بود و در حقیقت infinity خواهد بود.
۴. Full update در این پروتوکول هر 30 ثانیه یک‌بار در شبکه به صورت Broadcast از اینترفیس‌های متصل به روتر خارج شده، به روترهای مجاور ارسال می‌شود.
۵. Load Balancing: در RIP، روتر در صورتی که چند مسیر با متریک یکسان به یک شبکه پیدا کند، ترافیک را بین این مسیرها تقسیم می‌کند. بنابراین در این حالت از منابع شبکه و پهنای باند موجود به خوبی استفاده می‌شود. RIP به صورت پیش‌فرض توانایی پشتیبانی 4 مسیر با متریک یکسان جهت load balancing را دارد.
۶. IPv1 یک class full routing protocol می‌باشد، زیرا VLSM و CIDR را پشتیبانی نمی‌کند. بنابراین در update‌های که ارسال می‌کند، subnet mask را همراه با Network ID ارسال نمی‌کند.
۷. IPv2 یک classless routing protocol می‌باشد؛ زیرا VLSM و CIDR را پشتیبانی می‌کند. بنابراین در update‌هایی که ارسال می‌کند subnet mask را همراه با Network ID ارسال می‌کند.
۸. RIPng (RIP Next Generation) در IPv6 استفاده می‌شود.

۸.۴ ویژگی‌های Loop Free در پروتکل RIP

۸.۴.۱ مسمومیت مسیر (Route Poisoning)

در شبکه‌هایی که از تعداد روترهای بالا برخوردار هستند و از پروتکل RIP بهره می‌برند، در صورتی که نقطه انتهایی این مسیر قطع شود، به تعداد روترهای موجود در مسیر به دلیل مدت زمان Dead Time که ۱۸۰ ثانیه است، طول می‌کشد تا روتر ابتدایی از قطع شدن شبکه انتهایی با خبر شود. این مدت زمان ممکن است تا ۴۵ دقیقه طول بکشد. به منظور رفع این مشکل، در صورتی که یک مسیر قطع شود، روتر با استفاده از ویژگی Route Poisoning به جای اینکه ۱۸۰ ثانیه منتظر بماند تا اعلام قطعی یک شبکه را ارسال نماید، یک Advertisement با مقدار متریک ۱۶ برای آن شبکه به روترهای دیگر ارسال می‌نماید. در این صورت وقفه ایجاد شده از ۱۸۰ به ۳۰ ثانیه برای روترها کاهش می‌یابد و چون Metric در این ارسال ۱۶ قرار داده شده است، برای روترها به مفهوم عدم کارایی آن می‌باشد.

۸.۴.۲ تقسیم افق (Split Horizon)

در شرایطی که ارتباطات روترها بر روی یک لینک قرار داشته باشد و شبکه یک روتر قطع شود، براساس ویژگی Route Poisoning، مقدار متریک ۱۶ در ۳۰ ثانیه بعدی برای روتر همسایه ارسال می‌شود، اما روتر همسایه تا قبل از دریافت این مقدار، Metric خود را با یک عدد افزایش برای روتر همسایه خود ارسال می‌کند. اتفاقی که رخ می‌دهد این است که جدول روتینگ‌های این دو روتر به روزرسانی شده و این ارسال Route Update ها تا زمانی که هر دو روتر به ۱۶ Metric توافق کنند، ادامه می‌یابد. ویژگی Split Horizon که تقریباً در تمام پروتوکول‌های روتینگ وجود دارد، مانع از این کار می‌شود. براساس این ویژگی یک روتر حق ندارد یک مسیر یادگرفته از یک روتر دیگر را به همان روتر یاد دهد.

نکته: این ویژگی در مسیرهای Poisoned فعال نمی‌باشد. یعنی اگر مسیری را با ۱۶ Metric فراگیرد مجدداً آن را به تمام روترهای همسایه خود و همان روتری که این مسیر را برای این روتر ارسال کرده است، ارسال می‌کند. دلیل این امر، فراگیری سریع تمام روترهای مسیر از قطعی بودن یک ارتباط می‌باشد.

