نگارش از: مصطفی بنایی فریمان09351743786

فهرست مطالب

مقدمه

آموزش شبکه CCNA شبکه نوع CN

این تکنولوژی برای راحت کردن دسترسی کاربران به اینترنت مورد استفاده قرار می گیرد.CN ها اگاه به وضعیت شبکه هستند و از لایه های 4تا7 مدل OSI که برای آگاهی از وضعیت شبکه استفاده می کنند تا بهترین تصمیم را برای هدایت اطلاعات بر اساس نیاز کاربران اتخاذ کنند. CN ها در گروههای مختلفی قرار می گیرند:

Content Distribution .Content Routing . Content Switching .Content Management . Content Dlivery,Intelligent network Services.

کمپانی های مختلف دو نوع کلی CN را عرضه می کنند:

1- دستگاه هایی که به منظور کش کردن اطلاعات اینترنت مورد استفاده قرار می گیرند.

2- پخش کردن ترافیک رسیده از اینترنت میان سرورهای مختلف با استفاده از خصوصیت Load

آموزش شبکه CCNA Osi Reference Model

سازمان بین المللی استاندارد (OSI) استانداردی برای چگونگی انتقال اطلاعات بین کامپیوترها و دستگاه مختلف ارائه داده است که شامل تمام مراحل ، از مرحله ورود اطلاعات توسط کاربر تا مرحله تبدیل اطلاعات به سیگنال های نوری و قرار گرفتن آنها در داخل سیم به صورت بی سیم می شود. لازم به ذکر است که مدل OSI ایده های مطرح در زمینه انتقال اطلاعات را به صورت کلی بیان می کند و پروتکل هایی مثل IP و IPX کاملاً با استاندارد مزبور همخوانی ندارد.درک مدل 7 لایه ای OSI شما را در مدیریت آسان و دعیب یابی مشکلات شبکه یاری خواهد داد.

CCNA چیست؟

کارد ا ن شبکه(ccna)

مدرکccna که اولین و در واقع پیش نیاز سایر مدارک سیسکو است ، شامل اطلاعات پایه ای در مورد شبکه lan، wan و نحوه نصب و راه اندازی این نوع شبکه ها تا سطح کوچک (زیر یکصد کامپیوتر در شبکه) می باشد . برای کسب این مدرک فقط گذاراندن یک آزمون مورد نیاز است . اما برخی موسسات آموزشی جهت سهولت و راهنمایی بیشتر داوطلبان ، کلاس های آمادگی این مدرک را به دو دوره precisco (شامل مفاهیم موجود در مدرک +network شرکت کامپتیا و فصل Intro سیسکو) و دوره Icnd (فصل دوم تا آخر) تقسیم بندی می کنند . دردوره Icnd مفاهیم سو ییچینگ و روتینگ و همچنین نحوه نصب و راه اندازی سوییچ ها و روترها ی سیسکو در لایه های دوم و سوم شبکه مورد بررسی قرار می گیرد . ضمن این که پروتکل های ارتباطی شبکه هم تا سطح بالا تر ی نسبت به مدرک +NETWORK آموزشی داده می شود . شرکت سیسکو کسب این مدرک را به کسانی که قصد دارند به عنوان دستیار یا همکار با متخصصان شبکه در نصب و راه اندازی و رفع عیب شبکه استخدام شوند ، توصیه می نماید . طبق آمار مجله CERTIFICATION میانگین درآمد دارندگان مدرک CCNA در سال 2004 برابر 65 هزار دلار در سال بوده است که حکایت از یک افزایش 30 در صد نسبت به سال 2002 دارد.

یک شبکه شامل مجموعه ای از سخت افزار ها و نرم افزارهایی می گردد که باعث وصل شده کامپیوترهای به همدیگر شده و دسترسی هر چه سریعتر و آسانتر به منابع ها ، فولدرها ، چاپگرها و ... را فراهم می سازند. برای ایجاد شبکه نیاز به سه عامل مهم داریم: کامپیوترها ، اجزا شبکه و سیم های اتصال که شامل شبکه های بی سیم نیز می شوند.SOHO یعنی کاربرانی که در داخل خانه و یا ادارات کوچک کار انجام دهند .Branch Office یعنی گروهی از کاربران که در منطقه ای کوچک به هم وصل هستند. Users Mobile یعنی کاربرانی که از مناطق Remote و یا دوردست به یک شبکه دسترسی دارند.

در توپولوژی Point-to-Point دو دستگاه به هم وصل می شوند و بیشتر در محیط های Wan استفاده می گردد. در توپولوژی Star یک دستگاه مرکزی باعث وصل شدن دستگاه های دیگر به همدیگر می شود. برای مثال BaseT Hub10 یک دستگاه مرکزی است که در محیط Eternet دستگاه های مختلف همدیگر را متصل می نماید.در توپولوژی BUS یک قطعه سیم تمامی دستگاه ها را به هم وصل می کند و Base510 مثالی برای این نوع توپولوژی است.در توپولوژی Ring نیز دستگاه ها به هم دیگر به ترتیب وصل شده و دستگاه آخر نیز دوباره به دستگاه اول وصل می گردد که FDDI مثالی برای این نوع است. توپولوژی Physical نشان دهنده چگونگی اتصال دستگاه های مختلف توسط وسایلی مانند سیم ها است . توپولوژی Logical یا منطقی نشادهنده اینست که چگونه دستگاه ها توسط سیم های رابط با همدیگر ارتباط برقرا Meshing نشان دهنده چگونگی اتصال دستگاه ها به همدیگر است. در مواقعی که تمامی دستگاه ها ارتباط مستقیمی را با بقیه برقرار نمایند، همدیگر نباشند ، عبارت Partial Mashed بکار می اصطلاح رود. ر می کنند و چه دستگاهی با کدام دستگاه ارتباط دارد. Fully Meshed و در صورتیکه همه دستگاهها دارای ارتباطی مستقیمی با در شبکه های نوع LAN دستگاه های موجود در یک منطقه جغرافیایی خیلی کوچک ، مثل داخل یک ساختمان به همدیگر وصل می شوند . انواع Media های مورد استفاده در Lan عبارتند از : Ethernet.Token Ring.Fddi.Gigabit Ethernet (GE). Fast Ethernet (FE). شبکه های نوع wan برای وصل کردن LAN های مختلف با فواصل دور به همدیگر مورد استفاده قرار می گیرد. انواع WAN عبارتنداز : ... Dial-Up,ISDN,DSL,Cable,X.25,SMDS,Frame Relay. شبکه های نوع Man نیز شبیه شبکه های WAN هستند ولی باعث وصل شدن کامپیوتر هایی که در فواصل نسبتاً نزدیکتر به همدیگر قرار دارندمی شوند.مثلاً شعبه های یک شرکت در نواحی مختلف یک شهر قرار دارند.در ضمن سرعت MAN خیلی بیشتر از WAN است.

SAN یک محیط ذخیره سازی متمرکز و مرکزی را ایجاد می کند که دیسک های ذخیره اطلاعات بوسیله فیبرهای نوری با File Server ارتباط دارند. CN برای اسانتر کردن دستیابی کاربران به اینترنت مورد استفاده قرار می گیرند. کش کردن اطلاعات گرفته شده از اینترنت در حافظه سرور برای دستیابی اسانتر کاربران به اطلاعات گرفته شده و همچنین پخش کردن ترافیک بین سرورهای مختلف از مهمترین وظایف CN هاست INTERNET

شبکه ای است که در داخل یک کمپانی قرار دارد. یک Extranet شبکه ای است که در آن کاربران شناخته شده و مجاز می توانند توسط خطوط امن به منابع شبکه دسترسی داشته باشند. در INTERNET نیز دسترسی هر کاربری به منابع مشترک شبکه امکان پذیر است.

Physical Layer

این لایه اولین و در واقع پایین ترین لایه موجود در مدل OSI می باشد که وظایف زیر را بر عهده دارد.

- تعیین نوع Interface که در بر قراری ارتباط شرکت خواهد کرد.
- تعیین نوع سیم هایی که باید بکار برده شوند.

تعیین نوع Cannector هایی که سیم ها را به Interface ها اتصال می دهند.

یک نوع از Interface به نام NIC نامیده می شود که ممکن است برای مثال کارت BaseT10 و یا یک Interface ثابت روی دستگاه سوئیچ.

این لایه همچنین مسئول اینست که اطلاعات 0و1 را به سیگنال های الکتریکی و ی سیگنال های نوری تبدیل کند را با اندازه گرفتن ولتاژ سیم ها و یا اندازه گرفتن فرکانسهای نوری داخل فیبرهای نوری انجام می دهد. از جمله دستگاه هایی که در این لایه عمل می کنند DEC ها هستند. یک DEC نقطه پایانی WAN هست و عملیات Synchronization و Clocking را در ارتباط با DET (روترها و یا کامپیوترهای شخصی) انجام می دهد. گروه DCE ها شامل مودم ها ، CSU/DSU، NT1 می شوند. در برخی از حالات DCE ها را از همان اول در داخل DTE جاسازی می کنند.برای مثال برخی روتر های سیسکو دارای CSU/DSU و یا NT1 در داخل خودشان نیز می باشند . کلمه DTE و DCE بیشتر در شبکه های WAN کاربرد دارند ولی اگر در LAN بکار برده شوند ، منظور از DTE ، یعنی همان روتر ها ، کامپیوترهای شخصی و یا File Server ها و منظور از DCE یعنی بریج ها و سوئیچ ها . برخی از استانداردهایی که در لایه اول فعالیت می کنند عبارتند از سیم های , Category -5, Category-3 Fiber Channel Category-5E , EIA/TIA-232 , EIA/TIA -449 ,MMF ,SMF

و در موارد استانداردهای Connector ها نیز موارد زیر را برای مثال مطرح می کنیم :

Aui , BNC, DB-9 ,DB-25 , DB-60 ,Rj-11 , Rj-45

دستگاه های Hub و Repetar در این لایه عمل می کنند.

Dtat Link Layer

دومین لایه از مدل OSI است. بر خلاف لایه Network که آدرس دهی منطقی یا Logical شبکه را بر عهده دارد ، وظیفه این لایه آدرس دهی فیزیکی شبکه می باشد. این نوع آدرس به اسم آدرس MAC یا آدرس سخت افزاری نیز نامیده می شود . همچنین این لایه چگونگی اتصال دستگاه ها به Mwdia های مختلف همچنین نوع فریم آنان را مشخص می کند که شامل فیلد های موجود در فریم های لایه دوم یا فریم های Layer Dtat Link می شود. دستگاه هایی در این لایه عمل می کنند که به یک نوع Media وصل باشند . یا به عبارتی دیگر به یک قطعه سیم اتصال داشته باشند . همانطور که یاد دارید برای اتصال دستگاه هایی که به انواع Media اتصال دارند ، یک روتر لازم است.

این لایه همچنین مسئول تحویل گرفتن بیت 0 و 1 و از لایه اول و تبدیل انها به فریم های لایه دوم است. این لایه می تواند در حین انجام کار خطاهای ایجادی را شناسایی کرده و از فریم های بد چشم پوشی کند. البته خطای ایجاد شده به عهده این لایه نبوده و مسئولیت این کار را لایه چهارم بر عهده دارد. اما تعدادی از پروتکل های این لایه ویژگی اصلاح خطاهای ایجادی را نیز پشتیبانی می کنند. نمونه هایی از پروتکل هایی که در این لایه عمل می کنند ، در شبکه های LAN عبارتند از :

IEE's802.2, 802.3,802.5 Ethernet II ANSI's FDDI

و برای شبکه های WAN استانداردهای زیر را داریم:

ATM, PPP , HDLC , Frame Relay ,SLIP , X.25

NICدستگاه هایی که در این لایه عمل می کنند عبارتنداز سوئیچ ها ، روترها و کارتهای شبکه یا همان

Network Layer

سومین لایه از مدل OSI است. این لایه وظایف کم ولی مهمی را بر عهده دارد که از آن جمله می توان به موارد زیر اشاره نمود :

این لایه وظیفه آدرس دهی لایه سوم شبکه را بر عهده دارد. برای همین هم توپولوژی منطقی Logical Topologyشبکه را مشخص می کند. این آدرس های برای گروه کردن تعدادی از ماشینها با همدیگر مورد استفاده قرار می گیرند. در فصل سوم خواهیم دید که آدرس های لایه سوم دارای دو قسمت Host و Network می باشند که قسمت Network دستگاه های موجود را در گروه ها و یا شبکه های جدا گانه قرار می دهد. آدرس های لایه سوم همچنین باعث اتصال Media مختلف به شبکه های جداگانه قرار می هد. آدرس های لایه سوم همچنین باعث اتصال انواع Media های مختلف همدیگر می شوند. مثلاً , Token Ring , FDDI Ethernet به وسیله این لایه با همدیگر ارتباط برقرار می کنند. برای انتقال اطلاعات بین شبکه هایی که از آدرس های لایه سوم مختلف استفاده می کنند ، دستگاهی به اسم روتر مورد نیاز است . روتر های از اطلاعاتی که از آدرس دهی لایه سوم شبکه بدست می آورند ، در یافتن بهترین مسیر برای انتقال اطلاعات بهره می برند. روترها بصورت خیلی جزئی تر در فصل های 9.10و 11 مورد بحث قرار خواهند گرفت . از پروتکل هایی که در این لایه عمل می کنند ، می توان به IPX , IP و Apple talk اشاره نمود. Network Layer بصورت جزئی تر در همین فصل بحث خواهد شد.

Transport Layer .

چهارمین لایه از مدل OSI را تشکیل می دهد. این لایه نقش اصلی ایجاد ارتباط رابر عهده دارد.

ارتباط ایجادی می تواند هم بصورت مطمئن یا Reliable و هم بصورت نا مطمئن Unrelible باشد. در نوع Reliable این لایه مسئولیت کشف خطا و اصلاح آن را بر عهده دارد. به این صورت که در مواقع بروز مشکل ، این لایه اقدام به فرستادن دوباره اطلاعات خواهد کرد. در ارتباطات نوع Unrelible این لایه فقط وظیفه کشف خطا را بر عهده دارد و کار اصلاح خطا را برعهده لایه بالاتر ، مثلاً لایه Application می گذارد. مثال برای ارتباطات Reliable ، پروتکل TCP است و پروتکل UDP نمونه ای برای ارتباطات Unrelible می باشد. همچنین می توان به SPX به عنوان Reliable اشاره نمود. البته پروتکل های IP و IPX هر دو ارتباطات Unrelible را ایجاد می کنند ولی چون این پروتکل ها در لایه Network عمل می کنند و نه در لایه Transport ، برای همین در این دسته قرار نمی گیرند . در طی همنی فصل به صورت خیلی جزئی تر ، لایه Transport و عملکرد آن را شرح خواهیم داد.

Session Layer

پنجمین لایه از مدل OSI را تشکیل می دهد. این لایه وظیفه تصمیم گیری در مورد ایجاد ارتباط با دستگاه های دیگر را بر عهده دارد . به این صورت که اگر منابع درخواستی روی سیستم محلی قرار داشت که هیچ ، ولی اگر اطلاعات روی سیتمی دیگر درجایی دیگر قرار داشت ، تصمیم به برقراری ارتباط می گیرد. همچنین این لایه مسئول این است که اطلاعات در مسیرهای درست خود انتقال پیدا کنند. همچنانکه وظیفه دارد اطلاعات گرفته شده توسط یک ارتباط را به نرم افزار مخصوص به خود انتقال دهد. مکانیسم اصلی ایجاد ارتباط را لایه چهارم یا Transport Layer تشکیل می دهد و Session Layer برای ایجاد ارتباط ، با لایه چهارم مشورت میکند

Presentation Layer

این لایه مسئول اینست که اطلاعات به چه فرمتی به کاربران نشان داده شوند. OSI ششمین لایه از مدل مثلاً این لایه در مورد اینکه متنها ، تصاویر و فیلم و صدا چگونه به افراد نمایش داده شوند تصمیم می می تواند نمایش داده شود. ABCDIC و ASCII گیرند. به عنوان نمونه ، متن به صورت دو استاندارد همان استانداردی است که امروزه در دستگاه های مختلف استفاده می شودو استاندارد ASCII که مورد استفاده قرار می گیرد . در مورد تصاویر نیز Mainframe نیز در محیط های ABCDIC البته همین تنوع در مورد ... JPEG , Gif , BMP , PNG استاندارد های مختلفی وجود دارد. مثل فایلهای صوتی و تصویری نیز وجود دارد . در بین نرم افزارهای موجود ، مرورگرهای وب درارای توانایی های زیادی در نمایش دادن فایلهایی مثل متن ها و تصاویر هستند . همچنین این لایه می تواند به وسیله یا پنهان سازی ، امنیت فایلها را نیز تامین کند ولی در تکنولوژی امروز ، ارائه Encryption خصوصیت دادن راهکارهای امنیتی در انتقال اطلاعات کاری پیچیده بوده و به وسیله مجموعه نرم افزارها و پروتکل های مختلف انجام می گیرد که پردازش بیشتری را نیاز دارد

Layer Application

هفتمین یا بالاترین لایه مدل OSI است. این لایه یک محیط کاری را برای ارتباط بین کاربر و دستگاه ایجاد می کند که از آن طریق می توانند با دستگاه ارتباط بر قرار نمایند . این محیط می تواند گرافیکی یا با خط دستور Interface Command line باشد . این محیط برای دستگاه های سیسکو به صورت خط دستور است در حالیکه مرورگرهای وب مثل اینترنت اکسپلورر مایکروسافت از یک محیط گرافیکی استفاده می کنند . لازم به ذکر است که به منظور از نرم افزار های گفته شده ، آنهایی هستند که توانایی استفاده از شبکه را دارا هستند . در حالیکه شاید هزاران نرم افزار وجود داشته باشد که نتوانند از امکانات شبکه ها استفاده کرده و اطلاعات را از راه شبکه انتقال دهند. حدود 5 سال قبل مرز مشخصی بین نرم افزار هایی که می توانستند به وسیله شبکه ارتباط برقرار کند با آنهایی که نمی توانستند ، وجود داشت . مثلاً نسخه های اولیه Microsoft Word که فقط دارای یک وظیفه بوده و آن هم پردازش متن و مدیریت اسناد بود. در حالی که نسخه های جدید این نرم افزار دارای خصوصیت برقرای با دیگران و یا حتی انجام کارهای گروهی در شبکه نیز هستند . نرم افزارهای دیگر نیز همگام با بر تحویل در تکنولوژی قادر به برقراری ارتباط با شبکه می باشند.

