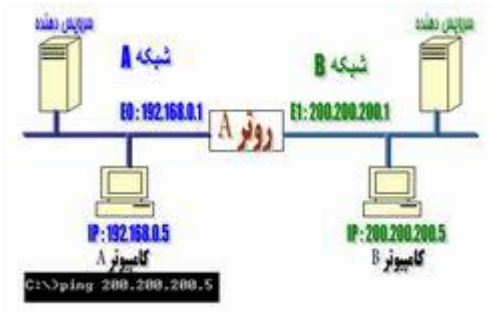
بررسی فرآیند روتینگ

روتینگ (Routing) یکی از مهمترین پتانسیل های مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد ، کامپیوترها قادر به مبادله داده نخواهند بود.بسیاری از علاقه مندانی که جدیدا" به دنیای گسترده شبکه های کامپیوتری پیوسته اند ، فکر می کنند که به منظور ارتباط با یک ماشین صرفا" به آدرس IP آن نیاز است . با مطالعه این مطلب مشخص خواهد شد که در این رابطه به اطلاعات بمراتب بیشتری نیاز می باشد. به منظور آشنائی با فرآیند روتینگ ، یک نمونه مثال را مرحله به مرحله دنبال نموده تا با فرآیند روتینگ اطلاعات، بیشتر آشنا شویم .

مثال : برررسی فرآیند روتینگ در دو شبکه LAN

دو شبکه فرضی A و B از طریق یک روتر (روتر A) که دارای دو اینترفیس E۰ و E۱ می باشد ، به یکدیگر متصل شده اند . اینترفیس های فوق ، مشابه اینترفیس های موجود بر روی کارت های شبکه بوده که درون روتر تعبیه شده اند (RJ-45) . کامپیوتر A (موجود بر روی شبکه A) ، قصد برقراری یک ارتباط با کامپیوتر B (موجود بر روی شبکه B) را دارد .



مرحله یک : کامپیوتر (میزبان) A از طریق خط دستور ، فرمان ping 200.200.200.5 را تایپ می نماید .

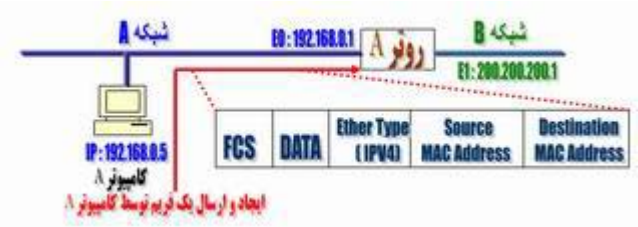
مرحله دوم : پروتکل IP با پروتکل ARP (اقتباس شده از کلمات Resolution Address protocol) کار نموده تا مشخص گردد که بسته اطلاعاتی فوق عازم چه شبکه ای است . بدین منظور آدرس IP و Subnet Mask کامپیوتر A بررسی می گردد. با توجه به این که درخواست فوق برای یک کامپیوتر راه دور می باشد ، می بایست بسته اطلاعاتی برای روتر (Gateway شبکه A) ارسال تا وی بتواند آن را به شبکه مورد نظر هدایت نماید (در این مورد خاص شبکه B) .

مرحله سوم : کامپیوتر A به منظور ارسال بسته اطلاعاتی برای روتر، نیازمند آگاهی از آدرس سخت افزاری اینترفیس روتر است که به شبکه A متصل شده است.(منظور آدرس MAC مربوط به اینترفیس E0 است که شبکه A از طریق آن به روتر متصل شده است) . به منظور دریافت آدرس MAC ، کامپیوتر A محتویات ARP cache خود را بررسی می نماید . ARP Cache ، محلی از حافظه است که آدرس های MAC برای چندین ثانیه در آنجا ذخیره می گردند .

