نگاه عمیق به بسته‌های شبکه با استفاده از

Wireshark

کریس سندرز

برگردان: محسن مصطفی جوکار

انتشارات پندار پارس

انتشارات پندارپارس

دفتر فروش: اقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ – تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸ **info@pendarepars.com**

نام کتاب : **نگاه عمیق به بسته‌های شبکه با استفاده از Wireshark**

ناشر : **انتشارات پندار پارس**

تالیف : **کریس ساندرز**

برگردان : **محسن مصطفی جوکار**

چاپ نخست : **مهر ۹۵**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۱۵۰۰۰ تومان** **شابک : ۵-۲۰-۸۲۰۱-۶۰۰-۹۷۸**

فهرست

پیش‌گفتار

ابزار Wireshark برای هر مدیر شبکه و کاربر معمولی ضروری است و دیگر به عنوان یک ابزار کمکی در نظر گرفته نمی شود. Wireshark که در ابتدا با نام Ethereal منتشر شده بود از یک پروژه شخصی به یک پروژه بزرگ و فرلگیر تبدیل شده است و دیگر به عنوان گزینه‌ای مثبت در رزومه‌های کاری وجود ندارد بلکه به عنوان یک "باید" در نظر گرفته می‌شود.

نکته مثبت در مورد Wireshark که آن را متمایز از دیگر برنامه‌های شنود در شبکه کرده است رایگان بودن و کدباز بودن آن است. کدباز بودن به Wireshark این امکان را می‌دهد که توسعه دهندگان از جمله خود شما پروتکل‌های جدید را به آن اضافه کنید و آن را طبق میل خود سفارسی‌سازی کنید. Wireshark از طیف وسیعی از پروتکل‌ها پشتیبانی می‌کند و تقریبا می‌توان گفت پروتکلی وجود ندارد که Wireshark آن را پشتیبانی نکند. با استفاده از این ابزار می‌توانید مشکلات موجود در شبکه را به راحتی ردیابی کنید و به نقطه درست مشکل برسید.

محسن مصطفی جوکار

تابستان ۹۵

قدردانی

در درجه‌ی نخست، می‌خواهم از خداوند به خاطر قدرت، صبر و شکیبایی که برای تکمیل این پروژه به من داد، قدردانی کنم. وقتی فهرست کارهایی که باید انجام می‌دادم، بزرگ و بزرگ‌تر می‌شد و هیچ پایانی هم نداشت، او کسی بود که در تمام زمان‌های پُراسترس، به من کمک می‌کرد.

از Bill، Tyler، Christina و بقیه‌ی تیم No Starch Press که فرصت نگارش این کتاب و اجازه‌ی آزادی خلاقانه را به من دادند، سپاس‌گزارم. از Gerald Combs برای همراهی و ایجاد انگیزه به‌خاطر برنامه Wireshark و همچنین انجام ویرایش‌های فنی این کتاب، قدردانی می‌کنم. سپاس ویژه از Laura Chappell برای ارائه‌ی برخی از بهترین مواد آموزشی در جهت تجزیه و تحلیل بسته‌ها، مانند چندین فایل ضبط شده که در این کتاب آورده شده است.

می‌خواهم شخصا از Tina Nance، Eddy Wright و Paul Fletcher برای کمک به من در طول این مسیر و رسیدن به این نقطه در زندگی حرفه‌ای قدردانی کنم. شما بچه‌ها بزرگ‌ترین مربیان معنوی و حرفه‌ای من و همچنین بهترین دوستانم هستید. همچنین چندین دوست خوب نیز داشتم که در هنگام نوشتن این کتاب مرا تحمل کردند و این به تنهایی یک موفقیت است؛ از Mandy، Barry، Beth، Chad، Jeff، Sarah و Brandon بسیار سپاس‌گزارم. بدون کمک این دوستان، نمی‌توانستم این کار را انجام دهم.

همچنین می‌خواهم از پدر و مادر دوست داشتنی‌ام Kenneth و Judy Sanders قدردانی کنم:

پدرم، با وجود اینکه به یک کامپیوتر تا به حال دست هم نزدید، پشتیبانی و پرورش شما، این کار را شدنی کرد. هیچ چیز بیشتر از این، مرا خوشحال نمی‌کند که بگویید افتخار شما هستم.

مادرم، در هنگام نوشتن این کتاب حدود پنج سال است که از میان ما رفته‌اید، هر چند می‌توانید این موفقیت را ببینید همیشه در قلب من و موتور محرک زندگی من هستید. شور و شوقی که در زندگی به من نشان دادید، چیزی است که در انجام این کار پُر شور از آن الهام گرفتم. این کتاب یک موفقیت بسیار کوچک از آن چیزی است که به من دادید.

مقدمه

وقتی ۹ ساله بودم، نخستین کامپیوترم را خریدم. کامپیوترم پس از یک سال، همزمان با پیشرفت فناوری، خراب شد. نخست، خانواده‌ام توان مالی کافی برای پرداخت هزینه‌ی یک کامپیوتر را نداشتند و پرداخت هزینه‌ی تعمیر آن نیز از لحاظ مالی غیرممکن بود. با این حال، پس از کمی خواندن و آزمایش کردن، خودم کامپیوترم را تعمیر کردم و در اینجا بود که علاقه‌ام به تکنولوژی آغاز شد.

این علاقه از طریق دبیرستان و کالج به شور و شوق تبدیل شد و همان‌طور که شور و شوق در من رشد می‌کرد، توانایی‌هایم نیز به‌طور طبیعی منجر به شرایطی شد که بیشتر نیاز به کاوش شبکه و مشکلات کامپیوتر داشتم. این زمانی بود که با پروژه Wireshark روبه‌رو شدم (در آن زمان Ethereal نامیده می‌شد). این نرم‌افزار به من اجازه‌ی ورود به جهان کاملا جدیدی را می‌داد. توانایی در تجزیه و تحلیل مشکلات در روش‌های جدیدتر و داشتن توانایی برای دیدن پروتکل‌های آغازین بر روی سیم، به من قدرت نامحدودی را در کامپیوتر و عیب‌یابی شبکه می‌داد.

نکته‌ی مهم درباره‌ی تجزیه و تحلیل بسته این است که به‌طور فزاینده‌ای، به یک روش محبوب از حل مسایل و یادگیری بیشتر درباره‌ی شبکه تبدیل شده است؛ با سپاس از پیدایش گروه‌های کاربری، ویکی‌ها و وبلاگ‌ها. تکنیک‌های پوشش داده شده در این کتاب، در حال تبدیل به پیش‌نیاز دانش برخی از مشاغل شده است. تجزیه و تحلیل بسته، یک نیاز برای مدیریت شبکه‌های امروزی است و این کتاب برای شما، نقطه‌ی آغاز یادگیری همه چیزهایی است که نیاز دارید.

