مقدمه :

Cisco Certificate Network Associate اولین گام برای ورود به دنیای سیسکو محسوب می‌شود .

در این سری از مطالب آموزشی سعی بر این است تا آموزش دوره CCNA Routing and switching از ابتدا و به‌صورت بسیار ساده و قابل‌درک توضیح داده شود . البته پیش‌نیاز دوره CCNA ، Network + است تا درک ابتدایی از مفاهیم شبکه داشته باشید . هرچند در ابتدای آموزش سعی شده است که این مطالب در حد رفع نیاز خواننده گفته شود .

مطالب با ترکیبی از ترجمه کتاب‌ها و ویدیوهای آموزشی است ، به همراه برخی از نکات مهم که خودم برای کامل‌تر شدن و درک بهتر مفاهیم ، به آن اضافه می‌کنم . همچنین در پایان هر فصل نمونه سوا لات آموزشی به همراه آزمودن‌های امتحان بین‌المللی با توضیحات لازم ارائه می‌گردد . هر هفته 2 مطلب جدید در سایت قرار می‌گیرد .

امیدوارم در پایان آموزش بتوانم جزوه کامل و جامعی برای علاقه‌مندان به CCNA فراهم نمایم .

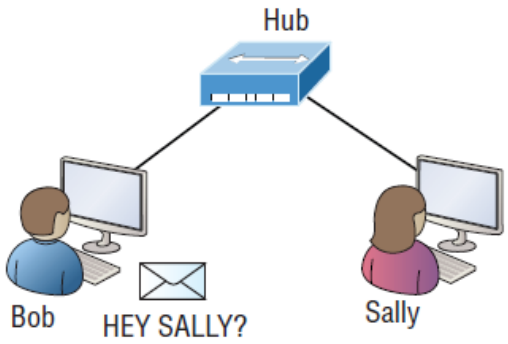
کد آزمون : 200-120

سرفصل‌ها :

Internetworking

آشنایی ابتدایی با شبکه :

در ابتدا می‌خواهیم با یک شبکه ساده آشنا شویم، شکل زیر نمایش‌دهنده یک شبکه محلی Local Area Network (LAN) است:



(1)

کامپیوترها توسط دستگاهی به نام Hub به یکدیگر متصل شده‌اند. به خاطر بسپارید که شبکه موردنظر از یک Collision Domain و یک Broadcast Domain تشکیل‌شده است. در ادامه به توضیح اصطلاحات فوق خواهیم پرداخت.

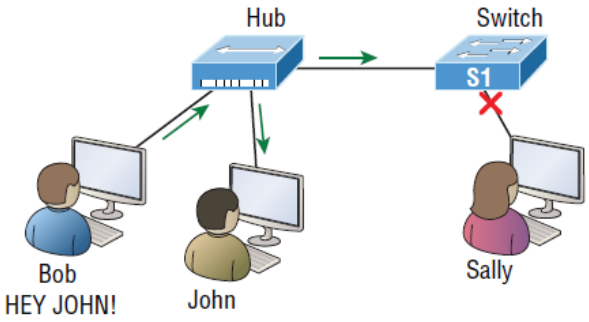
در سناریو بالا اگر Bob بخواهد فایلی را برای Sally ارسال کند در ساده‌ترین حالت ممکن، او می‌تواند فایل موردنظر را در شبکه پخش (Broadcast) نماید. به‌صورت ساده‌تر اگر بخواهیم آن را توضیح دهیم، می‌توان گفت که اگر Bob آدرسی از Sally نداشته باشد، فقط کافی است که برای رساندن پیغام خود آن را در شبکه فریاد بزند. با این کار مطمئناً تمامی کسانی که در شبکه LAN حضور دارند نیز پیغام Bob را دریافت می‌کنند. در شبکه‌هایی شامل دستگاه‌های بیشتر، اگر برای رساندن هر بسته، دستگاه موردنظر آن را فریاد بزند، به دلیل ترافیک بالا شبکه دچار اشکال می‌شود.

روش دیگر هم این است که Bob با داشتن آدرس Sally، مستقیم با او گفتگو کند . این به شما بستگی دارد که از کدام روش بخواهید استفاده کنید . اما برای گفتگوی مستقیم شما باید اطلاعات اولیه را داشته باشید . آدرس Sally را چگونه به دست می‌آورید ؟ برای انتقال آن از چه دستگاهی باید استفاده کنید ؟

در شبکه‌های بزرگ ، شما ممکن است دچار مشکل حجم بالای ترافیک شوید . با ترافیک بالا شبکه LAN شما کند و حتی ممکن است به‌صورت کامل از کار بیفتد . شما باید در این نوع شبکه‌ها ، آن را به تعداد کوچک‌تر تقسیم و بخش‌های آن را تا جای ممکن از هم جدا کنید . مانند یک خیابان شلوغ که با اضافه کردن خیابان و تقاطع‌های بیشتر و همچنین ایجاد قانون‌های جدید می‌توانید به روان شدن ترافیک کمک کنید .

تمامی این راه‌حل‌ها در شبکه توسط دستگاه‌هایی مانند Router , Switch قابل پیاده‌سازی است .

حال بیاید یک همسایه جدید به شبکه قبل اضافه کنیم :



(2)

در شکل شماره 2 مشاهده می‌کنید که Sally توسط یک سوییچ به شبکه متصل شده است . در این حالت سوییچ باعث ایجاد یک Collision Domain جدا می‌شود . این کار باعث کمتر شدن فریادها یا همان پخش و Broadcast شدن پیغام‌های ما می‌شود اما در نظر داشته باشید که شبکه جدید ما هنوز یک Broadcast Domain به‌حساب می‌آید . به این معنی که اگر Bob بخواهد پیغامی را برای John ارسال کند ولی آدرس آن را نداند ، پیغام را فریاد می‌زند که باعث می‌شود آن پیغام به Sally نیز برسد . اما سوییچ باعث جدا شدن Collision Domain در شبکه می‌شود . به این صورت که اگر Bob با داشتن آدرس John به‌صورت مستقیم بخواهد با او صحبت کند ، بسته فقط به John ارسال می‌شود و سوییچ با دیدن آدرس بسته و با درک اینکه این آدرس به کاربری که به او متصل است مربوط نمی‌شود ، از عبور آن جلوگیری می‌کند .

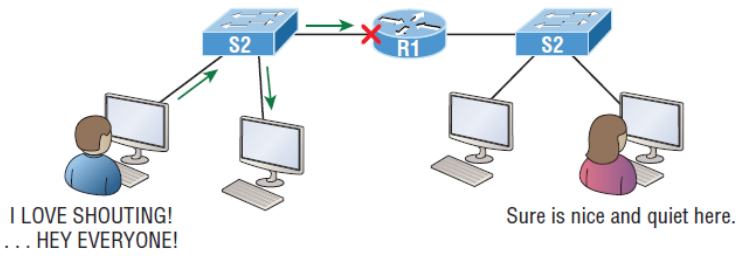
متوجه تفاوت و معنای Collision Domain و Broadcast Domain شدید ؟ هنوز نه ؟ نگران نباشید ، در ادامه بیشتر توضیح خواهم داد .

لیست مواردی که ممکن است باعث افزایش ترافیک شبکه شود عبارت است از :

- تعداد زیاد کاربران در یک Collision Domain یا Broadcast Domain
- Broadcast Storm
- تعداد زیاد ترافیک Multicast
- پهنای باند کم (Bandwidth)
- استفاده از Hub برای ارتباط کاربران با یکدیگر
- افزایش ARP Broadcast

حالا با توجه به توضیحات داده‌شده دوباره به شکل 2 نگاه کنید ، دلیل استفاده از سوییچ در شبکه و تفاوت آن با هاب را متوجه شدید ؟ به دلیل اینکه هاب جزئی از شبکه به‌حساب نمی‌آید ، سوییچ را به شبکه اضافه کردیم ، در واقعیت هاب فقط یک وسیله ارزان برای ارتباط کامپیوترها در شبکه است (که البته در دنیای واقعی دیگر استفاده نیز نمی‌شود) .