نگارش از: مصطفی بنایی فریمان09351743786

CCNA: برنامه ریزی و طراحی شبکه

CCNA (برگرفته از Cisco Certified Network Associate) اولین مدرک معتبر شرکت سیسکو در رابطه با شبکه است که می توان آن را پیش نیاز سایر مدارک این شرکت در نظر گرفت . علاقه مندان به دریافت این مدرک می بایست توانائی خود را در چهار زمینه زیر افزایش دهند :

برنامه ریزی و طراحی پیاده سازی و عملیات اشکال زدائی

فناوری

در بخش برنامه ریزی و طراحی می بایست بر روی موارد زیر متمرکز و دانش خود را افزایش داد .

طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو طراحی یک مدل آدرس دهی IP منطبق بر طراحی شبکه انتخاب یک پروتکل روتینگ مناسب طراحی یک ارتباط بین شبکه ای ساده با استفاده از فناوری سیسکو پیاده سازی یک لیست دستیابی منطبق بر نیاز کاربران

انتخاب سرویس های WAN منطبق بر نیاز مشتریان

بخش عمده ای از آزمون CCNA ، صرفا" مربوط به پیکربندی دستگاه های شبکه ای نمی باشد و به مواردی قبل از پیکربندی و اشکال زدائی اشاره دارد . در مجموعه مطالبی که بدین منظور آماده و بر روی سایت منتشر خواهد شد به بررسی مسائلی نظیر فرآیند طراحی شبکه ، اتخاذ تصمیم در خصوص استفاده از دستگاه های شبکه ای ، آدرس دهی IP و انتخاب پروتکل های روتینگ خواهیم پرداخت.

بخش اول : طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو

شبکه های محلی (LAN) اساس کار هر نوع ارتباط بین شبکه ای می باشند . در واقع یک ارتباط بین شبکه ای ، ماحصل اتصال مجموعه ای از شبکه های محلی به یکدیگر است . برای ایجاد یک شبکه محلی می توان از مجموعه ای دستگاه های شبکه ای (نظیر سوئیچ ، روتر و هاب) و فناوری استفاده نمود . با استفاده از دستگاه های فوق ، می توان هاست های متعددی را به یکدیگر متصل و یک شبکه محلی را ایجاد نمود . در ادامه و در صورت ضرورت می توان یک شبکه محلی را به شبکه محلی دیگر متصل تا یک ارتباط بین شبکه ای ایجاد گردد .

تعداد شبکه ها و ضرورت استفاده از آنها در سالیان اخیر به شدت رشد یافته است . شبکه های امروزی می بایست به منظور تامین طیف گسترده ای از خواسته ها نظیر اشتراک داده و یا چاپگر و درخواست هائی خاص نظیر ویدئو کنفرانس دارای سرعتی قابل قبول و مناسب باشند . علاوه بر ضرورت به اشتراک گذاشتن منابع بر روی یک شبکه این نیاز بیش از گذشته احساس می شود که بتوان شبکه های متعددی را به یکدیگر متصل تا کاربران آنها بتوانند از منابع موجود بر روی

هر شبکه استفاده نمایند .

همواره این احتمال وجود دارد که مجبور شویم یک شبکه بزرگ را به چندین شبکه کوچکتر تقسیم نمائیم . چراکه به موازات رشد شبکه و افزایش ترافیک آن ، زمان پاسخ به کاربران بتدریج کاهش خواهد یافت. افزایش ترافیک و یا شلوغی شبکه (Congestion) یکی از مسائل مهم در شبکه های کامپیوتری است که عوامل مختلفی در ایجاد آن موثر می باشند. وجود هاست های فراوان در یک Domain Broadcast,

Multicasting بیش از اندازه, پهنای باند کم و نارسا, استفاده از هاب برای ارتباطات شبکه

وجود حجم بالائی از ترافیک ARP و یا IPX (پروتکل روتینگ شرکت ناول که نظیر IP است ولی به شدت پرحرف ! است)

برای حل مشکلات فوق و کاهش بار ترافیکی شبکه می توان یک شبکه بزرگ را به چندین شبکه کوچکتر تقسیم نمود . به این کار segmentation گفته می شود و برای تحقق آن از روتر ، سوئیچ و bridge استفاده می گردد.

روتر

از روترها برای اتصال شبکه ها و مسیریابی بسته های اطلاعاتی از یک شبکه به شبکه دیگر استفاده می گردد . روترها به صورت پیش فرض باعث تفکیک broadcast domain می گردند . به مجموعه ای از دستگاه های موجود بر روی یک شبکه که به broadcast ارسالی بر روی سگمنت گوش می دهند ، broadcast domain گفته می شود . تفکیک broadcast domain در یک شبکه بسیار حائز اهمیت است چراکه پس از ارسال broadcast توسط یک هاست و یا سرویس دهنده ، هر دستگاه موجود در شبکه می بایست آن را دریافت و پردازش نماید . در صورت استفاده از روتر ، زمانی که اینترفیس آن یک broadcast را دریافت می نماید ، می تواند آن را بدون نیاز فورواردینگ به شبکه دیگر ، دور بیاندازد.

با این که روترها به صورت پیش فرض به عنوان دستگاه هائی جهت تفکیک broadcast domain مطرح و شناخته شده می باشند ولی لازم است به این نکته مهم نیز توجه گردد که روترها قادر به تفکیک collision domains نیز می باشند.

برای کاهش ازدحام و یا شلوغی شبکه توسط روتر از روش های متعددی استفاده می گردد:

روترها به صورت پیش فرض broadcast را فورووارد نمی نمایند (سوئیچ و bridge این کار را انجام نمی دهند) .

روترها قادر به روتینگ شبکه بر اساس اطلاعات لایه سه می باشند (مبتنی بر آدرس های IP) . سوئیچ و bridge این کار را انجام نمی دهند.

نگارش از: مصطفی بنایی فریمان09351743786

از روترها در شبکه برای تامین اهداف زیر استفاده می گردد:

سوئیچینگ بسته های اطلاعاتی

روتینگ بسته های اطلاعاتی ارتباطات بین شبکه ای

انتخاب مسیر و یا مسیریابی

سوئیچ

از سوئیچ های LAN برای ارتباطات بین شبکه ای استفاده نمی گردد . در مقابل ، از این نوع دستگاه های شبکه ای برای افزودن قابلیت های جدید به یک شبکه محلی استفاده می شود . مهمترین هدف از بکارگیری سوئیچ ، بهبود کارکرد شبکه های محلی (بهینه سازی کارآئی) از طریق ارائه پهنای باند بیشتر برای کاربران شبکه است. سوئیچ ها نظیر روتر بسته های اطلاعاتی را به سایر شبکه ها فوروارد نمی نماید . در مقابل ، آنها صرفا" فریم ها را از یک پورت به پورت دیگر فوروارد می نمایند . سوئیچ ها نمی توانند فریم ها را بین شبکه ها فوروارد نمایند و صرفا" می توانند حامل فریم ها برای روترها باشند تا توسط روترها به سایر شبکه ها فوروارد گردند.

به صورت پیش فرض ، سوئیچ ها باعث تفکیک Collision domain در یک شبکه می شوند . Collision domain ، یک اصطلاح اترنتی است که از آن به منظور تشریح سناریوی زیر در یک شبکه استفاده می گرد:

یک دستگاه خاص اقدام به ارسال یک بسته اطلاعاتی بر روی یک سگمنت شبکه می نماید و این تاکید را دارد که سایر دستگاه های موجود در سگمنت به آن توجه نمایند و در همان زمان دستگاهی دیگر در شبکه سعی در ارسال داده می نماید. وضعیت فوق یک collision را در سگمنت ایجاد می نماید .در زمان بروز collision ، هر دو دستگاه می بایست مجددا" و پس از طی یک زمان تصادفی اقدام به ارسال مجدد داده نمایند . بدیهی است که ماهیت collision بگونه ای است که در نهایت کاهش کارآئی یک شبکه را به دنبال خواهد داشت .

با توجه به این که هاب صرفا" یک collision domain و یک broadcast domain را ارائه می نماید ، استفاده از آن کارآئی شبکه را به شدت کاهش می دهد . در اینچنین شبکه هائی ، هر هاست موجود در سگمنت به یکی از پورت های هاب متصل می گردد . در مقابل ، هر پورت موجود در یک سوئیچ collision domain مربوط به خود را ارائه می نماید . در واقع ، سوئیچ ها collision domain جداگانه ای را ایجاد می نمایند ولی صرفا" یک broadcast domain را ارائه می نمایند. روترها broadcast domain جداگانه ای را ایجاد می نمایند .

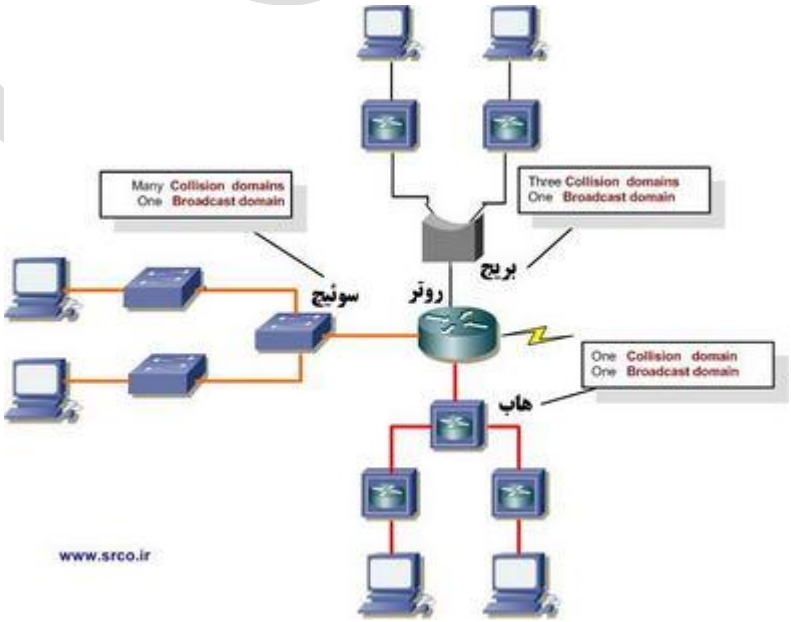
bridge

از واژه bridging قبل از پیاده سازی هاب و روتر ، استفاده می گردید . بنابراین طبیعی است

کـه برخـی افـراد از bridge بـه عنـوان سـوئیچ یـاد کننـد . در واقـع ، سـوئیچ و bridge دارای عملکـردی مشـابه مـی باشـند (کلیـات کـار) . دو دسـتگاه فـوق ، collision domain در یـک شبکه محلی را تفکیک می نمایند . ایـن بـدان معنـی اسـت کـه سـوئیچ اساسـا" یـک bridge چنـدین پـورت بـا قـدرک اداراک بیشـتری اسـت . علـی رغـم وجـود شـباهت هـای زیـاد بـین سـوئیچ و bridge ، تفاوت هائی نیز در ایـن رابطـه وجـود دارد . بـه عنـوان نمونـه سـوئیچ هـا بـه منظـور انجـام وظـایف خـود دارای امکانـات مـدیریتی و قابلیـت هـای پیشـرفته ای مـی باشـند . در اغلـب مـوارد bridge صـرفا" دارای یـــــــک ، دو و یـــــــا چهـــــــار پـــــــورت مـــــــی باشـــــــد.

از bridge زمـانی در شـبکه اسـتفاده مـی شـود کـه هـدف کـاهش collision در broadcast domain و افـزایش collision domain در شـبکه اسـت . در چنـین وضـعیتی bridge پهنـای بانـد بیشـتری را بـرای کـاربران ارائـه مـی نمایـد. یکـی از مزایـای اولیـه bridging ، افـزایش پهنای باند قابـل دسـترس بـر روی یـک سـگمنت شـبکه اسـت ، چراکـه بـا ایـن کـار تعـداد دسـتگاه هـای موجود در یک collision domain کاهش می یابد.

اســـــــــتفاده از روتـــــــــر ، ســـــــــوئیچ و bridge در شـــــــــبکه شـکل زیـر نحـوه اسـتفاده از تجهیـزات شـبکه ای فـوق را در یـک شـبکه فرضـی نشـان مـی دهـد . در شـکل فـوق سـه شـبکه فرضـی (شـبکه متصـل شـده از طریـق هـاب در قسـمت پـائین شـکل ، شـبکه متصـل شـده از طریـق سـوئیچ در قسـمت سـمت چـپ شـکل و شـبکه متصـل شـده از طریـق bridge در قســـمت بـــالای شـــکل) از طریـــق روتـــر بـــه یکـــدیگر متصـــل شـــده انـــد.



توضیحات :

همانگونه که در شکل فوق مشاهده می نمائید از روتر در مرکز شبکه استفاده شده است . علت این کار استفاده از فناوری های قدیمی تر نظیر هاب و bridge است . در صورتی که صرفا" از سوئیچ استفاده گردد ، در سناریوی فوق تغییرات عمده ای ایجاد خواهد شد .
در شبکه های جدید می توان سوئیچ را در مرکز شبکه قرار داد و از روتر برای اتصال شبکه های منطقی به یکدیگر استفاده نمود . در صورتی که قصد پیاده سازی اینچنین شبکه هائی را داشته باشیم ، می بایست شبکه های محلی مجازی (VLANs) را ایجاد نمود.
در قسمت بالای شکل فوق از یک bridge استفاده شده است تا به کمک آن هر دو هاب به روتر متصل شوند . همانگونه که در متن این مقاله اشاره گردید ، bridge باعث تفکیک collision domain می گردد ولی تمامی هاست های متصل شده به هر دو هاب همچنان در یک broadcast domain مشابه قرار می گیرند . همچنین ، bridge فوق صرفا" دو collision domain را ایجاد کرده است . بنابراین هر دستگاه متصل شده به یک هاب در یک collision domain مشابه قرار می گیرد.
در قسمت پائین شکل فوق ، سه عدد هاب متصل شده به هم به روتر متصل شده اند . وضعیت فوق باعث ایجاد یک collision domain بزرگ و یک broadcast domain بزرگ می شود (یک بهم ریختگی بزرگ).
بهترین شبکه متصل شده به روتر ، شبکه متصل شده از طریق سوئیچ موجود در قسمت سمت چپ شکل فوق است . چرا ؟ چون هر پورت موجود بر روی سوئیچ باعث تفکیک collision domain می گردد. ولی این یک وضعیت مطلوب نمی باشد چون تمامی دستگاه ها همچنان در یک broadcast domain مشابه قرار داشته و می بایست به تمامی broadcast ارسالی گوش فرا دهند و اگر broadcast domain خیلی بزرگ باشد ، کاربران پهنای باند کمتری را داشته و می بایست broadcast بیشتری را پردازش نمایند . ماحصل این وضعیت ، کاهش زمان پاسخ شبکه به کاربران خواهد بود.
بهترین شبکه ، شبکه ای است که به درستی پیکربندی و منطبق بر نیاز یک سازمان باشد . سوئیچ ها به همراه روترها زمانی که به درستی در یک شبکه کنار هم قرار داده شوند ، طراحی شبکه بهترین وضعیت ممکن را پیدا خواهد کرد.
در شبکه فوق ، نه collision domain و سه broadcast domain وجود دارد .
مشاهده broadcast domain در شکل فوق ساده است چراکه روتر به صورت پیش فرض broadcast domain را تفکیک می نماید و از آنجائی که روتر فوق دارای سه اتصال است ، سه broadcast domain ایجاد می گردد.

مشاهده collision domain در شکل فوق به سادگی broadcast domain نمی باشد. تمامی شبکه متصل شده از طریق هاب دارای یک collision domain است . شبکه متصل شده از طریق bridge شامل سه collision domain و شبکه متصل شده از طریق سوئیچ شامل پنج collision domain است (یکی برای هر پورت سوئیچ) . بنابراین در مجموع نه collision domain در شبکه فوق وجود دارد.

CCNA برنامه ریزی و طراحی شبکه

در بخش اول به این موضوع اشاره گردید که علاقه مندان به دریافت مدرک CCNA می بایست توانائی خود را در چهار زمینه زیر افزایش دهند :

برنامه ریزی و طراحی شامل :

- طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو
- طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه
- انتخاب یک پروتکل روتینگ مناسب
- طراحی یک ارتباط بین شبکه ای ساده با استفاده از فناوری سیسکو
- پیاده سازی یک لیست دستیابی منطبق بر نیاز کاربران
- انتخاب سرویس های WAN منطبق بر نیاز مشتریان <LI dir=rtl>پیاده سازی و عملیات اشکال زدائی

فناوری

در بخش اول با تمرکز بر روی "برنامه ریزی و طراحی " ، با نحوه طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو آشنا شدیم . در این بخش ضمن تداوم تمرکز خود بر روی " برنامه ریزی و طراحی "، به بررسی طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه خواهیم پرداخت.

بخش دوم : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه آدرس IP ، یک شناسه عددی است که به هر ماشین موجود بر روی یک شبکه IP نسبت داده می شود . آدرس فوق ، مکان خاص یک دستگاه بر روی شبکه را مشخص می نماید . آدرس IP یک آدرس نرم افزاری است (نه یک آدرس سخت افزاری) . هر اینترفیس شبکه دارای یک آدرس سخت افزاری نیز می باشد که از آن به منظور یافتن هاست بر روی یک شبکه محلی استفاده می گردد . آدرس دهی مبتنی بر IP ، امکان مبادله اطلاعات بین هاست موجود در یک شبکه محلی با هاست موجود بر روی شبکه دیگر صرفنظر از نوع شبکه محلی را فراهم می نماید .

