پیوست الف

پاسخ به پرسش‌های مرور درس

فصل ۱: مقدمه‌ای بر شبکه‌ها

۱. C. یک توپولوژی منطقی کلاینت – سرور به شما امکان داشتن پایگاه داده‌ی متمرکز کاربر را می‌دهد به طوری‌که احراز هویت در یک مکان فراهم گردد.

۲. C. برای نصب یک توپولوژی فیزیکی که توسعه‌پذیری را آسان می‌کند از شبکه‌ی ستاره استفاده کنید که از یک هاب یا سوئیچ تشکیل شده است و امروزه متداول‌ترین شبکه، شبکه‌ی LAN می‌باشد.

۳. D. فقط یک توپولوژی فیزیکی مِش است که در آن هر یک از دستگاه‌ها به بقیه‌ی دستگاه‌ها متصل‌اند. بنابراین، اتصالات بیشتری دارد و یک تکنولوژی رایج LAN نمی‌باشد.

۴. B. در یک توپولوژی ستاره، هر ایستگاه کاری به یک هاب، سوئیچ یا دستگاه مرکزی مشابه متصل می‌شوند نه به ایستگاه دیگر. مزایای این شبکه این‌است‌که وقتی ارتباط با دستگاه مرکزی از بین برود بقیه‌ی دستگاه‌های شبکه به کار خودشان ادامه می‌دهند.

۵. C. سوئیچینگ با برچسب چند پروتکلی (MPLS) به عنوان یک پروتکل LAN مزایای زیادی دارد. زمانی‌که برچسب‌ها استفاده می‌شوند، برای مثال صدا می‌تواند بر داده اولویت داشته باشد.

۶. B. یک گروه‌بندی منطقی میزبان‌ها، LAN نامیده می‌شود و شما معمولاً آن‌ها را با اتصال به سوئیچ گروه‌بندی می‌کنید.

۷. C. در یک محیط شبکه‌ی نظیر – به – نظیر موضوع امنیت می‌تواند زیاد جدی نباشد. به دلیل مشکلات استانداردسازی احراز هویت، یک رویکرد تدریجی شامل اولویت‌های خصوصی توسعه می‌یابد. در این توپولوژی سرورهای اختصاصی وجود ندارد و این شبکه را می‌توان با دو کامپیوتر تشکیل داد.

۸. A. زمانی که یک دفتر مرکزی نیاز به ارتباط مستقیم با دفاتر نمایندگی خود دارد، اما این دفاتر خواستار ارتباط مستقیم با یکدیگر نمی‌باشند، باید از مدل نقطه – به – چند نقطه استفاده نمود. سناریوهای دیگر استفاده از مدل نقطه – به – نقطه بین سایت‌ها را پیشنهاد می‌کنند.

۹. D. عموماً LANها دارای یک محدوده‌ی جغرافیایی به وسعت یک ساختمان یا کوچک‌تر می‌باشند. آن‌ها می‌توانند از یک شبکه‌ی ساده با دو میزبان تا یک شبکه‌ی پیچیده با هزاران میزبان تشکیل شوند.

۱۰. B. تنها عیب ذکر شده این‌است‌که یک نقطه‌ی منحصر به فرد عیب در شبکه وجود دارد. با این حال در این توپولوژی عیب‌یابی آسان‌تر انجام می‌شود و اگر کل شبکه از کار بیافتد می‌دانید که ابتدا کدام محل را بررسی کنید. وجود یک هاب مرکزی سبب می‌شود که قطع یک پورت و یا اضافه کردن یک دستگاه جدید به یک پورت موجود سبب قطع سایر ایستگاه‌های متصل به هاب نمی‌شود.

۱۱. D. یک WAN متعارف دو یا چند LAN راه دور را با استفاده از یک شبکه‌ی دیگر (ISP شما) و یک مسیریاب به هم متصل می‌کند. میزبان محلی و مسیریاب شما این شبکه‌ها را به عنوان شبکه‌های راه دور نه به عنوان شبکه‌های محلی یا منابع محلی می‌بیند. مسیریاب‌ها از اولویت ارتباطات سریال برای WAN استفاده می‌کنند.

۱۲. D. MPLS بین سایت‌ها لینک‌های منطقی برقرار می‌کند به طوری‌که دفاتر نمایندگی می‌توانند به آسانی و به سرعت اضافه شوند.

۱۳. A. در یک شبکه‌ی نظیر – به – نظیر تمام کامپیوترها دارای وضعیت مشابهی می‌باشند و اگر منابع مورد درخواست در اختیار یک کامپیوتر باشد، کامپیوترهای دیگر می‌توانند درخواست دسترسی به منابع را انجام دهند.

۱۴. D. در شبکه‌های مبتنی بر کلاینت – سرور، درخواست‌های دسترسی به منابع به جای این‌که مستقیماً به ماشینی ارائه شود که منابع مورد درخواست کلاینت را در اختیار دارد (مانند توپولوژی نظیر – به – نظیر) به سرور اصلی ارائه می‌شود. این سرور با انجام موارد امنیتی کلاینت را به منابع مورد درخواستش هدایت می‌کند.

۱۵. A. بهترین پاسخ به این سوال یک سوئیچ اترنت است که از توپولوژی فیزیکی ستاره با توپولوژی خطی منطقی استفاده می‌کند.

۱۶. D. مسیریاب‌ها دامنه‌های پخش فراگیر را به چند قسمت تقسیم می‌کنند و برای اتصال چند شبکه‌ی مختلف به یکدیگر به کار می‌روند.

۱۷. D. در توپولوژی مش از هر دستگاه به بقیه‌ی دستگاه‌ها در شبکه اتصال وجود دارد. یک توپولوژی مش دارای تحمل خطای مقاوم می‌باشد. اگر یک اتصال از بین برود، کامپیوترها و سایر دستگاه‌های شبکه می‌توانند از اتصالات اضافی موجود برای اجرا استفاده نمایند.

۱۸. A. در یک توپولوژی نقطه – به – نقطه، بین دو مسیریاب ارتباط مستقیم وجود دارد که یک مسیر مخابراتی را به وجود می‌آورد. مسیریاب‌ها در یک توپولوژی نقطه–به–نقطه می‌توانند یا با یک کابل سری به هم متصل شوند که یک شبکه‌ی فیزیکی را می‌سازند یا از دور تنها توسط یک مدار در داخل شبکه‌ی Frame Relay به یکدیگر متصل شوند که در این صورت یک شبکه‌ی منطقی را به وجود می‌آورند.

۱۹. B. یک توپولوژی هایبرید، ترکیبی از دو یا چند نوع توپولوژی منطقی یا فیزیکی است که در داخل یک شبکه با یکدیگر تعامل دارند.

۲۰. A، B، C، D. هر توپولوژی در رابطه با اجرا تعدادی طرفدار و منتقد دارد. بنابراین باید هزینه، سهولت نصب، نگهداری و تحمل خطا را در نظر گرفت.

فصل ۲: مشخصات اتصال سیستم‌های باز

۱. C. یک جلسه‌ی اتصال‌گرا با استفاده از آنچه دست دادن سه طرفه نامیده می‌شوند، برپا می‌شود. میزبان در طرف فرستنده‌ی یک بسته‌ی SYN ارسال و میزبان گیرنده‌ی یک SYN-ACK دریافت می‌کند و میزبان ارسال کننده با دریافت آخرین بسته‌ی ACK پاسخ می‌دهد. بدین ترتیب جلسه برقرار می‌گردد.

۲. D. TCP و UDP پروتکل‌های لایه‌ی انتقال هستند. لایه‌ی انتقال لایه‌ی 4 مدل OSI است.

۳. A. لایه‌ی بالایی مدل OSI دسترسی برنامه‌های کاربردی را به خدماتی ارائه می‌دهد که دسترسی به شبکه را مجاز نماید.

۴. A. اگر سرور راه دور مشغول باشد یا به درخواست مرورگر وب شما پاسخ ندهد، این مورد وجود یک مشکل را در لایه‌ی کاربرد نشان می‌دهد.
۵. B. لایه‌ی نمایش، داده را برای لایه‌ی کاربرد "قابل ارائه" می‌نماید.
۶. C. پل‌ها همانند سوئیچ‌ها، دستگاه‌های لایه‌ی پیوند داده می‌باشند. هاب‌ها مانند تکرار کننده‌ها، دستگاه‌های لایه‌ی فیزیکی هستند. مسیریاب‌ها دستگاه‌های لایه‌ی شبکه می‌باشند.
۷. D. وظیفه‌ی لایه‌ی فیزیکی این‌است‌که داده را به صورت سیگنال‌های مربعی مناسب برای رسانه با سیم و بی‌سیم به منظور انتقال تبدیل می‌کند.
۸. D. یک میزبان دریافت کننده می‌تواند با کنترل جریان داده، فرستنده را کنترل نماید (TCP به طور پیش‌فرض پنجره‌سازی می‌کند). با کاهش اندازه‌ی ویندوز، میزبان دریافت کننده می‌تواند سرعت ارسال داده توسط میزبان ارسال کننده را کاهش دهد به طوری‌که بافرهای میزبان دریافت کننده سرریز نشود.
۹. C، D. اگر می‌خواهید یک دامنه تصادم منفرد را توسعه دهید، هاب (تکرار کننده‌ی چند پورتی) این عمل را برای شما انجام می‌دهد.
۱۰. لایه‌ی انتقال جریان‌های داده‌ی بزرگ را از لایه‌های بالاتر دریافت و آن‌ها را به تکه‌های کوچک‌تر به نام سگمنت تقسیم می‌کند.
۱۱. C. ترتیب کپسوله‌سازی عبارت است از: داده، سگمنت، بسته، فریم، بیت‌ها.
۱۲. B، C. پل‌ها و سوئیچ‌ها دامنه‌های تصادم را به قسمت‌هایی تقسیم می‌کنند.
۱۳. C. یک ارتباط لایه‌ی انتقال معتبر از سیگنال‌های ACK برای حصول اطمینان از این‌که تمام داده‌ها به طور معتبر دریافت می‌شوند استفاده می‌کنند. ارتباط قابل اطمینان به صورت زیر تعریف می‌شود: استفاده از سیگنال‌های ACK، ترتیب‌دهی، و کنترل جریان که مشخصه‌ی لایه‌ی انتقال (لایه‌ی 4) می‌باشد.
۱۴. A، C، D. وقتی از ترتیب‌دهی و ACKها استفاده می‌کنید، ACK بسته‌های تحویل شده به گیرنده به فرستنده می‌رسد. در این‌جا هر بسته‌ای که ACK نشده باشد دوباره ارسال می‌گردد و پس از آن بسته‌ها به محض رسیدن به مقصد دوباره ترتیب‌دهی می‌شوند.
۱۵. C. کنترل جریان به دستگاه گیرنده امکان می‌دهد تا مراحل در حال اجرا توسط دستگاه فرستنده را کنترل کند به طوری‌که بافر دستگاه گیرنده به حالت سرریز نرسد.
۱۶. B. IP یک پروتکل لایه‌ی شبکه است. TCP یک مثال از پروتکل لایه‌ی انتقال و اترنت یک مثال از پروتکل لایه‌ی پیوند داده و T1 می‌تواند به عنوان پروتکل لایه‌ی فیزیکی در نظر گرفته شود.
۱۷. D. لایه‌ی نمایش ششمین لایه‌ی مدل OSI است. فقط لایه‌ی کاربرد بالاترین لایه است. لایه‌ی جلسه لایه‌ی 5 مدل است، لایه‌ی انتقال لایه‌ی 4 و شبکه لایه‌ی 3 می‌باشد.
۱۸. C. یک مسیریاب در لایه‌ی شبکه عمل کرده و بسته‌ها را مسیردهی می‌کند. به مسیریاب‌ها سوئیچ‌های لایه‌ی 3 نیز گفته می‌شود.
۱۹. C. جمله‌ی "Please Do Not Throw Sausage Pizza Away" شامل اولین حرف لایه‌های مدل OSI از لایه‌ی 1 تا لایه‌ی 7 می‌باشد. "All People Seem To Need Data Processing" شش حرف اول لایه‌ها را از بالا به پایین نشان می‌دهد، اما هر کلمه دقیقاً عملکرد آن لایه را نشان نمی‌دهد.

۲۰. B. استاندارد 802.3 که معمولاً مربوط به اترنت است، روش دسترسی به رسانه‌ی مورد استفاده توسط اترنت را مشخص می‌کند و به دسترسی چندگانه با نظارت کاربر و تشخیص تصادم (CSMA/CD) معروف است.

فصل ۳: توپولوژی‌های شبکه‌سازی، کانکتورها و استانداردهای سیم‌کشی

۱. B، C. Plenum-rated یعنی این‌که روکش کابل نمی‌سوزد مگر این‌که در معرض درجه حرارت زیادی قرار گیرد، وقتی بسوزد بیشتر از PVC دود سمی تولید نمی‌کند و برای استفاده در فضای معمولی که دارای هوای قابل تنفس می‌باشند رتبه‌بندی می‌شود. معمولاً در مسیر عبور کابل‌ها فضایی برای عبور هوای تازه در نظر گرفته می‌شود.

۲. D. UTP معمولاً در اترنت زوج سیم تابیده شده مانند 10BaseT، 100BaseTX، 1000BaseTX و غیره به کار می‌رود.

۳. D. زوج سیم تابیده شده بدون حفاظ برای استفاده در شبکه‌های اترنت دارای استانداردهایی از رده‌ی 2 تا رده‌ی 6 می‌باشد. Cat 8 تعریف نشده است.

۴. C. UTP معمولاً با RJ-45 متصل می‌شود. از crimper برای اتصال کانکتور RJ به یک کابل استفاده می‌شود.

۵. A. در یک فیبر تک – حالته سیگنال می‌تواند فاصله‌ی بیشتری را طی کند.

۶. B. شما از کابل straight-through برای اتصال یک میزبان به یک سوئیچ استفاده می‌کنید و pin-out متعارف 568A نامیده می‌شود.

۷. C. کابل فیبرنوری با به کار بردن ایمپالس‌های نور به جای جریان الکتریکی سیگنال‌های دیجیتالی را ارسال می‌کند و به همین دلیل در مقابل تأثیرات EMI و RFI مصون می‌باشد.

۸. B. همان‌طور که بیان شد، کابل فیبرنوری با استفاده از پالس‌های نور سیگنال‌های دیجیتالی را ارسال می‌کند. نور توسط هسته‌ی شیشه‌ای یا پلاستیکی حمل می‌شود.

۹. B. تفاوت میان فیبرهای تک‌حالته با فیبرهای چندحالته در تعداد شعاع‌های نوری (و بنابراین در تعداد سیگنال‌ها) که می‌توانند حمل کنند می‌باشد. به طور کلی فیبر چندحالته برای کاربردهای با فواصل کوتاه‌تر و فیبر تک‌حالته برای فواصلی طولانی‌تر به کار می‌رود.

۱۰. C. استانداردها، UTP را تا ۱۰۰ متر محدود می‌کنند. انواع مختلف فیبرنوری دارای حداکثر طول متفاوت هستند، اما فیبرنوری تنها کابلی است که می‌تواند فاصله‌ای بیشتر از ۱۰۰ متر را پشتیبانی کند.

۱۱. B، D، E. انواع مختلف فیبرنوری وجود دارند. SC، ST، LC، و MT-RJ چند عدد از انواع کانکتورهایی هستند که امروزه به کار می‌روند.