۸.۴.۳ Hold Down Timer

ویژگی Split Horizon برای مسیرهای Multi-Link به تنهایی پاسخگو نمی‌باشد؛ دلیل آن نیز مدت زمان ثابت همگرایی روترها در ۳۰ ثانیه می‌باشد. لذا ویژگی Hold Down Timer به کمک این ویژگی آمده است. در صورتی که یک روتر یک مسیر را با ۱۶ Metric دریافت کند، روتر را به Hold Down Timer به مدت ۱۸۰ ثانیه می‌برد و با دریافت Route Update ها برای آن، مسیر اعلام شده از سوی سایر روترها تغییرات را اعمال نمی‌کند تا این مدت‌زمان به پایان برسد. بنابراین، در این مدت‌زمان در صورتی که یک روتر اطلاعات مسیر اشتباه را در مدت ۳۰ ثانیه ارسال کند، در مدت ۳۰ ثانیه بعدی خود اطلاعات صحیح را به روتر ارسال می‌کند.

۸.۴.۴ Triggered (Flash) Updates

روترها براساس ویژگی Route Poisoning مدت‌زمان ارسال قطع شبکه خود را از ۱۸۰ ثانیه به ۳۰ ثانیه کاهش دادند، اما باز این مدت‌زمان برای شبکه‌یی که مثلاً ۱۵ روتر درون خود دارد، زیاد است. این ویژگی به روتر این امکان را می‌دهد که در صورت قطع شدن یک ارتباط در همان لحظه، یک Route Update با مقدار ۱۶ Metric برای روترهای دیگر ارسال نماید و بعداً در مدت‌زمانی ۳۰ ثانیه خود نیز این Update را برای روترها مجدداً ارسال می‌کند؛ در نتیجه زمان تشخیص خطا در شبکه می‌تواند به صفر ثانیه کاهش یابد.

۸.۵ کارکرد پروتوکول RIP

روترهایی که از پروتوکول RIP استفاده می‌کنند، برای اینکه از تمام مسیرها و شبکه موجود اطلاع پیدا کنند، تمام اطلاعات جدول مسیریابی خود را روی اینترفیس‌هایشان ارسال می‌کند تا سایر روترها اعلام کند که چه شبکه‌هایی را دارند. این ارسال هر ۳۰ ثانیه، یکبار انجام می‌شود. برای ارسال از پروتوکول UDP با شماره

پورت ۵۲۰ استفاده می‌کند. روتر با دریافت بسته Update جدول مسیریابی خود را با آن بروز رسانی می‌کند و فقط یک مسیر اطلاعات را برای یک مقصد در جدول مسیریابی نگه می‌دارد.

روترها از مقدار AD و Metric برای انتخاب مسیر استفاده می‌کند، اما در صورتی که از همسایه خود طی ۱۸۰ ثانیه Update دریافت نکند، آن را غیر قابل استفاده در نظر می‌گیرد و بعد از ۲۴۹ ثانیه از جدول مسیریابی خود، پاک می‌کند. RIP برای انتخاب بهترین مسیر از مفهومی به نام Hop Count استفاده می‌کند. Hop Count بر اساس تعداد روترهای موجود در مسیر، محاسبه می‌شود و حد اکثر مقدار آن ۱۵ می‌باشد. در صورتی که که تعداد از ۱۵ بیشتر باشد، RIP آن شبکه را غیر قابل دسترس در نظر می‌گیرد. RIP به وسیله این روش، از ایجاد Loop در شبکه جلوگیری می‌کند، اما این محدودیت باعث می‌شود که این پروتوکول برای شبکه‌های بزرگ مناسب نباشد.

۸.۶ اعلان اطلاعات به روز (Advertising Update)

RIP به طور مداوم اطلاعات مسیریابی را از همه پورت‌های آن پخش می‌کند. معمولاً این مرحله با پخش محلی (Local Broadcast) با IP مقصد 255.255.255.255 صورت می‌گیرد. در حال پخش اهمیتی نمی‌دهد که چه کسی این پخش را می‌شنود/به دست می‌آورد یا خیر؟ از هیچ مکانیزم برای تأیید شنونده استفاده نمی‌کند.