نگارش از: مصطفی بنایی فریمان09351743786

در زمان طراحی مدل آدرس دهی IP در یک شبکه ، می بایست به مواردی متعددی توجه شود چراکه با در نظر گرفتن برخی ملاحظات در زمان طراحی ، نگهداری شبکه در مدت زمان حیات آن راحت تر می گردد .

در ادامه به برخی از اصطلاحات اساسی در خصوص سیستم آدرس دهی IP ، سیستم سلسله مراتبی آدرس دهی IP ، کلاس های متفاوت آدرس دهی IP ، آدرس های IP خصوصی ، آدرس های broadcast و NAT (برگرفته از translation network address) اشاره خواهیم کرد .

اصطلاحات IP

بیت (bit) : یک بیت شامل یک رقم است . صفر و یا یک

بایت (byte) : یک بایت بسته به این که از parity استفاده شده باشد از هفت و یا هشت بیت تشکیل می گردد . در ادامه همواره فرض ما بر این است که یک بایت از هشت بیت تشکیل شده است .

اکتت (octet) : یک اکتت از هشت بیت تشکیل می گردد و صرفا" یک عدد هشت بیتی در مبنای دو را نشان می دهد . در ادامه به دفعات از واژه های بایت و اکتت به جای هم استفاده شده است .

آدرس شبکه (Network address) : از آدرس شبکه به منظور روتینگ و ارسال بسته های اطلاعاتی به یک شبکه راه دور استفاده می شود . آدرس های 0 . 0 . 0 . 0 و 10 . 0 . 0 . 0 و 10 . 168 . 192 نمونه هائی در این زمینه می باشند .

آدرس پخش (Broadcast address) : از آدرس های فوق ، برنامه ها و هاست ها جهت ارسال اطلاعات برای تمامی گره های موجود در یک شبکه استفاده می نمایند . 255 . 255 . 255 . 255 تمامی شبکه ها و تمامی گره ها 255 . 255 . 16 . 172 تمام subnet و هاست ها بر روی شبکه 0 . 0 . 16 . 172 255 . 255 . 255 . 10 به تمامی subnet و هاست موجود بر روی شبکه 0 . 0 . 0 . 10 نمونه هائی از آدرس های broadcast می باشند .

مدل آدرس دهی سلسله مراتبی IP

یک آدرس IP شامل 32 بیت اطلاعات است . این بیت ها به چهار بخش تقسیم می گردند که به هر بخش بایت و یا اکتت گفته می شود . هر بایت و اکتت شامل هشت بیت می باشد . برای نمایش یک آدرس IP می توان از روش های متعددی استفاده نمود :

آدرس های - جدا شده توسط نقطه (172 . 16 . 30 . 56)

باینری یا مبنای دو (10101100 . 00010000 . 00011110 . 00111000)

تمامی مثال های فوق یک آدرس IP مشابه را نمایش می دهند . در زمان بحث بر روی آدرس دهی IP از مبنای شانزده به میزانی که از "دهدهی - جدا شده توسط نقطه" و یا باینری استفاده می شود ، استفاده نمی گردد . در برخی برنامه ها ممکن است از یک آدرس IP به صورت مبنای شانزده استفاده گردد . ریجستری ویندوز یک نمونه مناسب از برنامه هائی است که آدرس IP ماشین را به صورت مبنای شانزده ذخیره می نماید .

آدرس سی و دو بیتی IP ، یک آدرس ساختیافته و یا سلسله مراتبی است (در مقابل آدرس های غیرسلسله مراتبی و flat) . با این که می توان از هر نوع مدل آدرس دهی استفاده نمود ، ولی توصیه می گردد که از آدرس دهی سلسله مراتبی استفاده شود . ارائه تعداد بسیار زیادی آدرس ، مزیت عمده استفاده از یک مدل آدرس دهی سلسله مراتبی است . با توجه به این که آدرس IP سی و دو بیتی است و هر بیت می تواند مقدار صفر و یا یک را دارا باشد ، در مجموع دو به توان سی و دو آدرس را خواهیم داشت (3 / 4 میلیارد و یا 4,294,967,296) .

اشکال مدل آدرس دهی flat و علت عدم استفاده از آن برای آدرس دهی IP به روتینگ مربوط می گردد . در صورتی که هر آدرس منحصربفرد باشد ، تمامی روترهای موجود در اینترنت می بایست آدرس هر ماشین موجود در اینترنت را ذخیره نمایند . این موضوع روتینگ موثر را غیرممکن می سازد حتی اگر صرفا" بخشی از آدرس های موجود استفاده شده باشد .

برای حل این مشکل می توان از مدل آدرسی دهی سلسله مراتبی با دو و یا سه سطح استفاده نمود که در آن آدرس ها بر اساس شبکه ، هاست (دو سطح) و یا شبکه ، زیر شبکه و هاست (سه سطح) سازماندهی می شوند .

مدل آدرس دهی سلسله مراتبی (با دو و یا سه سطح) را می توان با یک شماره تلفن مقایسه نمود . در یک شماره تلفن ، بخش اول مربوط به کد شهر است . بخش دوم مربوط به یک ناحیه محلی در شهر مورد نظر است و بخش نهائی شماره مشترک است . آدرس های IP از یک ساختار لایه ای مشابه استفاده می نمایند . در مقابل این که تمامی سی و دو بیت به عنوان یک شناسه منحصربفرد در نظر گرفته شود (نظیر مدل آدرس دهی flat) ، بخشی از آدرس ، شامل آدرس شبکه و سایر بخش ها به عنوان زیرشبکه و یا هاست (سه سطح) و یا صرفا" آدرس هاست (دو سطح) در نظر گرفته می شود .

آدرس دهی شبکه

آدرس شبکه که به آن شماره شبکه نیز گفته می شود ، بطور منحصربفرد هر شبکه را مشخص می نماید . آدرس شبکه هر ماشین موجود بر روی یک شبکه مشابه ، به عنوان بخشی از آدرس IP آن در نظر گرفته می شود . در آدرس IP:172.16.30.56 ، اعداد 16 . 172 آدرس

شبکه را مشخص می نماید .

آدرس گره بطور منحصربفرد هر ماشین موجود بر روی یک شبکه را مشخص می نماید. آدرس گره می بایست منحصربفرد باشد چراکه این آدرس یک ماشین خاص موجود بر روی یک شبکه را شناسائی می نماید . به عدد فوق (آدرس گره) به عنوان یک آدرس هاست مراجعه می گردد . در نمونه آدرس IP:172.16.30.56 ، اعداد 56 . 30 آدرس گره را مشخص می نماید .

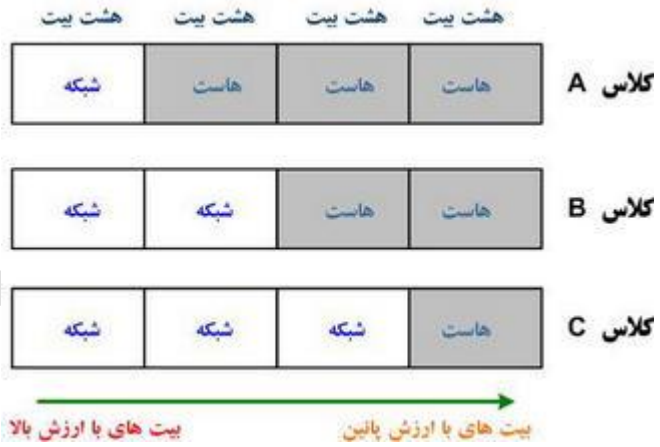
طراحان اینترنت ، با توجه به اندازه شبکه تصمیم به ایجاد کلاس های مختلف شبکه نموده اند:

برای تعداد شبکه های اندکی که گره های فراوانی را شامل می شوند، کلاس A در نظر گرفته شده است.

برای تعداد شبکه های زیادی که دارای گره های کمتری می باشند ، کلاس C در نظر گرفته شده است .

برای شبکه های بین شبکه های بسیار بزرگ و بسیار کوچک ، کلاس B در نظر گرفته شده است .

تقسیم یک آدرس IP به آدرس یک شبکه و گره (هاست) توسط کلاس استفاده شده در شبکه مشخص می گردد . شکل زیر کلاس های مختلف شبکه را نشان می دهد :



شکل یک : کلاس های مختلف شبکه

برای اطمینان از روتینگ موثر ، طراحان اینترنت یک قانون را برای بخش بیت های آغازین آدرس هر یک از کلاس های مختلف شبکه تعریف کرده اند . مثلا" ، با توجه به این که یک روتر می داند که آدرس های شبکه کلاس A همواره با صفر شروع می شوند ، وی می تواند صرفا" پس از خواندن اولین بیت آدرس مورد نظر با سرعت قابل قبول یک بسته اطلاعاتی را به مقصد مورد نظر هدایت نماید . این موضوع نکته مهم در خصوص مدل تعریف شده و وجه تمایز بین آدرس های کلاس A ، کلاس B و کلاس C می باشد .

در ادامه به بررسی کلاس های مختلف شبکه خواهیم پرداخت .

کلاس A

در یک آدرس شبکه کلاس A ، اولین بایت به آدرس شبکه اختصاص یافته است و سه بایت باقیمانده برای آدرس گره ها در نظر گرفته شده است . فرمت کلاس A به صورت network.node.node.node می باشد . به عنوان مثال در آدرس IP: 49.22.102.70 ، عدد 49 آدرس شبکه و 70 . 102 . 22 آدرس گره را مشخص می نماید . هر ماشین موجود بر روی این شبکه خاص می بایست دارای آدرس شبکه 49 باشد .

طول آدرس های شبکه کلاس A صرفا" یک بایت است. بیت اول این بایت رزو شده و از هفت بیت باقیمانده برای آدرس دهی استفاده می گردد . بدین ترتیب ، حداکثر 128 شبکه کلاس A را می توان ایجاد نمود (دو به توان هفت) .

اولین بیت مربوط به اولین بایت در یک آدرس شبکه کلاس A می بایست همواره صفر باشد. این بدان معنی است که یک آدرس کلاس A می بایست بین صفر و 127 باشد . با توجه به این که در آدرس های کلاس A صرفا" یک بایت برای آدرس شبکه در نظر گرفته می شود در صورتی که این آدرس را با توجه به محدودیت اشاره شده (مقدار صفر اولین بیت در بایت مربوطه) به صورت xxxxxxx0 در نظر بگیریم و در ابتدا تمامی هفت بیت باقیمانده را صفر (00000000) و در مرتبه دوم یک (01111111) در نظر بگیریم ، محدوده آدرس های شبکه کلاس A مشخص می گردد (بین صفر تا 127) .

آدرس شبکه تمام صفر (0000 0000) ، برای مسیر پیش فرض رزو شده می باشد . همچنین آدرس 127 برای اشکال زدائی رزو شده است و نمی توان از آن استفاده نمود . بدین ترتیب ، تعداد واقعی آدرس های شبکه کلاس A معادل 126 می باشد (126 = 2 - 128) .

هر آدرس کلاس A دارای سه بایت (24 بیت) برای آدرس دهی یک ماشین در شبکه است . این بدان معنی است که به تعداد دو به توان 24 (معادل 16,777,216) آدرس وجود خواهد داشت که بطور منحصربفرد برای آدرس دهی گره ها در هر شبکه کلاس A استفاده می شود . با توجه به این که آدرس های گره تمام صفر و تمام یک رزو شده می باشند تعداد واقعی گره ها برای یک شبکه کلاس A معادل 16,777,214 (دو به توان 24 منهای دو) می‌باشد. بدین ترتیب می توان تعداد بسیار فراوانی هاست را بر روی یک سگمنت شبکه آدرس دهی و استفاده نمود .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس A می توان از روش زیر استفاده نمود :

در صورت صفر کردن تمامی بیت های مربوط به هاست (سه بایت) ، آدرس شبکه مشخص می گردد :

10 . 0 . 0 . 0

در صورت یک کردن تمامی بیت های مربوط به هاست (سه بایت) ، آدرس broadcast مشخص می گردد :

10 . 255 . 255 . 255

هاست های معتبر ، اعداد بین آدرس شبکه و آدرس broadcast می باشند . (در مثال فوق از 10 . 0 . 0 . 1 تا 10 . 255 . 255 . 254) . بخاطر داشته باشید در مواردی که سعی در یافتن آدرس های معتبر هاست می نمائید ، بیت های هاست نمی توانند تمام صفر و یا تمام یک باشند .

کلاس B

در یک آدرس شبکه کلاس B ، دو بایت اول اختصاص به آدرس شبکه دارد و از دو بایت باقیمانده برای آدرس دهی گره استفاده می گردد. فرمت آدرس های کلاس B به صورت IP : network.network.node.node می باشد . به عنوان نمونه آدرس : 172.16.30.56 ، آدرس شبکه 172 . 16 و آدرس گره 30 . 56 است .

اولین بیت مربوط به اولین بایت می بایست همواره مقدار یک و دومین بیت همواره مقدار صفر را داشته باشد . در صورتی که سایر بیت های باقیمانده در بایت اول را صفر (10000000) و یا یک (10111111) در نظر بگیریم محدوده شبکه های کلاس B مشخص می گردد .(بین 128 تا 191) .

برای آدرس شبکه دو بایت در نظر گرفته شده است . بدین ترتیب ، دو به توان 16 عدد شناسه منحصربفرد برای آدرس دهی شبکه وجود خواهد داشت ولی با توجه به این که تمامی آدرس های شبکه کلاس B می بایست با 1 و صفر شروع شوند (دو بیت رزو شده) ، برای آدرس دهی شبکه از 14 بیت باقیمانده استفاده خواهد شد . بنابراین در نهایت دو به

توان 14 شناسه منحصر بفرد (16,384) برای آدرس دهی شبکه های کلاس B وجود خواهد داشت .

در آدرس های کلاس B از دو بایت برای آدرس دهی گره ها استفاده می شود . این بدان معنی است که به تعداد دو به توان 16 منهای دو (تمام صفر و تمام یک) یعنی معادل 65,534 گره را می توان برای هر شبکه کلاس B آدرس دهی نمود .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس B می توان از روش زیر استفاده نمود :

در صورت صفر کردن تمامی بیت های مربوط به هاست (دو بایت) ، آدرس شبکه مشخص می گردد :

172 . 16 . 0 . 0

در صورت یک کردن تمامی بیت های مربوط به هاست (دو بایت) ، آدرس broadcast مشخص می گردد :

172 . 16 . 255 . 255

هاست های معتبر، اعداد بین آدرس شبکه و آدرس broadcast می باشند. (در مثال فوق از 172 . 16 . 0 . 1 تا 172 . 16 . 255 . 254)

کلاس C

سه بایت اول آدرس های کلاس C به بخش آدرس شبکه و صرفا" یک بایت باقیمانده به آدرس گره اختصاص می یابد . فرمت آدرس های کلاس C به صورت network.network.network.node : است . به عنوان نمونه در آدرس IP:192.168.100.102 ، آدرس شبکه 192 . 168 . 100 و آدرس گره 102 می باشد.

در شبکه های کلاس C ، دو بیت اولین اکتت یک و سومین بیت همواره صفر است (110) برای مشخص کردن محدوده آدرس های شبکه کلاس C پس از دنبال نمودن فرآیندی مشابه با آنچه که در مورد کلاس A و B اشاره گردید می توان محدوده شبکه های کلاس C را بدست آورد (بین 192 تا 223) . بنابراین در صورت مشاهده یک آدرس IP که

شروع آن با 192 تا 223 است ، مشخص می گردد که آدرس فوق یک آدرس IP کلاس C می باشد .

در یک آدرس شبکه کلاس C ، سه بیت اول بایت اول 110 می باشد . بدین ترتیب می توان با انجام محاسباتی ساده تعداد شبکه دردسترس کلاس C را مشخص نمود . 3 بایت (و یا 24 بیت) منهای سه بخش رزو شده ، 21 بیت جهت آدرس دهی را ارائه می نماید که به کمک آنها می توان به تعداد 2 به توان 21 و یا 2,097,152 شبکه کلاس C را ایجاد نمود .

هر شبکه منحصربفرد کلاس C از یک بایت برای آدرس دهی گره ها استفاده می نماید . بدین ترتیب به تعداد دو به توان 8 و یا 256 منهای دو آدرس رزو شده (تمام صفر و یا تمام یک) را می توان برای هر شبکه کلاس C آدرس دهی نمود (254 گره) .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس C می توان از روش زیر استفاده نمود :

در صورت صفر کردن تمامی بیت های مربوط به هاست (یک بایت) ، آدرس شبکه مشخص می گردد :

192 . 168 . 100 . 0

در صورت یک کردن تمامی بیت های مربوط به هاست (یک بایت) ، آدرس broadcast مشخص می گردد :

192 . 168 . 100 . 255

هاست های معتبر ، اعداد بین آدرس شبکه و آدرس broadcast می باشند . (در مثال فوق از 192 . 168 . 100 . 1 تا 192 . 168 . 100 . 254) .

کلاس های D و E

آدرس های بین 224 و 255 برای شبکه های کلاس D و E رزو شده اند . از کلاس D (بین 224 تا 239) برای آدرس های multicast و از کلاس E (بین 240 تا 255) برای اهداف علمی و تحقیقاتی استفاده می گردد .

با توجه به طولانی شدن این بخش اجازه دهید ادامه بحث را در بخش بعدی دنبال نمائیم.

CCNA برنامه ریزی و طراحی شبکه

آنچه تاکنون گفته شده است :

بخش اول برنامه ریزی و طراحی : طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو

بخش دوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

در این بخش ، بحث بر روی طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه را ادامه داده و به مواردی همچون آدرس های رزو شده ، broadcast ، آدرس های IP خصوصی و NAT (برگرفته از address translation network) اشاره خواهیم کرد .

قبل از این که به موارد فوق اشاره نمائیم بد نیست به خلاصه مطالب گفته شده در بخش دوم نگاهی مجدد داشته باشیم . جدول زیر محدوده آدرس های IP را بر اساس مقدار اولین اکتت برای هر یک از کلاس های IP نشان می دهد .