حال اگر بخواهیم شبکه خود را بازهم گسترش دهیم ، نیاز به دستگاهی داریم که مسیرهای بیشتر به همراه کنترل ترافیک و حتی یک امنیت مقدماتی را برای ما تأمین کند . برای این اهداف ما از روتر در شبکه استفاده می‌کنیم . روتر دستگاهی است که شبکه‌های ما را به هم ارتباط می‌دهد . روترها در شبکه ، Broadcast Domain ها را از یکدیگر جدا می‌کنند . به شکل زیر توجه کنید :



(3)

در شکل 3 ، با اضافه کردن یک روتر به شبکه ، دارای دو Broadcast Domain مجزا خواهیم بود . اگر فردی در یک قسمت شبکه بخواهد پیامی را به‌صورت Broadcast در شبکه ارسال کند ، روتر آن پیام را از خود عبور

نخواهد داد . اگر Bob بخواهد پیامی را برای Sally ارسال کند ، باید به‌صورت مستقیم ارتباط برقرار کرده و آدرس (IP Address) آن را بداند .

پس با توجه به تعاریف بالا ، هرگاه در یک شبکه یکی از کاربران یک پیغام Broadcast را انتشار دهد ، تمامی اعضای شبکه موظف هستند که آن را دریافت و بخوانند ، مگر آنکه در شبکه روتر داشته باشیم . وقتی یک اینترفیس روتر پیغام Broadcast را دریافت کند آن را از بین برده و به دیگر شبکه‌های متصل به خود انتقال نمی‌دهد . و توجه داشته باشد که مسلماً روتر جداکننده Collision Domain نیز هست .

کارکرد روترها در شبکه :

- جداکننده پیغام‌های Broadcast
- آن‌ها می‌توانند بر اساس لایه 3 ، اطلاعات را فیلتر کنند .

در مورد لایه‌های شبکه در ادامه توضیح داده خواهد شد ، اما خوب است بدانید که روترها در لایه 3 و سوییچ‌ها در لایه 2 کار می‌کنند .

روترها مانند سوییچ‌های لایه 3 ، هستند . برخلاف سوییچ‌ها که بر اساس فریم (Frame) بسته‌ها را عبور و یا فیلتر می‌کند ، روترها از آدرس‌های منطقی (Logical address) و تحلیل بسته‌ها(Packets) ، بهره می‌برد که به آن Packet Switching گفته می‌شود . شما از طریق آن می‌توانید ارتباط بین شبکه‌ها را برقرار کنید و یا به‌اصطلاح Internetwork داشته باشید . روترها از یک جدول مانند یک نقشه برای ارتباط بین شبکه‌ها استفاده می‌کنند . جدول به روترها بهترین مسیر برای رسیدن به شبکه‌های دیگر را نشان می‌دهد .

پس می‌توان نتیجه گرفت شما هیچ‌وقت نمی‌توانید از یک سوییچ برای ارتباط بین شبکه‌ای استفاده کنید ، زیرا سوییچ‌ها به‌صورت پیش‌فرض Broadcast Domain ها را از یکدیگر جدا نمی‌کنند و کاربرد آن‌ها ارتباط کاربران در داخل یک شبکه محلی (LAN) است و همچنین سوییچ‌ها قادر به تحلیل بسته‌ها (Packets) نیستند و بر اساس فریم‌ها (Frames) اطلاعات را هدایت می‌کنند .

نگران نباشید ، در مورد Packet و Frames در ادامه توضیح داده خواهد شد .

تا به اینجا ما متوجه شدیم که سوییچ‌ها در شبکه باعث جدا شدن Collision Domain می‌شوند . اما Collision Domain چیست ؟

Collision Domain به معنی آن است که هرگاه در شبکه یک کاربر بسته‌ای را انتشار دهد ، تمامی دستگاه‌ها در یک Collision Domain آن را دریافت می‌کنند . توجه داشته باید که مهم نیست که بسته ارسالی یک بسته Broadcast و یا دارای آدرس مقصد مشخص باشد ، در هر دو حالت بسته برای همه ارسال می‌شود . این اثر می‌تواند تأثیرات بدی در شبکه داشته باشد .

اول آنکه باعث اختلال در شبکه می‌شود . اگر کاربری در حال ارسال اطلاعات باشد تمامی دستگاه‌ها فقط می‌توانند به آن گوش دهند . اگر دستگاه دیگری در همان زمان بسته‌ای ارسال کند باعث تداخل شده و در اصطلاح می‌گویند Collision روی می‌دهد .

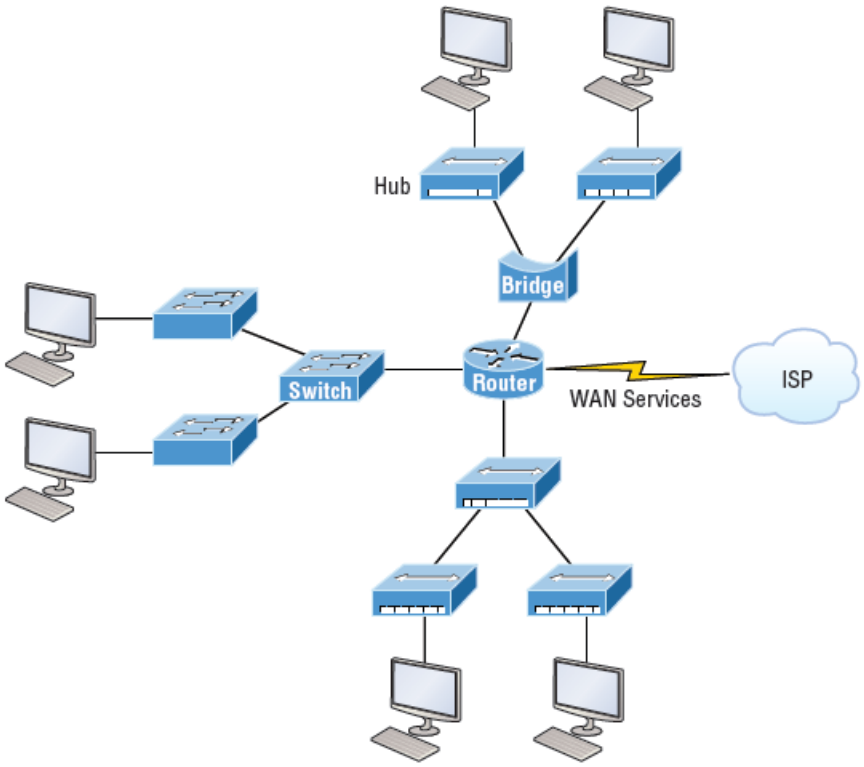
دوم مسئله امنیتی آن است که بسته برای تمامی کاربران ارسال می‌شود .

این مشکلات در شبکه‌هایی که توسط هاب ارتباط داده‌شده‌اند به وجود می‌آید . هاب ها تمامی کاربران را در یک Collision Domain قرار می‌دهند اما سوییچ‌ها ، هر پورت آن‌یک Collision Domain مجزا است .

" سوییچ‌ها Collision Domain را از هم جدا می‌کنند ولی دارای یک Broadcast Domain هستند اما روترها بر روی هر اینترفیس خود یک Broadcast Domain ایجاد می‌کنند "

نوع دیگری از دستگاه‌ها به نام بریج Bridge نیز وجود دارد که کارکردی مشابه سوییچ‌ها دارند . بریج ها قبل از سوییچ و روتر به وجود آمدن و برای ارتباط در شبکه‌های محلی (LAN) به کار گرفته می‌شدند . اما دارای پورت‌های محدودی بودند . امروزه دیگر از این دستگاه‌ها استفاده نمی‌شود زیرا سوییچ‌ها با کارایی بهتر و پورت‌های بیشتر جایگزین آن‌ها شده‌اند .