۱۲. B. برای اتصال دو دستگاه برای برقراری صدا روی یک اتصال عمودی، کابلی که می‌توانید به کار ببرید Cat 5 است.

۱۳. B. در ارتباط دو طرفه‌ی غیر همزمان (HDX)، یک دستگاه می‌تواند اطلاعات را یا بفرستد و یا آن را دریافت نماید، اما نمی‌تواند هر دو عمل را در یک زمان انجام دهد.

۱۴. B. کابل فیبرنوری فقط نور را ارسال می‌کند (نه مثل UTP که جریان الکتریکی را حمل می‌کند)، بنابراین EMI روی آن تأثیری ندارد.

۱۵. C. ارتباط دو طرفه‌ی همزمان (FDX) به یک پیکربندی نقطه–به–نقطه نیاز دارد، زیرا مدار اجتناب از تصادم غیر فعال است.

۱۶. B. هر دو استاندارد سیم‌کشی برای UTP (568A و 568B) فقط از پین‌های 1، 2، 3 و 6 استفاده می‌کند.
۱۷. D. تمام دستگاه‌هایی که برای ارسال و دریافت آماده کار می‌شوند به یک کابل crossover برای ارتباط مستقیم نیاز دارند.
۱۸. A. یک کابل T1 از زوج‌های 1 و 2، T568B استفاده می‌کند، بنابراین برای اتصال دو دستگاه T1 CSU/DSU به طور پشت به پشت به یک کابل crossover نیاز داریم که این زوج‌ها را معاوضه نماید. به طور مشخص پایه‌های 1، 2، 4 و 5 به ترتیب به پایه‌های 4، 5، 1 و 2 متصل می‌شوند.
۱۹. D. نقطه‌ی سر حد یا نقطه‌ی demarc، نقطه‌ای است که کنترل عملیاتی یا مالکیت از شرکت شما به یک تأمین کننده‌ی خدمات تغییر می‌کند. این عمل اغلب در رابطه با اتصالات تلفن و CSU/DSU مربوط به اتصالات WAN در MDF پیش می‌آید.
۲۰. B. یک 568B یک استاندارد سیم‌کشی RJ-45 است و این نوع کابل از دو زوج سیم استفاده می‌کند.

فصل ۴: مشخصات اترنت رایج

۱. B. در یک شبکه‌ی اترنت، آدرس MAC (آدرس سخت‌افزار) برای ارتباط یک میزبان با میزبان دیگر به کار می‌رود.
۲. B. 100BaseTX از CAT 5e استفاده می‌کند و وقتی از ارتباط FDX استفاده می‌کند می‌تواند تا 200Mbps را پشتیبانی نماید.
۳. D. وقتی یک دستگاه یک بسته‌ی داده را در یک سگمنت شبکه ارسال می‌کند، تمام دستگاه‌های دیگر روی همان سگمنت شبکه‌ی فیزیکی باید منتظر بمانند تا بسته ارسال شود.
۴. B. 100BaseTF یعنی که شما دارای یک اترنت با اجرا از طریق کابل فیبرنوری است.
۵. B. پروتکل CSMA/CD این مکان را فراهم می‌سازد تا بسته‌هایی که به طور همزمان از میزبان‌های مختلف ارسال می‌شوند، پهنای‌باند را عادلانه بین آن‌ها تقسیم کند.
۶. B. یک کابل 10GBaseSR می‌تواند حداکثر فاصله‌ی ۹۹۰ فوت (۳۰۲ متر) را تحت پوشش قرار دهد.
۷. B. با مدار ارتباطی HDX فقط از یک جفت سیم برای ارسال یا دریافت سیگنال دیجیتال استفاده می‌شود.
۸. A. اترنت FDX از دو زوج سیم در یک زمان استفاده می‌کند.
۹. C. یک اجرای 10GBaseLR می‌تواند تا فاصله‌ی 6 مایل را تحت پوشش قرار دهد.
۱۰. B. شما می‌توانید با یک اترنت 10Mbps اجرا شده با FDX یک سرعت 20Mbps و یا با یک اترنت سریع سرعت 200Mbps را به دست آورید.
۱۱. B. ارتباطات FDX نمی‌تواند با یک هاب به کار رود، زیرا هاب یک دستگاه ارتباطی HDX می‌باشد. یک میزبان، سوئیچ و مسیریاب توانایی پردازش ترافیک (فریم) را دارند در حالی‌که یک هاب یک تکرار کننده‌ی چند پورتی است.
۱۲. B. 11000000 برابر 192 و 10101000 برابر 168 و 00110000 برابر 48 و 11110000 معادل 240 است.
۱۳. A. پیوند می‌تواند پهنای‌باند را افزایش دهد و برای دستگاه‌هایی که لینک چندگانه‌ی متصل به هم دارند افزونگی فراهم نماید.

۱۴. C. مقادیر نیبل عبارتند از 1 + 2 + 4 + 8 که حداکثر عدد 15 را به ما می‌دهند. اگر یک عدد دهدهی معادل 10 داشته باشیم، این یعنی عدد 1010 در سیستم باینری و در نتیجه بیت با وزن 8 و بیت با وزن 2، معادل 1 هستند یعنی on هستند.

۱۵. D. بیت‌های با وزن 128، 64، 32 و 8، on هستند، بنابراین فقط کافی است این اعداد را جمع کنید:
128 + 64 + 32 + 8 = 232

۱۶. B. اولین 10 رقم سیستم عدد نویسی شانزده‌تایی (9-0) با اولین 10 رقم سیستم دهدهی یکسان است. می‌دانیم معادل باینری 10، عدد 1010 و در سیستم هگز با یک کاراکتر مانند A نمایش داده می‌شود، بنابراین در سیستم هگز، اعداد دو رقمی را با یک کاراکتر نشان می‌دهیم که معمولاً از حروف استفاده می‌شود.

۱۷. C. یک MAC یا آدرس سخت‌افزار یک آدرس 48 بیتی (6 بایت) است که به صورت فرمت شانزده‌تایی نمایش داده می‌شود.

۱۸. A. اترنت 100BaseT و 1000BaseT هر دو می‌توانند تا ۱۰۰ متر را پوشش دهند.

۱۹. B. FCS با محاسبه‌ی وارسی چرخه‌ای افزونگی (CRC) که تأیید می‌کند تمام بیت‌های یک فریم تغییر نمی‌کنند می‌تواند ترتیب فریم را تشخیص دهد.

۲۰. C. عدد 100 یعنی 100Mbps. کلمه‌ی *Base* یعنی *baseband* که به فناوری باند پایه اشاره دارد که یک روش ارتباطی در شبکه‌ها می‌باشد.

فصل ۵: دستگاه‌های شبکه‌سازی

۱. C. NICها اتصال‌های شبکه‌های فیزیکی برای کامپیوترمی‌باشند، اما جزو دستگاه‌ها یا رسانه‌هایی نیستند که برای تأمین دسترسی به اینترنت در یک تنظیم SOHO به کار می‌روند.

۲. C. سوئیچ شبیه هاب چندین سگمنت یک شبکه را به هم متصل می‌کند ولی یک تفاوت مهم با هاب دارد. هاب هر چیزی را که از پورت دریافت کند به تمام پورت‌ها ارسال می‌کند درحالی‌که یک سوئیچ محدوده‌های یک فریم را تشخیص می‌دهد و آدرس MAC مقصد فریم وارده و پورتی که دریافت می‌شود را مورد بررسی قرار می‌دهد.

۳. وقتی می‌گوییم سگمنت، منظور ایجاد تصادم چندتایی یا دامنه‌های پخش است. هاب‌ها در یک شبکه سگمنت‌سازی نمی‌کنند، آن‌ها فقط سگمنت‌های شبکه را به یکدیگر متصل می‌کنند. تکرار کننده‌ها در یک شبکه سگمنت‌سازی نمی‌کند، آن‌ها یک سیگنال را تکرار می‌کنند و فاصله‌ی تحت پوشش را افزایش می‌دهند. بنابراین تنها گزینه‌ی درست، گزینه‌ی B یعنی یک سوئیچ است.

۴. A. وظیفه‌ی اصلی یک پل، جداسازی ترافیک در دو طرف پل و تقسیم‌بندی دامنه‌های تصادم می‌باشد.

۵. A. هاب‌ها یک دامنه تصادم و یک دامنه پخش ایجاد می‌کنند.

۶. B. با اجرای ارتباط FDX در هر پورت، یک سوئیچ برای هر پورت پهنای‌باند اضافی تأمین می‌کند.

۷. B. یک سوئیچ نوعاً یک دستگاه لایه‌ی 2 است که با استفاده از آدرس‌های MAC شبکه را سگمنت‌بندی می‌کند. در هر حال بعضی از سوئیچ‌ها مرتبه‌های بالاتر می‌توانند سرویس‌های لایه‌ی 3 را تأمین کنند.

۸. D. به خاطر آورید که سرورهای DHCP آدرس‌های IP را برای میزبان‌ها تعیین می‌کند، بنابراین DHCP مدیریت ساده‌تر از تأمین اطلاعات IP برای هر یک از میزبان‌ها فراهم می‌کند (آدرس‌دهی IP استاتیک نامیده می‌شود).

۹. B. سوئیچ‌های چندلایه (که سوئیچ‌های لایه‌ی 3 نیز نامیده می‌شود) در مقایسه با سوئیچ‌های معمولی، ویژگی کمتر، پهنای‌باند کمتر یا پورت‌های کمتر ندارند، این سوئیچ‌ها وظایف مسیردهی بین زیرشبکه‌ها را دارا می‌باشند.

۱۰. B. یک متعادل کننده‌ی بار با استفاده از روش‌های مختلف، بسته‌های وارده را که در پشت یک آدرس IP منحصر به فرد پنهان شده به یک یا چند ماشین ارسال می‌کند. مسیریاب‌های متعادل کننده‌ی بار مدرن می‌تواند با استفاده از مقررات مختلف در خصوص مسیردهی ترافیک تصمیماتی را بگیرند. این مسیردهی می‌تواند بر اساس حداقل بار، سریع‌ترین زمان پاسخ، یا ساده‌تر درخواست‌های متعادل‌سازی انجام شود.

۱۱. A. DNS اسامی افراد را به منظور مسیردهی بسته از طریق اینترنت به آدرس‌های IP تبدیل می‌کند. میزبان‌ها می‌توانند آدرس IP این سرور DNS را دریافت نموده و سپس اسامی میزبان را به آدرس‌های IP تحلیل نمایند.

۱۲. C. مسیریاب‌ها، سوئیچ‌ها و پل‌ها دستگاه‌هایی هستند که کمک می‌کنند تا شبکه‌های بزرگ به شبکه‌های کوچک‌تر تقسیم شوند که این عمل را سگمنت‌بندی شبکه می‌نامند. هاب‌ها شبکه را به سگمنت‌ها تقسیم نمی‌کنند بلکه فقط سگمنت‌های شبکه را به هم متصل می‌کنند.

۱۳. A. البته حافظه‌ی پنهان وب! بیشتر برنامه‌های پراکسی وسیله‌ای را برای رد دسترسی به URLهای معینی در لیست سیاه فراهم می‌کند، بنابراین فیلترینگ محتوا را معمولاً در محیط‌های شرکت فراهم می‌کند.

۱۴. D. گزینه‌های A، B و C در افزایش عملکرد شبکه کمک می‌کنند، به طوری‌که تنها گزینه‌ای که باقی می‌ماند توفان‌های پخش می‌باشد. ترافیک افزایش یافته، تراکم LAN را افزایش می‌دهد.

۱۵. B. اگر سرور DHCP از کار متوقف شود، آن‌گاه آدرس‌های IP را به میزبان‌هایی که دوباره آغاز به کار می‌کنند ارائه می‌دهد. در هر حال میزبان‌هایی که خاموش نشده باشند هنوز دارای یک آدرس‌های IP هستند، زیرا زمان اجاره‌ی آن منقضی نشده است.

۱۶. D. یک سرور پراکسی برای جلوگیری از ترافیک خارجی از رسیدن به شبکه‌ی داخلی به طور مستقیم به کار می‌رود و همچنین می‌تواند برای فیلتر کردن سایت‌هایی که کاربران شما مجاز به ورود به آن‌ها هستند به کار می‌روند.

۱۷. C. سوئیچ‌ها دامنه‌های تصادم جداگانه، اما دامنه پخش منحصر به فرد ایجاد می‌کنند. توجه کنید که مسیریاب‌ها دامنه پخش جداگانه‌ای برای هر یک از رابط‌ها فراهم می‌کنند.

۱۸. A. با استفاده از دستگاه‌ها برای آفلود وظایفی مانند بی‌باری، رمزنگاری، فیلتر کردن محتوا و تمرکز VPN می‌توان بار مؤثر سایر سیستم‌ها را کاهش داده و عاملیت که ممکن است در این دستگاه‌های خصوصی ظاهر شود را افزایش دهد.

۱۹. C. یک سرور DNS رکوردهای مختلفی را به کار می‌برد. یک رکورد "A"، یک نام میزبان در رکورد آدرس IP است و یک رکورد اشاره‌گر، یک آدرس IP برای رکورد نام میزبان است.

۲۰. D. یک سرور پراکسی می‌تواند وظایف زیادی انجام دهد. یک سرور پراکسی می‌تواند از یک موتور ذخیره کننده استفاده کند و بنابراین درخواست‌های تکراری برای دسترسی به اطلاعات وب، دسترسی‌های تکراری به کاربران را شتاب می‌دهد. پراکسی سرورها همچنین می‌توانند دسترسی پذیری وب‌سایت‌ها را محدود کنند.

فصل ۶: مقدمه‌ای بر پروتکل اینترنت

۱. D. SMTP در لایه‌ی کاربرد مدل OSI و مدل DoD قرار دارد.

۲. D. HTTPS یا HTTP امن طبق پیش‌فرض از پورت 443 استفاده می‌کند.

۳. C. پروتکل پویای پیکربندی میزبان DHCP برای تأمین اطلاعات IP برای میزبان‌های روی شبکه‌تان به کار می‌رود. DHCP می‌تواند اطلاعات زیادی فراهم نماید، اما رایج‌ترین آن‌ها آدرس IP، ماسک زیرشبکه، گیت‌وی پیش‌فرض و اطلاعات DNS می‌باشد.

۴. B. پروتکل ARP برای پیدا کردن آدرس سخت‌افزاری از یک آدرس IP معلوم به کار می‌رود.

۵. B. SSH به شما اجازه می‌دهد تا از راه دور، مسیریاب، سوئیچ‌ها و حتی سرورها را به طور امن مدیریت کند.

۶. C. مشکل از DNS است که از TCP و UDP پورت 53 استفاده می‌کند.

۷. A، B. یک کلاینت که یک پیام DHCP Discover را به منظور دریافت یک آدرس IP می‌فرستد، یک سیگنال پخش را در هر دو لایه‌ی 2 و 3 ارسال می‌کند. لایه‌ی 2 پخش همه بر حسب *F* در سیستم هگز است، یعنی: FF:FF:FF:FF:FF:FF. پخش لایه‌ی 3 به صورت 255.255.255.255 است که یعنی تمام شبکه‌ها و تمام میزبان‌ها. DHCP غیر اتصال‌گرا است یعنی این‌که از پروتکل UDP در لایه‌ی انتقال که لایه‌ی میزبان –به– میزبان نیز نامیده می‌شود استفاده می‌کند.

۸. E. Telnet از TCP در لایه‌ی انتقال با شماره‌ی پورت پیش‌فرض 23 استفاده می‌کند.

۹. C، D. پروتکل ICMP برای ارسال پیام‌های خطا از طریق شبکه به کار می‌رود، اما این پروتکل تنها عمل نمی‌کند. هر سگمنت یا فیلد ICMP باید در داخل یک دیتاگرام IP (یا بسته) کپسوله شود.