کلاس IP	محدوده آدرس IP بر اساس مقدار اولین اکتت
Class A	1 to 126 (00000001 to 01111110)*
Class B	128 to 191 (10000000 to 10111111)
Class C	192 to 223 (11000000 to 11011111)
Class D	224 to 239 (11100000 to 11101111)
Class E	240 to 255 (11110000 to 11111111)
* : آدرس 127 (01111111) ، یک آدرس کلاس A رزو شده برای تست است و نمی توان آن را به یک شبکه نسبت داد .	

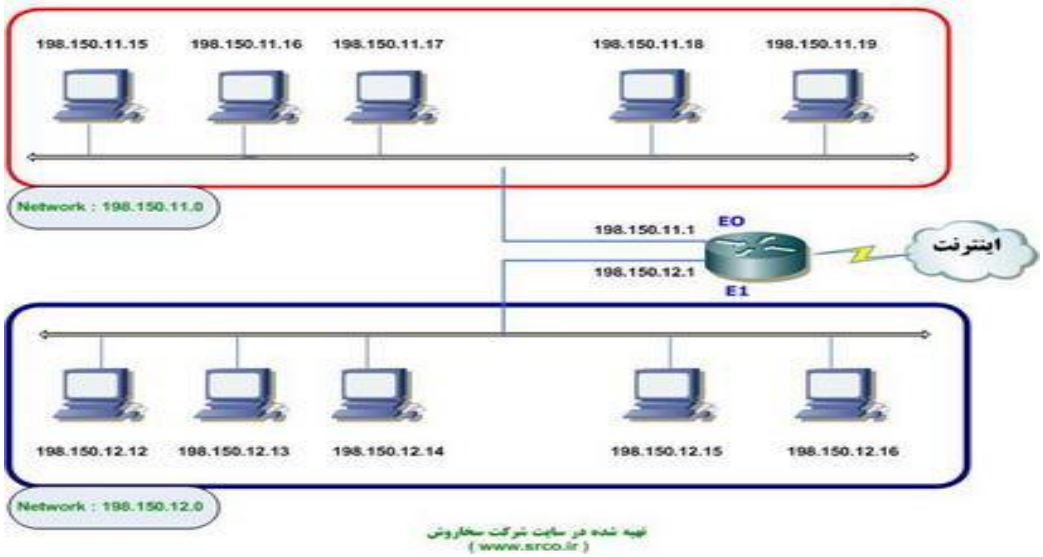
جدول یک : تشخیص کلاس IP بر اساس مقدار دهدهی اولین اکتت

آدرس های رزو شده

برخی از آدرس های IP برای اهداف خاصی رزو شده می باشند و مدیر شبکه نمی تواند از این نوع آدرس ها استفاده نماید:

آدرس هائی که از آنها به منظور شناسائی و یا مشخص کردن خود شبکه استفاده می گردد. همانگونه که در بخش بالای شکل 1 مشاهده می نمائید ، شبکه ای به آدرس 0 . 11 . 150 . 198 مشخص شده است (یک شبکه کلاس C که سه بایت اول آن آدرس شبکه و بایت آخر آدرس هاست را مشخص می نماید) . مادامی که داده بر روی شبکه محلی فوق حرکت می نماید و از یک هاست به هاست دیگر ارسال می گردد ، شماره هاست حائز اهمیت می باشد. زمانی که داده ئی از یک هاست موجود بر روی یک شبکه دیگر برای هر یک از هاست های موجود در این شبکه (محدوده آدرس های 1 . 11 . 150 . 198 تا 254 . 11 . 150 . 198) ، ارسال می گردد در مرحله اول شماره شبکه حائز اهمیت خواهد بود ، چراکه روتر با استفاده از آن قادر به فورواردینگ مناسب بسته اطلاعاتی به شبکه مقصد است (مثلا" ارسال داده از شبکه ای به آدرس 0 . 11 . 159 . 198) . شبکه محلی موجود در قسمت پائین شکل همانند شبکه محلی در بخش بالا عمل می نماید با این تفاوت

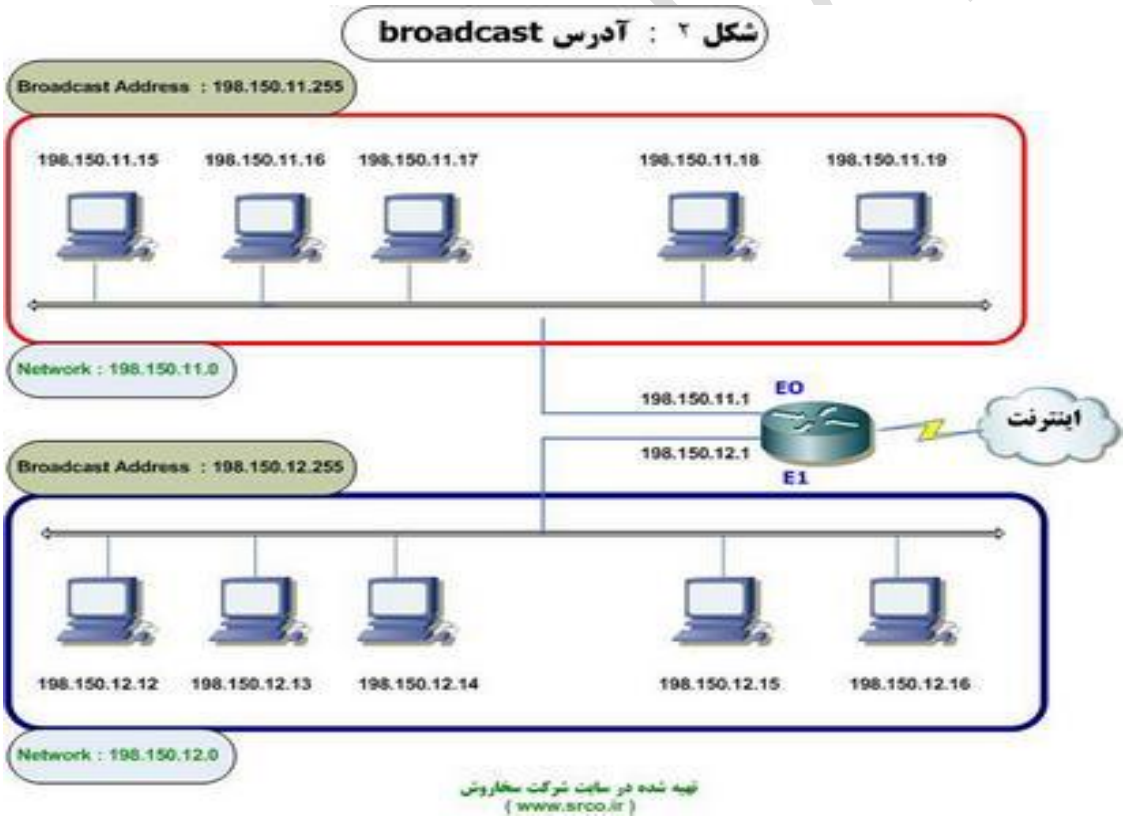
شکل ۱ : آدرس شبکه



که شماره شبکه آن 0 . 12 . 150 . 198 است .

شکل 1 : آدرس شبکه

آدرس های broadcast : از این نوع آدرس ها جهت انتشار بسته های اطلاعاتی برای تمامی دستگاه های موجود بر روی یک شبکه استفاده می گردد . در قسمت بالای شکل 2 ، برای شبکه 0 . 11 . 150 . 198 آدرس broadcast برابر 255 . 11 . 150 . 198 می باشد . داده ئی که به آدرس broadcast ارسال می گردد توسط هر یک از هاست های موجود بر روی آن شبکه (0 . 11 . 150 . 198) خوانده می شوند . شبکه محلی نشان داده شده در بخش پائین شکل (0 . 12 . 150 . 198) نیز عملکردی مشابه با شبکه نشان داده شده در بخش بالا دارد با این تفاوت که آدرس broadcast آن معادل 255 . 12 . 150 . 198 می باشد .



شکل 2 : آدرس broadcast

یک آدرس IP که تمامی بیت های مربوط به هاست آن صفر باینری در نظر گرفته شده است ، آدرس شبکه را مشخص می نماید . این آدرس رزو شده بوده و نمی توان از آن استفاده نمود .در شکل شماره 3 ، یک آدرس کلاس B که تمامی بیت های مربوط به هاست آن صفر در نظر گرفته شده است ، نشان داده شده است . آدرس 0 . 0 . 10 . 176 ، آدرس شبکه را مشخص می نماید .

شکل 3 : آدرس شبکه

در صورتی که یک آدرس شبکه کلاس A را در نظر بگیریم (در این کلاس از سه بایت برای آدرس دهی هاست و از یک بایت برای آدرس دهی شماره شبکه استفاده می گردد) ، آدرس 0 . 0 . 0 . 113 آدرس IP شبکه ای است که می تواند شامل هاستی به آدرس 3 . 2 . 1 . 113 باشد . روترها از آدرس های شبکه در زمان فورواردینگ بسته های اطلاعاتی بر روی شبکه استفاده می نمایند .

در یک آدرس شبکه کلاس B برای دو اکتت و یا بایت اولیه به صورت پیش فرض مقدار در نظر گرفته می شود . از دو بایت و یا اکتت آخر برای شماره هاست و مشخص نمودن دستگاه های متصل شده به شبکه استفاده می گردد . به این نوع آدرس ها اصطلاحا" unicast گفته می شود (uni مفهوم یک را می دهد) . یک آدرس unicast صرفا" به یک هاست بر روی یک شبکه اشاره می نماید . در مثال فوق آدرس IP: 176.10.0.0 برای آدرس شبکه رزو شده است و نمی توان آن را به

هیچیک از دستگاه های متصل شده به این شبکه نسبت داد . در چنین مواردی می توان به عنوان نمونه از آدرس 1 . 16 . 10 . 176 برای آدرس دهی یکی از هاست های موجود بر روی شبکه 0 . 0. 10 . 176 استفاده نمود . در این مثال 10 . 176 بخش مربوط به آدرس شبکه و 1 . 16 بخشی است که آدرس یک هاست را بر روی شبکه فوق مشخص می نماید .

برای ارسال داده به تمامی دستگاه های موجود بر روی یک شبکه به یک آدرس broadcast نیاز خواهیم داشت . broadcastزمانی اتفاق می افتد که یک فرستنده اقدام به ارسال داده برای تمامی دستگاه های موجود در یک شبکه می نماید. شکل 4، آدرس broadcast و شبکه یک نمونه آدرس کلاس B را نشان می دهد :

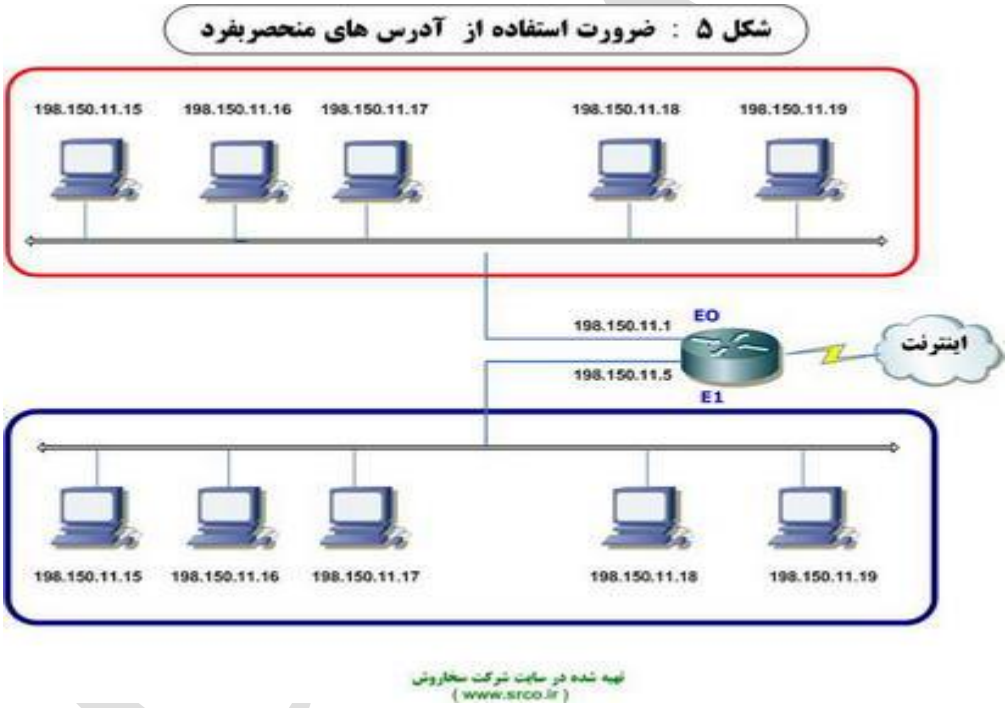
شکل 4: آدرس broadcast و شبکه یک نمونه آدرس کلاس B

آدرس broadcast شبکه فوق 255 . 255 . 10 . 176 می باشد . بسته های اطلاعاتی حاوی چنین آدرس مقصدی توسط هر یک از کامپیوترهای موجود بر روی شبکه (0 . 0 . 10 . 176) دریافت و پردازش می گردد . برای حصول اطمینان از این موضوع که سایر دستگاه های موجود در شبکه پیام broadcast را پردازش می نمایند ، فرستنده می بایست از یک آدرس IP خاص مقصد استفاده نماید تا هر یک از دستگاه های گیرنده بتوانند آن را شناسائی و پردازش نمایند . آدرس های broadcast در بخش هاست خود دارای مقدار یک می باشند (تمامی بیت های مربوط به بخش هاست در آدرس IP ، یک باینری در نظر گرفته می شود) .

بـرای شـبکه 0 . 0 . 10 . 176 کـه شـانزده بیـت آن مربـوط بـه آدرس دهـی هاسـت اسـت ، آدرس 255 . 255 . 10 . 176 به عنوان آدرس broadcast در نظر گرفته می شود .

آدرس هـــــــــــــــای عمـــــــــــــــومی و خصوصـــــــــــــــی

ثبـات و انسـجام اینترنـت بـه یکتـائی عمـومی آدرس هـای شـبکه بسـتگی دارد . همانگونـه کـه در شـکل 5 مشـاهده مـی نمائیـد ، مـدل آدرس دهـی شـبکه فـوق دارای مشـکل جـدی اسـت . هـر دو شـبکه دارای یـک آدرس شـبکه 0 . 11 . 150 . 198 مـی باشـند . زمـانی کـه داده ارسـالی بـه روتر می رسد ، وی آن را می بایست برای کدام شبکه فوروارد نماید ؟



شکل 5 : ضرورت استفاده از آدرس های منحصربفرد

تهیه شده در سایت شرکت سخاروش
(www.srco.ir)

شکل 5 : ضرورت استفاده از آدرس های منحصربفرد

مـدلی اینچنـین ، افـزایش بـار ترافیکـی شـبکه را بـه دنبـال داشـته و مـی توانـد در عمـل روتـر را بـه منظـور انجـام وظـایف خـود بـا شکسـت مواجـه نمایـد . بنـابراین ، مـی بایسـت از مکـانیزم هـای خاصـی بـه منظـور حصـول اطمینـان از یکتـائی آدرس هـا اسـتفاده گـردد . ایـن مسـئولیت در ابتـدا بـه InterNIC (برگرفتـه شـده از Internet Network Information Center)

واگذار گردید . این سازمان هم اینک غیرفعال است و مسئولیت واگذار شده به آنها توسط موسسه IANA (برگرفته شده از Internet Assigned Numbers Authority) دنبال می گردد . این سازمان با دقت مدیریت آدرس های IP را با هدف عدم تکرار در آدرس های عمومی انجام می دهد .

آدرس های IP عمومی منحصربفرد می باشند و نمی بایست ماشین های متصل شده به یک شبکه عمومی دارای آدرس های IP مشابه باشند . چراکه آدرس های IP عمومی ، سراسری و استاندارد می باشند . تمامی ماشین های متصل شده به اینترنت می بایست به این قانون وفادار و پایبند باشند . آدرس های IP عمومی را می توان از یک مرکز ارائه دهنده خدمات اینترنت (ISP) و سایر مراکز قانونی دریافت کرد .

با توجه به رشد سریع اینترنت ، تعداد آدرس های IP عمومی جوابگو نمی باشند . به همین دلیل و در جهت حل این بحران ، مدل های آدرس دهی جدیدی نظیر CIDR (برگرفته شده از classless interdomain routing) و یا IPv6 ، پیاده سازی شده است .

یکی دیگر از راه حل های پیاده سازی شده به منظور حل مشکل فوق ، استفاده از آدرس های خصوصی است . همانگونه که اشاره گردید هاست های اینترنت نیازمند یک آدرس IP منحصربفرد جهانی می باشند . شبکه های محلی که به اینترنت متصل نشده اند می توانند از هر آدرس معتبری استفاده نمایند (بشرطی که بر روی شبکه خصوصی منحصربفرد باشند) . امروزه تعداد زیادی از شبکه های خصوصی در کنار شبکه های عمومی وجود دارد که ممکن است سرانجام به اینترنت متصل شوند .

بر اساس RFC 1918 سه بلاک از آدرس های IP برای شبکه های خصوصی در نظر گرفته شده است (یک کلاس A ، یک مجموعه از آدرس های کلاس B و یک مجموعه از آدرس های کلاس C) . آدرس هائی از این نوع بر روی ستون فقرات اینترنت روت نشده و روترهای اینترنت بلافاصله آدرس های خصوصی را دورخواهند انداخت .

جدول زیر محدوده آدرس های خصوصی را نشان می دهد .

کلاس IP	محدوده آدرس های خصوصی تعریف شده
Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

آدرس های IP خصوصی

در صورتی که قصد تعریف یک اینترانت غیرعمومی ، یک آزمایشگاه تست و ... را داشته باشیم ، می توان از این نوع آدرس های خصوصی در مقابل آدرس های منحصربفرد سراسری استفاده نمود .