۸.۷ رابطه غیر فعال (Passive Interface)

به طور پیش فرض پخش RIP (RIP Broadcast) از تمام پورت (Interface)‌ها صورت می‌گیرد. RIP به ما اجازه می‌دهد این رفتار را کنترل کنیم. ما می‌توانیم پیکربندی نماییم تا کدام پورت (Interface) باید RIP Broadcast نماید. هنگامی که ما هر پورت (Interface) را به عنوان پورت غیر فعال (Passive Interface) علامت گذاری می‌کنیم، ارسال‌های به روز سازی RIP از آن پورت متوقف خواهد شد.

۸.۸ شمارش‌هاپ (Hop Count)

RIP هر هاپ، روتر را که یک بسته برای رسیدن به مقصدی از آن عبور می‌کند، شمارش می‌نماید و تعدادهاپ را به 15 محدود می‌کند. RIP از ساحه TTL بسته‌ها برای ردیابی تعدادهاپ‌ها استفاده می‌کند. بعد از عبور بسته‌ها از هر هاپ RIP، مقدار TTL را یک کاش می‌دهد. اگر این مقدار به صفر برسد، بسته رها (Drop) خواهد شد.

۸.۹ تایمرهای پروتوکول RIP (RIP Protocol Timer)

برای بهتر سازی شبکه ، RIP از چهار نوع تایمر ذیل استفاده می کند:

۱. Route update timer : زمان ارسال اطلاعات جدول مسیریابی که پیش فرض هر 30 ثانیه یکبار انجام می شود.
۲. Route invalid timer : حداکثر مدت زمانی که روتر منتظر دریافت advertisement از طرف مقابل می شود و در صورت عدم دریافت route های دریافتی را غیرقابل استفاده در نظر می گیرد که پیش فرض مقدار آن 180 ثانیه است.
۳. Route hold-down timer : در صورت دریافت یک update با متریک بالاتر آن را به مدت 180 ثانیه در حالت hold-down قرار می دهد. برای جلوگیری از بروز loop، اینکار انجام می شود.
۴. Route flush timer : اگر 180 ثانیه از دریافت advertisement گذشت 60 ثانیه دیگر منتظر می ماند، در غیر این صورت route ها را از جدول مسیریابی خود پاک می کند.

۸.۱۰ انواع نسخه های (RIP)

- RIP Version 1
- RIP Version 2
- RIPng (RIP Next Generation)

۸.۱۰.۱ ویژگی های RIP Version ۱

- یک پروتوکول Classful است و از VLSM پشتیبانی نمی کند.
- دارای امکان احراز هویت (Authentication) نیست.
- Advertisement ها را به صورت Broadcast ارسال می کند.

۸.۱۰.۲ ویژگی های RIP Version ۲

- در سال 1993 ارائه شد.
- یک پروتوکول Classless است و از VLSM پشتیبانی می کند.
- دارای امکان احراز هویت (Authentication) است.
- Advertisement ها را به جای Broadcast به صورت Multicast به آدرس 223.0.0.9 ارسال می کند.

۸.۱۰.۳ ویژگی های RIPng

- پشتیبانی از IPv6
- از پروتوکول UDP با شماره پورت 521 استفاده می کند.

نکته: Administrative Distance پروتوکول RIP برابر با 120 می باشد.

نکته: Load Balance را روی 16 خط دارد که مقدار 4 پیش فرض آن می باشد.

نکته: Route های پروتوکول RIP با حرف اختصار R در جدول مسیریابی نمایش داده می شود.

۸.۱۱ تفاوت ها و شباهت های RIP v۱ و RIP v۲

| RIP v1 | RIP v2 |
|---------------------------------------|---------------------------------|
| Distance Vector | Distance Vector |
| Maximum Hop Count of 15 | Maximum Hop Count of 15 |
| Classful | Classless |
| Broadcast Based | Uses Multicast 244.0.0.9 |
| No Support for VLSM | Supports VLSM Networks |
| No Authentication | Allows for MD5 Authentication |
| No Support for discontinuous Networks | Supports discontinuous Networks |

شکل (۸-۱) تفاوت های نسخه ۱ و ۲ پروتوکول Rip

۸.۱۲ تنظیم و فعال کردن پروتوکول RIP

کافی است دستور زیر را در Global Mode وارد کنیم

```
R(config)#router rip
```

با دستور زیر می توانیم نسخه RIP را مشخص کنیم:

```
R(config-router)#version 2
```