۱۰. B، D، E. SMTP، FTP و HTTP از TCP استفاده می‌کنند.

۱۱. A، C، F. DHCP، SNMP و TFTP از UDP، SMTP و FTP استفاده می‌کنند و HTTP از TCP استفاده می‌کند.

۱۲. C، D، E. Telnet و FTP و TFTP (Trivial FTP) تماماً از پروتکل‌های لایه‌ی کاربرد می‌باشند. IP یک پروتکل لایه‌ی شبکه و TCP یک پروتکل انتقال می‌باشند.

۱۳. C. SMTP توسط یک کلاینت برای ارسال نامه به سرور خود و به وسیله‌ی آن سرور برای ارسال نامه به سرور دیگر مورد استفاده قرار می‌گیرد. POP3 و IMAP توسط کلاینت‌ها برای بازیابی نامه‌ی آن‌ها از سروری که آن را ذخیره می‌کند مورد استفاده قرار می‌گیرد. HTTP فقط با سرویس‌ها نامه مبتنی بر وب به کار می‌رود.

۱۴. C. پروتکل RDP این امکان را برای شما فراهم می‌کند تا به یک کامپیوتر راه دور متصل شوید و برنامه‌ها را اجرا نمایید همان‌طور که Telnet این عمل را انجام می‌دهد. در هر حال، مزیت بزرگ RDP در مقایسه با Telnet این‌است‌که RDP اجازه می‌دهد یک اتصال رابط GUI داشته باشید.

۱۵. B. پروتکل مدیریت شبکه‌ی ساده (SNMP) نوعاً با استفاده از نسخه‌ی ۳ اجرا می‌شود که اجازه می‌دهد تا یک سرویس اتصال‌گرا، احراز هویت و نمونه‌برداری امن از دستگاه‌های شبکه و هشدار و گزارش به دستگاه‌های شبکه اجرا شود.

۱۶. B، E. پروتکل نسخه‌برداری امن SCP و پروتکل FTP می‌تواند برای انتقال فایل‌ها بین دو سیستم استفاده شود.

۱۷. B. چهار لایه‌ی پشته‌ی IP (که مدل DoD نیز نامیده می‌شود) عبارتند از: کاربرد، میزبان – به – میزبان، اینترنت و دسترسی به شبکه. لایه‌ی میزبان –به –میزبان معادل لایه‌ی انتقال مدل OSI است.

۱۸. C. پروتکل زمان شبکه وجود یک زمان پایدار در دستگاه‌های شبکه را تضمین می‌کند.

۱۹. A. با استفاده از شماره‌های پورت، TCP و UDP می‌توان نشست‌های چندگانه‌ای را بین دو میزبان مشابه بدون ایجاد هر نوع اشتباه برقرار نمود.

۲۰. D. DNS از TCP برای تعویض ناحیه بین سرورها و UDP وقتی که یک کلاینت سعی در تحلیل یک نام میزبان برای یک آدرس IP دارد به کار می‌رود.

فصل ۷: آدرس‌دهی IP

۱. D. آدرس‌های در محدوده‌ی 172.16.0.0 تا 172.31.255.255 تمام بر اساس RFC 1918 اختصاصی در نظر گرفته می‌شوند. به کار بردن این آدرس‌ها در اینترنت ممنوع است. این آدرس‌ها می‌توانند همزمان در دامنه‌های مختلف مدیریتی بدون نگرانی از ناسازگاری آن‌ها مورد استفاده قرار گیرند. بعضی از کارشناسان در صنعت باور دارند که این آدرس‌ها قابل مسیردهی نیستند که این درست نیست.

۲. B. APIPA از آدرس اختصاصی لینک محلی با محدوده‌ی 169.254.0.0 تا 169.254.255.255 و یک ماسک زیرشبکه‌ی 255.255.0.0 (RFC 3330 مراجعه شود) استفاده می‌کند. آدرس‌های APIPA توسط کلاینت‌های DHCP که نمی‌توانند با یک سرور DHCP ارتباط حاصل کنند و پیکربندی جایگزین استاتیک ندارند به کار می‌رود. این آدرس‌ها قابل مسیردهی در اینترنت نیستند و به طور پیش‌فرض نمی‌توانند در مسیریاب‌های شبکه‌های بزرگ به کار روند.

۳. C. آدرس‌های IP اختصاصی مانند آدرس‌های منبع و مقصد در اینترنت قابل مسیردهی نمی‌باشند. به همین دلیل، هر موجودیتی که مایل به استفاده‌ی داخلی از چنین آدرس‌هایی باشد می‌تواند بدون ایجاد ناسازگاری با سایر موجودیت‌ها یا بدون درخواست اجازه از هر ثبت کننده یا تأمین کننده‌ی خدمات این عمل را انجام دهد. علی‌رغم مجاز نبودن در اینترنت، آدرس‌های IP اختصاصی کاملاً قابل مسیردهی روی اینترانت‌های اختصاصی هستند.

۴. D. محدوده‌ی کلاس A از 1 تا 126 در اولین octet/byte می‌باشد، بنابراین این سبب نادرست بودن گزینه‌ی B می‌شود. فقط گزینه‌ی D یک آدرس کلاس A معتبر می‌باشد.

۵. C. محدوده‌ی کلاس B از 128 تا 191 در اولین octet/byte است. فقط گزینه‌ی C یک آدرس B معتبر است.

۶. B. اگر تمام بیت‌های میزبان روشن باشند (1 باشند). این یک آدرس پخش فراگیر برای آن شبکه خواهد بود.

۷. B. یک پخش لایه‌ی 2 نیز به عنوان یک پخش آدرس MAC به حساب می‌آید که بر حسب هگزا دسیمال و برابر FF:FF:FF:FF:FF:FF می‌باشد.

۸. C. یک ماسک زیرشبکه‌ی کلاس C به طور پیش‌فرض برابر 255.255.255.0 است که این یعنی این‌که اولین سه octets یا اولین 24 بیت تعداد شبکه را نشان می‌دهد.

۹. A. بسته‌هایی که به یک آدرس تک‌پخشی آدرس‌دهی شوند به یک رابط منفرد تحویل داده می‌شوند. برای متعادل‌سازی بار، رابط‌های چندتایی می‌توانند از یک آدرس استفاده نمایند.

۱۰. C. یک آدرس APIPA به صورت 169.254.*x.x* است. آدرس میزبان در این‌جا یک آدرس عمومی است.

۱۱. B. یک آدرس IPv6 دارای 128 بیت است.

۱۲. B. بسته‌هایی که به یک آدرس پخش گروهی آدرس‌دهی شوند مانند IPv4، به تمام رابطه‌های شناخته شده توسط آدرس پخش گروهی تحویل داده می‌شوند. یک آدرس پخش گروهی یک آدرس یک-به-چند نیز نامیده می‌شود. شما می‌توانید آدرس‌های پخش گروهی را بر حسب IPv6 بنویسید، زیرا آن‌ها همواره با *FF* شروع می‌شوند.

۱۳. C. آدرس‌های Anycast رابط‌های چندگانه را که مشابه‌ی آدرس‌های پخش گروهی است شناسایی می‌کند، به هر حال تفاوت بزرگ این‌است‌که بسته‌ی Anycast فقط به یک آدرس تحویل می‌شود، اولین آدرسی که پیدا می‌کند را بر حسب فاصله‌ی مسیریابی تعریف می‌کند. این آدرس یک-به-یک-از-چندتا نیز نامیده می‌شود.

۱۴. A، C. آدرس حلقه‌ی برگشتی با IPv4 برابر 127.0.0.1 است. با IPv6 آن آدرس به صورت 1:: است.

۱۵. B، D. به هنگام نوشتن یک آدرس IPv6، برای کوتاه‌تر کردن طول این آدرس، می‌توان به جای میدان‌های متوالی صفر، یک کولن دوبل قرار داد. تلاش برای کوتاه‌تر کردن بیشتر آدرس ممکن است منجر به حذف صفر شود. همانند IPv4 یک رابط دستگاه منفرد می‌تواند بیشتر از یک آدرس داشته باشد، اما با IPv6 انواع مختلف آدرس‌ها وجود دارند و مقررات مشابهی اعمال می‌شود. آدرس‌های لینک محلی، تک‌پخشی سراسری و پخش گروهی می‌تواند وجود داشته باشد که تمام به یک رابط مشابه اختصاص داده می‌شوند.

۱۶. C، D. آدرس‌های IPv4، 32 بیتی هستند و به صورت دهدهی نمایش داده می‌شوند.

۱۷. D. فقط گزینه‌ی D در کلاس C با محدوده از 192 تا 224 است. این ممکن است غلط به نظر برسد، زیرا یک 255 در آدرس وجود دارد، اما این غلط نیست شما می‌توانید یک 255 در آدرس شبکه داشته باشید.

۱۸. C، E. محدوده‌ی آدرس اختصاصی کلاس A از 0.0.0.0 تا 10.255.255.255 است. آدرس اختصاصی کلاس B از 172.16.0.0 تا 172.31.255.255 و آدرس اختصاصی کلاس C از 192.168.0.0 تا 192.168.255.255 می‌باشد.

۱۹. B. محدوده‌ی آدرس اختصاصی از 0.0.0.0 تا 10.255.255.255 از 172.16.0.0 تا 172.31.255.255 و از 192.168.0.0 تا 192.168.255.255 است. همچنین آدرس‌های 224.0.0.0 تا 239.255.255.255 برای آدرس‌دهی پخش گروهی رزرو شده است.

۲۰. C. گزینه‌ی C یک آدرس پخش گروهی است و نمی‌تواند برای آدرس‌دهی میزبان‌ها به کار رود.

فصل ۸: زیرشبکه‌سازی IP، عیب‌یابی IP و مقدمه‌ای بر NAT

۱. D. (255.255.255.224) 27/ A دارای 3 بیت on (3 بیت 1) و 5 بیت off (5 بیت "0") می‌باشد. این بیت‌ها 8 زیرشبکه را به وجود می‌آورد که هر کدام 39 میزبان دارند. آیا مهم است که ماسک با آدرس شبکه‌ی کلاس A، B، و C به کار رود؟ به هیچ وجه. تعداد بیت‌های میزبان هرگز تغییر نخواهد کرد.

۲. B. این یک کلاس A است. ماسک زیرشبکه‌ی شما چیست؟ 255.255.255.128. صرف‌نظر از کلاس آدرس، این یک بلوک با اندازه‌ی 128 در چهارمین octet است. زیرشبکه‌ها عبارتند از 0 و 128. محدوده‌ی میزبان زیرشبکه‌ی 0، از 126-1 با آدرس پخش برابر 127 می‌باشد. محدوده‌ی میزبان زیرشبکه‌ی 128 از 254-129 می‌باشد که یک آدرس پخش 255 دارد. شما به یک مسیریاب برای این دو میزبان برای برقراری ارتباط نیاز دارید زیرا آن‌ها در زیرشبکه‌های مختلف می‌باشند.

۳. C. این یک سوال نسبتاً ساده است. 28/ A برابر 255.255.255.240 است که یعنی اندازه‌ی بلوک ما در octet چهارم برابر 16 است (0، 16، 32، 48، 64، 80، و غیره). میزبان در زیرشبکه‌ی 64 است.

۴. F. یک آدرس CIDR از 19/ برابر 255.255.224.0 می‌باشد. این یک آدرس کلاس B است به طوری‌که 3 بیت زیرشبکه دارد، اما 13 بیت میزبان، یا 8 زیرشبکه دارد، هر کدام دارای 8,190 میزبان می‌باشد.

۵. C. ID میزبان 10.0.37.144 با یک ماسک 255.255.254.0 در زیرشبکه‌ی 10.0.36.0 قرار دارد (بله شما در این آزمون باید بتوانید زیرشبکه بسازید!) نگران این نباشید که این یک کلاس A است. آنچه که ما به آن توجه داریم این‌است‌که سومین octet دارای بلوکی با اندازه‌ی 2 است، به‌طوری‌که زیرشبکه‌ی بعدی 10.0.38.0 بوده و آدرس پخش برابر 10.0.37.255 خواهد شد. آدرس گیت‌وی پیش‌فرض، 10.0.38.1 به عنوان میزبان در یک زیرشبکه قرار ندارند. اگرچه این یک آدرس کلاس A است، باید به آسانی بتوانید آن را زیرشبکه‌سازی کنید، زیرا شما بیشتر ماسک زیرشبکه را مورد بررسی قرار می‌دهید و octet مورد توجه خودتان را می‌یابید که سومین octet در این سوال می‌باشد. 2 = 254 – 256. اندازه‌ی بلوک 2 است.

۶. D. صرف‌نظر از کلاس آدرس، 30/ A دارای یک 252 در چهارمین octet است. این یعنی که بلوکی با اندازه‌ی 4 داریم و زیرشبکه‌های‌مان عبارتند از 0، 4، 8، 12، 16، و غیره. آدرس 14 به طور آشکار در 12 زیرشبکه قرار دارد.

۷. D. یک لینک نقطه – به – نقطه فقط از دو میزبان استفاده می‌کند. 30/ A یا 255.255.255.252، ماسک به ازای هر زیرشبکه، دو میزبان فراهم می‌کند.

۸. C. دستگاه‌هایی که در لایه‌ی 3 عمل می‌کنند مانند مسیریاب‌ها و فایروال‌ها، تنها دستگاه‌هایی هستند که می‌توانند در پشتیبانی از NAT، سرآیند IP را دستکاری کنند.

۹. A. صرف‌نظر از کلاس آدرس، (255.255.255.248) 29/ A فقط دارای 3 بیت میزبان است. 6 میزبان حداکثر تعداد میزبان‌ها در این LAN از جمله رابط مسیریاب می‌باشد.

۱۰. C. یک کامپیوتر باید با آدرس IP پیکربندی شود که سرتاسر شبکه‌های بزرگ قابل دسترسی باشد. این کامپیوتر باید به یک ماسک زیرشبکه‌ای پیکربندی شود که با تمام دستگاه‌های دیگر در زیرشبکه‌ی محلی خود و نه الزاماً با دستگاه‌هایی که با ماسک مورد استفاده در هر زیرشبکه محلی خود سازگار باشد. این کامپیوتر همچنین باید با یک گیت‌وی پیش‌فرض که با آدرس IP رابط شبکه‌ی محلی خود سازگار است پیکربندی شود.

۱۱. A. (255.255.255.248) 29/ A دارای بلوکی با اندازه‌ی 8 در چهارمین octet می‌باشد. این یعنی زیرشبکه‌های 0، 8، 16، 24، و غیره. زیرشبکه‌ی بعدی 16 است و بنابراین 15، آدرس پخش است.

۱۲. B. یک ماسک 24 بیتی یا طول پیشوند نشان می‌دهد که تمام چهارمین octet برای شناسایی میزبان به کار می‌رود. در حالت خاص، مانند این مسئله ساده‌تر است، تمام مقادیر را 0 در نظر گرفت (172.16.1.0) و تمام مقادیر را 1 در نظر گرفت (172.16.1.255). بالاترین آدرس قابل استفاده، آخرین آدرس قبل از مقدار تمام "1" برابر 172.16.1.254 است.