آدرس های IP خصوصی می توانند با آدرس های IP عمومی ترکیب گردند . برای اتصال شبکه ای که از آدرس های IPخصوصی استفاده می نماید به اینترنت ، نیازمند ترجمه آدرس های خصوصی به آدرس های عمومی می باشیم . به این فرآیند ترجمه ، NAT (برگرفته شده از Network Address Translation) گفته می شود . معمولا" روتر دستگاهی است که عملیات NAT را انجام می دهد .

سه نوع مختلف NAT وجود دارد :

NAT ایستا : در این مدل یک تناظر یک به یک بین آدرس های محلی و سراسری ایجاد می گردد . بدین ترتیب ، مجبور خواهیم بود که برای هر هاست موجود بر روی شبکه محلی دارای یک آدرس IP واقعی باشیم .

NAT پویا : در این مدل یک آدرس IP خصوصی به یک آدرس IP عمومی map می شود . فرآیند فوق بر اساس مجموعه ای از آدرس های IP عمومی ذخیره شده در یک pool انجام می گردد . بدین ترتیب لازم نخواهد بود که همانندNATایستا پیکربندی روتر برای ایجاد تناظر یک به یک به صورت دستی انجام شود . توجه داشته باشید که در این مدل می بایست به تعداد کافی از آدرس های IP واقعی استفاده گردد تا هر هاست امکان مبادله بسته های اطلاعاتی بر روی اینترنت را داشته باشد .

NAT overload : این روش متداولترین نوع پیکربندی NAT است که می توان آن را نوع خاصی از NAT پویا در نظر گرفت که در آن چندین آدرس IP خصوصی صرفا" به یک آدرس IP عمومی با استفاده از پورت های مختلف map می شوند (مدل many-

to-one) . بـه ایـن مـدل PAT (برگرفتـه شـده از port address translation) نیـز گفتـه مـی شـود . بـا اسـتفاده از PAT (و یـا NAT Overload) ، مـی تـوان هـزاران کـاربر را صرفا" با استفاده از یک آدرس IP واقعی به اینترنت متصل نمود .

CCNA: برنامه ریزی و طراحی شبکه

آنچه تاکنون گفته شده است:

بخـش اول برنامـه ریـزی و طراحـی : طراحـی یـک شـبکه محلـی سـاده بـا اسـتفاده از فنـاوری سیسکو

بخـش دوم برنامـه ریـزی و طراحـی : طراحـی یـک مـدل آدرس دهـی IP منطبـق بـر طـرح شبکه

بخـش سـوم برنامـه ریـزی و طراحـی : طراحـی یـک مـدل آدرس دهـی IP منطبـق بـر طـرح شبکه

در ایـن بخـش بـه بررسـی انتخـاب یـک پروتکـل روتینـگ ، متناسـب بـا نیازهـای شـبکه خـواهیم پرداخت .

مفـــــــــــــــــــاهیم اولیـــــــــــــــــــه روتینـــــــــــــــــــگ

به گـرفتن یـک بسـته اطلاعـاتی از دسـتگاهی و ارسـال آن از طریـق شـبکه بـرای دسـتگاه موجـود بـر روی یـک شـبکه متفـاوت ، روتینـگ گفتـه مـی شـود . روترهـا بـرای انجـام روتینـگ بـا هاسـت هـای موجـود بـر روی شـبکه هـا کـاری نداشـته و صـرفا" در خصـوص شـبکه هـا و انتخـاب بهتـرین مسـیر تصـمیم گیـری مـی گیرنـد . روترهـا بـر اسـاس آدرس منطقـی شـبکه ای کـه هاسـت مـورد نظـر بـر روی آن مسـتقر اسـت ، بسـته اطلاعـاتی را دریافـت و در ادامـه ، از آدرس سـخت افـزاری هاسـت بـرای توزیـع بسـته اطلاعـاتی از روتـر بـه مقصـد صـحیح هاسـت اسـتفاده مـی نماینـد . در روتینـگ پویـا ، پروتکـل موجـود بـر روی یـک روتـر بـا پروتکـل مشـابه اجـراء شـده بـر روی روترهـای همسـایه ارتبـاط برقـرار مـی نمایـد . در ادامـه ، هـر یـک از روترهـا اطلاعـات مربـوط بـه شبکه هائی را که نسبت بـه آنهـا آگـاهی دارنـد بـه اطـلاع هـم رسـانده تـا در جـدول روتینـگ خـود ذخیره نمایند . بدین ترتیب و بـر اسـاس فرآینـد فـوق دانـش روترهـا نسـبت بـه شـبکه هـائی کـه آنهـا

را مـی شناسـند ، بهنگـام مـی گـردد . در صـورت بـروز تغییـر در شـبکه ، پروتکـل هـای روتینـگ پویـا بطـور اتوماتیـک ایـن موضـوع را بـه اطـلاع تمـامی روترهـا مـی رسـانند . در صـورتی کـه از روتینـگ ایسـتا اسـتفاده شـده باشـد ، مـدیریت شـبکه مسـئول بهنگـام سـازی و اعمـال تمـامی تغییـرات بـه صـورت دسـتی در تمـامی روترهـا مـی باشـد . معمـولا" در شـبکه هـای بـزرگ ، ترکیبی از دو روش روتینگ ایستا و پویا استفاده می گردد.

روتینگ ایستا

در روتینـگ ایسـتا ، مسـیرها بطـور دسـتی در هـر یـک از جـداول روتینـگ اضـافه مـی گـردد . ایـن روش دارای مزایـا و محدودیت های مختص به خود است :

مزایای روتینگ ایستا

عـدم تحمیـل بـار عملیـاتی اضـافه بـر روی پردازشـگر روتـر . بـدین ترتیـب مـی تـوان از یـک روتـر بـا پردازنـده سـبک تـر استفاده نمود .

بـرای بهنگـام سـازی اطلاعـات موجـود در جـداول روتینـگ از پهنـای بانـد (ظرفیـت لینـک هـای ارتبـاطی) بـین روترهـا استفاده نخواهد شد . بدین ترتیب هزینه لینک های ارتباطی WAN کاهش می یابد .

امنیت ، چراکه صرفا" مدیر شبکه می تواند اجازه روتینگ به شبکه هائی خاص را فراهم نماید .

محدودیت های روتینگ ایستا

مـدیریت شـبکه مـی بایسـت شـناخت مناسـب و واقعـی از ارتباطـات شـبکه ای و نحـوه اتصـال روترهـا بـه یکـدیگر را بداننـد تا بتواند بر اساس آنها پیکربندی روترها را بطرز صحیح انجام دهد .

در صـورتی کـه یـک شـبکه بـه مجموعـه شـبکه هـای ارتبـاطی اضـافه گـردد ، مـدیریت شـبکه مـی بایسـت یـک مسـیر را برای آن در تمامی روترها و بطور دستی اضافه نماید .

روتینـگ ایسـتا بـرای شـبکه هـای بـزرگ مناسـب نمـی باشـد چراکـه نگهـداری اینچنـین شـبکه هـائی مسـتلزم صـرف زمـان زیادی است .

روتینگ پویا

در روتینـگ پویـا از پروتکـل هـائی بـه منظـور یـافتن و بهنگـام سـازی جـداول روتینـگ بـر روی روترهـا اسـتفاده مـی شـود . در ایـن روش عـلاوه بـر افـزایش بـار عملیـاتی پردازنـده ، درصـدی از پهنـای بانـد بـین لینـک هـای شـبکه نیـز اشـغال

خواهد شد . (افزایش cost لینک ارتباطی) .
در واقع ، یک پروتکل روتینگ مجموعه ای از قوانین لازم به منظور ارتباط یک روتر با روترهای همسایه را تعریف می نماید . IGP(برگرفته شده از gateway interior protocols) و EGP (برگرفته شده از gateway exterior protocols) دو نمونه از پروتکل های روتینگ می باشند که از آنها در ارتباطات بین شبکه ای استفاده می گردد .
از پروتکل IGP به منظور مبادله اطلاعات روتینگ با روترهای موجود در یک سیستم خود مختار و یا AS (برگرفته شده از autonomous system) استفاده می شود . یک سیستم و یا ناحیه خود مختار ، شامل مجموعه ای از شبکه هائی است که تحت یک حوزه مدیریتی می باشند . این بدان معنی است که تمامی روترهائی که اطلاعات جدول روتینگ مشابهی را به اشتراک می گذارند در یک ناحیه خود مختار مشابه قرار دارند .
از پروتکل EGP برای ارتباط بین نواحی خودمختار استفاده می شود . BGP (برگرفته شده از Border Gateway Protocol) نمونه ای از یک پروتکل EGP است .
قبل از درگیر شدن با پروتکل های روتینگ و آشنائی با نحوه عملکرد هر یک از آنها ، می بایست به چند موضوع دیگر اشاره نمائیم . آشنائی با administrative distances و انواع محتلف پروتکل های روتینگ از جمله موضوعات مهم در این رابطه است که در ادامه به بررسی آنها خواهیم پرداخت .

Administrative Distances

در زمان پیکربندی پروتکل های روتینگ ، می بایست به AD و یا distance administrative توجه خاصی داشت . از AD برای ارزش گذاری و میزان قابلیت اعتماد به اطلاعات روتینگ دریافتی یک روتر از طریق روتر همسایه اطلاق می گردد . AD ، یک عدد صحیح بین صفر تا 255 است که عدد صفر نشاندهنده اعتماد بالا و عدد 255 نشاندهنده عدم وجود ترافیک بر روی مسیر مورد نظر است .
اگر روتری دو لیست بهنگام سازی را از یک شبکه راه دور مشابه دریافت نماید ، AD اولین چیزی است که توسط وی کنترل خواهد شد . در صورتی که یکی از مسیرهای توصیه شده و یا پیشنهادی دارای AD کمتری باشد ، انتخاب و در جدول روتینگ ذخیره می گردد . در صورتی که مسیرهای پیشنهادی برای یک شبکه مشابه دارای AD یکسانی می باشند ، از متریک پروتکل روتینگ (نظیر تعداد hop و یا پهنای باند موجود بین خطوط) استفاده خواهد شد و مسیری که دارای متریک پائین تر و یا کمتری باشد در جدول روتینگ ثبت خواهد شد . در صورتی که دو مسیر پیشنهادی دارای AD و متریک یکسان باشند ، پروتکل روتینگ از load-

balance به شبکه راه دور استفاده می نماید .

جدول زیر AD پیش فرض که یک روتر سیسکو از آن به منظور اتخاذ تصمیم در خصوص انتخاب مسیر به یک شبکه راه دور استفاده می نماید را نشان می دهد :

منبع مسیر	AD پیش فرض
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP)	90
Interior Gateway Routing Protocol (IGRP)	100
Open Shortest Path First (OSPF) protocol	110
Routing Information Protocol (RIP)	120
External EIGRP	170
Unknown	255 این مسیر هرگز استفاده نشده است

جدول یک : مقادیر AD پیش فرض

در صورتی که یک شبکه مستقیما" به روتر متصل شده باشد ، روتر همواره از اینترفیس متصل شده به شبکه استفاده می نماید . در صورتی که مدیر شبکه یک مسیر ایستا را پیکربندی نماید ، روتر به این مسیر بیش از هر نوع مسیری که خود آموخته است ، اعتماد خواهد کرد . مدیران شبکه می توانند مقدار AD مسیرهای ایستا را تغییر دهند ولی به صورت پیش فرض ، AD این نوع مسیرها یک در نظر گرفته می شود . در صورتی که دارای یک مسیر ایستا ، یک مسیر توصیه شده RIP و یک مسیر پیشنهادی IGRP از یک شبکه مشابه باشیم ، روتر به صورت پیش فرض همواره از مسیر ایستا استفاده خواهد کرد مگر این که AD مسیر ایستا تغییر یابد .

انواع پروتکل های روتینگ

پروتکل های روتینگ را می توان به سه گروه عمده زیر تقسیم نمود :

Distance vector : در پروتکل های روتینگ Distance vector ، بهترین مسیر به یک شبکه راه دور بر اساس مسافت تعیین می شود . هر مرتبه که یک بسته اطلاعاتی از یک روتر عبور می یابد (که به آن hop گفته می شود) ، یک واحد به hop آن اضافه می شود . مسیری که دارای تعداد hop کمتری به

شبکه مورد نظر باشد به عنوان بهترین مسیر انتخاب خواهد شد . در واقع vector ، نشاندهنده مسیر و یا جهت رسیدن به شبکه راه دور را مشخص می نماید . پروتکل های RIP و IGRP دو نمونه متداول از پروتکل های روتینگ vector-Distance می باشند . در این پروتکل ها ، تمامی اطلاعات جداول روتینگ برای روترهای همسایه که مستقیما" متصل شده اند ، ارسال می گردد .

Link state : در پروتکل های روتینگ link-state که به آنها پروتکل های shortest-path-first نیز گفته می شود ، هر روتر سه جدول جداگانه را ایجاد می نماید . یکی از این جداول مسئولیت نگهداری اطلاعات مربوط به همسایگانی را برعهده دارد که مستقیما" به روتر متصل شده اند ، یکی دیگر حاوی توپولوژی تمامی شبکه است و در آخرین جدول ، اطلاعات جدول روتینگ ذخیره می گردد . روترهائی که با استفاده از پروتکل های link state پیکربندی شده اند نسبت به پروتکل های روتینگ Distance vector دارای اطلاعات بمراتب بیشتری نسبت به شبکه می باشند . OSPF یکی از پروتکل های متداول در این زمینه است . پروتکل های Link state اطلاعات بهنگام شامل وضعیت لینک های ارتباطی خود به سایر روترهای شبکه را ارسال می نمایند .

Hybrid : این نوع پروتکل ها از ویژگی دو پروتکل روتینگ Distance vector و Link state استفاده می نمایند . پروتکل EIGRP نمونه ای متداول در این زمینه است .

برای پیکربندی پروتکل های روتینگ در هر سازمان و یا موسسه تجاری نمی توان یک روش ثابت و خاص را پیشنهاد داد . در چنین حالاتی می بایست هر مورد را جداگانه بررسی و با توجه به شرایط موجود نسبت به انتخاب یکی از پروتکل های روتینگ اقدام نمود . در صورت آشنائی مطلوب با نحوه عملکرد پروتکل های مختلف روتینگ ، می توان در خصوص انتخاب یک پروتکل روتینگ مناسب اقدام نمود .

در بخش پنجم به بررسی پروتکل های روتینگ vector-Distance و چالش های آنها خواهیم پرداخت.

آنچه تاکنون گفته شده است:

بخش اول برنامه ریزی و طراحی : طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو

بخش دوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش سوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش چهارم برنامه ریزی و طراحی : انتخاب یک پروتکل روتینگ متناسب با نیازهای شبکه

پروتکل های روتینگ Distance-Vector نظیر RIP و IGRP

در پروتکل های روتینگ Distance vector ، بهترین مسیر به یک شبکه راه دور بر اساس مسافت تعیین می شود . هر مرتبه که یک بسته اطلاعاتی از یک روتر عبور می یابد به آن hop گفته می شود. مسیری که دارای تعداد hop کمتری به شبکه مورد نظر باشد به عنوان بهترین مسیر انتخاب خواهد شد . در واقع vector ، نشاندهنده مسیر و یا جهت رسیدن به شبکه راه دور را مشخص می نماید . پروتکل های RIP (برگرفته شده از Routing Information Protocol) و IGRP (برگرفته شده از Interior Gateway Routing Protocol) دو نمونه متداول از پروتکل های روتینگ Distance-vector می باشند.

الگوریتم های روتینگ Distance-Vector ، اطلاعات جداول روتینگ را بطور کامل برای روترهای همسایه ارسال تا آنها در ادامه اطلاعات دریافتی را با اطلاعات موجود در جداول روتینگ خود ترکیب و دانش خود را در خصوص ارتباطات بین شبکه ای کامل نمایند .به روش فوق ، روتینگ مبتنی بر شایعه (rumor) گفته می شود چراکه روتر ، بهنگام سازی جدول روتینگ خود را بر اساس اطلاعات دریافتی از روتر همسایه انجام می

دهـد. در ایـن روش روتـر بـه اطلاعـات دریـافتی در خصـوص شـبکه هـای راه دور اعتمـاد مـی نمایـد بـدون ایـن کـه خـود مسـتقیما" بـه ایـن نتـایج رسـیده باشـد . همانگونـه کـه اشـاره گردیـد ، RIP یـک نمونـه از پروتکـل هـای روتینـگ Distance-vector اسـت کـه بـرای تشـخیص بهتـرین مسیر بـه یـک شـبکه صـرفا" از تعـداد hop اسـتفاده مـی نمایـد . در صـورتی کـه RIP بـیش از یـک لینـک را بـه یـک شـبکه مشـابه و بـا تعـداد hopبرابـر پیـدا نمایـد ، بطـور اتوماتیـک از load balancing گردشـی بـر روی هـر یـک از لینـک هـا اسـتفاده مـی نمایـد . پروتکـل RIP قـادر بـه انجـام load balancing بـر روی حداکثر شش خط با cost یکسان است .

نحـوه آغـاز بـه کـار یـک پروتکـل Distance-vector بـرای آشـنائی بـا پروتکـل هـای روتینـگ Distance-vector لازم اسـت در ابتـدا بـا نحـوه عملکـرد آنهـا پـس از آغـاز فعالیـت آشـنا شـویم . در شـکل 1 ، وضـعیت جـدول روتینـگ چهـار روتـر پـس از راه انـدازی نشـان داده شـده اسـت . در جـداول فـوق صـرفا" اطلاعـات مربـوط بـه شـبکه هـائی کـه مسـتقیما" بـه هـر یـک از روترهـا متصـل شـده انـد ، ذخیـره شـده اسـت . پـس از آغـاز بـه کـار یـک پروتکـل روتینـگ Distance-Vector بـر روی هـر یـک از روترهـا ، جـداول روتینـگ بـا اسـتفاده از اطلاعـات مسیرهای جمع آوری شـده توسـط هـر یـک از روترهای همسایه بهنگام می گردند .