حال به شکل 4 نگاه کنید . تمامی دستگاه‌هایی که معرفی کردیم در شبکه به کار گرفته‌شده است . به محل به‌کارگیری دستگاه‌ها دقت کنید . روتر در مرکز شبکه و نقش ارتباط دهی بین شبکه‌های محلی (LAN) را بر عهده دارد . می‌توانیم برای تعداد کاربران کم از Hub و Bridge استفاده کنیم (البته به دلیل وجود نداشتن این دستگاه‌ها در حال حاضر ، فقط به‌صورت تئوری استفاده می‌شود) ، از سوییچ‌ها برای ارتباط داخلی استفاده‌شده است .

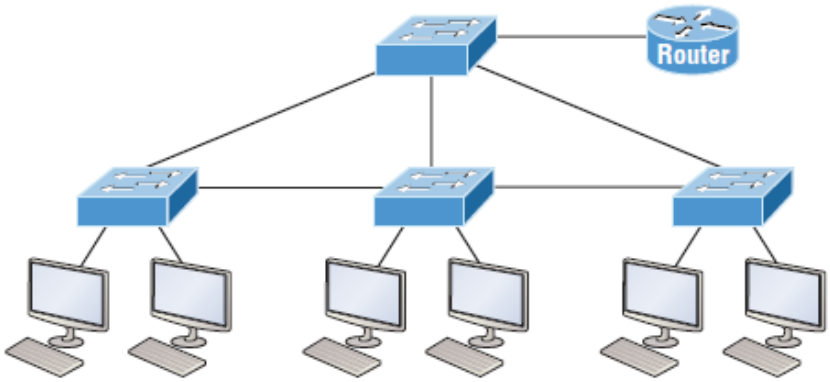


(4)

در شبکه پایین که فقط هاب به کار گرفته‌شده است، فقط یک Collision Domain و یک Broadcast Domain داریم ، در شبکه سمت بالا ، به ازای هر پورت بریج یک Collision Domain داریم و همچنان یک Broadcast Domain .

بهترین نوع ارتباط ، شبکه سمت چپ است . چرا ؟ به دلیل اینکه هر پورت سوییچ جداکننده یک Collision Domain است اما این کافی نیست ، به دلیل اینکه تمامی دستگاه‌های ما در یک Broadcast Domain قرار دارند . به یاد دارید چرا این باعث مشکل می‌شد ؟ چون در یک Broadcast Domain در هر جای شبکه یکی از کاربران اطلاعاتی را به‌صورت Broadcast ارسال می‌کرد ، تمامی کاربران آن را دریافت می‌کردند و در شبکه‌های بزرگ این می‌تواند بسیار مضر باشد . به همین دلیل باید شبکه را به قسمت‌های کوچک‌تر تقسیم کرد و این همان کاری است که روترها انجام می‌دهند . با قرار دادن یک روتر در مرکز شبکه می‌توانیم هم ارتباط بین شبکه‌ها را برقرار کنیم و هم اینکه Broadcast Domain ها را از هم جدا نماییم .

شکل 5 نمونه استاندارد یک شبکه است .



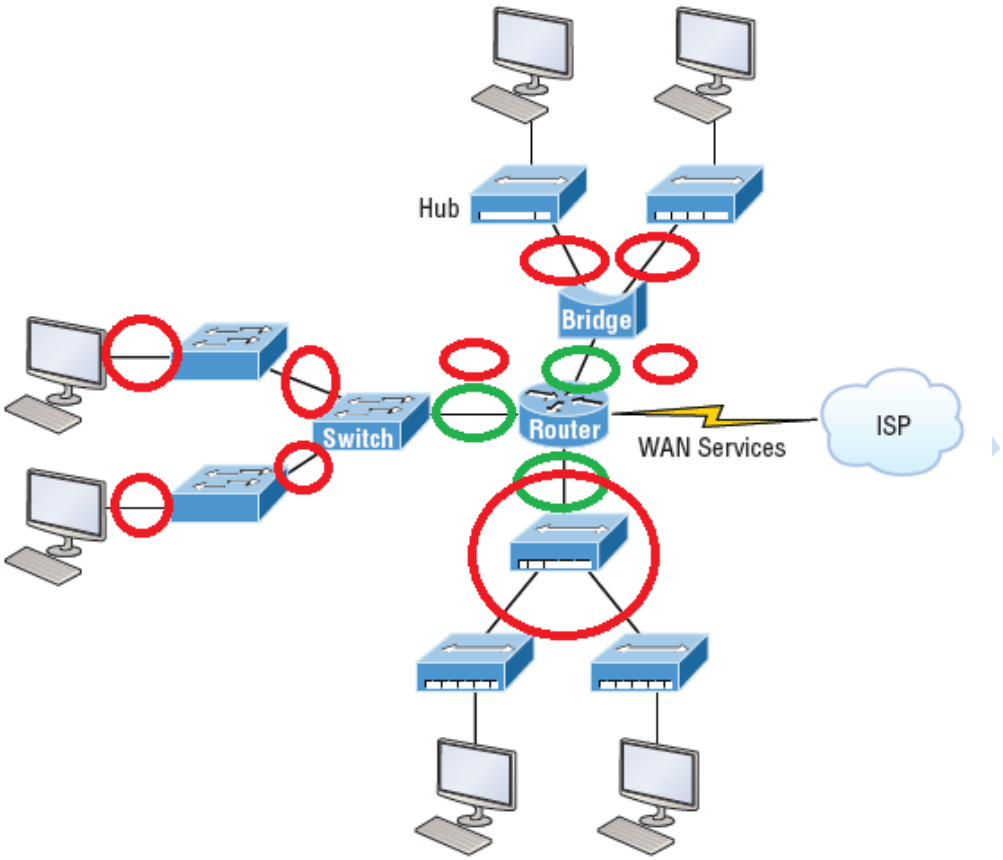
(5)

"سوییچی که در مرکز قرارگرفته است را با VLAN پیکربندی می‌کنند که فعلاً در بحث‌های ابتدایی شبکه نیست "

دوباره به شکل 4 توجه کنید ، حالا می‌توانید بگویید در شبکه چند Collision Domain و چند Broadcast Domain داریم ؟

امیدوارم جواب شما Collision Domain 9 و Broadcast Domain 3 باشد ! شمردن Broadcast Domain ها راحت‌تر است ، به دلیل اینکه به‌صورت پیش‌فرض فقط روترها باعث تفکیک آن‌ها می‌شوند . اما آیا می‌توانید Collision Domain ها را به‌راحتی تشخیص دهید ؟

به شکل 6 توجه کنید :



(6)

دایره‌های سبز نشان‌دهنده Broadcast Domain ها است ، هر اینترفیس روتر جداکننده یکی از آن‌هاست .

دایره‌های قرمز مشخص‌کننده Collision Domain هاست . تمامی هاب های به‌کاررفته در شبکه پایین تشکیل یک Collision Domain را می‌دهند . به یاد دارید که هاب ها فقط ارتباط‌دهنده دستگاه‌ها به یکدیگر هستند .

بریج در شبکه بالا ، تشکیل‌دهنده Collision Domain 3 است . بریج مانند سوییچ ، هر پورت آن جداکننده Collision Domain هاست .

در شبکه سمت چپ 3 عدد سوییچ داریم . که مجموع آن‌ها Collision Domain 5 را ایجاد می‌کند .