۱۳. A، B. ابتدا اگر همان‌طور که در شکل نشان داده شده است، دو میزبان به طور مستقیم به هم متصل شوند، در این صورت به یک کابل crossover نیاز دارید. یک کابل straight-through قابل استفاده نمی‌باشد. دوم این‌که میزبان‌ها ماسک‌های مختلف دارند که آن‌ها را در زیرشبکه‌های متفاوت قرار می‌دهند. راه حل آسان‌تر فقط تنظیم هر دو ماسک به (/24) 255.255.255.0 می‌باشد.

۱۴. A. ماسک 25/ A به صورت 255.255.255.128 است. سومین و چهارمین octet همراه با شبکه‌ی کلاس B برای زیرشبکه‌سازی با مجموع 9 بیت زیرشبکه به کار می‌روند: 8 بیت در سومین octet و 1 بیت در چهارمین octet. چون فقط 1 بیت در octet چهارم است، بیت یا off است یا on که برابر یک مقدار 0 یا 128 است. میزبان مورد سوال در زیرشبکه‌ی 0 قرار دارد که یک آدرس پخش 127 می‌باشد، زیرا 128، زیرشبکه‌ی بعدی است.

۱۵. A. 28/ A یک ماسک 255.255.255.240 است. بگذارید تا نهمین زیرشبکه را شمارش نماییم (ما باید آدرس پخش هشتمین زیرشبکه را بدانیم، بنابراین باید تا زیرشبکه‌ی نهم را شمارش کنیم). ما از 16 شروع می‌کنیم (توجه کنید که در سوال آمده است که ما زیرشبکه‌ی 0 را استفاده نخواهیم کرد، پس از 16، نه 0 شروع می‌کنیم): 16، 32، 48، 64، 80، 96، 112، 128، 144. هشتمین زیرشبکه 128 است و زیرشبکه‌ی بعدی 144 می‌باشد، بنابراین آدرس پخش ما از 128 زیرشبکه برابر 143 است. این سبب می‌شود محدوده‌ی میزبان 129-142 باشد. 142 آخرین میزبان معتبر می‌باشد.

۱۶. C. 28/ A یک ماسک 255.255.255.240 است. اولین زیرشبکه 16 است (به خاطر داشته باشید که طبق بیان مسئله از زیرشبکه‌ی 0 نباید استفاده شود) و زیرشبکه‌ی بعدی 32 است، بنابراین آدرس پخش برابر 31 می‌باشد. این سبب می‌شود که محدوده‌ی میزبان ما از 17-30 باشد. 30 آخرین میزبان معتبر است.

۱۷. A. بهترین روش در این‌جا بررسی پیکربندی دستگاه‌هایی است که در حال استفاده از مسیریاب کهنه به عنوان گیت‌وی برای بقیه‌ی شبکه‌های بزرگ می‌باشند. مسیریاب‌ها به طور تناوبی پیکربندی‌شان را برای سرورهای مختلف ذخیره نمی‌کنند. شما ممکن است پیکربندی مسیریاب‌های کهنه را به یک سرور TFTP یا شبیه آن کپی کرده باشید، اما اگر این کار با موفقیت انجام نشود، باید پیکربندی را دوباره انجام دهید که خیلی بیشتر از آدرس‌های رابط باشد. بنابراین نسخه‌برداری و نگهداری یک نسخه از پیکربندی جاری مسیریاب گزینه عاقلانه‌ای است. مسیریاب‌ها خودشان را به طور خودکار پیکربندی نمی‌کنند و ما هم نمی‌خواهیم آن‌ها این کار را انجام دهند.

۱۸. E. ID یک شبکه‌ی کلاس B با یک ماسک 22/ به صورت 255.255.252.0 است که اندازه‌ی بلوک در سومین octet برابر 4 است. آدرس شبکه در این سوال در زیرشبکه‌ی 172.16.16.0 با یک آدرس پخش 172.16.19.255 است. فقط گزینه‌ی E دارای ماسک زیرشبکه فهرست شده است و 172.16.18.255 یک میزبان معتبر است.

۱۹. D، E. آدرس IP مسیریاب در رابط E0 برابر 172.16.2.1/23، که یک 255.255.254.0 است. این سبب می‌شود تا سومین octet دارای بلوکی به اندازه‌ی 2 باشد. رابط مسیریاب در زیرشبکه 2.0 و آدرس پخش برابر 3.255 است، زیرا زیرشبکه‌ی بعدی 4.0 می‌باشد. محدوده‌ی میزبان معتبر از 2.1 تا 3.254 است. مسیریاب در حال استفاده‌ی اولین آدرس میزبان معتبر در محدوده می‌باشد.

۲۰. A. NAT می‌تواند اجازه دهد با به کار بردن PAT تا 65,000 میزبان با یک آدرس IP به اینترنت دسترسی پیدا کنید.

فصل ۹: مقدمه‌ای بر مسیریابی IP

۱. C. RIP، RIPv2، و EIGRP همه مثال‌هایی از پروتکل‌های مسیریابی هستند.

۲. C. در مسیریابی پویا، مسیریاب‌ها در تمام شبکه‌هایی که می‌شناسند یکدیگر را به‌روزرسانی کرده و این اطلاعات را در جدول مسیریابی قرار می‌دهند. این امر به دلیل وجود یک پروتکل مشابه در مسیریاب‌هایی که با یکدیگر ارتباط برقرار می‌کنند امکان‌پذیر است. اگر در شبکه تغییری صورت پذیرد، پروتکل مسیریابی پویا به طور خودکار تمام مسیریاب‌ها را از این رویداد آگاه می‌سازد.

۳. D. مسیریابی دینامیک در شبکه‌های بزرگ خوب عمل می‌کند و مسیرها به طور خودکار به جدول مسیریابی اضافه می‌شوند. مسیریابی استاتیک با دست انجام می‌شود. بدین صورت که در هر بار یک مسیر به مسیریاب داده می‌شود.

۴. B. آدرس‌های کنترل دسترسی به رسانه‌ی MAC همواره در LAN محلی هستند و هیچ‌گاه از مسیریاب عبور نمی‌کنند و آن را نادیده نمی‌گیرند.

۵. C. همگرایی مسیریابی زمان لازم برای پروتکل‌های مسیریابی است تا جداول مسیریابی (جداول ارسال) را در تمام مسیریاب‌های شبکه به‌روزرسانی کنند.

۶. D. فرمان arp -a کش ARP را روی میزبان شما نشان می‌دهد.

۷. D. یک مسیریاب سیگنال پخش را برای جستجوی شبکه‌ی راه دور نخواهد فرستاد، مسیریاب بسته را به دور می‌اندازد.

۸. C. 2 و RIPv1 و IGRP تمام پروتکل‌های بردار فاصله (DV) هستند. مسیریاب‌ها با استفاده از پروتکل DV تمام یا بخشی از جدول مسیریابی خودشان را به صورت یک پیام مسیریابی به‌روز شده در فواصل منظم به هر یک از مسیریابی مجاورشان ارسال می‌کنند.

۹. C، D. پروتکل‌های OSPF (ابتدا کوتاه‌ترین مسیر را باز کنید) و سیستم میانی – به – سیستم میانی (IS-IS) از پروتکل‌های مسیریابی LS می‌باشند.

۱۰. B. تنها پروتکلی که باید انتخاب کنید پروتکل EIGRP می‌باشد.

۱۱. A. پروتکل مسیریابی گیت‌وی داخلی یک پروتکل گیت‌وی داخلی DV می‌باشد.

۱۲. C. پروتکل گیت‌وی مرزی BGP متداول‌ترین انتخاب برای ISPها یا شرکت‌های بزرگ است.

۱۳. A، C. بردار فاصله‌ی DV و وضعیت لینک LS دو پروتکل مسیردهی هستند که باید مورد توجه قرار گیرند.

۱۴. A، D. یک فریم از آدرس‌های MAC برای ارسال یک بسته در LAN استفاده می‌کند. اگر بسته برای یک شبکه‌ی راه دور مقصددهی شده باشد، فریم بسته را یا به یک میزبان در LAN و یا به یک رابط مسیریاب می‌فرستد.

۱۵. A. بسته‌ها به طور مشخص باید به یک مسیریاب حمل شوند تا به یک شبکه مسیریابی شوند.

۱۶. C. به خاطر داشته باشید که فریم در هر گام تغییر می‌کند، اما بسته هرگز تغییر نمی‌کند تا به دستگاه مقصد برسد.

۱۷. D. وقتی جداول مسیریابی تکمیل شوند، چون این جداول شامل اطلاعاتی در مورد تمام شبکه‌های موجود در یک شبکه‌ی بزرگ می‌باشند، آن‌ها به عنوان جداول همگرا در نظر گرفته می‌شوند.

۱۸. A. این گام ۶ در فرآیند مسیردهی IP است. اگر آدرس سخت‌افزار در حافظه‌ی ARP میزبان وجود نداشته باشد، یک ARP پخش برای شبکه‌ی محلی برای جستجوی آدرس سخت‌افزار ارسال می‌کند.

۱۹. C. بهترین پاسخ این‌است‌که با استفاده از یک مسیر استاتیک موقت، ترافیک را دوباره مسیریابی کنیم تا نگهداری در مسیریاب کامل شود.

۲۰. A. وقتی که بسته‌ای به هنگام بازگشت به میزبان اولیه به دلیل خطای نامعلوم گم شود به احتمال زیاد یک پیام درخواست Time-Out را مشاهده خواهید کرد.

فصل ۱۰: پروتکل‌های مسیریابی

۱. C، D، F. RIPv1 و IGRP پروتکل‌های مسیریابی بردار فاصله‌ی واقعی می‌باشند و کار زیادی نمی‌توانند انجام دهند به جزء ساختن و نگهداری جداول مسیریابی و استفاده از پهنای‌باند زیاد! RIPv2، EIGRP و OSPF جداول مسیریابی را می‌سازند و نگهداری می‌کنند، اما همچنین مسیریابی بدون کلاس را فراهم می‌کنند که VLSM اختصارسازی و شبکه‌سازی ناپیوسته را مجاز می‌سازد.

۲. C، B. RIP و RIPv2 پروتکل مسیریابی بردار فاصله هستند. OSPF و IS-IS وضعیت لینک می‌باشند.

۳. A، D. RIP و RIPv2 پروتکل‌های مسیریابی بردار فاصله می‌باشند. OSPF و IS-IS وضعیت لینک هستند.

۴. E. RIP و RIPv2 پروتکل‌های مسیریابی بردار فاصله هستند. OSPF و IS-IS وضعیت لینک هستند. EIGRP از کیفیت‌های ناشی از بردار فاصله و وضعیت لینک هر دو برای ایجاد پروتکل مسیریابی ترکیبی استفاده می‌کند.

۵. C. مسیریابی دینامیک نوعاً در شبکه‌های امروزی به کار می‌رود، زیرا از آن برای بزرگ‌تر کردن شبکه‌ها و حجم کاری کم مدیریتی استفاده می‌شود.

۶. D. EIGRP یک پروتکل مسیریابی هایبرید نامیده می‌شود، زیرا از مشخصات پروتکل‌های مسیریابی بردار فاصله و وضعیت لینک هر دو استفاده می‌کند. به هر حال EIGRP فقط روی مسیریاب‌های Cisco اجرا می‌شود.

۷. C. مسیرهای استاتیک می‌تواند یک راه حل خوب باشد، اما توجه داشته باشید که آن‌ها دینامیک نیستند و اگر یک وسیله از کار بیافتد، مسیرهای جدید به شبکه‌های راه دور به طور خودکار به‌روز نمی‌شوند، بنابراین OSPF بهترین پاسخ است. این مسیر به طور دینامیکی جداول مسیریابی را به همگرایی سریع‌تر و سپس RIP را به روز خواهد کرد.

۸. C. فاصله‌ی مدیریت (AD) پارامتر بسیار مهمی در یک پروتکل مسیریابی می‌باشد. هر چه AD کمتر باشد مسیر مطمئن‌تر خواهد بود. اگر شما اجرای IGRP و OSPF را داشته باشید، طبق پیش‌فرض مسیرهای IGRP به‌جای جدول مسیریابی قرار داده می‌شود، زیرا IGRP دارای AD کمتر از 100 می‌باشد. OSPF دارای یک AD برابر 110 است. RIPv1 و RIPv2 هر دو دارای AD معادل 120 و EIGRP کمترین AD برابر 9 را دارد.

۹. B. پروتکل‌های مسیریابی که به‌روز می‌شوند تا مسیرهای IPv6 را اعلان نمایند عبارتند از RIPng، OSPFv3 و EIGRPv6. IS-IS هم می‌تواند مسیرهای IPv6 را اعلام نماید، اما برای IS-IS به‌روز شدن لازم نیست.

۱۰. C. پروتکل‌های مسیریابی دینامیک مانند RIP، EIGRP و OSPF به طور خودکار به‌روزرسانی‌های مسیر را در جدول مسیریابی اضافه می‌کنند. مسیرهای استاتیک باید با دست اضافه شوند.

۱۱. A. پروتکل‌های بردار فاصله RIPv1 و RIPv2 هر دو دارای حداکثر تعداد گام برابر 15 می‌باشند (توجه کنید که 16 غیر قابل دسترس می‌باشد). IGRP و EIGRP دارای تعداد گام 255 و OSPF ماکزیمم گام ندارد.

۱۲. B. زمان همگرایی مسیریابی در خیلی از پروتکل‌ها برای خیلی از دستگاه‌ها رخ می‌دهد، اما زمان همگرایی مسیریابی زمانی است برای تمام مسیریاب‌ها تا جداول مسیریابی خود را به‌روز کنند (جداول ارسال).

۱۳. C. BGP برای اتصال سیستم‌های خودگردان اینترنت به یکدیگر به کار می‌رود تا ویژگی آن‌ها مسیریابی بدون کلاس و اختصارسازی را ممکن سازد. این قابلیت‌ها کمک می‌کنند تا جداول مسیریابی در مرکز ISP کوچک‌تر و کارآمدتر نگه‌داشته شود.

۱۴. B. RIPv1 هر ۳۰ ثانیه سیگنال پخش را ارسال می‌کند و دارای AD برابر 120 است. RIPv2 هر ۳۰ ثانیه سیگنال پخش گروهی (224.0.0.9) را ارسال می‌کند و AD آن 120 می‌باشد. RIPv2 اطلاعات ماسک زیرشبکه را با به به‌روزرسانی مسیر ارسال می‌کند که سبب می‌شود تا شبکه‌های بدون کلاس و شبکه‌های جدا از هم را پشتیبانی نماید. RIPv2 همچنین احراز هویت بین مسیریاب‌ها را پشتیبانی می‌کند و RIPv1 این عمل را انجام نمی‌دهد.

۱۵. A، B. RIPv1 و RIPv2 دارای AD برابر 120 و EIGRP دارای AD برابر 90 می‌باشند.

۱۶. C. ویژگی‌های پروتکل گیت‌وی مرزی BGP شامل آدرس IP برای رسیدن به AS بعدی (ویژگی جهش-بعدی) و همچنین یک نشانه در این خصوص که چگونه شبکه‌ها در انتهای مسیر به داخل BGP معرفی می‌شوند می‌باشد (ویژگی کد مبدأ). اطلاعات مسیر AS برای ساخت یک گراف از سیستم‌های خودگردان حلقه-آزاد بهره‌مند هستند و برای شناسایی مقررات مسیریابی به کار می‌روند به طوری‌که محدودیت‌ها بر رفتار مسیریابی می‌تواند بر اساس مسیر AS اجرا شود.