شکل 1 : وضعیت اولیه جداول روتینگ روترها

همانگونـه کـه در شـکل 1 مشـاهده مـی نمائیـد ، در هـر یـک از جـداول روتینـگ صـرفا" اطلاعـات شـبکه هـائی کـه مسـتقیما" بـه هـر روتـر متصـل شـده انـد ، ذخیـره شـده اسـت . هـر روتـر

اطلاعات کامل جدول روتینگ خود را برای هر یک از اینترفیس های فعال ارسال می نماید .

جدول روتینگ هر روتر شامل اطلاعاتی نظیر شماره شبکه ، اینترفیس خروجی و تعداد hop به شبکه است . بدین ترتیب ، اطلاعات جدول روتینگ کامل و هر یک از آنها دانش لازم در رابطه با تمامی شبکه های موجود در ارتباطات بین شبکه ای را کسب می نماید .

شکل 2 ، وضعیت فوق را که به آن همگرائی (converge) گفته می شود نشان می دهد . پس از همگرائی روترها ، اطلاعات موجود در جداول روتینگ بین آنها ارسال نخواهد شد .

جدول روتینگ		
172.16.10.0	F0/0	0
172.16.20.0	F0/0	1
172.16.30.0	F0/0	2
172.16.40.0	F0/0	2
172.16.50.0	F0/0	3

جدول روتینگ		
172.16.10.0	E0	0
172.16.20.0	S0	0
172.16.30.0	S0	1
172.16.40.0	S0	1
172.16.50.0	S0	2

جدول روتینگ		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0
172.16.10.0	S0	1
172.16.50.0	S1	1

جدول روتینگ		
172.16.40.0	S0	0
172.16.50.0	E0	0
172.16.10.0	S0	2
172.16.20.0	S0	1
172.16.30.0	S0	1

شکل 2 : ایجاد همگرائی در شبکه

بدیهی است مدت زمانی که یک شبکه به همگرائی می رسد بسیار حائز اهمیت بوده و کند بودن این فرآیند می تواند پیامدهای نامطلوبی را برای شبکه به دنبال داشته باشد . یکی از مسائل در ارتباط با پروتکل RIP ، کند بودن زمان همگرائی آن است .

جدول روتینگ در هر روتر اطلاعاتی راجع به شماره شبکه راه دور ، اینترفیسی که روتر از آن برای ارسال بسته های اطلاعاتی به شبکه استفاده می نماید و تعداد hop و یا متریک به شبکه را نگهداری می نماید .

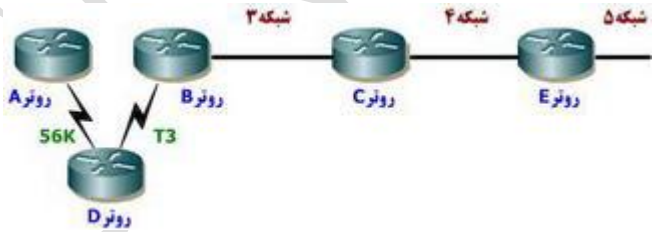
حلقه های روتینگ (Routing loops)

پروتکل های روتینگ Distance-Vector تغییرات ایجاد شده در ارتباطات بین شبکه ای را با انتشار مستمر اطلاعات بهنگام شده روتینگ به تمامی اینترفیس های فعال انجام می

دهند .

در این فرآیند تمامی اطلاعات موجود در جدول روتینگ منتشر می گردد. فرآیند فوق علاوه بر اشغال بخشی از پهنای باند لینک ارتباطی ، افزایش load پردازنده روتر را نیز به دنبال خواهد داشت . همچنین ، در صورتی که یک شبکه با مشکل مواجه شود ، سرعت کند همگرائی پروتکل های روتینگ Distance-Vector می تواند پیامدهای منفی نظیر جداول روتینگ متناقض و حلقه های روتینگ را به دنبال داشته باشد .

در پروتکل های روتینگ Distance-Vector همواره احتمال ایجاد حلقه های روتینگ وجود خواهد داشت چراکه هر روتر بطور همزمان بهنگام نمی گردد . برای آشنائی با نحوه ایجاد حلقه های روتینگ یک نمونه مثال را در شکل 3 بررسی می نمائیم . فرض کنید اینترفیس به شبکه شماره 5 با مشکل مواجه شود . تمامی روترها دانش خود را در رابطه با شبکه شماره 5 از طریق روتر E دریافت می نمایند . در جدول روتینگ روتر A یک مسیر به شبکه شماره 5 از طریق روتر B وجود دارد .



شکل 3 : حلقه های روتینگ

زمانی که شبکه شماره 5 دچار مشکل گردد ، روتر E این موضوع را به اطلاع روتر C می رساند . این کار باعث می شود که روتر C عملیات روتینگ به شبکه شماره 5 از طریق روتر E را متوقف نماید . روترهای B، A و D نسبت به بروز مشکل برای شبکه شماره 5 آگاهی نداشته و همچنان اقدام به ارسال اطلاعات بهنگام می نمایند .سرانجام روتر C اطلاعات بهنگام شده خود را ارسال و باعث می گردد که روتر B روتینگ به شبکه شماره 5 را متوقف نماید . علی رغم اطلاع به روتر B ، روترهای A وD هنوز به دلیل عدم دریافت اطلاعات بهنگام شده از این موضوع آگاهی نداشته و از نظر آنها شبکه شماره 5 همچنان از طریق روتر B با متریک شماره 3 دردسترس است .

مشکل زمانی ایجاد می شود که روتر A پیامی با این موضوع را ارسال نماید : " من همچنان این جا هستم و این لیست لینک هائی است که من آنها را می شناسم " . در پیام فوق قابلیت رسیدن به شبکه شماره 5 و نحوه دستیابی به آن تشریح شده است . بدین ترتیب روترهای B و D اخبار جالبی را دریافت می نمایند که به آنها اعلام شده است شبکه شماره 5 از طریق روتر A قابل دستیابی است . روترهای فوق نیز اقدام به ارسال اطلاعاتی مبنی بر در دسترس بودن شبکه شماره 5 می نمایند. بدین ترتیب هر بسته اطلاعاتی که مقصد آن شبکه شماره 5 باشد به روتر A و سپس به روتر B رسیده و مجددا" به روتر A برگردانده می شود .

بدین ترتیب یک "حلقه روتینگ " ایجاد می گردد که برای پیشگیری و برخورد با آنها می بایست یک فکر اساسی کرد .

شمارش نامحدود

به "حلقه های روتینگ " که در بخش قبل تشریح گردید ، " شمارش نامحدود " نیز گفته می شود و علت اصلی بروز اینچنین مسائلی ، شایعات بی‌اساس و اطلاعات نادرستی است که در شبکه توزیع شده است . بدون وجود یک سیستم کنترلی ، تعداد hop هر مرتبه که یک بسته اطلاعاتی از یک روتر عبور می یابد ، افزایش خواهد یافت . سرعت کند همگرائی شبکه در الگوریتم های روتینگ یکی از دلایل اصلی بروز اینچنین مشکلاتی در شبکه است .

برای پیشگیری از این نوع مسائل ، راه حل های مختلفی در هر یک از پروتکل های روتینگ پیاده سازی شده است . تعریف حداکثر تعداد hop ، روش route poising ، روش reverse poison و split horizon نمونه هائی در این رابطه می باشند .

حداکثر تعداد hop

یکی از روش های حل مشکل "شمارش نامحدود " ، تعریف یک حداکثر برای تعداد hop است . پروتکل های روتینگ Distance-Vector نظیر RIP صرفا" امکان افزایش تعداد hop را تا 15 فراهم می نمایند . بنابراین هر چیزی که نیازمند 16 hop باشد به منزله غیرقابل دسترس بودن تلقی می گردد . به عبارت دیگر ، در مثال

ارائه شده در بخش قبل (شکل شماره 3) ، پس از ایجاد یک حلقه با پانزده hop ، این موضوع به اثبات می رسد که شبکه شماره 5 غیرفعال است . بنابراین شمارش حداکثر تعداد hop ، باعث پیشگیری از گرفتار شدن بسته های اطلاعاتی در حلقه های تکرار می گردد . روش فوق با این که راه حلی قابل اعمال در شبکه است ولی قادر به حذف حلقه های روتینگ در شبکه نمی باشد و بسته های اطلاعاتی همچنان در حلقه های روتینگ گرفتار خواهند شد . ولی در مقابل این که بسته های اطلاعاتی بدون نظارت ، کنترل و بررسی در طول شبکه حرکت کنند ، حداکثر مسافتی را طی نموده (به عنوان نمونه تا 16 hop) و سپس از بین خواهند رفت .

Horizon Split

یکی دیگر از راه حل های برخورد با مشکل حلقه های روتینگ ، Split Horizon است . در این روش که کاهش اطلاعات نادرست و حجم عملیاتی اضافه روتینگ در یک شبکه Distance-Vector را به دنبال دارد از این اصل تبعیت می شود که اطلاعات نمی توانند در مسیری که از طریق آن دریافت شده اند مجددا" ارسال گردند . به عبارت دیگر ، پروتکل روتینگ ، اینترفیسی را که از طریق آن بسته اطلاعاتی را دریافت کرده است بخاطر سپرده و هرگز از اینترفیس فوق برای ارسال مجدد آن استفاده نخواهد کرد . بدین ترتیب و با تبعیت از اصل فوق ، روتر A از ارسال اطلاعات بهنگام شده ای که از طریق روتر B دریافت نموده است برای روتر B منع می شود .

poisoning route

یکی دیگر از روش هائی که باعث پیشگیری از اطلاعات بهنگام شده متناقض و توقف حلقه های روتینگ می گردد ، route poisoning نامیده می شود . مثلا" زمانی که شبکه شماره 5 با مشکل مواجه می گردد (شکل 3) ، روتر E یک سطر را در جدول روتینگ خود برای شبکه شماره 5 با مقدار hop شانزده (غیرقابل دسترس بودن شبکه) درج می نماید (مقدار دهی اولیه route poisoning) .
با نادرست اعلام کردن مسیر رسیدن به شبکه شماره 5 ، روتر C از بهنگام سازی اطلاعات جدول روتینگ خود مبنی بر وجود یک مسیر برای رسیدن به شبکه شماره 5 پیشگیری می نماید .زمانی که روتر C یک route poisoning را از طریق روتر Eدریافت می نماید

، یک poison reverse را برای روتر E ارسال می نماید تا این اطمینان ایجاد گردد که تمامی روترهای موجود در سگمنت اطلاعات مربوط به route poisoning را دریافت نموده اند .
route poisoning و Split Horizon یک شبکه distance-vector با قابلیت اطمینان و اعتماد بیشتر را ایجاد می نمایند که در آن از بروز حلقه های تکرار پیشگیری می گردد .

Holddown

با استفاده از holddown پیشگیری لازم در خصوص بهنگام سازی اطلاعات یک مسیر بی ثبات ، انجام می شود . این وضعیت معمولا" بر روی یک لینک سریال اتفاق می افتد که در یک لحظه برقرار و در لحظه ای دیگر غیرفعال می گردد (flapping) . در صورت عدم استفاده از روشی جهت تثبیت این وضعیت ، شبکه هرگز همگراء نشده و اینترفیسی که دائما" up و downمی گردد می تواند تمامی شبکه را با مشکل مواجه سازد .
با استفاده از holddown از ثبت مسیرهائی که وضعیت آنها با سرعت زیاد تغییر پیدا می نماید ، پیشگیری بعمل آمده و به آنها یک فرصت زمانی داده می شود تا وضعیت پایداری پیدا نمایند . بدین ترتیب ، به روترها اعلام می شود که برای یک بازه زمانی خاص هر گونه تغییراتی که بر روی مسیرهای حذف شده اخیر تاثیر می گذارد را محدود نمایند . با این کار از درج مسیرهای بی ثبات در سایر جداول روتینگ پیشگیری بعمل می آید .
زمانی که یک روتر اطلاعات بهنگام شده ای را از طریق یکی از همسایگان مبنی بر غیرقابل دسترس بودن یک شبکه دریافت می نماید (شبکه ای که تا پیش از این فعال بوده است) ، تایمر holddown آغاز به کار می کند . در صورتی که اطلاعات بهنگام شده جدیدی از یک همسایه دریافت شود که دارای متریک بهتری نسبت به وضعیت اولیه موجود در جدول روتینگ باشد ، holddown برداشته شده و داده عبور داده می شود ولی اگر اطلاعات بهنگام شده ای از یک روتر همسایه دریافت گردد (قبل از اتمام مدت زمان تایمر holddown) ، که دارای متریک برابر و یا کمتر از مسیر قبلی باشد ، از اطلاعات

جدید بهنگام صرفنظر و تایمر به فعالیت خود ادامه خواهد داد . بدین ترتیب زمان بیشتری برای ایجاد ثبات در شبکه قبل از آغاز فرآیند همگرائی آن فراهم می گردد . holddown از فرآیند بهنگام سازی مبتنی بر trigger استفاده می نماید . در این فرآیند تایمر reset می گردد تا به روترهای همسایه اطلاع داده شود یک تغییر در شبکه اتفاق افتاده است . برخلاف پیام های بهنگام از روترهای همسایه ، در این نوع بهنگام سازی (مبتنی بر trigger) یک جدول روتینگ جدید ایجاد و بلافاصله برای روترهای همسایه ارسال می گردد چراکه یک تغییر در ارتباطات بین شبکه ای تشخیص داده شده است . در بخش پنجم به بررسی پروتکل RIP ، IGRP و پروتکل های ترکیبی خواهیم پرداخت .

CCNA: برنامه ریزی و طراحی شبکه

آنچه تاکنون گفته شده است :

بخش اول برنامه ریزی و طراحی : طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو

بخش دوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش سوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش چهارم برنامه ریزی و طراحی : انتخاب یک پروتکل روتینگ متناسب با نیازهای شبکه

بخش پنجم برنامه ریزی و طراحی :مفاهیم اولیه پروتکل های روتینگ Distance-vector

در این بخش به بررسی پروتکل RIP ، IGRP و پروتکل های ترکیبی خواهیم پرداخت .

پروتکل RIP

RIP (برگرفته شده از Routing Information Protocol) به معنی واقعی یک

پروتکل distance-vector است . پروتکل فوق در هر 30 ثانیه تمام اطلاعات موجود در جدول روتینگ را برای تمامی اینترفیس های فعال ارسال می نماید . RIP صرفا" از تعدادhop برای تعیین بهترین مسیر به شبکه راه دور استفاده می نماید .حداکثر تعداد hop می تواند عدد 15 را داشته باشد و نسبت دهی عددی بالاتر از 15 به منزله غیرقابل دسترس بودن شبکه است.

RIP در شبکه های کوچک به خوبی کار می کند ولی برای شبکه های بزرگ که دارای لینک های ارتباطی WAN (برگرفته شده از wide area network) کند و تعداد بسیار زیادی روتر هستند مناسب نمی باشد.

در نسخه شماره یک RIP صرفا" از روتینگ classful استفاده می گردد . این بدان معنی است که تمامی دستگاه های موجود در شبکه می بایست از subnet mask مشابهی استفاده نمایند . محدودیت فوق به دلیل ماهیت ارسال اطلاعات بهنگام می باشد. در نسخه شماره یک RIP ، اطلاعات بهنگام ارسالی شامل اطلاعات subnet mask نمی باشند .

در RIP نسخه دو ، ویژگی جدیدی به نام روتینگ Prefix ارائه شده است که به کمک آن امکان ارسال اطلاعات subnet mask به همراه مسیرهای بهنگام شده فراهم می گردد . به این نوع روتینگ ، اصطلاحا" روتینگ classless گفته می شود .

RIP از سه نوع تایمر مختلف برای تنظیم کارآئی خود استفاده می نماید .

Route update timer ، فاصله زمانی ارسال یک نسخه کامل از اطلاعات بهنگام روتینگ را مشخص می نماید . در بازه زمانی فوق ، روتر یک نسخه کامل از اطلاعات موجود در جدول روتینگ خود را برای تمامی همسایگان ارسال می نماید . این زمان معمولا" 30 ثانیه در نظر گرفته می شود .

Route invalid timer ، مدت زمانی را مشخص می نماید که پس از سپری شدن آن ، روتر به این نتیجه خواهید رسید که یک مسیر غیرمعتبر است . این زمان معمولا" 180 ثانیه در نظر گرفته می شود و اگر یک روتر در بازه زمانی فوق هیچگونه اطلاعات جدیدی را در خصوص یک مسیر خاص دریافت ننماید ، آن مسیر را غیرمعتبر می نماید . در صورت تحقق

چنین شرایطی ، روتر اقدام به ارسال اطلاعات بهنگام برای تمامی همسایگان خود می نماید تا به آنها بگوید که مسیر غیرمعتبر است .

Route flush timer ، مدت زمان بین غیرمعتبر اعلام شدن یک مسیر و حذف آن از جدول روتینگ را مشخص می نماید . این زمان معمولا" 240 ثانیه در نظر گرفته می شود . قبل از این که یک مسیر از جدول روتینگ حذف گردد ، روتر این موضوع را به اطلاع همسایگان خود می رساند . مقدار Route invalid timer می بایست کمتر از route flush timer باشد تا روتر زمان کافی جهت اطلاع به همسایگان خود را قبل از بهنگام سازی جدول در اختیار داشته باشد .

پروتکل IGRP

IGRP (برگرفته شده از Interior Gateway Routing Protocol) یکی از پروتکل روتینگ distance-vector طراحی شده توسط شرکت سیسکو است . این بدان معنی است در صورت استفاده از پروتکل فوق در یک شبکه ، می بایست تمامی روترها از نوع سیسکو باشند . شرکت سیسکو هدف از ایجاد پروتکل IGRP را غلبه بر برخی محدودیت های پروتکل RIP عنوان کرده است .

IGRP می تواند حداکثر دارای 255 ، hop باشد که مقدار پیش فرض آن 100 در نظر گرفته می شود . این وضعیت در شبکه های بزرگ بسیار مفید است و مشکل داشتن حداکثر 15 hop در یک شبکه مبتنی بر پروتکل RIP را برطرف نماید .