مرحله چهارم : در صورتی که آدرس MAC مربوط به اینترفیس روتر که به شبکه A متصل شده است در ARP Cache کامپیوتر A پیدا نشود ، نشاند هنده این موضوع است که مدت زمان زیادی از ارتباط وی با روتر گذشته و یا وی قادر به یافتن آدرس MAC مربوط به روتر (اینترفیسی که به شبکه A متصل شده است) نمی باشد . با توجه به وضعیت فوق ، کامپیوتر A اقدام به ارسال یک ARP broadcast می نماید . پیام ارسالی در پی یافتن پاسخی مناسب بدین سوال است که : " آدرس MAC مربوط به IP:192.168.0.1 چیست ؟ ". پس از ارسال پیام broadcast ، روتر تشخیص می دهد که آدرس IP مربوط به وی بوده و می بایست به درخواست فوق ، پاسخ دهد . بدین ترتیب ، روتر با ارسال آدرس MAC مربوط به اینترفیس E0 ، پاسخ لازم را به کامپیوتر A خواهد داد . یکی از دلایلی که در برخی مواقع دستور Ping در اولین مرتبه با Time out مواجه می شود به موضوع اشاره شده برمی گردد. در چنین مواردی مدت زمان زیادی طول خواهد کشید که یک ARP ارسال و ماشین مربوطه با ارسال آدرس MAC خود به آن پاسخ دهد (Live TTL:Time To اولین بسته اطلاعاتی Ping به سر آمده و پیام Time out را خواهیم داشت) .

مرحله پنجم: روتر با ارسال آدرس IP:192.168.0.1 که به اینترفیس E0 آن نسبت داده شده است ، پاسخ مورد نظر را خواهد داد . بدین ترتیب ، کامپیوتر A تمامی اطلاعات مورد نیاز به منظور ارسال یک بسته اطلاعاتی به خارج از شبکه و برای روتر را دارا می باشد. لایه شبکه به لایه DataLink که بسته اطلاعاتی را توسط Ping (یک ICMP echo request) تولید نموده است ، به همراه آدرس سخت افزاری روتر ، اشاره می نماید. بسته اطلاعاتی شامل آدرس های IP مبداء و مقصد به همراه ICMP echo است که در لایه شبکه مشخص شده است .

مرحله ششم : لایه DataLink مربوط به کامپیوتر A ، یک فریم را تولید که یک بسته اطلاعاتی کپسوله شده به همراه اطلاعات مورد نیاز برای ارسال بر روی شبکه محلی است (شبکه A).اطلاعات فوق ، شامل آدرس سخت افزاری کامپیوترهای مبداء و مقصد (آدرس MAC) و فیلد نوع است که مسئولیت مشخص نمودن پروتکل لایه شبکه (مثلا" IPv4) و ARP را برعهده دارد. در انتهای فریم ، در بخش FCS فریم، لایه DataLink یک CRC را مستقر نموده تا ماشین دریافت کننده (روتر) قادر به تشخیص سالم بودن بسته اطلاعاتی دریافتی باشد .

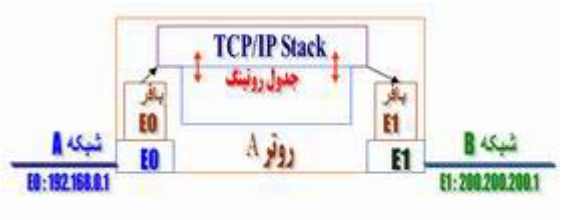


مرحله هفتم : لایه DataLink کامپیوتر A ، فریم را در اختیار لایه فیزیکی قرار داده تا صفر و یک های موجود در آن به یک سیگنال دیجیتال تبدیل و بر روی محیط فیزیکی شبکه ارسال گردد .

مرحله هشتم : سیگنال ارسالی توسط اینترفیس E0 روتر برداشته شده و فریم خوانده می شود . روتر در ابتدا بخش CRC آن را بررسی و آن را با مقدار CRC اضافه شده به فریم توسط کامپیوتر A مقایسه می نماید (حصول اطمینان از عدم خرابی فریم) .