چرا این کتاب؟

ممکن است تعجب کنید که چرا این کتاب را باید در برابر کتاب‌های دیگر درباره‌ی تجزیه و تحلیل بسته‌ها بخرید. پاسخ صحیح، در عنوان نهفته است: «تجزیه و تحلیل کاربردی بسته». اجازه دهید با آن روبه‌رو شویم؛ هیچ چیزی به تجربه در دنیای واقعی ضربه نمی‌زند و تنها چیزی که شما را به تجربه های کتاب نزدیک‌تر می‌کند، نمونه‌های کاربردی از تجزیه و تحلیل داده در دنیای واقعی است. نیمه‌ی نخست این کتاب پیش‌نیازهایی برای درک تجزیه و تحلیل بسته‌ها و Wireshark است. نیمه‌ی دوم نیز، به‌طور کامل به سناریوهای عملی اختصاص داده شده است که به آسانی می‌توانید در مدیریت شبکه با آن روبه‌رو شوید.

اگر یک تکنسین شبکه، مدیر شبکه، مدیر ارشد اطلاعات، تکنسین دسکتاپ یا حتی یک کارمند هستید، با استفاده از تکنیک‌های تجزیه و تحلیل بسته‌ها، مقدار فراوانی از درک و دانش را به دست خواهید آورد.

مفاهیم و روش

به‌طور کلی، فردی آرام هستم. بنابراین وقتی‌که یک مفهوم را تدریس می‌کنم، تلاش در انجام این کار به شیوه‌ای آسان دارم. این درباره‌ی زبان مورد استفاده در کتاب نیز صادق است. در هنگام برخورد با یک مفهوم فنی، استفاده از اصطلاحات ویژه آسان است، اما تلاش کرده‌ام که همه چیز را تا جایی که امکان دارد به بهترین روش ارائه دهم. تمام تعاریف را روشن، ساده و بدون هیچ زرق و برق اضافی ارائه کرده‌ام.

اگر واقعا می‌خواهید تجزیه و تحلیل بسته را یاد بگیرید، باید آن را به عنوان نقطه‌ای برای مدیریت مفاهیم در چند فصل نخست کتاب در نظر بگیرید، زیرا برای درک بقیه‌ی کتاب جدایی‌ناپذیر هستند. نیمه‌ی دوم کتاب کاملا مفهومی است. ممکن است نتوانید این سناریوها را دقیقا در کار خود ببینید، اما باید قادر به اعمال مفاهیم یاد گرفته شده در سناریوهایی که با آنها برخورد می‌کنید، باشید.

در اینجا یک تجزیه سریع از فصل‌های کتاب وجود دارد:

فصل ۱: تجزیه و تحلیل بسته‌ها و مبانی شبکه

تجزیه و تحلیل بسته‌ها چیست؟ چگونه کار می‌کند؟ چگونه آن را انجام می‌دهید؟ این فصل شامل اصول آغازین شبکه‌های ارتباطی و تجزیه و تحلیل بسته‌هاست.

فصل ۲ : ارتباط با سیم

این فصل شامل تکنیک‌های گوناگونی است که می‌توانید از آن برای جای دادن یک شنود کننده‌ی شبکه استفاده کنید.

فصل ۳ : مقدمه‌ای بر Wireshark

در اینجا اصول آغازین Wireshark را بررسی می‌کنیم. از کجا آن را دریافت کنیم؟ چگونه از آن استفاده کنیم؟ چه کاری انجام می‌دهد؟ چرا فوق‌العاده است؟ و خیلی از چیزهای خوب دیگر.

فصل ۴ : کار با بسته‌های گرفته شده

وقتی Wireshark را اجرا می‌کنید، می‌خواهید اصول آغازین را در تعامل با بسته‌های گرفته شده بدانید. در اینجا، این موارد را یاد می‌گیرید.

فصل ۵ : ویژگی‌های پیشرفته Wireshark

هنگامی‌که مقدمات را یاد گرفتید، زمان آن رسیده است که با ویژگی‌های پیشرفته Wireshark فراتر بروید. این فصل به کنکاش در این ویژگی‌ها می‌پردازد و پیاده‌سازی اسلسی و چیزهایی که همیشه خیلی آشکار نیست را نشان می‌دهد.

فصل ۶ : پروتکل‌های رایج

این فصل به شما برخی از رایج‌ترین پروتکل‌های ارتباطی شبکه را که در سطح بسته به چشم می‌آیند، نشان می‌دهد. برای درک این‌که چگونه پروتکل‌ها می‌توانند بد عمل کنند، باید نخست درک کنید که چگونه این پروتکل‌ها کار می‌کنند.

فصل ۷ : سناریوهای آغازین

این فصل شامل نخستین مجموعه از سناریوها در دنیای واقعی است. هر سناریو، در قالبی که به آسانی قابل دنبال کردن است، نمایش داده شده و در آن برای هر سناریوی دشوار، تجزیه و تحلیل و راه حل ارائه شده است. این سناریوهای آغازین، که تنها با چند کامپیوتر در برخورد است و مقدار محدودی تجزیه و تحلیل دارد، تنها به عنوان نخستین تجربه است.

فصل ۸ : مبارزه با یک شبکه‌ی کند

به‌طور کلی، رایج‌ترین مشکلی که از تکنسین‌های شبکه به گوش می‌رسد، درباره‌ی عمل‌کرد کُند شبکه است. این فصل به حل این نوع مشکلات اختصاص دارد.

فصل ۹ : تجزیه و تحلیل بر اساس امنیت

امنیت شبکه یکی از بزرگ‌ترین و داغ‌ترین موضوعات در مدیریت شبکه است. به همین دلیل، فصل ۹ تمام جزئیات حل و فصل مسائل امنیتی با تکنیک‌های تجزیه و تحلیل بسته‌ها را شان می‌دهد.

فصل ۱۰ : بو کشیدن چیزهای نامرئی

آخرین فصل از بخش عملی کتاب، مقدمه‌ای درباره‌ی تجزیه و تحلیل بسته‌ها در شبکه‌ی بی‌سیم است. این فصل به بحث درباره‌ی تفاوت میان تجزیه و تحلیل بسته‌ها در شبکه‌های بی‌سیم و سیمی می‌پردازد و یک سناریوی سریع برای تقویت آنچه آموخته‌اید، است.