IGRP از یک روش متفاوت نسبت به RIP جهت محاسبه متریک استفاده می کند . در این پروتکل ، بطور پیش فرض از پهنای باند و تاخیر خط به عنوان شاخص هائی جهت تعیین بهترین مسیر استفاده می گردد . به فرآیند فوق متریک ترکیبی(metric composite) گفته می شود . همچنین برای محاسبه متریک از شاخص هائی دیگر نظیر قابلیت اعتماد ، میزان load وMTU (برگرفته شده از maximum transmission unit) استفاده می گردد (از شاخص های اشاره شده بطور پیش فرض در محاسبه متریک استفاده نمی گردد) .

پروتکل IGRP با RIP دارای تفاوت های عمده ای است که به برخی از آنها اشاره می گردد :

امکان استفاده از IGRP در شبکه های بزرگ

IGRP برای فعال شدن از یک number AS (برگرفته شده از autonomous system) استفاده می نماید .

IGRP در هر 90 ثانیه یک مرتبه بهنگام سازی جدول روتینگ را بطور کامل انجام می دهد .

IGRP از پهنای باند و تاخیر خط به عنوان یک متریک استفاده می نماید .

برای کنترل کارآئی ، پروتکل IGRP از تایمرهای مختلف زیر با مقادیر پیش فرض استفاده می نماید :

Update timers ، فرکانس ارسال پیام های بهنگام روتینگ را مشخص می نماید . مقدار پیش فرض 90 ثانیه در نظر گرفته شده است .

Invalid timers ، مدت زمانی را که یک روتر می بایست منتظر بماند قبل از این که یک مسیر نادرست را به دیگران اعلام نماید (در صورتی که در بازه زمانی مورد نظر یک بهنگام جدید دریافت نگردد) ، مشخص می نماید . مقدار پیش فرض سه برابر زمان Update timer است .

Holddown timers ، مدت زمان holddown را مشخص می نماید . مقدار پیش فرض سه برابر زمان timer Update به اضافه 10 ثانیه در نظر گرفته شده است .

Flush timers، مشخص می نماید که چه مدت زمانی می بایست سپری شود قبل از این که بتوان یک مسیر را از جدول روتینگ حذف کرد . مقدار پیش فرض هفت برابر زمان Update timer در نظر گرفته می شود . در صورتی که مقدار timer Update برابر با 90 ثانیه در نظر گرفته شود ، 360 ثانیه طول خواهد کشید تا بتوان یک مسیر را از جدول روتینگ حذف کرد .

پروتکل های روتینگ ترکیبی و یا EIGRP

EIGRP (برگرفته شده از Enhanced IGRP) یک پروتکل distance-

vector و classless است که امکانات بیشتری را نسبت به IGRP ارائه می نماید . همانند IGRP ، پروتکل EIGRP از مفهوم یک ناحیه خودمختار برای تشریح مجموعه ای از روترهای همجوار که پروتکل های روتینگ مشابهی را اجراء و اطلاعات روتینگ را به اشتراک می گذارند ، استفاده می نماید . برخلاف IGRP ، پروتکل EIGRP در مسیرهای بهنگام خود از Subnet mask استفاده می نماید . همانگونه که اطلاع دارید ، ارائه اطلاعات subnet امکان استفاده از VLSM (برگرفته شد ه از Variable Length Subnet Masking) و خلاصه سازی را در زمان طراحی شبکه فر اهم می نماید . در برخی موارد به پروتکل EIGRP به عنوان یک پروتکل ترکیبی روتینگ نیز اشاره می شود چراکه دارای ویژگی هائی از پروتکل های distance-vector و link-state می باشد . مثلا" EIGRP اقدام به ارسال بسته های اطلاعاتی link-state همانندOSPF (برگرفته شده از Open Shortest Path First) نمی کند . در مقابل ، EIGRP داده بهنگام distance-vector شامل اطلاعاتی در رابطه با شبکه ها به اضافه هزینه رسیدن به آنها را از دیدگاه روتر پیشنهاد دهنده ارسال می نماید . همچنین ، پروتکل EIGRP دارای خصایص Link-state است . یکسان سازی جداول روتینگ بین همسایگان در زمان راه اندازی و ارسال اطلاعات بهنگام جدید و خاص در زمان بروز تغییرات در توپولوژی شبکه ، نمونه ای در این زمینه می باشد . وجود برخی ویژگی های قدرتمند در پروتکل EIGRP آن را از IGRP و سایر پروتکل های روتینگ کاملا" متمایز می نماید .

حمایت از IP ، IPX و AppelTalk از طریق PDM (برگرفته شده از Protocol-Dependent Modules)

ارتباط از طریق RTP (برگرفته شده از Reliable Transport Protocol)

انتخاب بهترین مسیر از طریق DUAL (برگرفته شده از diffusing update algorithm)

حمایت از چندین سیستم خودمختار (AS)

حمایت از خلاصه سازی و VLSM (برگرفته شده از Variable Length Subnet Masking)

CCNA: برنامه ریزی و طراحی شبکه

آنچه تاکنون گفته شده است :

بخش اول برنامه ریزی و طراحی : طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو

بخش دوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش سوم برنامه ریزی و طراحی : طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

بخش چهارم برنامه ریزی و طراحی : انتخاب یک پروتکل روتینگ متناسب با نیازهای شبکه

بخش پنجم برنامه ریزی و طراحی :مفاهیم اولیه پروتکل های روتینگ Distance-vector

بخش ششم برنامه ریزی و طراحی :بررسی پروتکل RIP ، IGRP و پروتکل های ترکیبی

پروتکل EIGRP دارای مجموعه پتانسیل هائی است که آن را با سایر پروتکل های روتینگ نظیر IGRP کاملا" متمایز می نماید . برخی از این ویژگی ها عبارتند از :

حمایت از IP ، IPX و AppelTalk از طریق PDM (برگرفته شده از Protocol-Dependent Modules)

تشخیص کارآمد همسایگان

ارتباط از طریق RTP (برگرفته شده از Reliable Transport Protocol)

انتخاب بهترین مسیر از طریق DUAL (برگرفته شده از diffusing update algorithm)

حمایت از چندین سیستم خودمختار (AS)

حمایت از خلاصه سازی و VLSM (برگرفته شده از Variable Length Subnet Masking)

در ادامه به بررسی هر یک از ویژگی های فوق خواهیم پرداخت.

ماژول های وابسته به پروتکل (Protocol-Dependent Modules)

یکی از ویژگی های جالب پروتکل EIGRP ، حمایت آن از روتینگ چندین پروتکل لایه شبکه نظیر IPX ، IP و AppelTalk است . پروتکل IS-IS (برگرفته شده از Intermediate System-to-Intermediate System) تنها پروتکل روتینگ نزدیک به پروتکل EIGRPاست که از چندین پروتکل لایه شبکه حمایت می نماید . با این تفاوت که پروتکل فوق صرفا" از IP و CLNS (برگرفته شده از Connectionless Network Service) حمایت می نماید .

EIGRP با بکارگیری پتانسیلی با نام PDM (برگرفته شده از protocol-dependent modules) از پروتکل های مختلف لایه شبکه حمایت می نماید . هر PDM پروتکل EIGRP ، مجموعه ای جداگانه از جداول حاوی اطلاعات روتینگ را نگهداری می نماید که در ارتباط با یک پروتکل خاص بکارگرفته می شوند . این بدان معنی است که EIGRP برای هر یک از پروتکل ها یک جدول جداگانه را نگهداری می نماید (نظیر جداول IP/EIGRP ، IPX/EIGRP و AppelTalk/EIGRP) .

تشخیص همسایگان

قبل از این که روترهای EIGRP تصمیم به مبادله مسیرها با یکدیگر نمایند ، می بایست همسایگان خود را شناسائی نمایند . برای ایجاد رابطه همسایگی می بایست شرایط زیر وجود داشته باشد :

دریافت Hello و یا ACK (برگرفته شده از acknowledgment)

تطبیق شماره سیستم خودمختار (AS)

متریک یکسان

پروتکل های Link-state علاقه مند به استفاده از پیام های Hello برای ایجاد رابطه همسایگی می باشند چراکه آنها معمولا" اقدام به ارسال اطلاعات بهنگام مسیرها بطور ادواری نمی نمایند و می بایست با بکارگیری مکانیزم هائی خاص قادر به تشخیص همسایگان خود بطور پویا (تشخیص یک همسایه جدید و یا خروج از لیست همسایگان) باشند . برای برقراری رابطه همسایگی ، روترهای EIGRP می بایست بطور پیوسته پیام هائی موسوم به Hello را از همسایگان خود دریافت نمایند .

روترهای EIGRP که به نواحی خودمختار (AS) مختلفی وابسته می باشند بطور اتوماتیک اطلاعات روتینگ را بین خود به اشتراک نمی گذارند و به عنوان همسایه تلقی نمی گردند . سیاست فوق مزایای متعددی را به دنبال خواهد داشت (خصوصا" زمانی که از پروتکل EIGRP در شبکه های بزرگ استفاده می گردد) . در چنین مواردی ، حجم اطلاعات روتینگ منتشر شده در بین یک ناحیه خود مختار خاص کاهش پیدا می نماید . تنها نکته قابل تامل در این رابطه ، لزوم توزیع مجدد بین نواحی خود مختار بطور دستی است .

زمانی که EIGRP یک همسایه جدید را تشخیص می دهد و قصد ایجاد یک رابطه همسایگی با آن را از طریق مبادله پیام هایHello دارد ، تمامی اطلاعات روتینگ خود را در اختیار آن قرار می دهد (تنها حالتی که تمامی اطلاعات جدول روتینگ ارسال می گردد) . زمانی که این اتفاق می افتد ، هر یک از آنها تمامی جداول روتینگ خود را برای دیگری منتشر می نماید . پس از این که هر یک از آنها از مسیرهای همسایه خود آگاهی یافت ، صرفا" تغییرات در جدول روتینگ بین آنها مبادله می گردد .

زمانی که روترهای EIGRP اطلاعات بهنگام را از همسایگان خود دریافت می نمایند ، آنها را در یک جدول توپولوژی محلی ذخیره می نمایند . این جدول حاوی تمامی مسیرهای شناخته شده از تمامی همسایگان شناخته شده است و از آن به عنوان مواد خام انتخاب بهترین مسیر و استقرار آن در جدول روتینگ استفاده می گردد .

ارتباط از طریق RTP

EIGRP از یک پروتکل اختصاصی با نام RTP (برگرفته شده از Reliable

Transport Protocol) به منظور مدیریت مبادله پیام بین روترهائی که بر اساس EIGRP با یکدیگر گفتگو می کنند ، استفاده می نماید .
یکی از ویژگی های مهم پروتکل RTP ، قابلیت اطمینان به آن است . شرکت سیسکو مکانیزمی را طراحی نموده است که به کمک آن بتواند پیام های multicast و unicast بهنگام سازی را با سرعت توزیع و وضعیت دریافت داده توسط گیرنده را پیگیری نماید .
زمانی که EIGRP ترافیک multicast را ارسال می نماید از آدرس 0. 0. 0. 224 کلاس D استفاده می نماید . همانگونه که اشاره گردید هر روتر EIGRP نسبت به همسایگان خود آگاهی داشته و برای هر پیام multicast که ارسال می نماید ، لیستی از همسایگان را که به آن پاسخ می دهند نگهداری می نماید . در صورتی که EIGRP پاسخی را از یک همسایه دریافت نکند ، در تلاشی مجدد برای آن یک پیام unicast را ارسال می نماید . در صورتی که پس از 16 مرتبه تلاش پاسخی از همسایه دریافت نگردد ، این فرضیه به اثبات می رسد که همسایه از بین رفته است . به فرآیند فوق reliable multicast گفته می شود .
روترها برای رهگیری اطلاعات ارسالی خود به آنها یک شماره ترتیب را نسبت می دهند . با استفاده از روش فوق ، امکان تشخیص اطلاعات قدیمی ، تکراری و یا خارج از ترتیب فراهم می گردد .
قابلیت انجام این گونه عملیات بسیار حائز اهمیت است چراکه EIGRP یک پروتکل آرام است که در زمان راه اندازی، بانک های اطلاعاتی روتینگ خود را با همسایگان مبادله و در ادامه و به منظور حفظ سازگاری بانک اطلاعاتی در طول زمان ، صرفا" اقدام به مبادله تغییرات می نماید . از دست دادن دائمی هر گونه بسته اطلاعاتی و یا پردازش بر روی بسته های اطلاعاتی بیهوده می تواند خرابی بانک اطلاعاتی روتینگ را به دنبال داشته باشد .
استفاده از الگوریتم DUAL برای انتخاب بهترین مسیر EIGRP از الگوریتم DUAL (برگرفته شده از diffusing update algorithm

) برای انتخاب و نگهداری بهترین مسیر به هر شبکه راه دور استفاده می نماید . الگوریتم فوق دارای ویژگی های زیر است :

backup از مسیرها

حمایت از VLSMs

بازیافت پویای مسیر

درخواست از همسایگان برای گزینش مسیرهای ناشناخته دیگر

ارسال درخواست برای یک مسیر جایگزین در صورت عدم یافتن مسیر

EIGRP با بکارگیری الگوریتم DUAL توانسته است سریعترین زمان همگرائی در بین سایر پروتکل های روتینگ را دارا باشد . سرعت همگرائی بالای EIGRP به دو عامل اساسی زیر بستگی دارد:

عامل اول : روترهای EIGRP یک نسخه از تمامی مسیرهای همسایگان خود را نگهداری می نمایند تا بتوانند از آن برای محاسبه cost هر شبکه راه دور استفاده نمایند . در صورت بروز مشکل برای بهترین مسیر ،محتویات جدول توپولوژی به منظور انتخاب بهترین مسیر جایگرین بررسی می گردد .

عامل دوم : در صورتی که یک مسیر جایگزین مناسب در جدول محلی توپولوژی وجود نداشته باشد ، روترهایEIGRP به سرعت از همسایگان خود برای یافتن یک مسیر مناسب درخواست کمک می نمایند .

همانگونه که اشاره گردید ، ایده ارسال پیام های Hello ، تشخیص سریع همسایگان جدید و همسایگانی خارج شده از لیست همسایگان است .

RTP ، مکانیزمی مطمئن برای حمل پیام ها را ارائه می نماید و DUAL با استناد به مکانیزم فوق ، مسئولیت انتخاب و نگهداری اطلاعات در رابطه با بهترین مسیرها را برعهده دارد .

چندین ناحیه خودمختار

EIGRP از شماره نواحی خود مختار (ASNs) برای شناسائی مجموعه ای از روترهائی که اطلاعات روتینگ را بین خود به اشتراک می گذارند ، استفاده می نماید . صرفا"

روترهائی که دارای ASN (برگرفته شده از numbers autonomous system) مشابه می باشند ، مسیرها را به اشتراک می گذارند . با استفاده از رویکرد فوق در شبکه های بزرگ ، به معظل جداول مسیر و توپولوژی پیچیده که کاهش سرعت همگرائی شبکه را به دنبال خواهد داشت، خاتمه داده می شود .

با تقسیم شبکه به چندین ناحیه خودمختار جداگانه EIGRP ، درصد بسیار زیادی از تبعات منفی مدیریت و نگهداری یک شبکه بزرگ کاهش می یابد. هر ناحیه خود مختار شامل مجموعه ای از روترهای همجوار است که اطلاعات مسیرها را بین خود به اشتراک گذاشته و با توزیع مجدد آنها زمنیه استفاده از اطلاعات فوق بین نواحی خودمختار جداگانه نیز فراهم می گردد .

استفاده از توزیع مجدد در EIGRP ، بیانگر یک ویژگی جالب دیگر از این پروتکل است . معمولا" AD (برگرفته شده از administrative distance) مسیرهای EIGRP معادل 90 در نظر گرفته می شود . این موضوع صرفا" برای مسیرهائی که از آنها به عنوان مسیرهای داخلی EIGRP نام برده می شود صادق می باشد . این گونه مسیرها ، مسیرهائی هستند که از درون یک ناحیه خودمختار خاص و توسط روترهای EIGRP که جملگی عضو یک سیستم خود مختار مشابه می باشند، سرچشمه می گیرند .

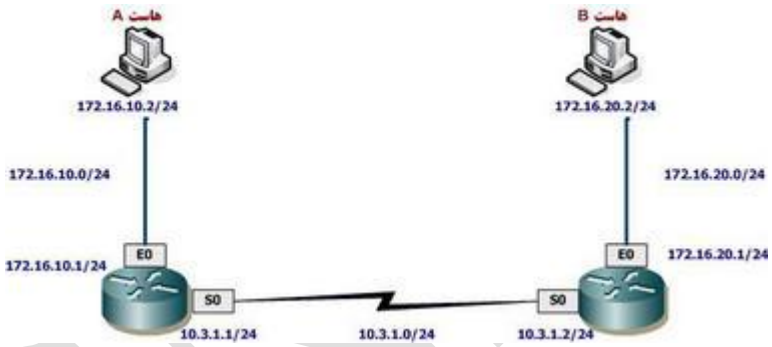
مسیرهای خارجی EIGRP ، نوع دیگری از مسیرها می باشند که دارای AD معادل 170 می باشند که خیلی هم خوب نیست . این گونه مسیرها ، در جداول مسیر EIGRP بطور دستی و یا توزیع مجدد اتوماتیک قرار می گیرند و شبکه هائی را مشخص می نمایند که در خارج از سیستم خود مختار EIGRP می باشند .

حمایت از VLSMs و خلاصه سازی

EIGRP به عنوان یکی از پروتکل های روتینگ classless ، از VLSMs حمایت می نماید . حمایت از ویژگی VLSM بسیار حائز اهمیت است چراکه با استفاده از پتانسیل فوق امکان نگهداری فضای آدرس دهی از طریق subnet mask فراهم می گردد (نظیر استفاده از 30 بیت subnet mask برای شبکه های point-to-point) .