برای تمرین بیشتر بر روی شکل شماره 5 ، ادامه دهید . می‌توانید Collision Domain 12 را پیدا کنید ؟

سناریو برای دنیای واقعی :

" آیا باید سوییچ‌های 10/100 خود را جایگزین کنیم ؟ "

فرض کنید شما مسئول یک شبکه هستید ، مدیر پیش شما می‌آید و می‌گوید: درخواست شما برای تعویض سوییچ‌های شبکه یا مدل‌های پرسرعت را بررسی کرده اما مبلغ پیشنهادی بسیار بالاست . آیا لزومی برای انجام آن وجود دارد ؟

اگر شما امکان استفاده از دستگاه‌هایی با بهترین توان را داشته باشید ، حتماً باید از آن استفاده کنید . به دلیل اینکه سوییچ‌هایی با سرعت بالاتر ، کارایی بهتری نیز دارند . اما در دنیای واقعی در بیشتر مواقع مشکل تأمین مالی یا همان بودجه رادارید . اگر شبکه در حال حاضر به‌درستی کار می‌کند پس فعلاً برای ارتقا آن دست نگه‌دارید ، در صورت نیاز در آینده نیز می‌توانید آن‌ها را با مدل‌های پرسرعت تعویض کنید .

سؤال دیگر می‌تواند این باشد : آیا واقعاً تمامی کاربران ما نیاز به پورت 1 Gbps دارند ؟ سرورها ، کامپیوترها و بقیه دستگاه‌ها ؟ شما به‌احتمال‌زیاد در سوییچ‌های لایه Core احتیاج به‌سرعت بالایی دارید اما معمول این سرعت برای کاربران عادی موردنیاز نیست .

شما می‌توانید 1 Gbps و یا حتی 10 Gbps را برای تمامی کاربران خود در نظر بگیرید ، به‌شرط آن‌که توانایی پرداخت تمامی هزینه‌های آن را نیز داشته باشید .

مدل‌های ارتباط شبکه : (Internetworking Models)

ابتدا کمی از تاریخ ایجاد ارتباط بین کامپیوترها صحبت کنیم : زمانی که شبکه‌ها به وجود آمد ، کامپیوترها فقط قادر بودن با کامپیوترهایی از نوع خودشان ارتباط برقرار کنند . به‌عنوان‌مثال کامپیوترهایی که از DECnet استفاده می‌کردند نمی‌توانستند با کامپیوترهایی از تکنولوژی IBM ارتباط برقرار کنند . در سال 1970 یک مدل مرجع به نام Open System Inter Connection (OSI) توسط سازمان International Organization for Standard (ISO) به وجود آمد .

هدف از ایجاد این پروتکل استاندارد ، برقراری ارتباط بین دستگاه‌های مختلف که از نرم‌افزارهای مختلف با تکنولوژی‌های گوناگون استفاده می‌کنند بود .

مدل OSI معماری اصلی برای شبکه است . این مدل نحوه ارسال اطلاعات از نرم‌افزار یک کامپیوتر به رابط شبکه و دریافت آن توسط نرم‌افزار کامپیوتر دیگر را شرح می‌دهد .

مدل OSI به لایه‌های کوچک‌تر تقسیم می‌شود .

" ISO و OSI و در ادامه نیز با IOS آشنا می‌شوید ! ممکن است کمی گیج‌کننده باشد . فقط به خاطر داشته باشید : ISO شروع به ساخت OSI کرد و بعدازآن سیسکو Internetworking Operating System (IOS) را ساخت "

عملکرد لایه‌ها :

درک مدل OSI و چگونگی عملکرد لایه‌ها کمک می‌کند تا نحوه ارتباط بین دستگاه‌های را در شبکه متوجه شویم . لایه‌ها به‌صورت طبقه‌بندی‌شده (Hierarchical) قرار می‌گیرد . هر لایه وظیفه مخصوص به خود را دارد .

برای درک بهتر فرض کنید شما به همراه دوستان خود قصد تأسیس یک شرکت رادارید . در ابتدا شما شروع به تقسیم وظایف می‌کنید . هر فرد چه‌کاری را باید انجام دهد و چه مسئولیتی به عهده دارد . شما باید کارهای شرکت را به بخش‌های مختلف سازمان‌دهی کنید . مثلاً بخش فروش ، بخش انبار و ... . هر بخش فقط بر روی کار خود متمرکز می‌شود تا آن را به بهترین نحو انجام دهد اما در انتها تمامی بخش‌ها به یکدیگر مربوط هستند و کار شرکت را به‌پیش می‌برند .

در مدل OSI نیز ، هر لایه مانند بخش‌های مختلف شرکت وظایف مخصوص به خود را دارد و درنهایت وظیفه اصلی که برقراری ارتباط است را انجام می‌دهند .

مدل مرجع OSI :

بهترین هدیه که مدل OSI به ما می‌دهد ، یک‌راه هموار برای تبادل ارتباط بین کاربران با سیستم‌عامل‌های متفاوت است . مانند لینوکس ، ویندوز و مک و حتی تلفن‌های هوشمند .

و فراموش نکنید ، OSI یک مدل منطقی است نه فیزیکی ! و دستور عمل‌هایی برای برنامه‌نویس‌ها وجود دارد تا اپلیکیشن ها را بر روی شبکه اجرا کنند .

OSI از هفت لایه تشکیل‌شده است که به دو بخش تقسیم می‌شود . سه لایه بالا مشخص می‌کند که اپلیکیشن ها در دو سمت ، چگونه با یکدیگر ارتباط برقرار کنند . چهار لایه پایین وظیفه انتقال داده‌ها را بر عهده دارد .

شکل 7 ، نشان‌دهنده 3 لایه بالایی است :

Application	تامین کننده رابط کاربر
Presentation	ارائه دیتا پردازش اطلاعات و رمزنگاری
Session	نگه دارنده اطلاعات جدا شده نرم افزارها

(7)

با توجه به لایه‌های بالا ، متوجه می‌شویم که کاربر توسط لایه Application با کامپیوتر ارتباط برقرار کرده و توسط دولایه دیگر نیز ، ارتباط بین نرم‌افزارها برقرار می‌شود . هیچ‌کدام از لایه‌های بالا ، آگاهی از شبکه و یا آدرس‌های شبکه ندارند زیرا ، این وظیفه 4 لایه پایین است .

در شکل 8 وظایف لایه‌های پایین را مشاهده می‌کنید . شما می‌توانید ببینید که این لایه‌ها مشخص می‌کنند که اطلاعات چگونه در داخل مدیا مانند سیم ، کابل ، فیبر ، سوییچ‌ها و روتر ها عبور کند . این لایه‌ها همچنین مشخص می‌کنند که اطلاعات چگونه از مبدأ کپسوله و در مقصد انکپسوله شوند .

Transport	مشخص کننده UDP و TCP اصلاح کننده error ها قبل از ارسال مجدد
Network	تامین کننده آدرس های منطقی (IP) که روتر ها توسط آن می توانند مسیر بسته ها را مشخص کنند
Data Link	ترکیب بسته ها به بایت در داخل فریم اجازه دسترسی مدیا به Mac Address مشخص کردن error ها (اصلاح نمی کند)
Physical	انتقال اطلاعات به صورت بیت مشخص کننده میزان ولتاژ ، سرعت کابل و ...

می‌توان برای حفظ کردن لایه‌ها ، از حروف اول آن‌ها استفاده کرد :

All People Seem To Need Data Processing

شکل شماره 9 ، توابع تعریف‌شده در هر لایه را نشان می‌دهد :

Application	• File, print, message, database, and application services
Presentation	• Data encryption, compression, and translation services
Session	• Dialog control

Transport	• End-to-end connection
Network	• Routing

Data Link	• Framing
Physical	• Physical topology

در شکل بالا ، لایه‌ها را به 3 دسته تقسیم کرده‌ایم .لایه‌های بالایی وظیفه ارتباط بین نرم‌افزار و کاربر را به عهده دارد ، لایه‌های میانی وظیفه فراهم کردن ارتباطی قابل‌اعتماد و مسیریابی اطلاعات در بین شبکه‌ها را بر عهده دارد و لایه‌های انتهایی وظیفه ارتباط در شبکه محلی (LAN) را انجام می‌دهد .