۱۷. A. RIPng دارای ویژگی‌های مشابه‌ی زیادی با RIPv2 می‌باشد: این یک پروتکل بردار فاصله است و حداکثر تعداد جهش آن 15 می‌باشد؛ و از افق تقسیم شده، و سایر مکانیسم‌های اجتناب از حلقه نیز استفاده می‌کند. این پروتکل از پخش گروهی برای ارسال به‌روزرسانی‌هایش استفاده می‌کند، اما در IPv6، از FF02::9 برای آدرس انتقال استفاده می‌شود. برای RIPv2، آدرس پخش گروهی 224.0.0.9 بود، بنابراین این آدرس باز هم یک 9 در انتهای محدوده‌ی پخش گروهی IPv6 جدید دارد.

۱۸. B، C. EIGRP در RAM خود سه جدول را نگهداری می‌کند: همسایه، توپولوژی و مسیردهی. جداول همسایه و توپولوژی با به کار بردن بسته‌های hello ساخته شده و نگهداری می‌شود.

۱۹. D. یک مسیر جانشین توسط EIGRP برای ارسال ترافیک به یک مقصد و ذخیره در جدول مسیریابی به کار می‌رود. این توسط یک مسیر جانشین عملی که در جدول توپولوژی در صورت وجود ذخیره می‌شود پشتیبانی می‌گردد. توجه داشته باشید که تمام مسیرها در جدول توپولوژی هستند.

۲۰. A. RIP و RIPv2 فقط از شمارش گام به عنوان یک معیار با حداکثر گام 15 برای پیدا کردن بهترین مسیر به یک شبکه‌ی راه دور استفاده می‌کند.

فصل ۱۱: سوئیچینگ و LANهای مجازی

۱. D. با ایجاد و اجرای VLANها در شبکه‌ی سوئیچ شده، می‌توانید دامنه‌های پخش را در لایه‌ی 2 تقسیم‌بندی نمایید. برای میزبان‌ها در VLANهای مختلف جهت برقراری ارتباط باید دارای یک مسیریاب یا سوئیچ لایه‌ی 3 باشید.

۲. B، D. میزبان‌ها به یک سوئیچ متصل‌اند و اعضای یک VLAN هستند. این یک پورت دستیابی نامیده می‌شود. لینک‌های اصلی بین سوئیچ‌ها متصل می‌شوند و اطلاعات مربوط به تمام VLANها را عبور می‌دهند.

۳. C. LANهای مجازی، دامنه‌های پخش را به شبکه‌های سوئیچ شده در لایه‌ی 2 را به دامنه‌های کوچک‌تر تقسیم‌بندی می‌کند.

۴. C، E. 802.1d و 802.1w هر دو نسخه‌های IEEE STP هستند که در آن 802.1w جدیدترین و بزرگ‌ترین نسخه می‌باشد.

۵. E، D. بهترین پاسخ‌ها این‌است‌که عضویت VLAN برای پورت به طور نادرست پیکربندی می‌شود و این‌که STP پورت را خاموش می‌کند.

۶. B، C، F. VLANها دامنه‌های پخش را به شبکه‌ی لایه‌ی 2 سوئیچ شده تقسیم‌بندی می‌کند یعنی به دامنه‌های پخش کوچک‌تر تقسیم می‌کند. آن‌ها با استفاده از تابع منطقی به‌جای محل فیزیکی پیکربندی می‌شوند و اگر خوب پیکربندی شوند می‌توانند امنیت لازم را فراهم کنند.

۷. B. پروتکل درخت پوشا برای متوقف نمودن حلقه‌های سوئیچینگ در یک شبکه‌ی سوئیچ شده با مسیرهای افزونه به کار می‌رود.

۸. A، E. پل‌ها دامنه‌های تصادم را به قسمت‌های کوچک‌تر تقسیم می‌کند که این عمل تعداد دامنه‌های پخش در یک شبکه را افزایش می‌دهد.

۹. C. برای این‌که تمام فریم‌هایی که از سوئیچ می‌گذرند را ببینیم و بسته را با یک تحلیل‌گر شبکه بخوانیم باید قرینه‌سازی پورت را روی پورتی که میزبان تشخیص عیب شما قرار دارد فعال‌سازی کنید.

۱۰. C. Trunking این امکان را برای سوئیچ‌ها فراهم می‌سازد تا اطلاعات را در اطراف بسیاری از VLANها یا تمام آن‌ها که روی سوئیچ‌ها پیکربندی شده‌اند عبور دهد.

۱۱. A، C، E. ویژگی‌های لایه‌ی 2 شامل فراگیری آدرس، ارسال داده و فیلتر کردن شبکه و اجتناب از حلقه می‌باشد.

۱۲. B. سوئیچ‌ها دامنه‌های تصادم و مسیریاب‌ها دامنه‌های پخش را به قسمت‌های کوچک‌تر تقسیم می‌کنند.

۱۳. C. به استثنا پورت منبع، سوئیچ‌ها تمام فریم‌هایی را که دارای آدرس مقصد نامعلوم‌اند سرریز می‌کند. اگر یک دستگاه به فریم پاسخ دهد، سوئیچ جدول آدرس MAC را برای انعکاس محل دستگاه به‌روز خواهد کرد.

۱۴. C. چون آدرس MAC منبع در جدول آدرس MAC وجود ندارد، سوئیچ، آدرس منبع و پورتی که به آن متصل است را به جدول آدرس MAC اضافه می‌کند، و سپس فریم را به پورت ارسال کننده‌ی بسته‌ها می‌فرستد.

۱۵. D. پروتکل VTP یک روش اختصاصی سیسکو برای داشتن یک پایگاه داده‌ی VLAN مجرد است که با تمام سوئیچ‌های دیگر در شبکه‌ی‌تان ارتباط دارد. این امر مدیریت VLAN را در شبکه‌های بزرگ‌تر آسان‌تر می‌سازد. گزینه‌ی C یک پیکربندی مناسب و ممکن نمی‌باشد.

۱۶. A، B. ترتیب گام‌های همگرایی STP به طور پیش‌فرض، غیر فعال، متوقف، شنیده، یاد گرفته شده و ارسال می‌گردد. وقتی تمام پورت‌ها در وضعیت توقف یا ارسال می‌باشند، STP همگرا می‌شود.

۱۷. C، D. در وضعیت‌های بلوک شده و در حال شنیدن، جدول آدرس MAC در حال یادگیری نمی‌باشد. فقط در وضعیت‌های فراگیری و ارسال، جدول آدرس MAC، آدرس‌های MAC را یاد می‌گیرد و در جدول آدرس MAC جای می‌دهد.

۱۸. B. به طور پیش‌فرض، سوئیچ‌ها دامنه‌های تصادم را به قسمت‌های کوچک‌تر تقسیم می‌کنند، اما شبکه باز هم یک دامنه پخش بزرگ است. برای این‌که دامنه‌های پخش در یک شبکه‌ی سوئیچ شده لایه‌ی 2 به قسمت‌های کوچک‌تر تقسیم شود باید LAN مجازی ایجاد نمود.

۱۹. C. اگر VLANهای صوت را پیکربندی می‌کنید، می‌خواهید QoS را روی پورت سوئیچ پیکربندی کنید تا اولویت بیشتری برای ترافیک صوت در مقایسه با ترافیک داده فراهم گردد تا کیفیت خط افزایش یابد.

۲۰. B. وقتی از پورتی در حال قرینه‌سازی/پوشاسازی در یک سوئیچ استفاده می‌کنید دقت کنید، زیرا فیلد payload روی سوئیچ به وجود می‌آورد و شبکه‌ی شما را متوقف می‌کند. بنابراین ایده‌ی خوبی است این ویژگی را در زمان‌های استراتژیک و فقط برای زمان‌های کوتاه به کار برد.

فصل ۱۲: شبکه‌سازی بی‌سیم

۱. C. قبل از نصب شبکه‌ی بی‌سیم، لازم است که سایت خوب بازدید و پیمایش آن کامل انجام شود. آزمایش انواع مختلف آنتن‌ها و محل آن‌ها مسئله‌ی مهمی برای پوشش دادن تمام ناحیه‌ی بی‌سیم می‌باشد.

۲. D. استاندارد IEEE 802.11a در محدوده‌ی RF، با فرکانس 5GHz اجرا می‌شود.

۳. C. IEEE 802.11b و IEEE 802.11g هر دو در فرکانس 2.4GHz محدوده‌ی RF اجرا می‌شوند.

۴. B، D. اگر شما از فرکانس 802.11b/g استفاده می‌کنید که بیشتر شبکه‌ها در این محدوده کار می‌کنند، در این صورت از آون‌های مایکروویو و تلفن‌های بی‌سیم تداخل دریافت خواهید کرد.

۵. D. 802.11n از پیوند دو محدوده‌ی فرکانس 2.4GHz و 5GHz به منظور به دست آوردن پهنای‌باند بیشتر و سرعت 100Mbps استفاده می‌کند.

۶. استانداردهای IEEE 802.11b,g سه کانال غیر هم‌پوشان را فراهم می‌کنند.

۷. B. استاندارد IEEE 802.11b تا 12 کانال غیر هم‌پوشان را ارائه می‌دهد و اگر استاندارد 802.11b به آن اضافه شود تا 23 کانال را پشتیبانی می‌کند.

۸. D. استاندارد IEEE 802.11a حداکثر سرعت 54Mbps را برای داده فراهم می‌کند.

۹. C. اگر می‌خواهید ناحیه‌ی بزرگی را با دستگاه‌های بی‌سیم پوشش دهید باید نگران هم‌پوشانی کانال باشید.

۱۰. B. استاندارد IEEE 802.11b حداکثر سرعت 11Mbps را برای داده فراهم می‌کند.

۱۱. B. اگر همه چیز به درستی روی میزبان پیکربندی شود، آن‌گاه فیلتر کردن MAC، میزبان را از اتصال به AP متوقف می‌سازد. اگر سعی کنید اتصال به AP را برقرار سازید و موفق نشوید آن‌گاه تنظیمات AP را بررسی کنید.

۱۲. A. استاندارد IEEE 802.11i جایگزین WEP با حالت خاصی از استاندارد احراز هویت پیشرفته‌ی AES معروف به پروتکل (CBC-MAC[1]) است. این به AES-CCMP[2] اجازه می‌دهد تا محرمانه بودن (رمزنگاری) و یکپارچگی داده حفظ شود.

۱۳. C. اگر پخش SSID را غیر فعال سازید (بر حسب ضرورت) آن‌گاه باید نام SSID را در کلاینت‌ها که نیاز به اتصال به AP دارند پیکربندی نمایید.

1. Cipher Block Chaining-Message Authentication Code 2. Aes-Counter Mode CBC-MAC Protocol

۱۴. B. استاندارد IEEE 802.11b از طیف گسترده با توالی مستقیم[1] (DSSS) استفاده می‌کند. اگر شما 802.11g را به کار می‌برید، این استاندارد از مالتی‌پلکس تقسیم فرکانسی متعامد[2] (OFDM) استفاده می‌کند.

۱۵. B. اگر شما در حال اجرای یک مجموعه خدمات توسعه یافته می‌باشید (یعنی بیشتر از یک AP با نام SSID)، باید پوشش سلول را 10 درصد یا بیشتر هم‌پوشان کنید تا فعالیت کلاینت‌ها به هنگام رومینگ متوقف نشود.

۱۶. B. شما باید آنتن جهت‌دار را مانند آنتن یاگی به کار ببرید تا بین دو آنتن بهترین سیگنال را دریافت کنید.

۱۷. A. ID مجموعه خدمات توسعه یافته یعنی که شما بیش از یک نقطه دسترسی دارید که آن‌ها به یک SSID تنظیم می‌شوند و تمام آن‌ها در یک VLAN یا سیستم توزیع به یکدیگر متصل می‌شوند به طوری‌که کاربر می‌تواند رومینگ کند.

۱۸. D. WPA ابزار مناسبی است، زیرا پیکربندی آن آسان است و خوب کار می‌کند. با ورود پسورد می‌توانید کار لازم را انجام دهید. به‌علاوه امنیت بسیار خوب و بالایی دارد، زیرا کلیدها به طور دینامیکی تغییر می‌کنند.

۱۹. C. 802.11n از دو کانال وسیع 20MHz برای ایجاد یک کانال وسیع 40MHz استفاده می‌کند که در بی‌سیم 100Mbps فراهم می‌شود.

۲۰. B. 802.11n MIMO فریم‌های متعددی را از چندین آنتن و از طریق چندین مسیر ارسال می‌کند. فریم‌ها آن‌گاه به وسیله‌ی مجموعه‌ی دیگر از آنتن‌ها ترکیب می‌شوند تا توان عملیاتی و مقاومت مسیر چندگانه بهینه شود. این را مالتی‌پلکسینگ فضایی می‌نامند.

فصل ۱۳: احراز هویت و کنترل دسترسی

۱. B. یک فایروال از یک شبکه‌ی اختصاصی در مقابل کاربران غیر مجاز موجود در یک شبکه‌ی عمومی محافظت می‌کند.

۲. C. در یک شبکه‌ی اختصاصی، فقط کاربران مجاز به داده دسترسی دارند، در مقابل یک شبکه‌ی عمومی هر کاربر داخل شبکه می‌تواند به داده دسترسی داشته باشد.

۳. B. بعد از تعیین این‌که کاربر دسترسی به شبکه‌ی محلی دارد، گام بعدی تأیید آدرس VPN و پسورد است.

۴. D. برای داشتن امنیت خوب در شبکه، آدرس‌های از شبکه‌ی داخلی، آدرس‌های میزبان محلی (127.0.0.0/8)، آدرس‌های اختصاصی رزرو شده و هر آدرس در محدوده‌ی آدرس پخش گروهی IP (224.0.0.0/4) را رد کنید.

۵. D. تونل‌زنی، کپسوله کردن یک پروتکل در داخل پروتکل دیگر جهت تکمیل یک انتقال امن می‌باشد. گزینه‌های A، B و C تمام پروتکل‌های تونل‌زنی هستند که باید آن‌ها را بشناسید، همچنین پروتکل‌های SSL VPN و پروتکل‌های تونل‌زنی نقطه – به – نقطه (PPTP) را نیز باید آشنا باشید.

۶. A. SSL بر اساس رمزنگاری کلید عمومی RSA است و برای تأمین اتصالات لایه‌ی نشست امن در اینترنت بین یک مرورگر وب و یک سرور وب به کار می‌رود.

۷. C. حداقل طول باید 8 و حداکثر طول باید 15 باشد. یک پسورد قوی باید ترکیبی از حروف و اعداد و یک کاراکتر خاص یاشد که به خاطر سپردن آن آسان و حدس آن برای اشخاص دیگر مشکل باشد.

1. Direct Sequence Spread Spectrum 2. Orthogonal Frequency Division Multiplexing

۸. B. IPSec در لایه‌ی شبکه‌ی مدل OSI (لایه‌ی 3) کار می‌کند و تمام کاربردهایی که در بالای آن کار می‌کنند را امن می‌سازد (لایه‌ی 4 و بالا). به‌علاوه، چون توسط IETF و برای کار با IPv4 و IPv6 طراحی شد، پشتیبانی وسیعی از طرف صنعت به عمل می‌آید و سریعاً به عنوان استاندارد VPN روی اینترنت عمل خواهد کرد.

۹. D. IPSec در هر دو حالت انتقال و تونل‌زنی کار می‌کند. در حالت انتقال، یک ارتباط IP مطمئن بین دو میزبان ایجاد می‌شود. از داده با احراز هویت یا رمزنگاری (یا هر دو) محافظت می‌شود. حالت تونل بین نقاط انتهایی شبکه برای محافظت از تمام داده‌هایی که از تونل عبور می‌کنند به کار می‌رود.