فصل ۱۱: مطالعه‌ی بیشتر

فصل پایانی کتاب، چکیده‌ای است از آنچه یاد گرفته‌اید و شامل برخی از ابزارهای مرجع و وب سایت هایی است که در هنگام استفاده از تکنیک‌های تجزیه و تحلیل بسته‌های شبکه، ممکن است برای‌تان مفید واقع شود.

نحوه‌ی استفاده از این کتاب

به نظر من، این کتاب به دو روش مورد استفاده قرار می‌گیرد. نخست به عنوان یک متن آموزشی که با خواندن فصل به فصل آن، درک درستی از تجزیه و تحلیل بسته‌ها به دست می‌آورید. این به معنی توجه ویژه به سناریوهای واقعی در چند فصل گذشته است. استفاده‌ی دیگر این کتاب، به عنوان یک

منبع مرجع است. برخی از ویژگی‌های Wireshark ممکن است اغلب استفاده نشود، بنابراین نحوه‌ی استفاده از آنها را فراموش می‌کنید. به همین دلیل، «تجزیه و تحلیل کاربردی بسته» یک کتاب مرجع در کتابخانه‌ی شماست که برای چگونگی استفاده از ویژگی‌ها، نیاز دارید آن را سریع مرور کنید.

دربارهی فایل‌های ضبط شدهی نمونه

تمام فایل‌های ضبط شده‌ای که در این کتاب استفاده شده است در آدرس http://www.nostarch.com/packet.htm در دسترس است. برای به بیشترین حد رساندن پتانسیل این کتاب، توصیه می‌کنم این فایل‌ها را دانلود و از آنها در طول کتاب استفاده کنید.

شماری از این فایل‌ها توسط Laura Chappell از مؤسسه‌ی تجزیه و تحلیل بسته‌ها و دانشگاه Wireshark ضبط شده است. این فایل‌ها به شرح زیر است:

- blaster.pcap
- destunreachable.pcap
- dosattack.pcap
- double-vision.pcap
- email-troubles.pcap
- evilprogram.pcap
- ftp-crack.pcap
- ftp-uploadfailed.pcap
- gnutella.pcap
- hauntedbrowser.pcap
- http-dient-refuse.pcap
- http-fault-post.pcap
- icmp-tracert-slow.pcap
- osfingerprinting.pcap
- slowdownload.pcap
- tcp-con-lost.pcap

فصل ۱

تجزیه و تحلیل بسته و مبانی شبکه

روزانه یک میلیون اطلاعات گوناگون می‌تواند با یک شبکه‌ی کامپیوتری به اشتباه رد و بدل شود؛ از یک نرم‌افزار جاسوسی ساده تا یک پیکربندی اشتباه و پیچیده‌ی یک مسیریاب و حل بی‌درنگ هر مشکلی غیرممکن است. بهترین کاری که می‌توانیم انجام دهیم این است که امیدوار باشیم تا با دانشی که از پیش به دست آورده‌ایم و ابزارهای بایسته، به این نوع از مشکلات پاسخ دهیم. تمام مشکلات بنیادی شبکه از سطح بسته است، جایی که برنامه‌های کاربردی به ظاهر زیبا، می‌توانند پیاده‌سازی وحشتناک خود را آشکار کنند و پروتکل‌های به ظاهر قابل اعتماد، می‌توانند مخرب بودن خود را اثبات کنند. برای درک بهتر و حل مشکلات شبکه، به سطح بسته، جایی که هیچ چیز از ما پنهان نیست، می رویم. جایی که در آن ساختار گمراه‌کننده و مبهم منوی برنامه، گرافیک چشم‌نواز و کارمندان غیر قابل اعتماد وجود ندارد. در اینجا هیچ رازی وجود ندارد و بیشترین کارهای ما در سطح بسته انجام می شود و می‌توانیم شبکه را بیشتر کنترل و مشکلات آن را حل کنیم. این دنیای تجزیه و تحلیل بسته است.

این کتاب به دنیای تجزیه و تحلیل بسته‌ها شیرجه می‌زند. پیش از اینکه ارتباطات شبکه را بررسی کنیم، یاد خواهید گرفت که تجزیه و تحلیل بسته‌ها چیست؟ بنابراین برخی از زمینه‌های اساسی را که برای بررسی سناریوهای گوناگون به آن نیاز دارید، یاد خواهید گرفت. همچنین با چگونگی استفاده از ویژگی های ابزار تجزیه و تحلیل بسته‌ها یعنی Wireshark برای مقابله با شبکه‌های ارتباطی کند، شناسایی تنگناهای برنامه و حتی ردیابی هکرها از طریق برخی از سناریوهای واقعی آشنا خواهید شد. وقتی این کتاب را کامل بخوانید، توانمند خواهید بود تا تکنیک‌های پیشرفته تجزیه و تحلیل بسته‌ها را پیاده سازی کنید و به شما در حل سخت‌ترین مشکلات شبکه کمک خواهد کرد.

تجزیه و تحلیل بسته چیست؟

از تجزیه و تحلیل شبکه، اغلب به عنوان بو کشیدن بسته‌ها یا تجزیه و تحلیل پروتکل یاد می‌شود که فرایند دریافت و تفسیر داده‌های فعال شبکه را برای درک بهتر از آنچه در شبکه رخ می‌دهد، شرح می‌دهد. به‌طور معمول، تجزیه و تحلیل بسته توسط یک برنامه‌ی شنود بسته انجام می‌شود که ابزاری

است، برای گرفتن اطلاعات خامی که در سراسر سیم در حال حرکت است. تجزیه و تحلیل بسته‌ها می تواند به ما در درک ویژگی‌های شبکه، آگاهی از اینکه چه کسی در شبکه است، تعیین اینکه چه کسی یا چه چیزی از پهنای باند موجود استفاده می‌کند شناسایی زمان اوج استفاده از شبکه، شناسایی حملات احتمالی یا فعالیت‌های مخرب و پیدا کردن برنامه‌های کاربردی ناامن یا بیش از حد بزرگ کمک کند.

انواع گوناگونی از برنامه‌های شنود بسته وجود دارد؛ هم تجاری و هم آزاد. هر برنامه با هدف‌های گوناگونی در ذهن طراحی شده است. شماری از برنامه‌های محبوب تجزیه و تحلیل بسته‌ها عبارت‌اند از: tcpdump (یک برنامه خط دستوری)، OmniPeek و Wireshark (هر دو دارای محیط گرافیکی است).