با توجه به توضیحات داده‌شده ، حالا می‌توانیم لایه‌ها را با جزییات تشریح کنیم .

The Application Layer :

لایه Application درواقع نقطه ارتباط کاربر با کامپیوتر است اما به‌تنهایی برای ارتباط با شبکه کافی نیست . مثال را در مورد مرورگر (IE) کامپیوتر می‌زنیم . فرض کنید بر روی کامپیوتر خود تمامی اجزای شبکه را پاک می‌کنید ، مانند : کارت شبکه ، پروتکل TCP/IP ولی شما همچنان می‌توانید صفحات HTML که بر روی کامپیوتر خود ذخیره دارید (local) مشاهده کنید . اما اگر بخواهید این صفحات را بر از طریق شبکه و یا اینترنت مشاهده کنید این کار امکان‌پذیر نیست .

درواقع لایه Application رابطی است میان نرم‌افزارهای کامپیوتر شما و لایه‌های پایینی که ارتباط با شبکه را برقرار می‌کنند . درواقع جستجوگر شما به‌عنوان یکی از لایه‌های مدل OSI به‌حساب نمی‌آید . آن وسیله ارتباطی (interface) برای اجرای پروتکل‌هایی است که شما نیاز دارید اطلاعات صفحات وب را در شبکه مشاهده کنید .

" لایه Application به‌عنوان یک رابط برای نرم‌افزارهای نصب‌شده بر روی کامپیوتر عمل می‌کند . در فصل‌های آینده نحوه کارکرد پروتکل TCP/IP و چند برنامه مهم که در این لایه کاربرد فراوانی دارد مانند : Telnet , FTP و TFTP را با جزییات خواهم گفت "

The Presentation Layer :

کارکرد لایه Presentation از اسم آن مشخص است : این لایه اطلاعات را به لایه Application ارائه می‌دهد و همچنین وظیفه ترجمه دیتاها و کد کردن آن‌ها را نیز به عهده دارد .

یک‌راه مطمئن برای انتقال اطلاعات این است که ابتدا دیتاها را قبل از انتقال به فرمت استاندارد تبدیل کنیم . از این طریق لایه Presentation مطمئن می‌شود که لایه Application در دستگاه مقصد می‌تواند اطلاعات را به‌درستی بخواند .

The Session Layer :

وظیفه این لایه راه‌اندازی ، مدیریت و اتمام session های (راه‌های ارتباطی ایجادشده بین دو دستگاه) بین لایه‌های Presentation دستگاه‌های مبدأ و مقصد است و همچنین نگه‌داری دیتاهای پراکنده کاربران .

نحوه چگونگی برقراری ارتباط به‌عنوان‌مثال بین یک کاربر و یک سرور در این لایه انجام می‌شود مانند : half duplex , full duplex .

Half duplex نوعی از ارتباط است که در یک‌زمان فقط یکی از دستگاه‌ها می‌تواند اطلاعات ارسال کند و دستگاه دیگر فقط باید گوش دهد تا نوبت به آن برسد . مانند ارتباط دستگاه‌های بی‌سیم واکی تاکی که درآن‌واحد فقط یک نفر می‌تواند صحبت کند .

Full duplex : ارتباط همزمان دوطرفه است که درآن‌واحد هر دو طرف می‌توانند اطلاعات را ارسال و دریافت کنند بدون اینکه تداخلی به وجود آید مانند مکالمه با تلفن‌های معمول .

The Transport Layer :

سرویس‌های واقع در لایه Transport ، تمامی بخش‌های دیتاها را از لایه‌های بالا جمع‌آوری کرده سپس آن را در یک‌رشته دیتا یکسان قرار می‌دهد . این پروتکل‌ها همچنین وظیفه ایجاد یک ارتباط منطقی بین دستگاه فرستنده و گیرنده رادارند .

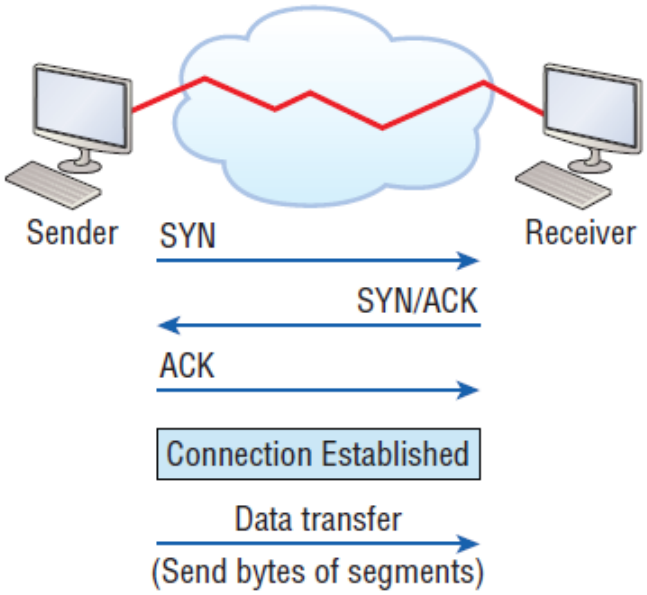
دو پروتکل شناخته‌شده در این لایه TCP و UDP هستند . اگر آشنا با این دو پروتکل نیستید نگران نباشید . در فصل‌های آینده به‌صورت کامل در مورد آن‌ها صحبت خواهیم کرد اما فعلاً تا همین حد بدانید که TCP به‌عنوان یک پروتکل قابل‌اطمینان عمل می‌کند ولی UDP نه ! این به برنامه‌نویس‌ها اختیارات بیشتری می‌دهد ، آن‌ها می‌توانند در هنگام طراحی نرم‌افزار ، از بین این دو پروتکل یکی را انتخاب کنند . (هرکدام از این دو دارای ویژگی‌هایی هستند که در فصل‌های آینده با آن آشنا می‌شوید)

Connection-Oriented Communication

برای ایجاد یک ارتباط قابل‌اعتماد ، دستگاه مبدأ ابتدا باید یک ارتباط پایدار با دستگاه مقصد برقرار کند . این روش به نام three-way handshake شناخته می‌شود . وقتی انجام این پروسه کامل شد انتقال اطلاعات انجام می‌گیرد .

شکل شماره 10 ، مراحل انجام three-way رابین دو سیستم فرستنده و گیرنده نشان می‌دهد :

هر دو سیستم‌عامل با فرستادن پیغام‌هایی بر روی شبکه ، آمادگی خود را برای برقراری ارتباط اعلام می‌کنند .