مرحله نهم : در ادامه ، آدرس سخت افزاری مقصد (MAC) فریم دریافتی، بررسی می گردد . با توجه به وجود یک مورد آدرس که با آن مطابقت خواهد کرد، فیلد "نوع فریم" بررسی تا نحوه برخورد روتر با بسته اطلاعاتی ، مشخص گردد . IP در "فیلد نوع " بوده و روتر بسته اطلاعاتی را در اختیار پروتکل IP که بر روی روتر در حال اجراء است ، قرار خواهد داد . فریم از وضعیت موجود خارج و بسته اطلاعاتی اولیه ای که توسط کامپیوتر A تولید شده است در بافر روتر ذخیره می گردد .

مرحله دهم : پروتکل IP بررسی لازم در خصوص آدرس IP مقصد را انجام داده تا مشخص گردد که آیا بسته اطلاعاتی برای روتر است.با توجه به اینکه آدرس IP : 200.200.200.5 ، می باشد ، روتر با استفاده از جدول روتینگ خود تشخیص خواهد داد که آدرس فوق مربوط به شبکه ای است که از طریق اینترفیس E1 مستقیما" به روتر متصل شده است .



مرحله یازدهم : روتر ، بسته اطلاعاتی را در بافر اینترفیس E1 مستقر نموده و می بایست یک فریم به منظور ارسال بسته اطلاعاتی برای کامپیوتر مقصد را تولید نماید. روتر در ابتدا ARP Cache خود را به منظور یافتن آدرس سخت افزاری مربوط به IP:200.200.200.5 ، بررسی می نماید . در صورت عدم وجود آدرس فوق در ARP cache ، روتر یک broadcast ARP را از طریق اینترفیس E1 به منظور پیدا نمودن آدرس سخت افزاری فوق ، ارسال می نماید .

مرحله دوازدهم : کامپیوتر B با ارائه یک ARP Reply پاسخ لازم در خصوص آدرس سخت افزاری کارت شبکه مربوط به خود را خواهد داد . بدین ترتیب ، اینترفیس E1 روتر تمامی اطلاعات لازم به منظور ارسال بسته اطلاعاتی به مقصد نهائی را دارا می باشد .

مرحله سیزدهم : فریم تولید شده توسط اینترفیس E1 روتر دارای آدرس سخت افزاری مبداء مربوط به اینترفیس E1 و آدرس سخت افزاری مقصد مربوط به کارت شبکه کامپیوتر B می باشد.با این که آدرس های سخت افزاری مبداء و مقصد فریم در هر یک از اینترفیس های روتر تغییر می نماید ، آدرس IP کامپیوترهای مبداء و مقصد هرگز تغییر پیدا نمی نماید (بسته اطلاعاتی هرگز تغییر نکرده و صرفا" فریم تغییر می نماید) .

مرحله چهاردهم : کامپیوتر B ، فریم را دریافت و بررسی لازم در خصوص CRC را انجام می دهد . در صورتی که ماحصل بررسی انجام شده موفقیت آمیز نباشد ، فریم دورانداخته می شود. در ادامه، آدرس IP مقصد بررسی می گردد. با توجه به این که آدرس مقصد با پیکربندی IP انجام شده بر روی کامپیوتر B ، مطابقت می نماید ، فیلد پروتکل بسته اطلاعاتی بررسی تا اهداف بسته اطلاعاتی مشخص گردد .

مرحله پا نزدهم:با توجه به این که بسته اطلاعاتی یک درخواست ICMP echo است، کامپیوتر B یک ICMP echo-reply جدید را که شامل آدرس IP مبداء (کامپیوتر B) و آدرس IP مقصد مربوط به کامپیوتر A می باشد را ایجاد می نماید . فرآیند فوق، مجددا" و در جهت معکوس تکرار می گردد. در این مرحله ، آدرس سخت افزاری هر یک از دستگاه های موجود درطول مسیر شناخته شده بوده و هر دستگاه صرفا" نیازمند بررسی ARP cache مربوط به خود به منظور تشخیص آدرس سخت افزاری هر یک از اینترفیس ها می باشد (آدرس MAC) .