۱۰. B. شرکت‌هایی که می‌خواهند مطمئن شوند که داده‌ی آن‌ها در خلال عبور امن است. باید قبل از ارسال داده آن‌ها را رمزنگاری کنند. رمزنگاری فرآیندی است که داده را رمزگذاری و رمزگشایی می‌کند.

۱۱. A، C. بعضی از برنامه‌های کاربردی سودمند قدیمی‌تر شبکه مانند FTP و Telnet قابلیت رمزنگاری پسوردها را ندارند.

۱۲. C. برای رمزگذاری یک پیام و رمزگشایی یک پیام رمزنگاری شده، به کلید یا کلیدهای رمزنگاری مناسب نیاز دارید. کلید رمزنگاری یک جدول یا فرمولی است که تعریف می‌کند کدام کاراکتر در داده به کدام کاراکتر رمزگذاری شده تبدیل می‌شود.

۱۳. C. TLS برای استفاده با VPNها در نسخه‌های جدیدتر TLS موجود بود.

۱۴. D. استاندارد رمزنگاری داده[1] (DES) یک نوع کلید عمومی رمزنگاری نمی‌باشد.

۱۵. D. PPTP یک پروتکل VPN است که توسط مایکروسافت ایجاد شد. و از پورت 1723 برای رمزنگاری داده در سطح کاربرد استفاده می‌کند.

۱۶. B. PPPoE فقط دارای دو مرحله است: مرحله‌ی کشف و نشست. در فاز کشف آدرس MAC هر یک از نقاط انتهایی ارتباط به یکدیگر داده می‌شوند به طوری‌که یک ارتباط PPP امن می‌تواند ایجاد گردد.

۱۷. C. یک اثر انگشت مثالی از چیزی است که شما هستید. سایر مثال‌ها اسکن‌های شبکیه‌ی چشم و تشخیص صورت است.

۱۸. A. سرورهای RADIUS خدمات رمزنگاری و احراز هویت را فراهم کرده و می‌توانند این دو را ترکیب کرده و به یک سرویس تبدیل کنند. RADIUS می‌تواند با رد یا قبول دسترسی در هر دو نوع بی‌سیم و با سیم در سطح دامنه به کار رود.

۱۹. A. RADIUS احراز هویت و اجازه‌ی کاربر را به پایگاه داده متمرکز ترکیب کرده و پروفایل‌های کاربر را نگهداری می‌کند.

۲۰. D. معماری محاسبه با کامپیوتر مستقل[2] (ICA) پروتکلی است که با سیستم‌های Citrix برای تأمین ارتباط بین سرورها و کلاینت‌ها طراحی می‌شود.

فصل ۱۴: شبکه، تهدیدها و کاهش خطرات

۱. D. حمله‌ی رد سرویس (DoS)، از دسترسی کاربران به سیستم جلوگیری می‌کند. تمام گزینه‌ها می‌تواند حملات رد سرویس ممکن می‌باشند.

1. Data Encryption Standard 2. Independent Computing Architecture

۲. C. کرم‌ها، سرقت هویت (phishing) و نقاط دسترسی بدون هویت تمام تهدیداتی هستند که ممکن است بر شبکه تأثیر بد بگذارد.

۳. A. گزینه‌های B، C، و D تمام جزو تهاجم‌های DoS می‌باشند، بنابراین تنها گزینه‌ی واقعی یک ویروس فایل است. یک ویروس فایل به برنامه‌های کاربردی قابل اجرا و فایل‌های برنامه‌ی سیستم حمله می‌کند.

۴. A. در war driving حمله کننده به طور ساده با یک آنتن با قدرت زیاد در اطراف گشت می‌زند. این آنتن به یک کامپیوتر کیفی بی‌سیم متصل است که در حال اسکن شبکه‌ها می‌باشد.

۵. D. تمام این‌ها مثال‌هایی از ویروس‌های سکتور راه‌انداز هستند که وارد رکورد راه‌انداز اصلی شده است. یک ویروس سکتور راه‌انداز، سکتور راه‌انداز را دو مرتبه می‌نویسد و در نتیجه سبب می‌شود این‌طور به نظر برسد که اشاره‌گر برای سیستم عامل وجود ندارد. وقتی کامپیوتر را روشن می‌کنید، پیام سیستم عامل وجود ندارد یا پیام خطای هارددیسک شناخته نمی‌شود را مشاهده خواهید کرد.

۶. A. یک ویروس پخش گروهی ویروسی است که هم بر سکتور راه‌انداز و هم بر فایل‌های روی کامپیوترتان اثر می‌گذارد.

۷. C. یک کرم می‌تواند به طور فعال و بدون دخالت کاربر خود را تکرار کند در حالی‌که یک ویروس فقط اگر یک برنامه‌ی کاربردی را باز کند می‌تواند فعال شده و گسترده شود.

۸. B. یک تهاجم بسیار قوی یک تهاجم وابسته به نرم‌افزار است که برنامه‌ای را به کار می‌برد که روی یک شبکه‌ی هدف اجرا می‌شود و سعی می‌کند به بعضی از انواع منابع شبکه به اشتراک گذاشته شده شبیه یک سرور وارد شود.

۹. A. مهندسی اجتماعی، یا سرقت هویت به تلاش برای به دست آوردن غیر قانونی اطلاعات حساس با وانمود کردن این‌که یک منبع معتبر می‌باشند گفته می‌شود. سرقت هویت معمولاً به صورت یکی از دو فرم زیر انجام می‌شود: از یک ایمیل یا از یک تماس تلفنی.

۱۰. B. مقررات یک میزکار پاک یعنی وقتی که کارمندان، میزکار خود را ترک می‌کنند تمام اسناد مهم مانند کتاب‌ها، طرح‌ها نامه‌های محرمانه و شبیه آن‌ها باید از روی میزکار برداشته شود (و در محلی دیگر نگهداری شوند).

۱۱. D. آموزش تمام کارکنان با آگاه نمودن آن‌ها که افراد ممکن است با تماس با آن‌ها یا با ارسال ایمیل اطلاعاتی را به منظور تهاجم به شرکت جمع‌آوری نمایند بسیار مهم است. این عمل را سرقت هویت یا مهندسی اجتماعی می‌نامند.

۱۲. B. وقتی شما AP را طوری تنظیم می‌کنید تا SSID را پخش نکند، در این صورت AP، SSID را از بسته‌هایی به نام بیکن‌ها (بسته‌هایی هستند که وقتی شبکه‌ها را اسکن می‌کنید، نمایش‌ها را در یک‌جا نشان می‌دهند) حذف می‌کنند، اما هنوز هم SSID در بسیاری دیگر از انواع بسته‌ها وجود دارند.

۱۳. A. یک روال امنیتی یعنی پاسخ مناسب به یک رویداد امنیتی در شبکه‌ی شما.

۱۴. A. به‌زودی بعد از پذیرش آن به عنوان یک معیار امنیتی، مشخص شد که به دلیل ضعف در روش اعمال الگوریتم، برنامه‌هایی که به طور گسترده در اینترنت موجودند می‌توانند برای رخنه در کلید WEP به کار روند.

۱۵. B. برنامه Windows Update برنامه‌ی سودمندی است که به هنگام نصب ویندوز؛ به طور خودکار نصب می‌شود. موتور به‌روز شدن به طور تناوبی سیستم شما را برای نسخه‌ای از اجزای ویندوزی که نصب کرده‌اید اسکن می‌کند و آن‌ها را با جدیدترین نسخه‌های موجود مایکروسافت مقایسه می‌کند. اگر نرم‌افزار شما منقضی شده باشد، یک پنجره‌ی دیالوگ به‌روز شدن ویندوز روی صفحه ظاهر می‌شود و از شما می‌پرسد که آیا می‌خواهید به‌روز شدن‌های نرم‌افزار را نصب کنید.

۱۶. C. با این همه کُد نوشته شده برای برنامه‌های کاربردی و سیستم‌های عامل، تولید کنندگان بعد از اولین تولید دوباره بر می‌گردند تا هر مشکلی که قبلاً مورد بررسی قرار نگرفته است برطرف کنند. این بررسی نهایی به عنوان یک hotfix یا patch ارائه می‌شود.

۱۷. C. ایستگاه‌های بی‌سیم (کامپیوترهای کیفی لپ‌تاپ، PDAها و غیره) یک نقطه‌ی دسترسی انتخاب می‌کنند تا توسط SSID نه توسط کانال، آدرس MAC یا نسبت سیگنال به نویز به آن متصل می‌شوند.

۱۸. D. اسکن ذهنی برای این نوع اسکن به کار می‌رود. موتور به دنبال فعالیت مشکوک که ممکن است یک ویروس باشد به جستجو می‌پردازد.

۱۹. A. هر هفته باید فهرست ویروس‌های خودتان را که فایل‌های تعریف ویروس نام دارد به‌روزرسانی کنید. این کار را از طریق وب‌سایت کارخانه‌های سازنده می‌توانید به طور خودکار یا دستی انجام دهید. در شرکت خودتان می‌توانید از یک سرور جابه‌جایی مرحله به مرحله استفاده کنید تا برنامه‌ی به‌روزرسانی را دانلود و سپس توزیع نماید یا می‌توانید هر کامپیوتر را برای دانلود برنامه‌های به‌روزرسانی تنظیم کنید.

۲۰. D. یک برنامه‌ی آنتی‌ویروس کامپیوتری که مظنون به آلودگی به ویروس است را مورد بررسی قرار داده و ویروس‌ها را که به روش‌های مختلف پیدا می‌کند از بین می‌برد.

فصل ۱۵: امنیت فیزیکی و سخت‌افزاری

۱. C. فایروال‌ها فقط با اجازه دادن بسته‌هایی که از محدودیت‌های امنیتی عبور کرده و ارسال می‌شوند، عمل می‌کند. یک فایروال همچنین می‌تواند اجازه دهد، امتناع ورزد، رمزنگاری کند، رمزگشایی نماید و ترافیک‌های تمام کامپیوترهایی که از طریق آن جریان می‌یابد را پراکسی نماید. این عمل می‌تواند بین شبکه‌ی عمومی و اختصاصی یا بین دامنه‌های امنیتی متفاوت (یا ناحیه‌ها) در یک شبکه‌ی اختصاصی انجام شود. شما به عنوان یک مدیر سیستم می‌توانید مقرراتی را تنظیم کنید که بر اساس آن فایروال برای ارسال یا رد بسته‌های داده تصمیم‌گیری نماید.

۲. A، D. فایروال‌ها در لایه‌ی کاربرد یا لایه‌ی شبکه عمل می‌کنند.

۳. B. یک *فایروال مبتنی بر شبکه* چیزی است که شرکت‌ها برای محافظت شبکه‌ی اختصاصی خودشان از شبکه‌های عمومی به کار می‌برند. مشخصه‌های تعریف شده‌ی این نوع فایروال طوری طراحی می‌شود که از تمام شبکه‌ی کامپیوترها به عنوان یک سیستم محافظت نماید. این معمولاً ترکیبی از سخت‌افزار و نرم‌افزار می‌باشد. یک فایروال مبتنی بر میزبان روی یک ماشین اجرا می‌شود و فقط برای محافظت آن ماشین طراحی می‌شود. غالباً این فایروال به صورت یک نرم‌افزار اجرا می‌شود و به نصب سخت‌افزار اضافی در کامپیوتر شما برای اجرای فایروال مبتنی بر میزبان نیازی نیست.

۴. B. مزیت بزرگ یک فایروال بدون حالت بر فایروال با حالت این‌است‌که از حافظه‌ی کمتری استفاده می‌کند. امروزه فایروال‌های بی‌حالت اگر در یک شبکه‌ی داخلی به کار روند که تهدیدات امنیتی کمتر و محدودیت‌های اندکی وجود دارند بهترین نوع فایروال می‌باشند.

۵. B. NESSUS نمی‌تواند آدرس‌های IP نادرست را شناسایی کند.

۶. C. یکی از سودمندی‌های به کار بردن یک فایروال این‌است‌که کمک می‌کند تا منابع LAN از تهاجم‌های نامطلوب محافظت شود.

۷. B. یک سیستم کشف مزاحمت (IDS)، ترافیک شبکه را تحت نظارت قرار می‌دهد و به جستجوی علائم مزاحمت می‌گردد. مزاحمت‌ها با یک کد تهاجم شناسایی می‌شوند.

۸. B. فایروال‌ها که از فهرست‌های دستیابی استفاده می‌کنند، می‌توانند برقراری ارتباط و ترافیک ورود و خروج بسته‌ها از شبکه را اجازه دهند یا امتناع ورزند.

۹. C. استاندارد، توسعه یافته و خارج از محدوده‌ی همه انواع مختلف ACL می‌باشند.

۱۰. B. شما گاهی می‌توانید از تهاجم چشم‌پوشی کنید، چون ممکن است بر شبکه‌ی شما اثری نداشته باشد. این عمل را اجتناب کردن می‌نامند.

۱۱. C. یک DMZ می‌تواند به روش‌های مختلف زیادی برقرار شود، اما بهترین توصیف DMZ این‌است‌که ضمن ارائه‌ی امکان دسترسی میزبان‌های اینترنت به سرورتان، برای جداسازی و امن نگهداشتن شبکه‌ی داخلی‌تان به کار می‌رود.

۱۲. E. بیشتر فایروال‌ها فیلترینگ محتوا، شناسایی امضا، توانایی جداسازی سگمنت‌های شبکه به نواحی امنیتی جدا از هم را فراهم می‌کنند. بیشتر فایروال‌ها می‌توانند خدمات اسکن کردن را نیز انجام دهند این یعنی آن‌ها انواع مختلف اسکن را روی ترافیک بسته‌های وارده به منظور شناسایی مشکلات انجام می‌دهند.

۱۳. A. یک سیستم تشخیص مزاحمت (IDS)، ترافیک شبکه را تحت نظر قرار می‌دهد و به جستجوی علائم مزاحمت می‌پردازد. مزاحمت‌ها با سازگاری فعالیت در مقابل کدهای مجوز شناخته شده در داخل بانک اطلاعاتی IDS تشخیص داده می‌شود. اگر مزاحمتی تشخیص داده شود، یک پاسخ غیر فعال مانند ثبت‌وقایع یا آگاهی دادن به یک مدیر شبکه اجرا می‌شود. یک سیستم جلوگیری از مزاحمت IPS مانند یک IDS است ولی با دو تفاوت مهم. ابتدا، می‌آموزد که وضعیت "عادی" در شبکه چیست و چگونه می‌تواند در مقابل اوضاع غیر عادی حتی اگر بخشی از بانک اطلاعاتی کد مجوز نداشته نباشند عکس‌العمل نشان دهد. ثانیاً می‌تواند یک پاسخ فعال را صادر نماید مانند بستن یک پورت، ریست کردن ارتباطات یا تلاش برای آرام کردن یک مهاجم پس از به تله انداختن آن.

۱۴. B. NESSUS یک برنامه‌ی اسکن اختصاصی آسیب‌پذیر است که برای استفاده‌ی تجارتی به مجوز نیاز دارد، هنوز رایج‌ترین برنامه‌ی اسکن مورد استفاده است.

۱۵. C. NESSUS پسوردها را جمع‌آوری نمی‌کند.

۱۶. D. تغییر پیکربندی شبکه، پایان دادن به جلسه‌ها، و فریب دادن تهاجم همه اعمالی هستند که می‌توانند توسط یک دستگاه IPS انجام شوند.