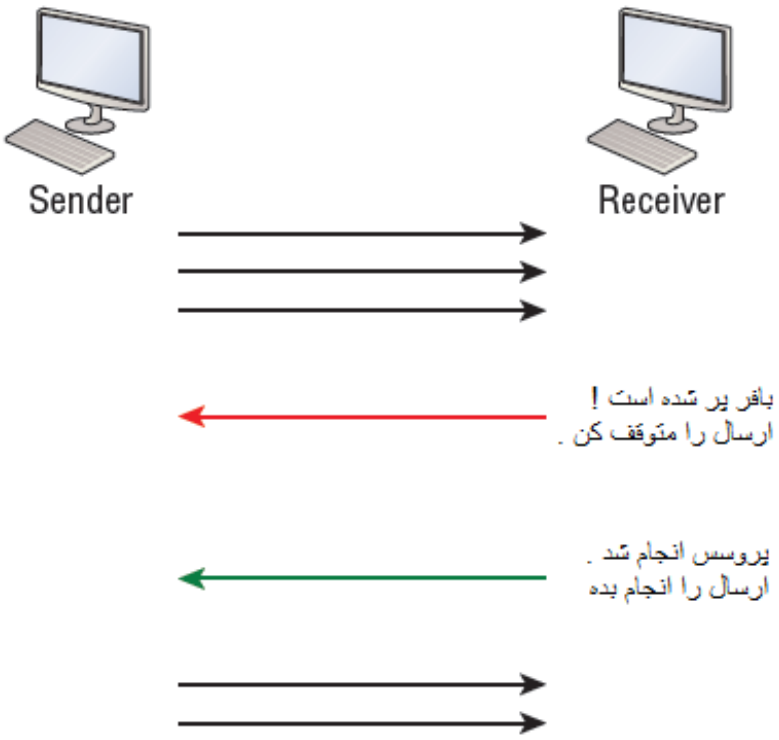
(10)

- ابتدا سیستم مبدأ یک پیغام Synchronization ارسال می‌کند .
- سیستم مقصد با دریافت آن ، در صورت آماده بودن با پیغام Acknowledge ، به همراه پیغام SYN ، آمادگی خود را اعلام می‌کند .
- درنهایت سیستم ارسال‌کننده با فرستادن یک ACK ، موافقت خود را اعلام کرده و ارتباط برقرار می‌شود .

بعد از برقراری ارتباط ، اطلاعات بین دو سیستم انتقال پیدا می‌کند . تا اینجای کار به نظر نباید مشکلی ایجاد شود اما ممکن است در فرایند انتقال دیتاها مشکلاتی به وجود آید . ممکن است سیستم ارسال‌کننده دارای سرعت بالاتری نسبت به مقصد باشد . در این حالت اطلاعات با سرعت بر روی شبکه ارسال می‌شود اما سیستم مقصد توان دریافت تمامی آن‌ها را ندارد . برای حل این مشکل حافظه‌ای در سیستم طراحی‌شده است که اطلاعات اضافی در آن ذخیره شود تا سیستم در فرصت مناسب بتواند آن را تحلیل کند . به این حافظه بافر (buffer) گفته می‌شود . اما بافر نیز ظرفیت محدودی دارد و در حجم اطلاعات بالا می‌تواند سرریز (overflow) شود .

Flow Control :

ازآنجایی‌که سرریز شدن اطلاعات باعث از بین رفتن آن‌ها می‌شود ، راه‌حلی برای آن در نظر گرفته‌شده که به آن Flow Control می‌گویند . وظیفه آن جلوگیری از ارسال اطلاعات از طرف سیستم فرستنده، زمانی که حافظه بافر آن پرشده است . نحوه انجام پروسه به ترتیب زیر است :



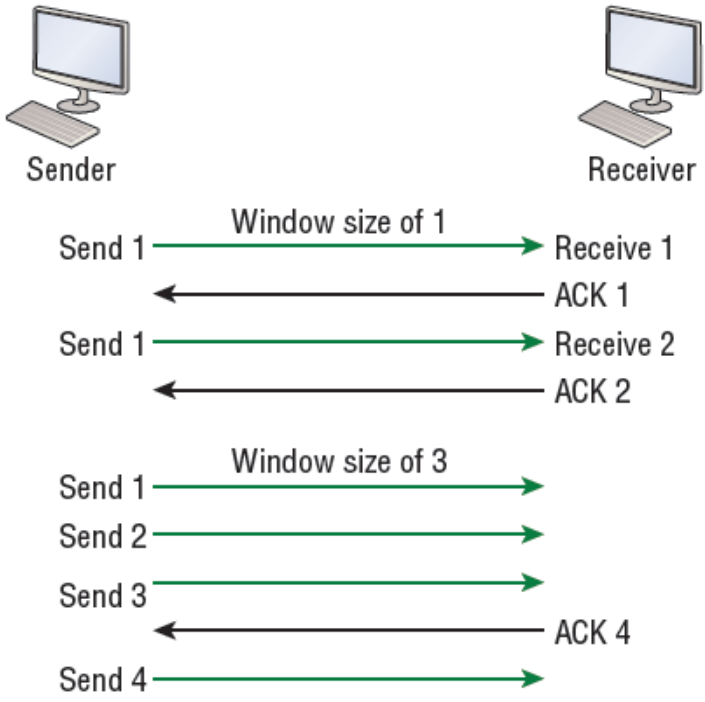
(11)

Windowing :

در ارتباط قابل‌اعتماد ، سیستم ارسال‌کننده اطلاعات برای هر بسته‌ای که می‌فرستد باید به پیغام ACK از سیستم گیرنده دریافت کند . حال در نظر بگیرید چقدر سرعت انتقال اطلاعات می‌تواند کم شود اگر قرار باشد برای هر قسمتی که ارسال می‌شود یک پیغام ACK دریافت گردد ، به همین دلیل از فلگی (Flag) به نام Window استفاده می‌شود .

" فلگ Windows برای کنترل مقدار دیتایی که بدون دریافت ACK می‌تواند انتقال یابد استفاده می‌شود "

مقدار Window مشخص می‌کند که چه میزان از اطلاعات فقط با دریافت یک ACK جابه‌جا شود . فرض کنید ارتباط بین دو سیستم مانند شکل 12 برقرارشده است . ابتدا یک بسته ارسال می‌شود و ACK آن نیز دریافت می‌گردد . سپس بسته دوم ارسال می‌شود و بازهم به‌درستی ACK به سیستم ارسال‌کننده می‌رسد . سیستم ارسال‌کننده متوجه می‌شود که بستر ایجادشده با سیستم دیگر تا حدی قابل‌اعتماد است . به همین دلیل در نوبت بعدی مقدار فلگ Window را 3 قرار می‌دهد تا سیستم دریافت‌کننده متوجه شود ، تا سه بسته نیازی به ارسال ACK وجود ندارد . مقدار Window با توجه به شرایط ارتباطی می‌تواند بالا رود و همان نسبت میزان سرعت ارتباط .

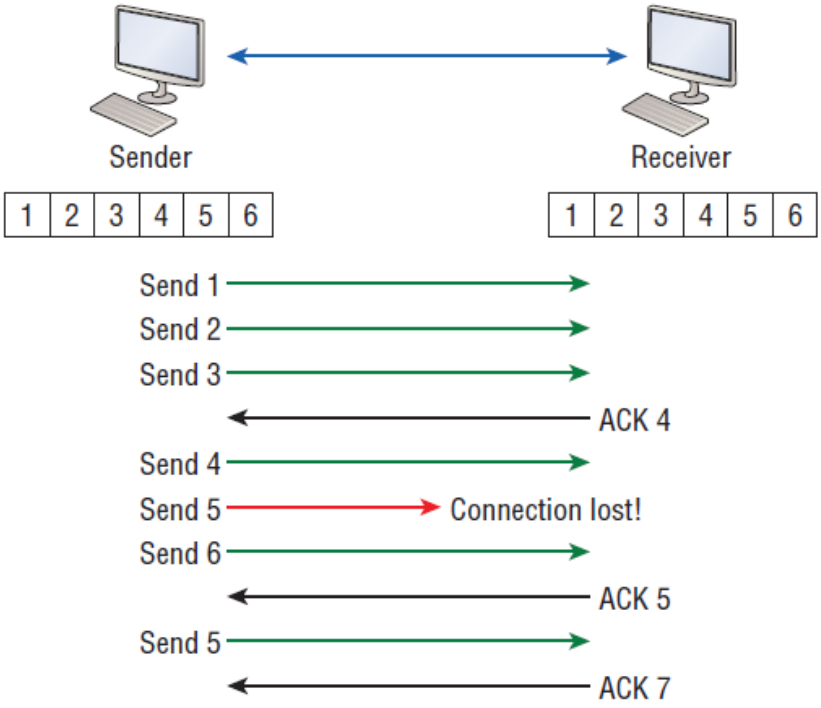


(12)

" اگر سیستم گیرنده نتواند تمامی اطلاعات را به‌درستی دریافت کند ، سیستم فرستنده می‌تواند مقدار Window را کاهش دهد "

Acknowledgments :

همان‌طور که گفتیم در یک ارتباط قابل‌اطمینان ،به ازای هر بسته‌ای که از طرف فرستنده ارسال می‌شود ، انتظار یک ACK از طرف گیرنده را دارد . این نوع ارتباط می‌تواند تضمین‌کننده انتقال اطلاعات به‌صورت سالم باشد . شکل شماره 13 نحوه انجام تبادل اطلاعات و دریافت پیغام ACK را نشان می‌دهد .