آشنائی با روتر

استفاده از روترها در شبکه به امری متداول تبدیل شده است . یکی از دلایل مهم گسترش استفاده از روتر ، ضرورت اتصال یک شبکه به چندین شبکه دیگر (اینترنت و یا سایر سایت ها ی از راه دور) در عصر حاضر است . نام در نظر گرفته شده برای روترها ، متناسب با کاری است که آنان انجام می دهند : " ارسال داده از یک شبکه به شبکه ای دیگر " . مثلا" در صورتی که یک شرکت دارای شعبه ای در تهران و یک دفتر دیگر در اهواز باشد ، به منظور اتصال آنان به یکدیگر می توان از یک خط leased (اختصاصی) که به هر یک از روترهای موجود در دفاتر متصل می گردد ، استفاده نمود . بدین ترتیب ، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود از طریق روتر محقق شده و تمامی ترافیک های غیرضروری دیگر فیلتر و در پهنای باند و هزینه های مربوطه ، صرفه جوئی می گردد .

انواع روترها

روترها را می توان به دو گروه عمده سخت افزاری و نرم افزاری تقسیم نمود:

- روترهای سخت افزاری : روترهای فوق ، سخت افزارهائی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نمایند (در حال حاضر صرفا" به صورت black box به آنان نگاه می کنیم).نرم افزار فوق ، قابلیت روتینگ را برای روترها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را بخوبی انجام دهند . اکثر شرکت ها ترجیح می دهند که از روترهای سخت افزاری استفاده نمایند چراکه آنان در مقایسه با

روترهای نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند . شکل زیر یک نمونه روتر را نشان می دهد . (Cisco 2600 Series Multiservice Platform)

منبع : سایت سیسکو

- روترهای نرم افزاری : روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT ، یک سرویس دهنده نت ور و یا یک سرویس دهنده لینوکس باشد . تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند .

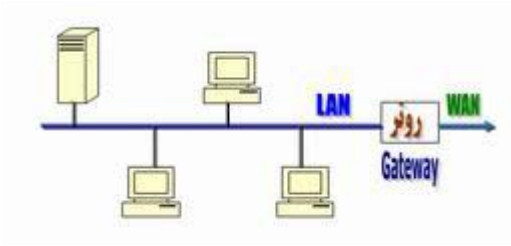
در اکثر موارد از روترها به عنوان فایروال و یا gateway اینترنت ، استفاده می گردد . در این رابطه لازم است به یکی از مهمترین تفاوت های موجود بین روترهای نرم افزاری و سخت افزاری ، اشاره گردد : در اکثر موارد نمی توان یک روتر نرم افزاری را جایگزین یک روتر سخت افزاری نمود ، چراکه روترهای سخت افزاری دارای سخت افزار لازم و از قبل تعبیه شده ای می باشند که به آنان امکان اتصال به یک لینک خاص WAN (از نوع Frame Relay ، ISDN و یا ATM) را خواهد داد .یک روتر نرم افزاری (نظیر سرویس دهنده ویندوز) دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه های WAN از طریق روترهای سخت افزاری ، انجام خواهد شد .

مثال ۱ : استفاده از روتر به منظور اتصال دو شبکه به یکدیگر و ارتباط به اینترنت

فرض کنید از یک روتر مطابق شکل زیر به منظور اتصال دو شبکه LAN به یکدیگر و اینترنت ، استفاده شده است . زمانی که روتر داده ای را از طریق یک شبکه LAN و یا اینترنت دریافت می نماید ، پس از بررسی آدرس مبداء و مقصد ، داده دریافتی را برای هر یک از شبکه ها و یا اینترنت ارسال می نماید . روتر استفاده شده در شکل زیر ، شبکه را به دو بخش متفاوت تقسیم نموده است .(دو شبکه مجزاء) . هر شبکه دارای یک هاب است که تمامی کامپیوترهای موجود در شبکه به آن متصل شده اند . علاوه بر موارد فوق ، روتر استفاده شده دارای اینترفیس های لازم به منظور اتصال هر شبکه به آن بوده و از یک اینترفیس دیگر به منظور اتصال به اینترنت ، استفاده می نماید . بدین ترتیب ، روتر قادر است داده مورد نظر را به مقصد درست ، ارسال نماید .