ارزیابی یک برنامه شنود بسته

انواع گوناگونی از برنامه‌های شنود بسته وجود دارد. در هنگام انتخاب یکی از آنها برای استفاده، باید متغیرهای زیر را در نظر بگیرید:

- پروتکل‌های پشتیبانی شده
- کاربر پسند بودن.
- هزینه.
- پشتیبانی برنامه.
- سیستم عامل قابل پشتیبانی.

پروتکل‌های پشتیبانی شده

تمام برنامه‌های شنود بسته می‌تواند پروتکل‌های گوناگون را تفسیر کند. بیشتر برنامه‌های شنود، می تواند رایج‌ترین پروتکل‌ها مانند DHCP، IP و ARP را تفسیر کند، اما نمی‌تواند همه پروتکل‌های غیرسنتی را تفسیر کند. در هنگام انتخاب یک برنامه‌ی شنود، مطمئن شوید از پروتکل‌هایی که قصد استفاده از آنها را دارید، پشتیبانی می‌کند.

کاربر پسند بودن

چیدمان یک برنامه‌ی شنود بسته را در نظر بگیرید. آسانی نصب و جریان کلی از عملیات استاندارد برنامه‌ای که انتخاب می‌کنید، باید با سطح تخصص شما متناسب باشد. اگر تجربه‌ی کمی در تجزیه و تحلیل بسته‌ها دارید، از برنامه‌های پیشرفته‌ی شنود بسته مانند tcpdump که از طریق خط دستور کار

می‌کنند، دوری کنید. برعکس اگر تجربه‌ی فراوانی دارید برنامه‌های پیشرفته‌تر را برای انتخاب، مفید خواهید یافت.

هزینه

نکته‌ی مهم درباره‌ی برنامه‌ی شنود بسته این است که بسیاری از آنها رایگان و با برنامه‌های تجاری در رقابت است. هرگز نباید برای یک برنامه‌ی شنود بسته، پولی پرداخت کنید.

پشتیبانی برنامه

حتی وقتی اصول آغازین برنامه‌ی شنود بسته را آموخته‌اید، احتمالا هنوز هم نیاز به پشتیبانی‌های گاه و بی‌گاه برای حل مشکلات جدیدی که به وجود می‌آید، دارید. وقتی پشتیبانی در دسترس را ارزیابی کردید، به چیزهایی همچون اسناد توسعه، انجمن‌های عمومی و لیست‌های پستی نگاهی بیاندازید. گرچه ممکن است عدم پشتیبانی توسعه برای برنامه‌های رایگان شنود بسته مانند Wireshark وجود داشته باشد، اما جوامعی که اغلب از این برنامه‌ها استفاده می‌کنند، این امکان را فراهم می‌کنند. این جوامع از کاربران و همکاران، تالارهای گفتگو، ویکی‌ها و طراحی بلاگ‌ها برای کمک به شما استفاده می‌کنند.

سیستم عامل قابل پشتیبانی

متأسفانه، تمام برنامه‌های شنود بسته، از همه‌ی سیستم‌های عامل پشتیبانی نمی‌کند. مطمئن شوید برنامه‌ای که برای یادگیری انتخاب کرده‌اید، بر روی تمام سیستم‌های عاملی که نیاز به حمایت دارید، کار می‌کند.

چگونه برنامه‌های شنود بسته کار می‌کند؟

فرایند شنود بسته سه گام است: گردآوری، تبدیل و تجزیه و تحلیل.

گردآوری

در گام نخست، برنامه‌ی شنود بسته کارت شبکه‌ی انتخاب شده را به حالت بی‌قاعده یا فاقد استاندارد تغییر می‌دهد. در این حالت، کارت شبکه می‌تواند به تمام ترافیک شبکه، در بخش دیگر شبکه گوش دهد. برنامه‌ی شنود می‌تواند از این حالت، همراه با دسترسی سطح پایین به کارت شبکه، برای گرد-آوری داده‌های باینری خام از سیم استفاده کند.

تبدیل

در این گام، داده‌های باینری گردآوری شده، به یک قالب قابل خواندن تبدیل می‌شود. در اینجا، برنامه های پیشرفته‌ی شنود که از خط دستور استفاده می‌کنند، متوقف می‌شوند. در این گام، اطلاعات شبکه در فرمی است که می‌تواند تنها در یک سطح بسیار ابتدایی تفسیر شود و بسیاری از تجزیه و تحلیل‌ها به کاربر واگذار می‌شود.

تجزیه و تحلیل

گام سوم و گام پایانی، شامل تجزیه و تحلیل واقعی از اطلاعات دریافت و تبدیل شده است. در این گام، برنامه‌ی شنود، داده‌های شبکه را گردآوری و پروتکل آن را بر اساس اطلاعات استخراج شده، تأیید و بازبینی می‌کند و تجزیه و تحلیل ویژگی‌های ویژه‌ی پروتکل آغاز می‌شود.

تجزیه و تحلیل، بیشتر از طریق مقایسه‌ی بسته‌های گوناگون و همچنین دیگر عناصر شبکه انجام می‌شود.

کامپیوترها چگونه با یکدیگر ارتباط برقرار می‌کنند؟

برای درک کامل تجزیه و تحلیل بسته‌ها، باید درک کنید که چگونه کامپیوترها با یکدیگر ارتباط برقرار می‌کنند. در این بخش اصول آغازین پروتکل‌های شبکه، مدل OSI، فریم‌های داده در شبکه و سخت-افزاری که تمام آن را پشتیبانی می‌کند، بررسی می‌کنیم.

پروتکل‌های شبکه

شبکه‌های مدرن، از انواع سیستم‌های در حال اجرا بر روی سیستم‌های عامل گوناگون ساخته می‌شود. برای کمک به این ارتباط، از مجموعه‌ی زبان‌های رایج که پروتکل شبکه نامیده می‌شود و ارتباطات شبکه را اداره می‌کند، استفاده می‌کنیم. پروتکل‌های رایج شبکه عبارت‌اند از TCP، IP، ARP و DHCP. پشته‌ی پروتکل یک گروه منطقی از پروتکل‌هایی است که با هم کار می‌کنند.

یک پروتکل شبکه، بسته به عملکرد آن می‌تواند بسیار ساده و یا بسیار پیچیده باشد. اگرچه پروتکل-های گوناگون شبکه، اغلب به‌طور چشمگیری متفاوت هستند، اما بیشتر آنها به مسائل زیر رسیدگی می‌کنند:

کنترل جریان: تولید پیام توسط سیستم گیرنده که به سیستم ارسال‌کننده، سرعت انتقال داده را می آموزد.

تصدیق بسته: انتقال یک پیام بازگشت، از سیستم گیرنده به سیستم ارسال‌کننده، برای تصدیق دریافت اطلاعات.