(13)

همان‌طور که مشاهده می‌کنید ، اگر در حین برقراری ارتباط مشکلی به وجود بیاید و بسته به دست گیرنده نرسد ، سیستم دریافت‌کننده فقط با ارسال ACK موردنظر ، کامپیوتر ارسال‌کننده را باخبر کرده تا آن را دوباره ارسال کند .

The Network Layer :

Network Layer یا لایه 3 ، آدرس دستگاه‌های را مدیریت می‌کند . موقعیت آن‌ها را بر روی شبکه مشخص کرده و بهترین مسیر برای رسیدن بسته‌ها به آدرس مقصد را تعیین می‌کند . این به معنی آن است که دستگاه‌هایی که در لایه 3 کار می‌کنند مانند روتر ، وظیفه ارتباط شبکه‌های مختلف را بر عهده‌دارند و در شبکه‌های محلی (LAN) استفاده نمی‌شوند .

نحوه کار آن‌ها به این صورت است :

ابتدا که بسته‌ای به یکی از اینترفیس های روتر می‌رسد ، آدرس (IP Address) مقصد آن چک می‌شود . روتر به جدولی که دارد (Routing Table) نگاهی می‌اندازد تا متوجه شود که بسته را از طریق کدام اینترفیس خود باید منتقل کند . اگر در جدول خود مسیری برای آدرس مقصد بسته داشته باشد آن را هدایت می‌کند ، در غیر این صورت روتر بسته را از بین می‌برد ! توجه داشته باشید روتر برخلاف سوییچ ، فقط بسته‌هایی که آدرس مقصد آن‌ها در جدولش وجود داشته باشد را منتقل می‌کند .

دیتا و بسته‌های آپدیت دو نوع از بسته‌هایی هستند که در لایه Network استفاده می‌شوند :

Data packets :

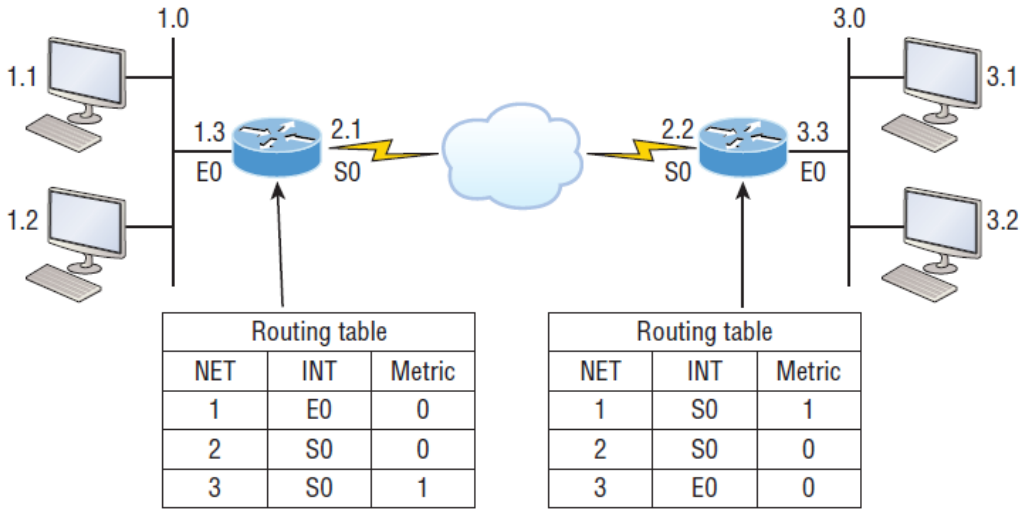
بسته‌هایی که توسط آن‌ها اطلاعات کاربران انتقال پیدا می‌کند . پروتکل‌هایی که برای این کار استفاده می‌شوند را Routed Protocols می‌گویند مانند IP و IPv6 . در فصل 3 IP Address ها را به‌صورت کامل پوشش خواهیم داد .

Route update packet :

این بسته‌ها برای انتقال آپدیت روترهای همسایه به یکدیگر استفاده می‌شود . که شامل توسط آن روترها به یکدیگر شبکه‌های متصل به خود را خبر می‌دهند .

پروتکل‌هایی که این کار را انجام می‌دهند را Routing Protocols می‌نامند . مانند :RIP , EIGRP و OSPF . آپدیت‌ها به روتر کمک می‌کند تا جدول خود را کامل کند .

برای درک بهتر ، به شکل شماره 14 دقت کنید . در این مثال از دو روتر استفاده‌شده است که هرکدام توسط اینترفیس های خود به یک شبکه متصل هستند .



Routing table		
NET	INT	Metric
1	E0	0
2	S0	0
3	S0	1

Routing table		
NET	INT	Metric
1	S0	1
2	S0	0
3	E0	0

(14)

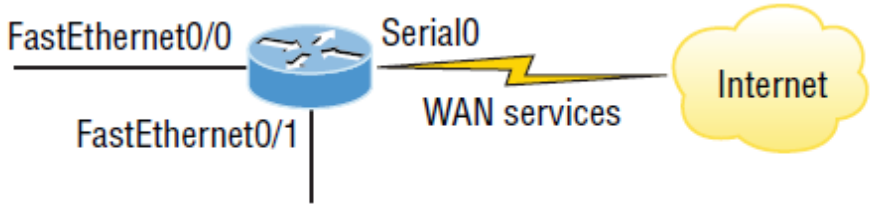
Network Addresses : بخش اول جدول که با NET مشخص‌شده است . Routing table باید برای هر پروتکل مسیریابی (Routing Protocol) یک بخش مجزا داشته باشد . برای مثال ، جدول مسیریابی برای IP ، IPv6 و IPX باید جدا از یکدیگر باشد .

Interface : مشخص‌کننده اینترفیس خروجی است که بسته برای رسیدن به مقصد باید از آن خارج شود .

Metric : مقدار فاصله تا شبکه را تعیین می‌کند . همان‌طور که گفتیم بخشی از اطلاعاتی که بین روتر ها تبادل می‌شود مربوط به Routing Protocol هاست . هر پروتکل فاصله تا شبکه مقصد را توسط فرمول منحصربه‌فرد خود محاسبه می‌کند که حاصل آن عددی می‌شود که در جدول روتینگ به‌عنوان Metric قرار می‌گیرد . در فصل 8 و 9 به‌صورت کامل در مورد آن صحبت خواهیم کرد .

خب همان‌طور که قبلاً گفتیم ، روترها جداکننده Broadcast domain هستند ، به این معنی که اگر پیغام Broadcast به آن‌ها برسد آن را از بین می‌برند و اجازه عبور نخواهند داد . به یاد دارید که این خاصیت چه فایده‌ای داشت ؟ همین‌طور روترها جداکننده Collision domain ها نیز بودند . البته سوییچ‌ها در لایه 2 نیز Collision domain ها را جدا می‌کنند .