نکته: در صورتی که بخواهیم از RIPng استفاده کنیم، از دستور زیر کار می گیریم:

```
R(config)#IPv6 router rip
```

در صورتی که بخواهیم روی برخی از انترفیس ها advertisement ارسال نشود، مانند انترفیس متصل به LAN از دستور زیر استفاده می کنیم:

```
R(config-router)#passive-interface fastethernet 0/0
```

جهت مشخص یا معرفی کردن شبکه هایی که می خواهیم آن ها را advertise کنیم:

```
R(config-router)#network 192.168.1.0
```


- نکته: شبکه مشترک بین دو روتر باید Advertise شود؛ در غیر این صورت بین آن‌ها اطلاعات رد و بدل نمی‌شود.

برای تعیین کردن Authentication برای Advertisement ها به صورت زیر عمل می‌کنیم:

- در ابتدا باید یک دسته کلید تعریف کنیم، به دستورات زیر:

```
R(config)#key chain itpro
```

```
R(config-keychain)#key 1
```

```
R(config-keychain-key)#key-string IT
```

- سپس باید روی انترفیس موردنظر Authentication را فعال کنیم

```
R(config)#interface fastethernet 0/0
```

```
R(config-if)#ip rip authentication key-chain itpro
```

- حالا باید نوع authentication را مشخص کنیم. برای RIP به دو صورت MD5 (Encrypted) و text (Encription) می‌توان تعریف کرد:

```
R(config-if)#ip rip authentication mode md5
```

جهت مشاهده اطلاعات جدول مسیریابی، از دستور زیر استفاده می‌کنیم:

```
R#show ip route
```

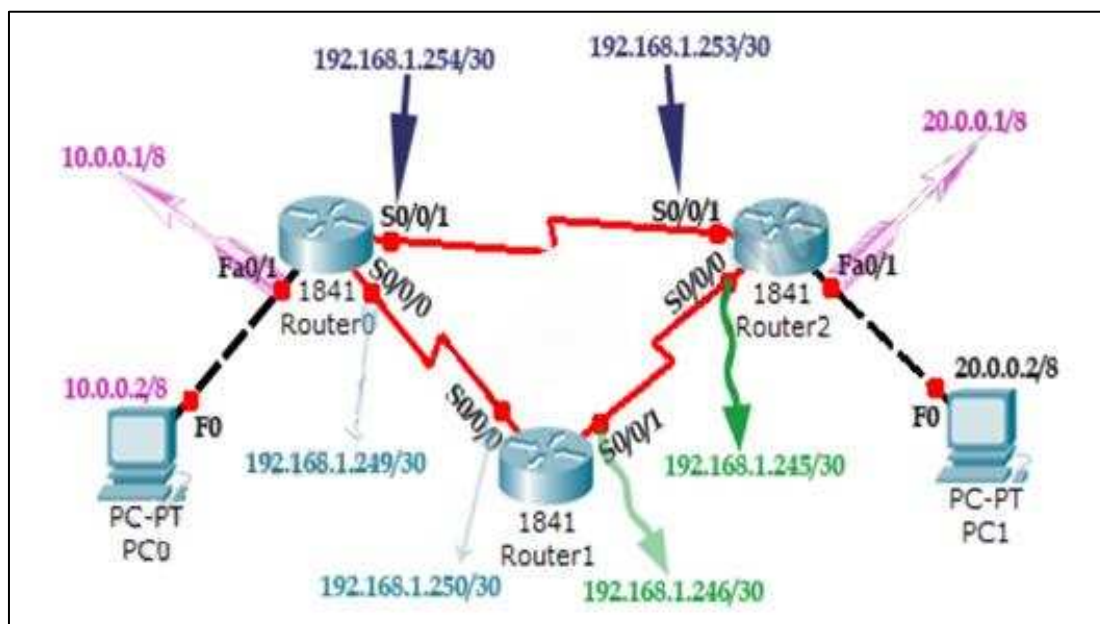
برای عیب‌یابی از دستور زیر استفاده می‌کنیم:

```
R#debug ip rip
```

۸.۱۳ مثال پیاده سازی پروتوکول RIP

با توجه به شکل زیر، می‌خواهیم بین روترهای R0، R1 و R2 پروتوکول RIP را راه‌اندازی کنیم تا این روترها از شبکه موجود مطلع شوند و به آن‌ها دسترسی پیدا کنند.