خطایابی: استفاده از کدهایی توسط سیستم ارسال‌کننده، برای بررسی عدم آسیب اطلاعات فرستاده شده در هنگام انتقال.

خطاگیری: ارسال دوباره داده‌هایی که در حین انتقال آغازین، از دست رفته و یا آسیب دیده‌اند.

قطعه‌بندی: تقسیم جریان طولانی داده‌ها، به جریان‌های کوچک‌تر برای انتقال کارآمدتر.

رمزگذاری داده‌ها: تابعی که از کلیدهای رمزگذاری، برای حفاظت از اطلاعات منتقل شده در سراسر شبکه استفاده می‌کند.

فشرده‌سازی داده: یک روش برای کاهش حجم داده‌های منتقل شده در شبکه، با استفاده از حذف اطلاعات زائد.

هفت لایه‌ی مدل OSI

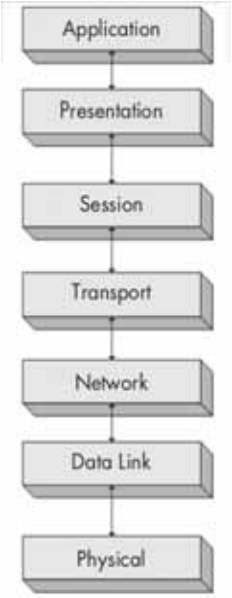
پروتکل‌ها بر اساس عملکرد خود، با استفاده از یک مدل مرجع استاندارد در صنعت که سیستم‌های باز مرتبط به هم (OSI) نامیده می‌شود، از هم جدا می‌شود. در اصل این مدل، در سال ۱۹۸۳ توسط سازمان جهانی استانداردسازی (ISO) به عنوان یک سند که ISO 7498 نامیده می‌شود، منتشر شد.

مدل OSI روند ارتباطات شبکه را به هفت لایه مجزا تقسیم می‌کند:

- کاربرد (لایه ۷)
- نمایش (لایه ۶)
- جلسه (لایه ۵)
- انتقال (لایه ۴)
- شبکه (لایه ۳)
- پیوند داده (لایه ۲)
- فیزیکی (لایه ۱)

هفت لایه در مدل سلسله مراتبی OSI (شکل ۱-۱) درک ارتباطات شبکه را بسیار آسان‌تر می‌کند. لایه‌ی کاربرد در بخش بالا، نشان‌دهنده‌ی برنامه‌های کاربردی است که برای دسترسی به منابع شبکه استفاده می‌شود. لایه‌ی پایینی، لایه‌ی فیزیکی است که از طریق آن داده‌های واقعی شبکه انتقال پیدا می‌کند. پروتکل‌ها در هر لایه، برای بسته‌بندی داده‌ها، برای لایه‌ی بعدی با یکدیگر کار می‌کنند.

نکته: مدل OSI چیزی بیش از یک استاندارد صنعتی توصیه شده نیست و توسعه‌دهندگان پروتکل لازم نیست که دقیقا آن را دنبال کنند. در واقع، مدل OSI تنها مدل موجود شبکه نیست. برای نمونه، برخی از افراد مدل وزارت دفاع (DoD) را ترجیح می‌دهند. در این کتاب درباره‌ی مفاهیم مدل OSI کار می کنیم، بنابراین مدل وزارت دفاع را پوشش نمی‌دهیم.



شکل ۱-۱: سلسله مراتب ۷ لایه مدل OSI

اجازه دهید یک نگاه دقیق به عملکرد هر یک از لایه‌های مدل OSI و همچنین برخی از پروتکل‌های استفاده شده در آنها بیاندازیم.

لایه‌ی کاربرد

لایه‌ی کاربرد، بالاترین لایه در مدل OSI است و ابزاری را برای کاربران فراهم می‌کند تا به منابع واقعی شبکه دسترسی داشته باشند. این تنها لایه‌ای است که به‌طور معمول توسط کاربر دیده می‌شود و رابطی را فراهم می‌کند که به عنوان پایه‌ای برای تمام فعالیت‌های شبکه است.

لایه‌ی نمایش

لایه‌ی نمایش، داده را در قالبی که می‌تواند توسط لایه‌ی کاربرد خوانده شود، انتقال می‌دهد. رمزگذاری و رمزگشایی داده‌ها در این لایه انجام می‌شود و بستگی به پروتکل لایه‌ی کاربرد دارد که داده را ارسال یا دریافت می‌کند. این لایه همچنین چندین نوع از رمزگذاری‌ها و رمزگشایی‌ها را برای تأمین امنیت اطلاعات انجام می‌دهد.

لایه‌ی جلسه

لایه‌ی جلسه، یک گفتگو یا جلسه میان دو کامپیوتر را مدیریت می‌کند. این لایه ایجاد، مدیریت و پایان این ارتباط را در میان تمام دستگاه‌های ارتباطی انجام می‌دهد. لایه‌ی جلسه همچنین مسئول برقراری یک اتصال دوطرفه کامل یا دوطرفه ناقص است و ارتباط شکل گرفته میان میزبان‌ها را به جای رها کردن آن به‌طور ناگهانی، به آرامی می‌بندد.

لایه‌ی انتقال

هدف اصلی لایه‌ی انتقال، فراهم کردن انتقال مطمئن خدمات به لایه‌های پایین‌تر است. از طریق ویژگی هایی مانند کنترل جریان، بخش‌بندی، کامل کردن یا کنترل خطا، لایه‌ی انتقال اطمینان می‌یابد که داده های دریافت شده، نقطه به نقطه خالی از خطا هستند. از آنجا که اطمینان از حمل و نقل قابل اعتماد داده ها می‌تواند بسیار سنگین باشد، مدل OSI یک لایه‌ی کامل را به آن اختصاص داده است. لایه‌ی انتقل، این خدمات را هم به پروتکل‌های اتصال‌گرا و هم به پروتکل‌های بدون اتصال ارائه می‌دهد. فایروال‌ها و سرورهای پروکسی در این لایه کار می‌کنند.

لایه‌ی شبکه

لایه‌ی شبکه، مسئول مسیریابی داده‌ها میان شبکه‌های فیزیکی است و این یکی از پیچیده‌ترین لایه‌های OSI است. این لایه، مسئول آدرس‌دهی منطقی میزبان‌های شبکه (برای نمونه از طریق یک آدرس IP) است و همچنین بخش‌بندی بسته‌ها، شناسایی پروتکل و در برخی موارد تشخیص خطا را انجام می دهد. مسیریاب‌ها در این لایه کار می‌کنند.