با توجه به شکل 15 ، چند ویژگی روترها که نباید آن‌ها ا فراموش کنید :



(15)

- روترها به‌صورت پیش‌فرض پیغام‌های Broadcast و Multicast را عبور نمی‌دهند
- روترها از آدرس‌های منطقی (IP Address) برای هدایت بسته‌ها به مقصد استفاده می‌کنند .
- روترها می‌توانند از Access list ها ، که توسط ادمین شبکه ایجاد می‌شود برای کنترل امنیت شبکه استفاده کنند .
- روترها می‌توانند ارتباط بین virtual LAN (VLAN) ها را برقرار کنند .
- روترها همچنین برای تأمین quality of service (QOS) که یک نوع خاص از ترافیک شبکه است استفاده می‌شوند .

" نگران متوجه نشدن اصطلاحاتی مانند VLAN و یا QOS نباشید . تا انتهای دوره CCNA به‌تمامی آن‌ها به‌صورت کامل اشاره خواهیم کرد . هدف از گفتن آن‌ها در این بخش ، اشاره به ویژگی دستگاه‌های لایه 3 است "

The Data Link Layer :

لایه Data Link ، وظیفه انتقال اطلاعات بر اساس آدرس‌های فیزیکی (Mac Address) و دسته‌بندی ارور های به وجود آمده را بر عهده دارد . و همچنین اطلاعات لایه Network را برای استفاده لایه Physical آماده می‌کند .

فرمتی که لایه دیتا بسته‌ها را آماده می‌کند ، فریم (Frame) نامیده می‌شود . در این لایه آدرس‌های فیزیکی مبدأ و مقصد به بسته‌ها اضافه می‌شود .

مهم است که بدانید بسته‌هایی که بین کاربران منتقل می‌شوند ، حاوی فقط اطلاعات خالص نیستند ! برای اینکه یک بسته به کاربر دیگر برسد ، لازم است بر روی آن اطلاعاتی مانند آدرس مبدأ و مقصد اضافه شود . هر لایه بر روی بسته‌ها ، اطلاعات خود را اضافه می‌کند . این اطلاعات اضافی با رسیدن به سیستم مقصد از بسته اصلی جداشده و دوباره به حالت اول تبدیل می‌شود .

در IEEE Ethernet Data Link دو زیر لایه قرار دارد :

Media Access Control (MAC) :

مشخص‌کننده ارسال بسته‌ها در شبکه محلی (LAN) است و همچنین وظیفه خطایابی (اصلاح نمی‌کند) را در شبکه به عهده دارد .

Logical Link Control (LLC) :

این را به خاطر داشته باشید که همیشه لایه‌های OSI فقط می‌توانند با لایه‌های بالا و پایین خود در ارتباط باشند . و برای این ارتباط نیاز است که دیدی نسبت به این لایه‌ها داشته باشند . وظیفه LLC در لایه Data Link ، ارتباط با لایه Network است و با شناسایی پروتکل در این لایه ، فریم را کپسوله می‌کند . به‌عنوان‌مثال اگر یک فریم به سیستم یک کاربر برسد ، با نگاه به LLC می‌تواند IP Protocol آن را تشخیص دهد .

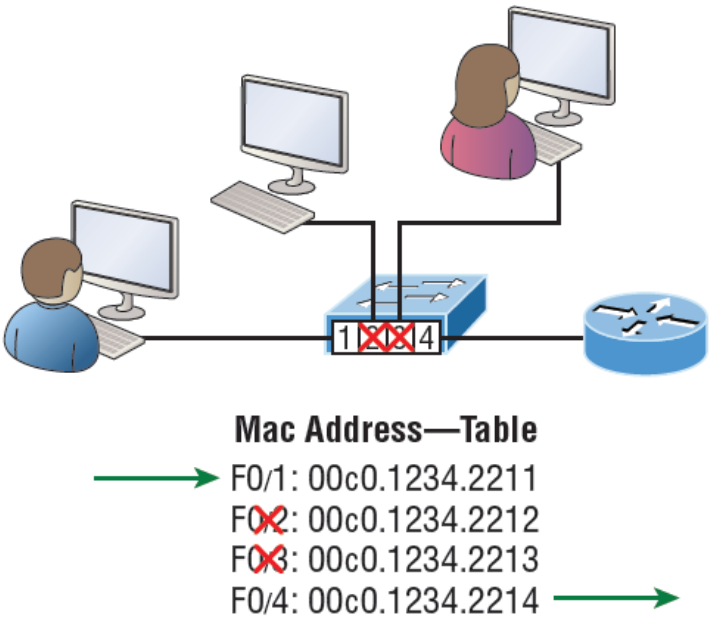
LLC همچنین وظیفه Flow Control (در بخش قبلی کارکرد آن را توضیح دادیم) را نیز به عهده دارد .

" هر لایه با توجه به نیاز قسمت‌هایی را به بسته‌ها اضافه می‌کند ، بسته در هر لایه اسمی دارد :

اسم بسته	لایه
Segment	Transport
Packet	Network
Frame	Data Link
Bits	Physical

سوییچ در لایه Data Link :

سوییچ با عبور هر فریم از پورت‌های آن ، آدرس سخت‌افزاری (Mac Address) آن را در جدول خود ثبت می‌کند . این اطلاعات به سوییچ کمک می‌کند که با رسیدن بسته‌های بعدی ، با توجه به MAC آن ، بسته را به محل درست هدایت کند . شکل 16 نحوه کارکرد سوییچ در داخل یک شبکه را نشان می‌دهد .



(16)

در این سناریو ، John می‌خواهد بسته‌ای را به سمت شبکه بیرون (توسط روتر) ارسال کند . در داخل فریم آدرس MAC روتر در داخل بسته قرار می‌گیرد . سوییچ با دریافت بسته ابتدا آدرس MAC آن را می‌خواند و با توجه به جدول خود آن را فقط به سمت پورت متصل به روتر هدایت می‌کند . توجه داشته باشید که دیگر پورت‌های سوییچ این بسته را دریافت نمی‌کنند . البته این نکته را نیز بدانید که اگر بسته‌ای به سوییچ برسد و آدرس MAC آن در داخل جدول قرار نداشته باشد ، سوییچ آن را به‌تمامی پورت‌ها ارسال می‌کند .

کارکرد تمامی دستگاه‌های شبکه بر اساس پیدا کردن مکان مناسب برای ارسال بسته‌هاست . هم در لایه 2 و هم 3 دستگاه‌هایی که در آن کار می‌کنند باید ب درستی بدانند که بسته دریافتی به کجا ارسال می‌شود . دستگاه‌ها در لایه 3 (مانند روتر) آدرس شبکه‌های مختلف را در جدول خود قرار می‌دهند . دستگاه‌ها در لایه 2 (مانند سوییچ و بریج) ، آدرس MAC دستگاه‌های دیگ را در جدول قرار می‌دهند .

در لایه 2 ، اگر پیغام Broadcast دریافت شود ، سوییچ آن را به‌تمامی پورت‌ها ارسال می‌کند . اگر این پیغام‌ها افزایش یابد می‌تواند باعث کم شدن کارایی شبکه شود و تنها راه جلوگیری از پیغام‌های Broadcast استفاده از یک دستگاه لایه 3 مانند روتر است .

Physical Layer :

و در انتها لایه فیزیکی . همان‌طور که قبلاً نیز گفتیم وظیفه این لایه تبدیل بسته‌ها به سیگنال‌های الکتریکی برای انتقال در داخل مدیا یا همان کابل‌ها و رابط‌های شبکه است . این لایه همچنین محل تعیین DCE (Data Communication Equipment) و DTE (Data Terminal Equipment) نیز هست .

DCE محلی است که ارائه‌دهنده سرویس‌های ما قرار دارد (service provider) و DTE محل قرارگیری سرویس‌های مشتری است .