در مرحله اول یک توپولوژی به صورت زیر می سازیم:



شکل (۸-۲) توپولوژی پیکربندی پروتوکول RIP

جدول (۸-۱) راهنمای ساختار شکل (۸-۲)

| در مرحله دوم، آی پی آدرس را به پورت های روتر و کامپیوتر طوری که در جدول ذیل دیده می شود، اختصاص می دهیم. | | | |
|--|---------------|------------------|--------------------|
| Device | Interface | IP Cofiguration | Connected With |
| PC0 | Fast Ethernet | 10.0.0.2/8 | Router0s Fa0/1 |
| Router0 | 1Fa0/ | 10.0.0.1/8 | PC0s Fast Ethernet |
| Router0 | S0/0/1 | 192.168.1.254/30 | Router2s S0/0/1 |
| Router0 | S0/0/0 | 192.168.1.249/30 | Router1s S0/0/0 |
| Router1 | S0/0/0 | 192.168.1.250/30 | Router0s S0/0/0 |
| Router1 | S0/0/1 | 192.168.1.246/30 | Router2s S0/0/0 |
| Router2 | S0/0/0 | 192.168.1.245/30 | Router1s S0/0/1 |
| Router2 | S0/0/1 | 192.168.1.253/30 | Router0s S0/0/1 |
| Router2 | Fa0/1 | 20.0.0.1/30 | PC1s Fast Ethernet |
| PC1 | Fast Ethernet | 20.0.0.2/30 | Router2s Fa0/1 |

در مرحله سوم به کامپیوترها آدرس آی پی را می دهیم.

۸.۱۴ اختصاص آدرس IP به پورت‌های روترها (Router Interface):

سه پورت 0 / 0 FastEthernet، Serial 0/0/0 و Serial 0 / 0/1 از روتر 0 در این توپولوژی مورد استفاده قرار می‌گیرد.

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration command, one per line. End with CNTL/z.

```
Router (config)#
```

```
Router (config)#interface fastEthernet 0/1
```

```
Router (config-if)#ip address 10.0.0.1 255.0.0.0
```

```
Rputer (config-if)no shutdown
```

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

```
Router (config)#
```

ما می‌توانیم دستور show controllers interface را برای بررسی پایان کیبل استفاده کنیم.

```
Router#show controllers serial 0/0/0
```

```
Interface Serial 0/0/0
```

```
Hardware is powerQUICC MPC860
```

```
DCE V.35, clock rate 2000000
```

```
[Outepute omitted]
```

۸.۱۵ پیکربندی پورت‌های serial مسیر یاب (Router۰):

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.249 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.254 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
```

۸.۱۶ پیکربندی پورت‌های serial مسیر یاب (Router۱):

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.250 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.246 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
```

۸.۱۷ پیکربندی پورتهای مسیریاب (Router۲)

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.245 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.253 255.255.255.252
Router(config-if)#no shutdown
```

حال، پروتوکول RIP را فعال می‌کنیم.

دستور Router Rip برای فعال کردن پروتوکول مسیریابی Rip در مسیریاب استفاده می‌شود. دستور Network ما را قادر می‌سازد تا شبکه‌هایی را که می‌خواهیم تبلیغات (Advertisement) را انتشار دهند، مشخص کنیم. ما فقط نیاز به مشخص کردن شبکه‌هایی را داریم که طور مستقیم با روتر ارتباط دارند. حال پروتوکول RIP را به ترتیب در این سه روتر فعال می‌کنیم

```
Router0(config)#router rip
Router0(config-router)# network 10.0.0.0
Router0(config-router)# network 192.168.1.252
Router0(config-router)# network 192.168.1.248

Router1(config)#router rip
Router1(config-router)# network 192.168.1.244
Router1(config-router)# network 192.168.1.248

Router2(config)#router rip
Router2(config-router)# network 20.0.0.0
Router2(config-router)# network 192.168.1.252
Router2(config-router)# network 192.168.1.244
```

دستور پیکربندی برای RIPv2 به شرح زیر است:

در پیکربندی پروتوکول RIPv2 صرف دستور version 2 اضافه می‌شود، دیگر هیچ تفاوتی با پیکربندی RIPv1 ندارد.