لایه‌ی پیوند داده‌ها

لایه‌ی پیوند داده‌ها، شرایط استفاده از داده‌های منتقل شده در سراسر یک شبکه‌ی فیزیکی را فراهم می‌کند. هدف اصلی این لایه، فراهم کردن یک مدل آدرس‌دهی است که می‌تواند برای شناسایی دستگاه های فیزیکی و فراهم کردن ویژگی چک کردن خطا، برای اطمینان از درستی داده‌ها استفاده شود. پل‌ها و سوئیچ‌ها، دستگاه‌های فیزیکی هستند که در این لایه کار می‌کنند.

لایه‌ی فیزیکی

لایه‌ی فیزیکی، در پایین مدل OSI است که رسانه‌های فیزیکی از طریق آن، داده‌های شبکه را منتقل می‌کنند. این لایه ماهیت فیزیکی و الکتریکی تمام سخت‌افزارهای استفاده شده از جمله ولتاژ، هاب‌ها، کارت‌های شبکه، تکرارکننده‌ها و مشخصات کابل‌کشی را تعریف می‌کند. لایه‌ی فیزیکی ارتباطات را ایجاد می‌کند، پایان می‌دهد، ابزاری را برای به اشتراک‌گذاری منابع ارتباطی فراهم می‌کند و سیگنال‌ها را از دیجیتال به آنالوگ و برعکس تبدیل می‌کند.

جدول (۱-۱) لیستی از پروتکل‌های رایج را که در هر لایه از مدل OSI استفاده می‌شود، نشان می‌دهد.

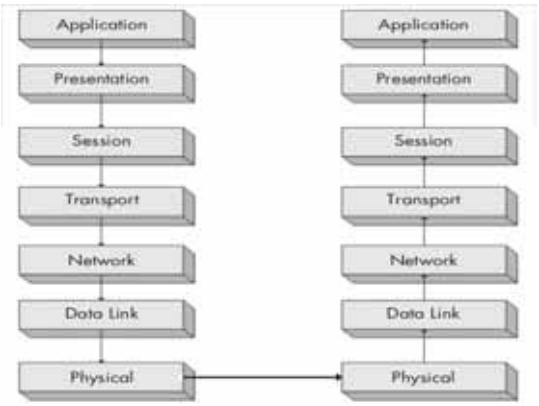
لایه	پروتکل
کاربرد	HTTP, SMTP, FTP, Telnet
نمایش	ASCII, MPEG, JPEG, MIDI
جلسه	NetBIOS, SAP, SDP, NWLink
انتقال	TCP, UDP, SPX
شبکه	IP, ICMP, ARP, RIP, IPX
پیوند داده‌ها	Ethernet, Token Ring, FDDI, AppleTalk

جدول ۱-۱: پروتکل‌های رایج که در هر لایه از مدل OSI استفاده می‌شوند

تعامل پروتکل

داده‌ها چگونه از بالا و پایین مدل OSI جریان پیدا می‌کنند؟ انتقال داده‌های آغازین در شبکه، در لایه‌ی کاربرد سیستم فرستنده آغاز می‌شود. داده‌ها راه خود را در هفت لایه‌ی مدل OSI ادامه می‌دهند تا به لایه‌ی فیزیکی برسند که در آن نقطه، از لایه‌ی فیزیکی سیستم فرستنده، اطلاعات به سیستم دریافت کننده ارسال می‌شود. سیستم دریافت‌کننده، داده‌ها را از لایه‌ی فیزیکی برمی‌دارد و داده‌ها به لایه‌های باقی‌مانده از سیستم دریافت‌کننده، ادامه پیدا می‌کنند تا به لایه‌ی کاربرد در بالا برسند.

سرویس‌ها، به‌وسیله‌ی پروتکل‌های گوناگون در هر سطح از مدل OSI که برکنار نشده‌اند، ارائه داده می‌شود. برای نمونه، اگر یک پروتکل در یک لایه، یک سرویس ویژه را فراهم می‌کند، هیچ پروتکلی در هیچ لایه‌ای، سرویس مشابه را ارائه نمی‌دهد پروتکل‌ها در لایه‌های مربوطه، بر روی کامپیوترهای فرستنده و گیرنده مکمل یکدیگر هستند اگر یک پروتکل در لایه‌ی ۷ کامپیوتر فرستنده، مسئول رمزگذاری داده‌های در حال انتقال است، پروتکل مربوطه بر روی لایه‌ی ۷ کامپیوتر گیرنده، مسئول رمزگشایی داده‌هاست. شکل (۱-۲) یک نمودار گرافیکی از مدل OSI را نشان می‌دهد که مربوط به برقراری ارتباط میان دو سرویس‌گیرنده و فرستنده است. همان‌طور که می‌بینید، ارتباط از بالا به پایین بر روی سرویس فرستنده در حال حرکت است و هنگامی که به سرویس‌گیرنده می‌رسد، معکوس می‌شود.



شکل ۱-۲: پروتکل هم در سیستم فرستنده و هم در سیستم گیرنده بر روی لایه‌ی مشابه کار می‌کند

هر لایه در مدل OSI تنها قادر به برقراری ارتباط به‌طور مستقیم با لایه‌ی بالا یا پایین آن است. برای نمونه، لایه‌ی دوم تنها می‌تواند داده‌ها را به لایه‌های یکم و سوم ارسال و یا از آنها دریافت کند.

کپسوله کردن داده‌ها

پروتکل‌ها در لایه‌های گوناگون، با کمک کپسوله کردن داده‌ها با یکدیگر ارتباط برقرار می‌کنند. هر لایه در پشته، مسئول افزودن یک هدر (header) یا فوتر (footer) به داده‌های در حال ارتباط است و این بیت‌های اضافی از اطلاعات، اجازه می‌دهند تا لایه‌ها با یکدیگر ارتباط برقرار کنند برای نمونه، هنگامی که لایه‌ی انتقال، داده را از لایه‌ی جلسه دریافت می‌کند، پیش از اینکه داده را به لایه‌ی بعدی منتقل کند، اطلاعات هدر مربوط به خود را به آن می‌افزاید.

واحد پروتکل داده

فرایند کپسوله کردن یک پروتکل، واحد داده (PDU) را می‌سازد که شامل داده‌های در حال ارسال و تمام اطلاعات هدر و فوتر افزوده به آن است. همان‌گونه که داده‌ها در مدل OSI حرکت می‌کنند، PDU تغییر می‌کند و به عنوان اطلاعات هدر و فوتر که از پروتکل‌های گوناگون به آن افزوده شده است، رشد می‌کند. PDU در شکل نهایی آن، به لایه‌ی فیزیکی و سپس به کامپیوتر مقصد می‌رسد. کامپیوتر گیرنده، هدرها و فوترهای پروتکل را از PDU به عنوان داده‌هایی که به لایه‌های بالای OSI منتقل می‌شوند، پاک می‌کند. هنگامی که PDU به لایه‌ی بالای مدل OSI می‌رسد، تنها داده‌های اصلی باقی می‌ماند.