۱۷. D. پراکسی‌ها در کل شبکه طوری عمل می‌کنند تا کاملاً بسته‌ها را از میزبان‌های داخلی و میزبان‌های خارجی جدا سازند.

۱۸. B. NESSUS با انجام اسکن یک پورت و سپس پیگیری آزمایش‌های خاص عمل می‌کند، اما نمی‌تواند ناسازگاری‌های آدرس IP را شناسایی کند.

۱۹. C. یک فایروال با حالت مسیر ارتباطات برقرار شده‌ی گذرنده از آن را تعقیب می‌کند. وقتی که بسته‌ی دیگری دریافت شود که بخشی از یک ارتباط موجود است (بخشی از یک حالت فعلی)، بسته بدون بررسی ACLها عبور می‌کند.

۲۰. C. یک سیستم جلوگیری از مزاحمت (IPS) شبیه یک IDS است، اما با دو تفاوت مهم. تفاوت اول این‌که وضعیت عادی را در شبکه می‌آموزد و می‌تواند در مقابل اوضاع غیر عادی حتی اگر آن‌ها بخشی از بانک اطلاعاتی کدهای مجوز نباشند عکس‌العمل نشان دهند. تفاوت دوم این‌که می‌تواند یک پاسخ فعال را صادر کند مانند بستن یک پورت، ریست کردن ارتباطات یا تلاش برای آرام کردن یک مهاجم پس از به تله انداختن آن.

فصل ۱۶: شبکه‌های WAN

۱. D. پروتکل اطلاعات مسیریابی (RIP) یک پروتکل WAN نیست، اما یک پروتکل مسیریابی مورد استفاده در شبکه‌های بزرگ است.

۲. C. تمام این پروتکل‌ها و فناوری‌های مختلف سه لایه‌ی پایینی مدل OSI را اشغال می‌کنند: لایه‌ی فیزیکی، لایه‌ی پیوند داده و گاهی‌اوقات لایه‌ی شبکه. بیشتر پروتکل‌های WAN فقط در لایه‌ی فیزیکی و لایه‌ی پیوند داده‌ها عمل می‌کنند.

۳. B. نقطه سر حد، نقطه‌ای است که مسئولیت تأمین کننده‌ی سرویس به پایان می‌رسد و مسئولیت CPE شروع می‌شود.

۴. C. نسخه‌ی اروپایی T1، E1 است که در سرعت 2.048Mbps عمل می‌کند و از 30 کانال 64Kbps (30 DS0s) استفاده می‌کند.

۵. C. نقطه سر حد، نقطه‌ای است که مسئولیت تأمین کننده‌ی خدمات (حامل تبادل محلی) به پایان می‌رسد و مسئولیت CPE شروع می‌شود. معمولاً این در قفسه‌ی دستگاه‌های مخابراتی دستگاهی است که متعلق به شرکت ارتباطات (telco) است و توسط آن‌ها نصب می‌شود.

۶. D. کابل برای یک اداره‌ی کوچک یا یک دفتر (SOHO) مقرون به صرفه است.

۷. C. یک T1 دارای سرعت خط معادل 1.544Mbps است. این ارتباط با سرعت 1.544Mbps از سیگنال دیجیتال 1 (DS1) و 24 کانال 64Kbps را که سیگنال دیجیتال 0 را به کار می‌برند (DS0) در یک‌جا جمع می‌کند. سایر ارتباطات سری T دارای حداکثر سرعت ارتباط بزرگ‌تر می‌باشد.

۸. C. LTE یک 4G واقعی است و دارای بهترین سرعت داده است.

۹. B. OC-1، OC-3، OC-12، OC-48، و OC-192 سرویس‌های عادی هستند. OC-1 دارای کم‌ترین نرخ داده در 51.84Mbps و OC-192 دارای بالاترین نرخ داده در 9.953Gbps است.

۱۰. A. بلوتوث از یک فناوری رادیویی به نام طیف گسترده با جهش فرکانسی[1] (FHSS) استفاده می‌کند. در این فناوری داده‌ای که باید ارسال شود را به قطعاتی تقسیم می‌کند و بخش‌هایی از قطعات داده را از طریق هوا و با 75 فرکانس مختلف ارسال می‌کند.

1. Frequency hopping spread spectrum

۱۱. C. حرف *x* در *x*DSL نشان دهنده‌ی حروف مختلفی است که انواع مختلف DSL را به وجود می‌آورد. *x*DSL از سیگنال‌های با فرکانس بالا استفاده می‌کند در حالی‌که در تلفن‌های معمولی از سیگنال‌هایی با فرکانس پایین در روی همان خط استفاده می‌شود.

۱۲. C. ADSL، HDSL، SDSL، VDSL یا VHDSL و VDSL2 تمام انواع مختلف و رایج *x*DSL می‌باشند. شبکه‌ی نوری همزمان[1] (SONET) استانداردی برای انتقال داده‌ی همزمان از طریق فیبرنوری می‌باشد.

۱۳. D. DOCSIS مخفف کلمات data over cable service interface specification است. تمام مودم‌های کابلی و دستگاه‌هایی شبیه آن را باید بر اساس این استاندارد اندازه‌گیری نمایند.

۱۴. C. حامل نوری 12 دارای سرعت 622Mbps می‌باشد.

۱۵. C. ATM از یک فناوری با سوئیچینگ سلول‌ها و با سرعت بالا استفاده می‌کند. در این فناوری نسبت به انتقال صوت و ویدیو به طور بلادرنگ اقدام می‌شود. پروتکل ATM[2]، داده‌های ارسال شده را به سلول‌ها 53 بایتی تقسیم می‌کند.

۱۶. A. Frame Relay، فناوری WAN فریم است که در آن بسته‌هایی با طول متغیر با سوئیچینگ ارسال می‌شوند.

۱۷. C. سرعت اطلاعات ارسال شده (CIR) سرعت اطلاعات بر حسب بیت بر ثانیه است که سوئیچ Frame Relay انتقال داده را تضمین می‌کند.

۱۸. B. چون ما درباره WAN در حال بحث هستیم، لذا B یک گزینه‌ی درست است. حالت آسنکرون انتقال ATM، طراحی شد تا پروتکل ارتباط با سرعت بالا باشد که به توپولوژی LAN مخصوص بستگی ندارد.

۱۹. B. یک T3 شبیه ارتباط T1 عمل می‌کند، اما دارای سرعت بیشتر 44.736Mbps می‌باشد. این معادل 28 مدار T1 است (یا مجموعاً 672 کانال DS0 است)، که یک سیگنال به نام سیگنال دیجیتال 3 (DS3) را به کار می‌برد.

۲۰. C. مالتی‌پلکسینگ WDM (مالتی‌پلکسینگ تقسیم طول موج) فناوری است که چندین حامل نوری با طول موج‌های مختلف را مالتی‌پلکس کرده و از یک فیبرنوری منفرد ارسال می‌کند.

فصل ۱۷: ابزار عیب‌یابی

۱. C. برنامه‌ی پیدا کننده‌ی اینترنتی بسته (ping)، برای تعیین این‌که آیا یک میزبان دارای پشته‌ی IP با مقدار اولیه است به کار می‌رود.

۲. A. برنامه‌ی سودمند arp برای نمایش محتوای حافظه‌ی ARP به کار می‌رود. این محتوا تحلیل آدرس‌های IP به آدرس‌های فیزیکی (MAC) را دنبال می‌کند و خروجی نمایش داده شده را تولید خواهد کرد.

۳. A. مایکروسافت بعد از ارائه‌ی Windows NT، نرم‌افزار میزکار از راه دور را به طور رایگان با محصولات ویندوز ارائه نمود. وقتی این نرم‌افزار روی کامپیوترهای (در نسخه‌های قدیمی‌تر به طور پیش‌فرض نصب می‌شد) منبع و مقصد هر دو نصب شود یک ارتباط میزکار راه دور ایجاد می‌شود.

۴. B. هدف برنامه‌ی ping، تست کانال ارتباطی بین دو میزبان IP و تعیین این‌که چقدر طول می‌کشد تا بسته‌ها از یک میزبان به میزبان دیگر می‌رسند می‌باشد.

۵. C. برنامه‌ی ipconfig /all پیکربندی TCP/IP فعلی شامل آدرس IP فعلی، پیکربندی DNS، پیکربندی WINS و گیت‌وی پیش‌فرض را روی ایستگاه کاری جاری نشان می‌دهد.

---

1. Synchronous Optical Network 2. Asynchronous Transfer Mode

۶. B، D. آدرس 172.0.0.1 آدرس IP خاص تعیین شده برای رابط TCP/IP محلی است. نام میزبان، میزبان محلی، نام میزبان داده شده به رابط محلی است. بنابراین، ping کردن آدرس IP یا نام میزبان برای رابط محلی به شما خواهد گفت که آیا رابط محلی کار می‌کند یا خیر؟

۷. A. فرمان nbtstat -r تمام تحلیل نام‌های انجام شده توسط کلاینت محلی و آدرس‌های IP مربوطه را نمایش می‌دهد.

۸. C. برنامه‌ی سودمند arp به شما آدرس تحلیل شده‌ی MAC به IP تمام میزبان‌های سگمنت شبکه‌تان را نشان می‌دهد، به خاطر داشته باشید که این برنامه فقط برای میزبان‌های محلی نه میزبان‌های راه دور کار می‌کند.

۹. B. برای پاک‌سازی و بارگذاری مجدد حافظه نام NetBIOS راه دور، باید فرمان nbtstat -R را به کار ببرید. به خاطر داشته باشید که R باید حرف بزرگ باشد و خط فاصله قبل از آن باید نوشته شود در غیر این صورت کار نخواهد کرد.

۱۰. B. استراق سمع و سرقت اطلاعات شبکه‌های تجاری مانند Wireshark و OmniPeek می‌تواند بسته‌ها را به دام اندازند، زیرا آن‌ها NIC را طوری تنظیم می‌کنند تا در حالت بی‌قاعده عمل کند یعنی NIC تمام بسته‌هایی را که می‌بینید پردازش می‌کند.

۱۱. B. برنامه‌ی tracert آن خروجی را به شما می‌دهد. فرمان tracert (یا به طور خلاصه trace) مسیر را از میزبان IP منبع تا میزبان مقصد ردیابی می‌کند.

۱۲. C. برنامه Tracert به شما می‌گوید کدام مسیریاب مشکل عملکرد دارد و چقدر طول می‌کشد تا بتوانید بین هر میزبان حرکت کنید. Tracert می‌تواند برای تعیین ناحیه‌ی بروز مشکل در شبکه‌ی مورد استفاده قرار گیرد.

۱۳. A. سوئیچ ipconfig /all کامل‌ترین فهرست اطلاعات پیکربندی TCP/IP و همچنین نمایش آدرس MAC، زمان‌های اجاره DHCP و آدرس‌های DNS را نشان می‌دهد.

۱۴. C. برنامه‌ی tracert اسامی و آدرس‌های تمام مسیریاب‌ها که از آن طریق بسته‌ها به هنگام رفتن به میزبان مقصد از آن عبور می‌کند را بر می‌گرداند.

۱۵. E. اگر یک میزبان خاص در حال پاسخ دادن روی یک پورت TCP خاص باشد می‌توان از برنامه‌ی telnet برای تست استفاده نمود.

۱۶. C. فرمان arp /a محتوای جاری حافظه‌ی ARP در ایستگاه کاری محلی را نمایش می‌دهد.

۱۷. C. Dig یک فرمان قدیمی unix است که اطلاعات سرور DNS را نشان می‌دهد.

۱۸. D، A. سوئیچ‌های g- و a- برنامه‌ی arp یک عمل مشابه را انجام می‌دهند. این سوئیچ‌ها هر دو حافظه‌ی جاری ARP را نشان می‌دهند.

۱۹. F، E، B. فرمان‌های nslookup، ipconfig و ifconfig به شما سرورهای DNS که کامپیوتر برای استفاده پیکربندی شده است را نشان می‌دهد.

۲۰. C. فرمان nbtstat -s آمارهای پروتکل IP، IPv6، ICMP، ICMPv6، TCP، TCPv6، UDP و UDPv6 را نمایش می‌دهد.

فصل ۱۸: ابزار سخت‌افزاری و نرم‌افزاری

۱. D. اهداف شبکه‌ی CompTIA Network+ تمام سه گزینه را با توجه به ابزار استفاده شده برای تحلیل شبکه‌های امروزه پوشش می‌دهد.

۲. هدف اولیه‌ی استراق سمع ترافیک شبکه و سرقت اطلاعات یا تحلیل کننده‌های شبکه، جمع‌آوری و تحلیل هر یک از بسته‌های منفرد می‌باشد که در یک سگمنت شبکه‌ی خاص اخذ می‌شود تا تعیین شود که آیا مشکلاتی اتفاق افتاده است. شما می‌توانید آن‌ها را برای مشاهده این‌که آیا ترافیک زیادی روی یک سگمنت وجود دارد به کار ببرید.

۳. A. یک toner probe سیگنالی را به یک جفت سیم ارسال می‌کند، به طوری‌که بتوان سیم‌ها را ردیابی نمود. نوعاً یک مجموعه‌ی butt برای پیدا کردن این سیگنال به کار می‌رود، اما پروب تونر بهترین پاسخ به این سوال است.

۴. B. یک بازتاب‌سنج نوری حوزه‌ی زمان (OTDR) یک وسیله‌ی اپتوالکترونیکی است. محل پارگی فیبرنوری را نشان می‌دهد. طرز کار آن بدین صورت است که یک سری پالس‌نوری وارد فیبر خاصی که باید تست شود ارسال می‌گردد. با این عمل می‌توان ملاحظه کرد که آیا پارگی در فیبر اتفاق افتاده است یا خیر و در کجا.

۵. B. برای ایجاد یک کابل patch[1] (568A) به منظور اتصال میزبان‌تان به یک گیره روی دیوار، شما به یک سیم‌چین نیاز دارید.

۶. A. به یاد داشته باشید که فایروال خط مقدم دفاع از شبکه متصل به اینترنت است. اگر شبکه‌ای مستقیماً و بدون فایروال به اینترنت متصل شود، آن‌گاه یک مهاجم با اندکی تلاش می‌تواند به طور نظری به کامپیوترها و سرورهای آن شبکه دسترسی پیدا کند. نرم‌افزار IDS/IPS معمولاً بین مسیریاب داخلی‌تان و فایروال به شبکه‌ی خارجی (اینترنت) متصل می‌شود.

۷. C. یک اسکنر پورت یک قطعه‌ی نرم‌افزار است که برای جستجوی یک شبکه برای میزبان‌های باز طراحی می‌شود. مدیران شبکه از اسکنر پورت برای اطمینان از وجود امنیت استفاده می‌کنند.

۸. D. تست کردن با استفاده از نقشه‌ی سیم‌کشی معمول‌ترین تست کابل‌های زوج سیم به هم تابیده شده می‌باشد. این تست سیم‌های جابه‌جا شده (transposed) اتصال باز (سیم‌های قطع شده یا متصل نشده)، اتصال کوتاه (سیم‌ها و سرهای آن‌ها به طور نامناسب به یکدیگر متصل شده‌اند) را شناسایی می‌کند.

۹. B. یک بازتاب‌سنج حوزه‌ی زمان (TDR) وسیله‌ای است که معایب کابل‌های فلزی مانند زوج سیم‌های تابیده شده و کابل‌های کواکسیال را پیدا کرده و آن‌ها را توصیف می‌کند، معادل این دستگاه برای فیبرهای نوری دستگاه بازتاب‌سنج نوری حوزه‌ی زمان (OTDR) است. یک TDR می‌تواند همچنین سرعت و وضعیت سیگنال در کابل را بررسی نماید.