```
#router rip
```

```
#version 2
```

برای اینکه جدول مسیریابی روترها را ببینیم، از دستور show ip route استفاده می‌کنیم.



یکی از مباحث مهم در شبکه و زیرساخت، نحوه ایجاد ارتباط بین شبکه‌ها و هدایت بسته‌ها از یک شبکه به شبکه دیگر و تحویل آن به مقصد می‌باشد که به آن مسیریابی گفته می‌شود.

Routing Information Protocol یا به اختصار RIP قدیمی‌ترین پروتوکول مسیریابی است و RIP جزء دسته Distance Vector است.

روترهایی که از پروتوکول RIP استفاده می‌کنند، تمام اطلاعات جدول مسیریابی خود را روی اینترفیس‌هایشان ارسال می‌کنند. این ارسال هر 30 ثانیه یکبار انجام می‌شود. برای ارسال از پروتوکول UDP با شماره پورت 520 استفاده می‌کند. روتر با دریافت بسته Update جدول مسیریابی خود را با آن بروز (update) می‌کند و فقط یک مسیر اطلاعات را برای یک مقصد در جدول مسیر نگه می‌دارند.

هنگامی که یک Router متوجه شد که هر یک از مسیر مستقیم مرتبط آن شکست (Disconnect) خورده است، آن مسیر را مسموم خواهد کرد. به‌طور پیش‌فرض یک بسته فقط می‌تواند در RIP تا 15 هاب سفر نماید. هر مسیر که فراتر از 15 مرتبه است، مسیر نا معتبر برای RIP است.

پروتوکول RIP از چهار نوع تایمر (Timer) استفاده می‌کند:

۱. (Hold Down Timer)

۲. (Router Invalid Timer)

۳. (Route Flash Timer)

۴. (Update Timer)

RIP دارای نسخه‌های Version 1، Version 2 و (RIP Next Generation) RIPv2 می‌باشد. برای فعال کردن پروتوکول RIP در روتر از دستور router rip استفاده می‌شود.



۱. اصطلاحات Neighborhood، Update و Advertisement را توضیح کنید.
۲. پروتوکول RIP را خلاص توضیح دهید.
۳. Metric در پروتوکول RIP چیست؟ واضح سازید.
۴. Advertising Update و Passive Interface را توضیح کنید.
۵. Split – Horizon و Hop Count را توضیح نمایید.
۶. Route Poisoning را تشریح کنید.
۷. Timerهای پروتوکول RIP را توضیح نمایید.
۸. تفاوت‌های عمده RIPv1 و RIPv2 را واضح سازید.
۹. ویژگی‌های RIPng را توضیح کنید.
۱۰. ویژگی‌های RIPv2 را تشریح نمایید.
۱۱. نحوهٔ تنظیم و فعال کردن RIP را در Packet Tracer با دستورات آن عملی نمایید.



با استفاده از نرم افزار packet tracer توپولوژیی را دیزاین نمایید که دارای دو کامپیوتر، دو سوئیچ و سه مسیریاب (Router) باشد.

۱. پیکربندی ابتدایی مسیریاب (Router) را انجام دهید.
۲. پیکربندی ابتدایی سوئیچ را انجام دهید.
۳. پروتوکول مسیریابی RIP را پیکربندی نمایید.
۴. با استفاده از دستور show مسیریاب و سوئیچ را بررسی نمایید.

1. Wendell, O. (2020). CCNA 200-301 Official Cert Guide Volume1. Cisco Press 221 River St.(3D11C) Hoboken, NJ 07030
2. Todd Lammle, S. O., & Kevin, W. (2015). CCNA Routing and Switching.
3. Wendel, O. & Scott, H. (2017). CCNA Routing and Switching ICND2 200-105 Official Cert Guide. Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.
4. Wendel, O (2016). CCENT/CCNA ICND1 100-105 Official Cert Guide. Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.
5. Todd, L (2016). CCNA Routing and Switching Complete Study Guide/ISBN: 978-1-119-28830-5 Manufactured in the United States of America.
6. Todd Lammle. (2017). CCNA Cisco Certified Network Associate Study Guide/ISBN: 0-7821-2647-2 Manufactured in the United States of America.
7. ([http//cisco.com](http://cisco.com))