نکته: واژه‌ی بسته با واژه‌ی واحد پروتکل (PDU) در ارتباط است. وقتی که از واژه‌ی بسته استفاده می‌کنم به یک PDU کامل که شامل اطلاعات هدر و فوتر از تمام لایه‌های مدل OSI است، اشاره می‌کنم.

سخت‌افزار شبکه

اینک وقت آن است که به سخت‌افزار شبکه نگاهی بیاندازیم، جایی که همه‌ی کارهای کثیف در آن انجام می‌شود. تنها بر روی شمار کمی از سخت‌افزارهای رایج شبکه تمرکز می‌کنیم؛ به ویژه هاب‌ها، سوئیچ‌ها و مسیریاب‌ها.

هاب

به‌طور معمول هاب، چیزی بیش از یک جعبه با چند پورت RJ-45 نیست، مانند هاب Netgear که در شکل (۱-۳) نشان داده شده است. هاب‌ها از هاب کوچک با ۴ پورت تا هاب بزرگ با ۴۸ پورت، برای نصب در یک محیط سازمانی طراحی می‌شوند. هاب‌ها برای اتصال دستگاه‌های شبکه طراحی شده‌اند، به‌طوری که می‌توانند با یکدیگر ارتباط برقرار کنند.

شکل ۱-۳: یک نمونه از هاب چهار پورت اترنت

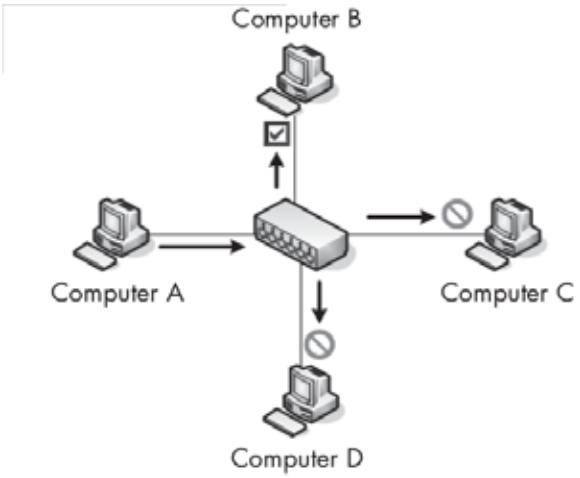
هاب، چیزی بیش از یک دستگاه تکرار که بر روی لایه‌ی فیزیکی از مدل OSI عمل می‌کند، نیست. یک دستگاه تکرار به سادگی بسته‌های فرستاده شده از یک پورت را گرفته و آنها را به هر پورت دیگر بر روی دستگاه منتقل می‌کند. برای نمونه، اگر کامپیوتر بر روی پورت یک از چهار پورت هاب، نیاز به ارسال داده به کامپیوتر دیگر بر روی پورت دو را داشته باشد، هاب بسته را به پورت یک، دو، سه و چهار می‌فرستد. سرویس‌گیرنده‌هایی که به پورت سه و چهار متصل هستند، از داده‌ها چشم‌پوشی می کنند، زیرا داده‌ها برای آنها نیست و آنها بسته را رها می‌کنند. در نتیجه مقدار فراوانی ترافیک غیرضروری ایجاد می‌شود.

تصور کنید ایمیلی را به کارمندان یک شرکت می‌فرستید. ایمیل عنوانی با نام "قابل توجه همه کارکنان بازاریابی" دارد، اما به جای فرستادن آن به کارمندان بخش بازاریابی، آن را به همه‌ی کارکنان شرکت فرستاده‌اید. کارمندانی که در بخش بازاریابی کار می‌کنند، می‌دانند که این ایمیل مربوط به آنهاست و آن را باز می‌کنند. کارمندان دیگر وقتی می‌بینند که ایمیل مربوط به آنها نیست، آن را پاک می‌کنند. می‌توانید ببینید که چگونه این امر در بسیاری از ارتباطات غیرضروری، منجر به اتلاف وقت می‌شود. این دقیقا همان کاری است که هاب انجام می‌دهد.

شکل (۱-۴) تصویری را از آنچه در جریان است، نشان می‌دهد. در این شکل کامپیوتر A اطلاعات را به کامپیوتر B منتقل می‌کند. با این حال زمانی که کامپیوتر A داده‌ها را ارسال می‌کند، تمام کامپیوترهایی که متصل به هاب هستند، آن را دریافت می‌کنند در واقع تنها کامپیوتر B داده‌ها را قبول می‌کند و کامپیوترهای دیگر آن را دور می‌اندازند.

آخرین نکته درباره‌ی هاب این است که تنها قابلیت کار در حالت نیمه دوطرفه را دارد؛ یعنی نمی‌تواند هم‌زمان داده‌ها را ارسال و دریافت کند. این قابلیت آن را از سوئیچ‌ها، که دستگاه‌های دوطرفه کامل هستند و می‌توانند داده‌ها را هم‌زمان ارسال یا دریافت کنند، متمایز می‌کند.

با این حال، هاب‌ها را در شبکه‌های مدرن و با چگالی بالا نخواهید دید (به جای آن از سوئیچ‌ها استفاده می‌شود). از آنجا که هاب‌ها در تجزیه و تحلیل بسته‌ها بسیار مهم هستند، باید بدانید که چگونه کار می‌کنند.



شکل ۱-۴: جریان ترافیک زمانی که کامپیوتر A داده‌ها را از طریق یک هاب به کامپیوتر B می‌فرستد

سوئیچ

بهترین جایگزین برای هاب‌ها در یک شبکه با چگالی یا تولید بالا، دستگاه‌هایی هستند که سوئیچ نامیده می‌شوند. مانند هاب، سوئیچ برای تکرار بسته‌ها طراحی شده است، اما این کار بسیار متفاوت است. همچنین مانند هاب، سوئیچ نیز مسیر ارتباطی را برای دستگاه‌ها اما با بازدهی بیشتر فراهم می‌کند. به جای پخش اطلاعات به تمام پورت‌ها، سوئیچ داده‌ها را تنها به کامپیوتری که داده‌ها برای آن در نظر گرفته شده است، می‌فرستد. از لحاظ فیزیکی، سوئیچ مانند هاب به نظر می‌رسد. در حقیقت، اگر دستگاه، خود را معرفی نکند، ممکن است در دانستن اینکه کدام یک سوئیچ و کدام یک هاب است، سختی داشته باشید (شکل ۱-۵).