با توجه به این که subnet mask به همراه هر مسیر بهنگام نیز ارسال می گردد ، این امکان برای پروتکل EIGRP فراهم می گردد که از زیر شبکه های ناپیوسته نیز حمایت نماید . بدین ترتیب ، طراحان شبکه های کامپیوتری در زمان طراحی یک شبکهIP دارای انعطاف بیشتری می باشند .

یک شبکه ناپیوسته دارای دو شبکه classful است که از طریق یک شبکه با کلاس متفاوت به یکدیگر متصل شده اند . شکل 1 ، یک شبکه ناپیوسته را نشان می دهد .



شکل 1 : شبکه ناپیوسته

در شکل فوق دو زیر شبکه به آدرس های 0 . 10 . 16 . 172 و 0 . 20 . 16 . 172 از طریق یک شبکه 0 . 1 . 3 . 10 به یکدیگر متصل شده اند . هر روتر این گونه فکر می کند که دارای تمامی شبکه کلاس B با آدرس 0 . 0. 16 . 172 و به صورت پیش فرض است .

EIGRP ، همچنین از ایجاد دستی خلاصه ها بر روی هر روتر EIGRP حمایت می نماید . این کار کاهش اندازه جدول مسیر را به دنبال خواهد داشت . EIGRP ، بطور اتوماتیک شبکه ها را در محدوده های classful مربوطه خلاصه می نماید .

آنچه تاکنون گفته شده است :

بخش اول	برنامه ریزی و طراحی :	طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو
بخش دوم	برنامه ریزی و طراحی :	طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه
بخش سوم	برنامه ریزی و طراحی :	طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه
بخش چهارم	برنامه ریزی و طراحی :	انتخاب یک پروتکل روتینگ متناسب با نیازهای شبکه
بخش پنجم	برنامه ریزی و طراحی :	مفاهیم اولیه پروتکل های روتینگ Distance-vector
بخش ششم	برنامه ریزی و طراحی :	بررسی پروتکل RIP، IGRP و پروتکل های ترکیبی
بخش هفتم	برنامه ریزی و طراحی :	بررسی برخی از ویژگی های پروتکل EIGRP

در این بخش به بررسی پروتکل های روتینگ link state نظیر OSPF خواهیم پرداخت .

پروتکل های روتینگ link state نظیر OSPF

در پروتکل های link-state که به آنها پروتکل های shortest path first نیز گفته می شود ، هر روتر سه جدول جداگانه را ایجاد می نماید . یکی از این جداول وضعیت همسایگانی را که مستقیما" به آن متصل شده اند در خود نگهداری می نماید . در جدول دیگر ، توپولوژی تمامی شبکه نگهداری می گردد و از جدول سوم برای نگهداری اطلاعات روتینگ استفاده می شود.

روترهای link-state نسبت به پروتکل های روتینگ distance-vector دارای اطلاعات بیشتری در ارتباط با شبکه و ارتباطات بین شبکه ای می باشند. پروتکل های link-state اطلاعات بهنگام خود را برای سایر روترهای موجود در شبکه ارسال می نمایند (وضعیت لینک).

OSPF (برگرفته شده از Open Shortest Path First) یک پروتکل روتینگ IP است که دارای تمامی ویژگی های یک پروتکل link-state است .پروتکل فوق ، یک پروتکل روتینگ استاندارد باز است که توسط مجموعه ای از تولیدکنندگان شبکه از جمله شرکت سیسکو ایجاد شده است . در صورتی که در یک شبکه از روترهائی استفاده می گردد که تمامی آنها متعلق به شرکت سیسکو نمی باشند ، نمی توان از پروتکل EIGRP استفاده کرد . در چنین مواردی می توان از گزینه هائی دیگر نظیر RIP ، RIPv2 و یا OSPF استفاده نمود . در صورتی که ابعاد یک شبکه بسیار بزرک باشد ، تنها گزینه موجود پروتکل OSPF و یا استفاده از route redistribution است (یک سرویس ترجمه بین پروتکل های روتینگ) .

OSPF ، با استفاده از الگوریتم Dijkstra کار می کند . در ابتدا ، اولین درخت کوتاهترین مسیر ایجاد می گردد و در ادامه جدول روتینگ از طریق بهترین مسیرها توزیع می گردد . این پروتکل دارای سرعت همگرائی بالائی است (شاید به اندازه سرعت همگرائی EIGRP نباشد) و از چندین مسیر با cost یکسان به مقصد مشابه حمایت می نماید . برخلاف EIGRP ، پروتکل OSPF صرفا" از روتینگ IP حمایت می نماید .

در بحث مربوط به پروتکل های link-state ، اکثر علاقه مندان به دریافت مدرک CCNA ، در آغاز با پروتکل OSPF آشنا می شوند . بدین منظور این پروتکل با پروتکل های سنتی distance-vector نظیر RIPv1 مقایسه و ماحصل آن در جدول 1 نشان داده شده است .

OSPF	RIPv1	ویژگی
Link-state	Distance-vector	نوع پروتکل
بلی	خیر	حمایت از classless
بلی	خیر	حمایت از VLSM
خیر	بلی	خلاصه سازی اتوماتیک
بلی	خیر	خلاصه سازی دستی
ارسال multicast در صورت بروز تغییرات	ارسال متناوب broadcast	انتشار مسیر
پهنای باند	hops	متریک مسیر
ندارد	15	محدودیت تعداد hop
سریع	کند	همگرائی
بلی	خیر	Peer authentication
بلی (استفاده از نواحی)	خیر (فقط flat)	شبکه سلسله مراتبی
Dijkstra	Bellman-Ford	الگوریتم محاسبه مسیر

جدول 1 : مقایسه پروتکل های RIPV1 و OSPF

OSPF دارای ویژگی های متعددی است که صرفا" تعداد اندکی از آنها در جدول 1 نشان داده شده است . تمامی شواهد موجود نشان دهنده این واقعیت است که پروتکل OSPF یک پروتکل سریع ، قابل توسعه و مستحکم است که می توان از آن در هزاران شبکه عملیاتی استفاده کرد .

OSPF بگونه ای طراحی شده است که بتواند از شبکه های سلسله مراتبی حمایت نماید . با بکارگیری ویژگی فوق می توان ارتباطات بین شبکه ای بزرگ را به چندین شبکه کوچکتر که به آنها ناحیه گفته می شود ، تقسیم نمود . بکارگیری پتانسیل فوق مزایای متعددی را به دنبال خواهد داشت :

کاهش اضافه عملیات روتینگ

افزایش سرعت همگرائی

محدود کردن بی ثباتی شبکه در یک ناحیه و عدم اشاعه آن به سایر نواحی شبکه

OSPF، درون یک ناحیه خودمختار (AS) اجراء می شود ولی این امکان نیز وجود دارد که از آن برای اتصال چندین ناحیه خودمختار به یکدیگر استفاده کرد. به روترهائی که نواحی خود مختار را به یکدیگر متصل می نمایند، ASBR (برگرفته شده از autonomous system boundary router) گفته می شود. فلسفه ایجاد نواحی خود مختار، کاهش زمان بهنگام سازی و عدم انتشار مشکلات ایجاد شده در یک ناحیه خاص به سایر نواحی شبکه است.

CCNA: برنامه ریزی و طراحی شبکه

آنچه تاکنون گفته شده است:

بخش اول	برنامه ریزی و طراحی :	طراحی یک شبکه محلی ساده با استفاده از فناوری سیسکو
بخش دوم	برنامه ریزی و طراحی :	طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه
بخش سوم	برنامه ریزی و طراحی :	طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه
بخش چهارم	برنامه ریزی و طراحی :	انتخاب یک پروتکل روتینگ متناسب با نیازهای شبکه
بخش پنجم	برنامه ریزی و طراحی :	مفاهیم اولیه پروتکل های روتینگ Distance-vector
بخش ششم	برنامه ریزی و طراحی :	بررسی پروتکل RIP، IGRP و پروتکل های ترکیبی
بخش هفتم	برنامه ریزی و طراحی :	بررسی برخی از ویژگی های پروتکل EIGRP
بخش هشتم	برنامه ریزی و:	بررسی پروتکل های روتینگ link state نظیر OSPF

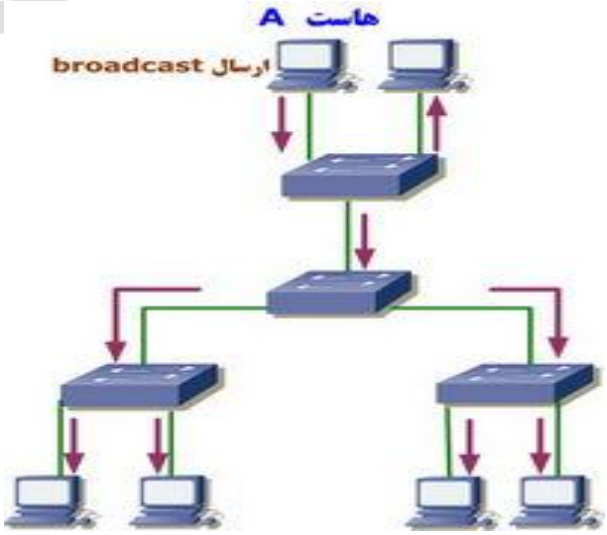
طراحی

در این بخش با نحوه طراحی یک شبکه با استفاده از فناوری های سیسکو با تاکید بر روی شبکه های محلی مجازی (VLANs) آشنا خواهیم شد . در ارتباطات بین شبکه ای مجموعه ای از شبکه ها به یکدیگر متصل می گردند . یکی از روش های ساده ایجاد یک ارتباط بین شبکه ای ، اتصال چندین شبکه محلی مجازی (VLANs) با یکدیگر است . در ادامه با روش انجام این کار بیشتر آشنا می شویم .

مبانی شبکه های محلی مجازی

شبکه های مبتنی بر سوئیچ های لایه دو عموما" به عنوان یک شبکه flat از منظر یک broadcast طراحی می گردند.

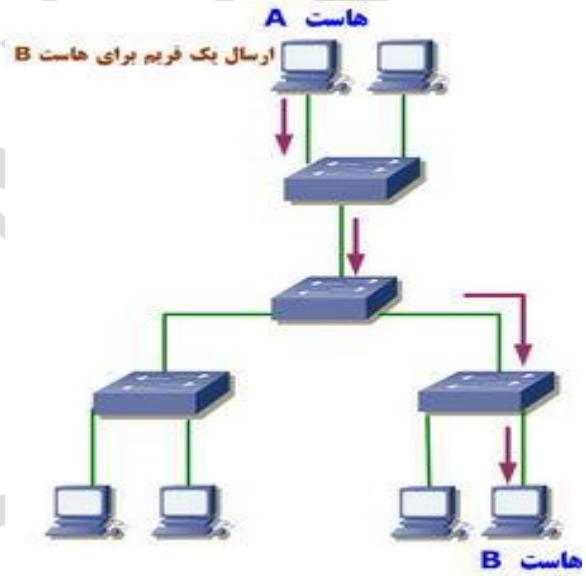
در شکل 1 ، یک شبکه نمونه نشان داده شده است . هر بسته اطلاعاتی broadcast ارسالی توسط هر دستگاه موجود در شبکه مشاهده می گردد (صرفنظر از این که دستگاه مورد نظر نیازمند دریافت آن داده باشد و یا نباشد) . به صورت پیش فرض ، سوئیچ ها broadcast را برای تمامی سگمنت های شبکه فوروارد می نمایند . علت این که گفته می شود شبکه به صورت flat است ، بدین دلیل است که صرفا" دارای یک broadcast domain می باشیم نه این که طراحی آن بطور فیزیکی flat انجام شده است .



شکل 1 : ساختار شبکه flat

در شکل 1 ، هاست A اقدام به ارسال یک broadcast می نماید و تمامی پورت های موجود بر روی تمامی سوئیچ ها این broadcast را فوروارد می نمایند (به جزء پورتی که broadcast از طریق آن دریافت شده است) .

در شکل 2 ، یک شبکه مبتنی بر سوئیچ نشان داده شده است که در آن هاست A اقدام به ارسال یک فریم برای هاست B می نماید . همانگونه که مشاهده می نمائید ، فریم صرفا" برای پورتی فوروارد شده است که هاست B به آن متصل شده است . روش فوق تاثیر غیرقابل انکاری را بر روی کارآئی شبکه نسبت به بکارگیری هاب به دنبال خواهد داشت .



شکل 2 : مزایای یک شبکه مبتنی بر سوئیچ

بزرگترین مزیت داشتن یک شبکه مبتنی بر سوئیچ های لایه دو ، ایجاد سگمنت های domain collision جداگانه برای هر دستگاه متصل شده به سوئیچ است . در چنین وضعیتی می توان به سادگی بر محدودیت مسافت در اترنت غلبه و شبکه های بزرگتری را ایجاد نمود . به موازات رشد شبکه و افزایش تعداد دستگاه های موجود در آن ، با مسائل جدیدی مواجه خواهیم شد . بدیهی است هر اندازه که تعداد کاربران و دستگاه ها بیشتر گردد ، یک سوئیچ می بایست با بسته های اطلاعاتی و broadcast بیشتری برخورد نماید .

مزیت دیگر شبکه های مبتنی بر سوئیچ های لایه دو ، امنیت است که به صورت یک مشکل واقعی خود را نشان خواهد داد ، چراکه در ارتباطات بین شبکه ای بر اساس سوئیچ های لایه دو ، بطور پیش فرض تمامی کاربران قادر به دیدن تمامی دستگاه ها می باشند . علاوه بر این ، نمی توان فعالیت یک دستگاه در خصوص ارسال broadcasting را متوقف و یا کاربران را ملزم به عدم ارسال broadcast کرد . گزینه های امنیتی صرفا" محدود به تعریف رمزهای عبور بر روی سرویس دهندگان و دستگاه های موجود در شبکه می باشند . بسیاری از مشکلات در ارتباط با سوئیچ های لایه دو را می توان با بکارگیری شبکه های محلی مجازی برطرف نمود . شبکه های محلی مجازی با بکارگیری روش های مختلف قادر به بهبود مدیریت شبکه می باشند .

شبکه های محلی مجازی می توانند چندین broadcast domain را به چندین subnet منطقی گروه بندی نمایند .

برای اضافه کردن ، انتقال و یا اعمال تغییرات مورد نظر می توان یک پورت را درون VLAN مورد نظر پیکربندی کرد .

می توان گروهی از کاربران را که نیازمند امنیت بالائی می باشند در یک VLAN قرار داد تا کاربران خارج از VLAN نتوانند با آنان ارتباط برقرار نمایند.

با توجه به گروه بندی منطقی کاربران بر اساس نوع فعالیت ، می توان شبکه های محلی مجازی را مستقل از مکان فیزیکی و جغرافیائی کاربران پیاده سازی کرد .

شبکه های محلی مجازی باعث بهبود وضعیت امنیت شبکه می گردند .

شبکه های محلی مجازی تعداد broadcast domain را افزایش و اندازه آنها را کاهش می دهند .

کنترل Broadcast

Broadcast در هر پروتکلی اتفاق می افتد ولی تعداد دفعات آن به سه عامل زیر بستگی دارد :

نوع پروتکل

برنامه و یا برنامه هائی که در شبکه اجراء می گردند .

با توجه به کاهش قیمت سوئیچ و توجیه اقتصادی استفاده از آنها ، بسیاری از سازمان ها شبکه های مبتنی بر هاب را که به صورت flat طراحی شده بودند با یک شبکه شامل سوئیچ و محیط VLAN جایگزین می نمایند . تمامی دستگاه های موجود در یک VLAN عضوی از broadcast domain مشابه بوده و تمامی broadcast را دریافت می نمایند . به صورت پیش فرض ، broadcast توسط تمامی پورت های موجود بر روی سوئیچ که عضو یک VLAN مشابه نمی باشند ، فیلتر می گردد .

امنیت

در ارتباطات بین شبکه های flat که از طریق اتصال هاب و سوئیچ ها به یکدیگر و در نهایت روتر ایجاد می گردد ، ما شاهد یک الگوی امنیتی flat نیز خواهیم بود . عده ای زیادی بر این باور هستند که این وظیفه روتر است که امنیت مورد نیاز در یک شبکه را تامین نماید . تفکر فوق به دلایل متعددی فاقد توجیه علمی و منطقی است .

هر شخصی که به شبکه فیزیکی متصل گردد قادر به دستیابی منابع موجود بر روی آن است .

کاربران صرفا" با اتصال ایستگاه های کاری خود به هاب موجود می توانند یک workgroup را به شبکه ملحق نمایند .

موارد فوق وجود امنیت در یک شبکه را نمی تواند تائید نماید ! با ایجاد شبکه های محلی مجازی و چندین گروه broadcast ، مدیران شبکه می توانند بر روی هر پورت و کاربر نظارت و کنترل داشته باشند .

دورانی که کاربران صرفا" با اتصال ایستگاه های کاری خود به یکی از پورت های سوئیچ قادر به استفاده از منابع شبکه می شدند سپری شده است .چراکه مدیران شبکه هم اینک می

توانند بر روی هر پورت و این که چه منابعی از طریق آن قابل دسترسی است کنترل و نظارت داشته باشند .

همچنین ، با توجه به این که می توان شبکه های محلی مجازی را بر اساس نوع نیاز کاربران به منابع شبکه طراحی نمود ، مدیران شبکه می توانند سوئیچ ها را بگونه ای پیکربندی نمایند تا در صورت دستیابی غیرمجاز به منابع شبکه ، موضوع به اطلاع یک ایستگاه مدیریت شبکه برسد .

در صورتی که نیازمند ارتباط بین شبکه های محلی مجازی باشیم ، می توان محدودیت های مورد نظر را بر روی روتر اعمال نمود . همچنین ، این امکان وجود دارد که بتوان محدودیت هائی را بر روی آدرس های سخت افزاری ، پروتکل ها و برنامه ها ایجاد کرد . بدین ترتیب امکان پیاده سازی چندین لایه امنیتی در یک شبکه فراهم می گردد .