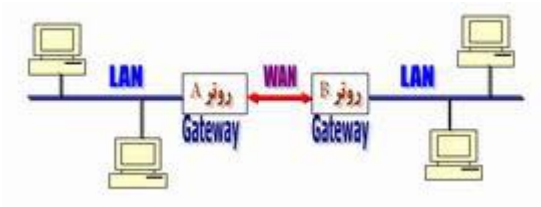
مثال ۲: استفاده از روتر در یک شبکه **LAN**

فرض کنید از یک روتر مطابق شکل زیر در یک شبکه LAN ، استفاده شده است . در مدل فوق ، هر یک از دستگاههای موجود در شبکه با روتر موجود نظیر یک gateway برخورد می نمایند . بدین ترتیب ، هر یک از ماشین های موجود بر روی شبکه LAN که قصد ارسال یک بسته اطلاعاتی (اینترنت و یا هر محل خارج از شبکه LAN) را داشته باشند ، بسته اطلاعاتی مورد نظر را برای gateway ارسال می نمایند . روتر (gateway) نسبت به محل ارسال داده دارای آگاهی لازم می باشد . (در زمان تنظیم خصلت های پروتکل TCP/IP برای هر یک از ماشین های موجود در شبکه یک آدرس IP برای gateway در نظر گرفته می شود) . شکل زیر نحوه استفاده از یک روتر به منظور دستیابی کاربران به اینترنت در شبکه LAN را نشان می دهد :



مثال ۳: استفاده از روتر به منظور اتصال دو دفتر کار

فرض کنید ، بخواهیم از روتر به منظور اتصال دو دفتر کار یک سازمان به یکدیگر ، استفاده نمائیم . بدین منظور هر یک از روترهای موجود در شبکه با استفاده از یک پروتکل WAN نظیر ISDN به یکدیگر متصل می گردند . عملا" ، با استفاده از یک کابل که توسط ISP مربوطه ارائه می گردد ، امکان اتصال به اینترفیس WAN روتر فراهم شده و از آنجا سیگنال مستقیما" به شبکه ISP مربوطه رفته و سر دیگر آن به اینترفیس WAN روتر دیگر متصل می گردد . روترها ، قادر به حمایت از پروتکل های WAN متعددی نظیر Frame Relay , HDLC , ATM و یا PPP ، می باشند .



مهمترین ویژگی های یک روتر :

- روترها دستگاههای لایه سوم (مدل مرجع OSI) می باشند .
- روترها مادامیکه برنامه ریزی نگردند ، امکان توزیع داده را نخواهند داشت .
- اکثر روترهای مهم دارای سیستم عامل اختصاصی خاص خود می باشند .
- روترها از پروتکل های خاصی به منظور مبادله اطلاعات ضروری خود (منظور داده نیست) ، استفاده می نمایند .

- نحوه عملکرد یک روتر در اینترنت : مسیر ایجاد شده برای انجام مبادله اطلاعاتی بین سرویس گیرنده و سرویس دهنده در تمامی مدت زمان انجام تراکش ثابت و یکسان نبوده و متناسب با وضعیت ترافیک موجود و در دسترس بودن مسیر ، تغییر می نماید .
-

آشنائی با مفهوم روتینگ

روتینگ (Routing) یکی از مهمترین ویژگی های مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد ، کامپیوترها قادر به مبادله داده نخواهند بود .