۱۰. B. یک دستگاه تأیید کننده ترکیبی از یک تستر کابل و تحلیل کننده‌ی شبکه می‌باشد. این دستگاه می‌تواند عملکرد و پاسخ زمانی منابع شبکه را تست کرده و در یک زمان نصب کابل با رده‌ی 6 را تأیید نماید.

۱۱. D. بر خلاف اسکنر پورت، سرقت کننده‌ی اطلاعات در واقع داخل هر بسته در سطح یک فریم و در یک سگمنت شبکه را بررسی می‌کند.

۱۲. C. به دلیل حساسیت به هر گونه تغییر در امپدانس، تمام گزینه‌های A، B، D و E دلایلی هستند که می‌توان یک TDR را به کار برد.

---

1. patch cable

۱۳. A. یک مالتی‌متر یا یک دستگاه اندازه‌گیری ولت/اهم برای اندازه‌گیری ولتاژ، جریان و مقاومت به کار می‌رود.
۱۴. D. یک پروب تونر دستگاهی است که سیگنالی در داخل کابل منتشر می‌کند که وقتی این سیگنال به انتهای دیگر کابل برسد، یک سیگنال صوتی تولید می‌کند. به این دستگاه ردیاب سیم نیز می‌نامند.
۱۵. A. اگر لازم باشد برای اتصال یک کابلUTP اقدام کنید، باید از وسیله‌ای به نام بلوک punch-down استفاده نمایید. بیشتر شبکه‌های امروزی دارای جعبه سیم‌کشی و جعبه تقسیم می‌باشند و برای ختم کردن کابل‌ها، مطمئناً به یک وسیله‌ی punch down نیاز دارید.
۱۶. B. یک crimper سیم یا ساده‌تر یک crimper برای اتصال سرهای انتهایی به انواع کابل‌های مختلف شبکه به کار می‌رود.
۱۷. C. یک وسیله‌ی اتصال کابل‌های UTP برای punch down یک کابل RJ-45 به یک کانکتور عایق به کار می‌رود که نوعاً از یک بلوک 110 به استفاده می‌شود.
۱۸. D. یک محافظ جریان‌های زیاد، سطح ولتاژ وارده را تحت نظر می‌گیرد و وقتی ولتاژ به سطح معینی برسد که به آن آستانه‌ی ولتاژ زیاد می‌نامند، جریان مدار قطع می‌شود.
۱۹. B. آزمایش حلقه‌ی برگشتی یک روال تشخیص عیب است که یک سیگنال ارسال می‌شود و پس از عبور این سیگنال از تمام یا بخشی از یک شبکه یا مدار به دستگاه ارسال کننده بر می‌گردد. یک پریز حلقه‌ی برگشتی این تست را ممکن می‌سازد.
۲۰. B. دستگاه‌های الکترونیکی مستعد گرم شدن بیش از اندازه می‌باشند، به همین دلیل باید از یک نشان دهنده‌ی درجه حرارت استفاده کنید.

فصل ۱۹: عیب‌یابی شبکه

۱. A، F. راه‌اندازی مجدد سرورها و مسیریاب‌ها بخشی از مدل عیب‌یابی نمی‌باشند.
۲. B. شما می‌خواهید برقراری یک ارتباط را بررسی کنید. چراغ لینک نشان می‌دهد که کارت شبکه در حال ایجاد یک ارتباط سطح مقدماتی به بقیه‌ی شبکه است. این یک مورد بسیار ساده برای بررسی می‌باشد. اگر چراغ روشن نباشد، برطرف کردن این عیب بسیار ساده است (اتصال کابل قطع شده).
۳. B. وقتی شبکه‌ی بی‌سیم از کند بودن شکایت داشته باشد یا این‌که در خلال یک نشست ارتباط شبکه از دست برود، معمولاً کندی یا رکود ارتباط از موضوع ظرفیت ناشی می‌شود.
۴. اگرچه تمام این تست‌ها برای برقرار بودن ارتباط شبکه خوب است، بررسی سرور برای ارتباطات کاربر، به شما خواهد گفت که آیا سایر کاربران می‌توانند وارد سیستم شوند. اگر بتوانند، مشکل با احتمال زیاد مربوط به یک ایستگاه کاری کاربران است. و اگر نتوانند، مسئله و مشکل مربوط به ارتباط به سرور یا مربوط به ارتباط شبکه است. این عمل محل ناحیه‌ی عیب را محدودتر می‌کند.
۵. B. به دلیل تمام تست‌های داده شده و نتایج آن‌ها، می‌توانید محدوده‌ی عیب را کوچک و کوچک‌تر نموده و به برقرار بودن ارتباط شبکه از آن ایستگاه کاری محدود نمایید.
۶. A. چون سایر کاربران در یک ناحیه مشکلی ندارند، نمی‌تواند از یک سرور غیر فعال، هاب شبکه یا jabbering NIC باشد. و چون شما و کاربر هر دو نمی‌توانید وارد سیستم شوید، به احتمال زیاد خرابی باید از نوع خرابی خاص ایستگاه کاری باشد. تنها مشکلی که از ایستگاه بر توانایی ورود شما به سیستم اثر

می‌گذارد کلید قفل حروف بزرگ (Caps Lock) است که باید فشار داده شود. این عمل سبب می‌شود حروف پسورد به صورت بزرگ شوند (که بیشتر سیستم حامل سرورها به عنوان یک پسورد متفاوت تلقی می‌کنند) و بنابراین احتمالاً مورد پذیرش نخواهد شد.

۷. D. چون یک ارتباط جدید است باید با عیب‌یابی و شناسایی علائم کار را آغاز کنید.

۸. B. بر طبق مدل عیب‌یابی +Network، گام بعدی گام 2 است که محتمل‌ترین علت بروز عیب را نشان می‌دهد.

۹. C. بعد از تعیین ناحیه تحت تأثیر واقع شده باید پی ببرید آیا هیچ تغییری رخ داده است.

۱۰. A. چون کاربر نمی‌تواند به درستی از هر ماشین وارد سیستم شود، احتمال زیاد دارد که در حال به کار بردن روال غلط برای ورود به سیستم است. چون کس دیگری آن مشکل را ندارد (از جمله خود شما)، مسئله مربوط به آن کاربر است.

۱۱. C. بعد از اجرای یک راه حل باید تست کنید که آیا راه حل عمل می‌کند و سایر اثرات راه حل را شناسایی کنید.

۱۲. B. چون شما نمی‌توانید به صفحه‌ی وب که در سرور قرار دارد دسترسی داشته باشید، مسئله به احتمال زیاد به مشکل مرورگر شما مربوط است.

۱۳. D. از نقطه نظر طراحی، محیط فیزیکی یک سرور باید برای مواردی مانند محل، درجه حرارت و رطوبت بهینه شود. به هنگام عیب‌یابی فراموش نکنید که شرایط فیزیکی که تحت آن دستگاه شبکه در حال کار است بررسی شود. مسائلی که در این‌جا ذکر شد و همچنین مشکلات EMI/RFI، برق و کابل‌های از اتصال قطع شده باید بررسی شوند.

۱۴. D. چون اغلب شبکه‌های امروزه هنوز دارای کابل‌های مسی هستند، شبکه‌ها از آغاز از مشکلات فیزیکی اطراف کابل‌ها به زحمت می‌افتاده‌اند. فناوری‌های جدید و پروتکل‌ها این موارد را کاهش داده‌اند، اما آن‌ها را کاملاً حل نکرده‌اند.

۱۵. A. به محض این‌که تعیین کرده‌اید که مشکل از سوئیچ یا پیکربندی سوئیچ است باید موضوع جدی‌تر بررسی شود.

۱۶. D. چون سایر افراد نیز با این مشکلات مواجه می‌شوند، به احتمال زیاد یا به شبکه و یا به سرور مربوط است. چون شما می‌توانید فایل‌ها را از/یا به یک سرور منتقل کنید، نمی‌تواند از شبکه باشد. بنابراین، مشکل به وب‌سرور مربوط می‌باشد.

۱۷. D. بعد از تحقیق کامل در مورد مشکل و تست موفقیت‌آمیز و تحلیل موضوع، باید راه حل را مستندسازی کنید.

۱۸. B. چون کاربران می‌توانند به اینترنت دسترسی داشته باشند این یعنی که سرور DNS کار می‌کند و آن‌ها دارای گیت‌وی پیش‌فرض درست می‌باشند. احتمالاً سرور اینترانت خراب است.

۱۹. C. ابزار نظارتی عملکرد می‌تواند به شما این ایده را بدهد که چگونه سرور و بقیه‌ی شبکه مشغول هستند. این ابزار از گراف‌ها برای نشان دادن وضعیت ترافیک سرور استفاده می‌کند.

۲۰. C. وقتی مشکل را بررسی کنید شما با مدل هفت مرحله‌ای کار ا انجام داده‌اید. سپس با ملاقات گروه بررسی، مرحله‌ی بعد را تعیین کنید.

فصل ۲۰: مدیریت، نظارت و بهینه‌سازی

۱. C. کابل‌های UTP از کانکتورهای RJ-45 استفاده می‌کنند. از RJ-11 و RJ-25 اغلب برای خطوط تلفن استفاده می‌شود.

۲. B. کابل‌های Straight-through که به کابل‌های patch یا drop معروف‌اند دارای پین‌هایی هستند که در هر سیم یک ترتیب را دارا هستند.

۳. B. در کابل crossover، یک کانکتور به دور سیم‌ها می‌پیچند. در حالت خاص پین 1 و پین 3 با هم و پین‌های 2 و 6 با هم سوئیچ می‌شوند.

۴. C. اگر قصد دارید کابل‌های UTP خودتان را از نظر طول اختصاصی کنید، باید مطمئن شوید که سیم‌های درست به پین‌های درست متصل می‌شوند.

۵. A، B، C، D. خط مبنا یک سطح استاندارد عملکرد یک جزء مهم عبارتند از: دیسک سخت، حافظه، پردازنده و آداپتور شبکه.

۶. C. مقررات در مورد این‌که شبکه‌ها چگونه پیکربندی شوند و عمل کنند و همچنین چگونه مردم باید در شبکه عمل کنند مانند این‌که چگونه کاربران بتوانند به منابع دسترسی داشته باشند و کدام یک از کارمندان می‌توانند به شبکه وارد شوند نظارت می‌کنند.

۷. A. یک دیاگرام شبکه‌ی فیزیکی شامل تمام دستگاه‌های فیزیکی و مسیرهای ارتباطی روی شبکه‌ی شما است و باید دقیقاً نحوه‌ی اتصال فیزیکی شبکه‌ی شما را به تفصیل نشان دهد.

۸. C. گزینه‌ی مناسب در این‌جا استفاده از استراق سمع ترافیک شبکه است. برنامه‌ی packet sniffer به شما اجازه می‌دهد تا ترافیک شبکه را به تفصیل برای هر بسته بررسی کنید. قطعه‌ی مهم که مدیران شبکه معمولاً به جستجوی آن می‌پردازند سرآیند بسته‌ها یا شروع هر یک از بسته‌ها می‌باشد. سرآیند بسته شامل پروتکل و آدرس‌های IP منبع و مقصد می‌باشد.

۹. B. نظارت بر شبکه می‌تواند اسامی مختلفی داشته باشد، از جمله تست بارگذاری، تست برقراری ارتباط و تست توان عملیاتی. شما همچنین مانیتورهای شبکه را به عنوان تحلیل کننده‌های پروتکل می‌شناسید.

۱۰. A. ثبت وقایع کاربردی شامل رویدادهایی است که توسط کاربردها یا برنامه‌ها به وجود آمدند. این رویدادها توسط برنامه‌نویس‌ها تعیین می‌شوند. مثال‌هایی از نرم‌افزار که وقایع کاربرد را ثبت می‌کند عبارتند از LiveUpdate، مجموعه‌ی Microsoft Office و سرورهای SQL و Exchange.

۱۱. C. ثبت وقایع سیستم شامل رویدادهای تولید شده توسط اجزای سیستم ویندوز است. این شامل شروع رویدادهایی مانند درایوها و سرویس‌هایی است که آغاز شده‌اند و یا نمی‌توانند شروع شوند.

۱۲. D. QoS سطوح اولویتی مختلف برای کاربردها متفاوت مانند جریان داده‌ها یا کاربرها را فراهم می‌کند به طوری‌که بتوانند سطح معینی از عملکرد را تضمین نمایند.

۱۳. B. پروتکل عمومی افزونگی آدرس (CARP) را می‌توان برای افزایش دسترس‌پذیری گیت‌وی‌ها و فایروال‌ها مورد استفاده قرار داد.

۱۴. B. اگر یک سگمنت کابل جدید به شبکه اضافه کنید، باید نقشه‌ی طرح سیم‌کشی را تغییر دهید.

۱۵. C، E. کیفیت سرویس (QoS) اساساً توانایی تأمین اولویت‌های مختلف است برای یک یا چند نوع ترافیک در مقایسه با سطوح دیگر که برای کاربردهای مختلف، جریان‌های داده یا کاربران استفاده شود به طوری‌که این اولویت‌ها بتوانند سطح عملکرد معینی را تضمین نمایند.

۱۶. A. شکل‌دهی ترافیک که شکل‌دهی بسته نیز نامیده می‌شوید یک فرم از بهینه‌سازی پهنای‌باند است. این برنامه بسته‌هایی که معیار معینی را برای تضمین پهنای‌باند قابل استفاده برای کاربردهای دیگر برآورده می‌سازند را به تأخیر می‌اندازد. اساساً با برنامه‌ی شکل‌دهی ترافیک، شما تعدادی ترافیک را به تأخیر می‌اندازید به طوری‌که سایر ترافیک بتوانند عبور کنند. شکل‌دهی ترافیک با کنترل پهنای‌باند بستر را برای جریان داده‌ی معینی فراهم می‌کند که در یک پریود زمانی داده‌ی زیادی را ارسال نکند.

۱۷. C. پروتکل عمومی افزونگی آدرس (CARP) را می‌توان برای افزایش دسترس‌پذیری گیت‌وی‌ها و فایروال به کار برد. این پروتکل به مجازی‌سازی مربوط نیست.

۱۸. F. برنامه‌های زیادی با پهنای‌باند فشرده وجود دارند مانند VoIP و جریان ویدیو. این‌ها تعدادی از دلایلی هستند که لازم است برای بهینه‌سازی عملکرد شبکه انجام شود.

۱۹. C. پروتکل صدا از طریق اینترنت VoIP، پروتکلی است که فناوری‌های زیادی را توصیف می‌کند که می‌توانند صدا را از طریق اینترنت یا سایر شبکه‌های داده تحویل دهند.

۲۰. E. نظریه‌ها و استراتژی‌های زیادی وجود دارند که می‌تواند برای بهینه ساختن عملکرد شبکه‌تان استفاده شوند. تمام آن‌ها به نوعی با کنترل ترافیک سر و کار دارند. استراتژی‌ها شامل QoS، شکل‌دهی ترافیک، متعادل‌سازی بار، دسترس‌پذیری بالا و استفاده از سرورهای ذخیره‌ی اطلاعات می‌باشند. شما می‌خواهید مطمئن شوید برای آن برنامه‌های کاربردی که مورد نیاز است پهنای‌باند به اندازه‌ی لازم موجود می‌باشد. این برنامه‌های کاربردی عبارتند از عملیات سرویس بحرانی، VoIP، جریان چندرسانه‌ای بلادرنگ.