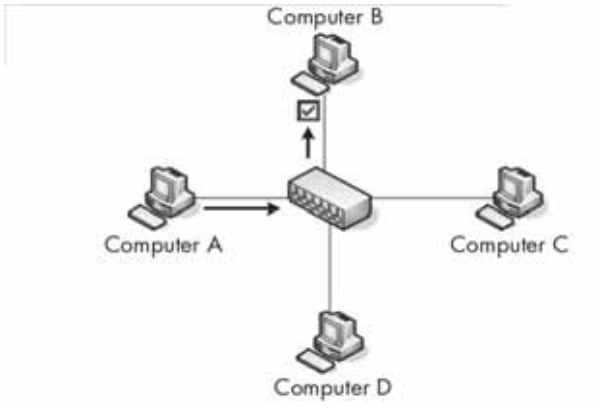
سوئیچ‌های بزرگ در بازار، به روش‌های گوناگون مدیریت می‌شوند؛ یا از طریق نرم‌افزار فروشنده یا از طریق رابط وب. معمولا از این سوئیچ‌ها با عنوان «سوئیچ‌های قابل مدیریت» یاد می‌شود و ویژگی-های گوناگونی را فراهم می‌کنند که می‌توانند در مدیریت شبکه مفید باشند. این شامل توانایی برای فعال یا غیرفعال کردن پورت‌های ویژه، مشاهده جزئیات پورت، تغییر پیکربندی و راه‌اندازی دوباره سوئیچ از راه دور است.

شکل ۱-۵ یک سوئیچ ۲۴ پورت اترنت و قابل نصب در رک

سوئیچ‌ها قابلیت‌های پیشرفته‌ای در مدیریت انتقال بسته‌ها دارند. برای فراهم شدن قابلیت ارتباط مستقیم با دستگاه‌های ویژه، سوئیچ‌ها باید به‌طور یکتایی قادر به شناسایی دستگاه‌ها بر اساس آدرس آنها باشند. همه‌ی این موارد، بدین معنی است که باید در لایه‌ی پیوند داده‌ی مدل OSI کار کنند.

سوئیچ‌ها آدرس لایه‌ی دوم هر دستگاه متصل را در جدول CAM ذخیره می‌کنند که مانند یک پلیس ترافیک عمل می‌کند. هنگامی که یک بسته منتقل می‌شود، سوئیچ اطلاعات هدر لایه‌ی دوم بسته را می‌خواند و از جدول CAM به عنوان یک مرجع استفاده می‌کند تا پورتی که بسته باید به آن فرستاده شود را مشخص کند. سوئیچ تنها بسته‌ها را به پورت‌های ویژه ارسال می‌کند که این کار تا حد فراوانی ترافیک شبکه را کاهش می‌دهد.

شکل (۱-۶) جریان ترافیک را از طریق یک سوئیچ نشان می‌دهد. در این شکل، کامپیوتر A یک بار دیگر بسته را به کامپیوتر B ارسال می‌کند. در این نمونه، کامپیوترها از طریق یک سوئیچ متصل هستند که اجازه می‌دهد تا کامپیوتر A داده را به‌طور مستقیم و بدون اینکه دستگاه‌های دیگر در شبکه از این ارتباط آگاه شوند، به کامپیوتر B ارسال کند. افزون بر این، گفتگوهای گوناگون می‌تواند هم‌زمان روی دهد.



شکل ۱-۶: جریان ترافیک زمانی که کامپیوتر A داده را به کامپیوتر B از طریق سوئیچ ارسال می‌کند

مسیریاب

مسیریاب یک دستگاه پیشرفته‌ی شبکه با سطح بسیار بالاتری از عمل‌کرد، نسبت به سوئیچ یا هاب است. مسیریاب می‌تواند اشکال و فرم‌های بسیاری داشته باشد، اما بیشتر آنها شماری چراغ LED در جلو و چند پورت شبکه‌ی بسته به اندازه‌ی شبکه در پشت دارند (شکل ۱–۷). مسیریاب‌ها در لایه‌ی سوم مدل OSI عمل می‌کنند، جایی که مسئول ارسال بسته‌ها میان دو یا چند شبکه هستند. فرایندی که مسیریاب‌ها برای هدایت جریان ترافیک در شبکه استفاده می‌کنند، مسیریابی نامیده می‌شود.

انواع گوناگونی از پروتکل‌های مسیریابی وجود دارد که بیان می‌کند، چگونه انواع گوناگون بسته‌ها به شبکه‌های دیگر مسیریابی می‌شوند. مسیریاب‌ها معمولا از آدرس‌های لایه‌ی سه، برای شناسایی دستگاه‌ها در شبکه استفاده می‌کنند.

شکل ۱–۷: یک روتر کوچک که برای استفاده در شبکه‌های کوچک مفید است

یک راه ساده برای نشان دادن مفهوم مسیریابی این است که محله‌ای را با شبکه‌ای از خیابان‌ها تصور کنید. در هر خیابان خانه‌ای است و هر خانه آدرس مربوط به خود را دارد (شکل ۱–۸). در یک خیابان زندگی می‌کنید. بنابراین می‌توانید در میان همه‌ی خانه‌ها در خیابان حرکت کنید. این بسیار همانند عمل‌کرد یک سوئیچ است که امکان ارتباط میان تمام کامپیوترها را در شبکه فراهم می‌کند. با این حال برای ارتباط برقرار کردن با همسایه در خیابان دیگر، شخص باید علایم خیابان را برای رسیدن به خانه‌ی همسایه دنبال کند.

اجازه دهید از طریق نمونه‌ای که مربوط به ارتباطات در خیابان است، کار را ادامه دهیم. با استفاده از شکل (۱–۸) اجازه دهید که بگویم در Vine Street 503 نشسته‌ام و می‌خواهم به Dogwood Lane 202 بروم. برای انجام این کار باید از Oak Street رد شده و سپس به Dogwood Lane بروم. این را به عنوان عبور از بخش شبکه در نظر بگیرید. اگر دستگاه با آدرس 192.168.03 بخواهد با دستگاه به آدرس 192.168.0.54 ارتباط برقرار کند، باید از یک مسیریاب برای رسیدن به شبکه‌ی 10.100.1.1 استفاده کند و پیش از اینکه بتواند به شبکه‌ی مقصد برود، باید از مسیریاب شبکه‌ی مقصد عبور کند.