پیوست ب

پاسخ به آزمایش‌های نوشتاری

فصل ۱: مقدمه‌ای بر شبکه‌ها

۱. Bus، حلقوی، و ستاره
۲. Multiprotocol Label Switching (MPLS)
۳. سرور
۴. کلاینت – سرور
۵. نقطه – به – نقطه
۶. هاب
۷. MPLS
۸. WAN
۹. یک سگمنت
۱۰. Bus

فصل ۲: مشخصات اتصال سیستم‌های باز

۱. لایه‌ی کاربرد مسئول پیدا کردن منابع شبکه‌ی پخش از سرور و اضافه کردن کنترل جریان و کنترل خطا می‌باشد.
۲. لایه‌ی فیزیکی فریم‌ها را از لایه‌ی پیوند داده‌ها می‌گیرد و رمزگذاری می‌کند و با استفاده از 0ها و 1ها آن‌ها را به صورت سیگنال دیجیتال مناسب برای انتقال از طریق رسانه در می‌آورد.
۳. لایه شبکه مسیردهی را از طریق یک شبکه و آدرس‌دهی منطقی تأمین می‌کند.
۴. لایه ارائه اطمینان حاصل می‌کند که داده در یک فرمت قابل خواندن برای لایه‌ی کاربرد به وجود می‌آید.
۵. لایه‌ی نشست، جلسات بین کاربردها را تنظیم، نگهداری و خاتمه می‌دهد.
۶. واحدهای داده پروتکل (PDUs) در لایه‌ی پیوند داده فریم‌ها نامیده می‌شوند. هر گاه در یک سوال کلمه‌ی *frame* را مشاهده کردید، پاسخ آن را حال می‌دانید.
۷. لایه انتقال از مدارهای مجازی، برای ایجاد یک رابطه‌ی مطمئن بین دو میزبان استفاده می‌کند.
۸. لایه شبکه، آدرس‌دهی منطقی، نوعاً آدرس‌دهی IP و مسیردهی را فراهم می‌کند.
۹. لایه‌ی فیزیکی مسئول ارتباطات الکتریکی و مکانیکی بین دستگاه‌ها می‌باشد.
۱۰. لایه‌ی پیوند داده مسئول فریم‌سازی بسته‌های داده می‌باشد.

فصل ۳: توپولوژی‌های شبکه‌سازی، کانکتورها و استانداردهای سیم‌کشی

۱. Cat 6
۲. نقطه‌ی Demarc
۳. Crossover
۴. RG-6
۵. Cat 5e
۶. Straight-through
۷. برای اتصال دو CSU/DSUs
۸. ۱، ۲، ۳، و ۶
۹. ۱ به ۳ و ۲ به ۶
۱۰. کاملاً در مقابل EMI و RFI مصونیت دارد و می‌تواند تا 40 Km (25 مایل) ارسال گردد.

فصل ۴: مشخصات اترنت فعلی

۱. از آدرس IP دهدهی به فرمت باینری تبدیل کنید.

جدول زیر را برای بیان 192.168.10.15 به فرمت باینری تکمیل کنید:

باینری	1	2	4	8	16	32	64	128	دهدهی
11000000	0	0	0	0	0	0	1	1	192
10101000	0	0	0	1	0	1	0	1	168
00001010	0	1	0	1	0	0	0	0	10
00001111	1	1	1	1	0	0	0	0	15

جدول زیر را برای بیان 172.16.20.55 به فرمت باینری تبدیل کنید:

باینری	1	2	4	8	16	32	64	128	دهدهی
10101100	0	0	1	1	0	1	0	1	172
00010000	0	0	0	0	1	0	0	0	16
00010100	0	0	1	0	1	0	0	0	20
00110111	1	1	1	0	1	1	0	0	55

جدول زیر را برای بیان 10.11.12.99 به فرمت باینری تبدیل کنید:

باینری	1	2	4	8	16	32	64	128	دهدهی
00001010	0	1	0	1	0	0	0	0	10
00001011	1	1	0	1	0	0	0	0	11
00001100	0	0	1	1	0	0	0	0	12
01100011	1	1	0	0	0	1	1	0	99

۲. فرمت باینری زیر را به صورت آدرس IP دهدهی تبدیل کنید.

جدول زیر را برای بیان 11001100.00110011.10101010.01010101 به فرمت آدرس IP دهدهی کامل کنید:

دهدهی	1	2	4	8	16	32	64	128	باینری
204	0	0	1	1	0	0	1	1	11001100
51	1	1	0	0	1	1	0	0	00110011
170	0	1	0	1	0	1	0	1	10101010
85	1	0	1	0	1	0	1	0	01010101

جدول زیر را برای بیان 11000110.11010011.00111001.11010001 به فرمت آدرس IP دهدهی تکمیل کنید:

دهدهی	1	2	4	8	16	32	64	128	باینری
198	0	1	1	0	0	0	1	1	11000110
211	1	1	0	0	1	0	1	1	11010011
57	1	0	0	1	1	1	0	0	00111001
209	1	0	0	0	1	0	1	1	11010001

جدول زیر را برای بیان 10000100.11010010.10111000.10100110 به فرمت آدرس IP دهدهی تکمیل کنید:

دهدهی	1	2	4	8	16	32	64	128	باینری
132	0	1	0	0	0	0	0	1	10000100
210	0	1	0	0	1	0	1	1	11010010
184	0	0	0	1	1	1	0	1	10111000
166	0	1	1	0	0	1	0	1	10100110

۳. اطلاعات باینری جداول زیر را به صورت هگزا دسیمال بنویسید.