تعریف

از روتینگ به منظور دریافت یک بسته اطلاعاتی (packet) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاهی دیگر و بر روی شبکه ای متفاوت ، استفاده می گردد . در صورتی که شبکه شما دارای روتر نباشد ، امکان روتینگ داده بین شبکه شما و سایر شبکه ها وجود نخواهد داشت . یک روتر به منظور مسیریابی یک بسته اطلاعاتی ، می بایست آگاهی لازم در خصوص اطلاعات زیر را داشته باشد :

- آدرس مقصد
- روترهای مجاور که با استفاده از آنان امکان اخذ اطلاعات لازم در خصوص شبکه های از راه دور، فراهم می گردد .
- مسیرهای موجود به تمامی شبکه های از راه دور
- بهترین مسیر به هر یک از شبکه های از راه دور
- نحوه نگهداری و بررسی اطلاعات روتینگ

همگرائی (Convergence)

فرآیند مورد نیاز برای تمامی روترهای موجود در یک شبکه به منظور بهنگام سازی جداول روتینگ و ایجاد یک نگرش سازگار از شبکه با استفاده ار بهترین مسیرهای موجود . در زمان انجام فرآیند فوق (همگرائی) ، داده کاربر ارسال نخواهد شد .

مسیر پیش فرض (Default Route)

یک مسیر استاندارد درج شده در جدول روتینگ که به عنوان اولین گزینه در نظر گرفته می شود . هر بسته اطلاعاتی که توسط یک دستگاه ارسال می گردد در ابتدا به مسیر پیش فرض ارسال خواهد شد . در صورتی که مسیر فوق مشکل داشته باشد ، یک مسیر دیگر انتخاب می گردد .

مسیر ایستا (Static Route)

یک مسیر دائم که به صورت دستی درون یک جدول روتینگ درج می گردد . مسیر فوق حتی در مواردیکه ارتباط غیر فعال است در جدول روتینگ باقی مانده و صرفا" به صورت دستی حذف می گردد .

مسیر پویا (Dynamic Route)

یک مسیر که به صورت پویا (اتوماتیک) و متناسب با تغییرات شبکه ، بهنگام می گردد .مسیرهای پویا نقطه مقابل مسیرهای ایستا می باشند .

آشنائی با پروتکل های روتینگ

پروتکل های روتینگ به منظور استفاده در روترها ، ایجاد شده اند . پروتکل های فوق ، بدین منظور طراحی شده اند که امکان مبادله اطلاعات جداول روتینگ بین روترها را فراهم نماید . تاکنون پروتکل های متفاوتی به منظور استفاده در شبکه هائی با ابعاد گوناگون ، طراحی و پیاده سازی شده است .

دو نوع عمده روتینگ : پویا و ایستا

روتر ، با استفاده از روترهای مجاور (همسایه) و یا توسط مدیر شبکه، آگاهی لازم در خصوص شبکه های راه دور را پیدا می نماید . روتر در ادامه ، یک جدول روتینگ را ایجاد که مسئولیت آن تشریح نحوه یافتن شبکه های راه دور است . در صورتی که شبکه مستقیما" متصل شده باشد ، روتر در خصوص شبکه ، مشکل خاصی نخواهد داشت . در صورتی که شبکه ها به یکدیگر متصل نمی باشند ، روتر می بایست آگاهی لازم در خصوص شبکه های راه دور را پیدا نماید . در این رابطه از روتینگ ایستا (درج دستی مسیرها در جدول روتینگ توسط مدیر شبکه) و یا روتینگ پویا (درج اتوماتیک مسیرها در جدول روتینگ با استفاده از پروتکل های روتینگ)، استفاده می گردد.

روترها در ادامه اقدام به بهنگام سازی اطلاعات خود در ارتباط با تمامی شبکه هائی می نمایند که نسبت به آنان آگاهی لازم را پیدا نموده اند . در صورتی که تغییری ایجاد گردد (مثلا" یک روتر با مشکل مواجه شده و عملا" قادر به سرویس دهی نباشد) ، پروتکل های روتینگ پویا ، به صورت اتوماتیک به تمامی روترها این موضوع را اطلاع خواهند داد . در صورت استفاده از روتینگ ایستا ، می بایست مدیر شبکه تغییرات لازم را در تمامی روترها ، اعمال نماید (عدم استفاده از پروتکل های روتینگ) .

در روتینگ پویا از پروتکل های روتینگ به منظور نیل به اهداف زیر استفاده می گردد .

- تشخیص و نگهداری پویای روترها
- محاسبه مسیرها
- توزیع اطلاعات بهنگام شده روتینگ برای سایر روترها
- حصول توافق با سایر روترها در خصوص توپولوژی شبکه

در صورت برنامه ریزی ایستای روترها ، امکان یافتن روترها و یا ارسال اطلاعات برای سایر روترها وجود نخواهد داشت . آنان داده مورد نظر را بر روی روترهائی که توسط مدیر شبکه تعریف شده است ، ارسال می نمایند .

پروتکل های روتینگ پویا

در این رابطه از سه نوع(گروه) پروتکل روتینگ پویا استفاده می گردد . تفاوت عمده بین آنان ، روش استفاده شده به منظور یافتن روترها و محاسبات لازم در خصوص مسیریابی آنان است.

- **Distance Vector** : این نوع روترها بهترین مسیر را از طریق اطلاعات ارسال شده توسط سایر روترهای مجاور ، محاسبه می نمایند .
- **Link state** : این نوع روترها هر یک دارای نسخه ای از تمامی مپ شبکه بوده و بهترین مسیر را با استفاده از آن محاسبه می نمایند .
- **Hybrid** : پروتکل های روتینگ Hybrid حد فاصل بین پروتکل های روتینگ Link state و Distance Vector می باشند .

MAC Address چیست ؟

هر کامپیوتر موجود در شبکه به منظور ایجاد ارتباط با سایر کامپیوترها ،می بایست شناسائی و دارای یک

آدرس منحصربفرد باشد . قطعا" تاکنون با آدرس های IP و یا MAC (اقتباس شده از کلمات Media Access Control) برخورد داشته اید و شاید این سوال برای شما مطرح شده باشد که اولا" ضرورت وجود دو نوع آدرس چیست و ثانیا" جایگاه اسفاده از آنان چیست ؟

MAC Address ، یک آدرس فیزیکی است در حالی که آدرس های IP ، به منزله آدرس های منطقی می باشند. آدرس های منطقی شما را ملزم می نمایند که به منظور پیکربندی کامپیوتر و کارت شبکه ، درایورها و یا پروتکل های خاصی را در حافظه مستقر نمائید (مثلا" استفاده از آدرس های IP) . این وضعیت در رابطه با MAC Address صدق نخواهد کرد و اینگونه آدرس ها نیازمند درایور های خاصی نخواهند بود ، چراکه آدرس های فوق درون تراشه کارت شبکه قرار می گیرند .

دلیل استفاده از MAC Address

هر کامپیوتر موجود در شبکه ، می بایست با استفاده از روش هائی خاص شناسائی گردد . برای شناسائی یک کامپیوتر موجود در شبکه ، صرف داشتن یک آدرس IP به تنهائی کفایت نخواهد کرد . حتما" علاقه مندید که علت این موضوع را بدانید . بدین منظور، لازم است نگاهی به مدل معروف Open Systems Interconnect (OSI) و لایه های آن داشته باشیم :

...		
Network Layer	لایه سوم	آدرس IP در این لایه قرار دارد
DataLink Layer	لایه دوم	آدرس MAC در این لایه قرار دارد
Physical Layer	لایه اول	
شبکه فیزیکی		

همانگونه که مشاهده می نمائید ، MAC Address در لایه DataLink (لایه دوم مدل OSI) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوترهای موجود در شبکه است . زمانی که یک بسته اطلاعاتی (Packet) به لایه Datalink می رسد (از طریق لایه اول) ، وی آن را در اختیار لایه بالائی خود (لایه سوم) قرار خواهد داد . بنابراین ما نیازمند استفاده از روش خاصی به منظور شناسائی یک کامپیوتر قبل از لایه سوم هستیم . MAC Address ، در پاسخ به نیاز فوق در نظر گرفته شده و با استقرار در لایه دوم ، وظیفه شناسائی کامپیوتر قبل از لایه سوم را بر عهده دارد. تمامی ماشین های موجود بر روی یک شبکه ، اقدام به بررسی بسته های اطلاعاتی نموده تا مشخص گردد که آیا MAC Address موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با آدرس آنان مطابقت می نماید؟ لایه فیزیکی (لایه اول) قادر به شناخت سیگنال های الکتریکی موجود بر روی شبکه بوده و فریم هائی را تولید می نماید که در اختیار لایه Datalink ، گذاشته می شود . در صورت مطابقت MAC Address موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با MAC Address یکی از کامپیوترهای موجود در شبکه ، کامپیوتر مورد نظر آن را دریافت و با ارسال آن به لایه سوم ، آدرس شبکه ای بسته اطلاعاتی (IP) بررسی تا این اطمینان حاصل گردد که آدرس فوق با آدرس شبکه ای که کامپیوتر مورد نظر با آن پیکربندی شده است بدرستی مطابقت می نماید .

یک MAC Address بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می باشند . (شش بایت و یا ۴۸ بیت) . در صورت بررسی Address MAC یک کامپیوتر که بر روی آن کارت شبکه نصب شده است ، آن را با فرمت مبنای شانزده (Hex) ، مشاهده خواهید دید . مثلا" MAC Address کارت شبکه موجود بر روی یک کامپیوتر می تواند به صورت زیر باشد :

مشاهده MAC Address					
استفاده از دستور IPconfig/all و مشاهده بخش Physical address:					
6A	DB	79	BA	50	00
تعریف شده توسط تولید کننده			تعریف شده توسط IEEE با توجه به RFC ۱۷۰۰		

زمانی که یک تولید کننده نظیر اینتل ، کارت ها ی شبکه خود را تولید می نماید ، آنان هر آدرس دلخواهی را نمی توانند برای MAC Address در نظر بگیرند . در صورتی که تمامی تولید کنندگان کارت های شبکه بخواهند بدون وجود یک ضابطه خاص ، اقدام به تعریف آدرس های فوق نمایند ، قطعا" امکان تعارض بین آدرس های فوق بوجود خواهد آمد . (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت با آدرس های یکسان).حتما" این سوال برای شما مطرح می گردد که MAC Address توسط چه افراد و یا سازمان هائی و به چه صورت به کارت های شبکه نسبت داده می شود ؟ به منظور برخورد با مشکلات فوق ، گروه IEEE ، هر MAC Address را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یک شماره سریال را در آن درج نمایند .

کد تولید کنندگان بر اساس RFC-1700 به آنان نسبت داده می شود . در صورت مشاهده RFC فوق حتما"

متوجه خواهید شد که برخی از تولید کنندگان دارای بیش از یک کد می باشند .علت این امر به حجم گسترده محصولات تولیدی آنان برمی گردد .

با این که MAC Address در حافظه کارت شبکه ثبت می گردد ، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص ، بتوانید بخش دوم MAC Address کارت شبکه خود را تغییر دهید(شماره سریال کارت شبکه) . علت این موضوع به استفاده مجدد از سریال های استفاده شده در سایر محصولات تولید شده توسط آنان برمی گردد (تجاوز از محدود مورد نظر) . در حال حاضر احتمال این که شما دو کارت شبکه را خریداری نمائید که دارای MAC Address یکسانی باشند، بسیار ضعیف و شاید هم غیرممکن باشد.