جدول زیر را برای تبدیل 11011000.00011011.00111101.01110110 به صورت هگزادسیمال تکمیل کنید:

هگزا دسیمال	1	2	4	8	16	32	64	128	باینری
D8	0	0	0	1	1	0	1	1	11011000
1B	1	1	0	1	1	0	0	0	00011011
3D	1	0	1	1	1	1	0	0	00111101
76	0	1	1	0	1	1	1	0	01110110

در جدول زیر به 11001010.11110101.10000011.11101011 را به صورت هگزا دسیمال بنویسید:

هگزا دسیمال	1	2	4	8	16	32	64	128	باینری
CA	0	1	0	1	0	0	1	1	11001010
F5	1	0	1	0	1	1	1	1	11110101
83	1	1	0	0	0	0	0	1	10000011
EB	1	1	0	1	0	1	1	1	11101011

در جدول زیر به صورت باینری 10000100.11010010.01000011.10110011 را به صورت هگزا دسیمال بنویسید:

هگزا دسیمال	1	2	4	8	16	32	64	128	باینری
84	0	1	0	0	0	0	0	1	10000100
D2	0	1	0	0	1	0	1	1	11010010
43	1	1	0	0	0	0	1	0	01000011
B3	1	1	0	0	1	1	0	1	10110011

فصل ۵: دستگاه‌های شبکه‌سازی

توصیف	دستگاه یا لایه‌ی OSI
این دستگاه اطلاعات را از لایه‌ی شبکه ارسال و دریافت می‌کند.	مسیریاب
این دستگاه قبل از ارسال اطلاعات بین دو ایستگاه انتهایی یک مدار مجاز ایجاد می‌کند.	انتقال
یک سوئیچ لایه‌ی 3 یا سوئیچ چند لایه‌ای	مسیریاب
این وسیله از آدرس سخت‌افزاری برای فیلتر کردن یک شبکه استفاده می‌کند.	پل یا سوئیچ
اترنت در این لایه‌ها تعریف می‌شود.	پیوند داده و فیزیکی
این لایه توالی و کنترل جریان داده را پشتیبانی می‌کند.	انتقال
این دستگاه می‌تواند فاصله تا یک شبکه‌ی دور را اندازه‌گیری کند.	مسیریاب
آدرس‌دهی منطقی در این لایه انجام می‌شود.	شبکه
آدرس‌های سخت‌افزاری در این لایه تعریف می‌شوند.	پیوند داده (زیر لایه‌ی MAC)
این وسیله یک دامنه تصادم بزرگ و یک دامنه پخش بزرگ ایجاد می‌کند.	هاب
این دستگاه دامنه‌های تصادم کوچک‌تر زیادی را ایجاد می‌کند، اما شبکه هنوز یک دامنه پخش بزرگ است.	سوئیچ یا پل
این دستگاه هرگز نمی‌تواند ارتباط FDX را اجرا کند.	هاب
این دستگاه دامنه‌های تصادم و دامنه‌های پخش را به دامنه‌های کوچک‌تر تقسیم می‌کند.	مسیریاب

فصل ۶: مقدمه‌ای بر پروتکل اینترنت

۱. محتمل‌ترین مشکل این‌است‌که یک سرور DHCP به شبکه معرفی شده است و به طور نامناسب و نادرست از آن استفاده می‌شود.

۲. FTP از هر دو پورت 20 و 21، TCP به ترتیب برای کانال داده و کانال کنترل استفاده می‌کند.

۳. یک سرور DNS از پورت 53، TCP برای انتقالات ناحیه و از پورت 53، UDP برای تحلیل نام‌ها استفاده می‌کند.

۴. ICMP مستقیماً از IP برای ساختن بسته‌های گزارش خطا استفاده می‌کند. این بسته‌ها وقتی که مواردی در خلال تحویل بسته‌های داده پیش بیاید دوباره به میزبان منبع اصلی ارسال می‌گردد.

۵. به طور ساده، این سرویس در حال حاضر روی سرور اجرا نمی‌شود. امکان دیگر ممکن است این باشد که یک فایروال بین کلاینت و سرور مانع عبور پروتکل مورد نظر شده است.

۶. بیشتر ISPها سرورهای mail خودشان را دارند. وقتی که سرویس را سوئیچ می‌کنید، ممکن است لازم باشد کاربرد mail خودتان را به سرعت سرورهای تأمین شده توسط تأمین کننده‌های سرویس جدید نشان دهند.

۷. فرمان rlogin، Unix شبیه Telnet عمل می‌کند.

۸. ICMP پروتکلی است که فرمان‌های ping و tracert به آن استناد می‌کنند. اگر برای گرفتن ping و Traceroutes از طریق مسیریاب مشکل دارید باید بررسی کنید که آیا می‌توانید از ICMP استفاده کنید.

۹. سرورهای TFTP به پیام‌های UDP ارسال شده به پورت 69 پاسخ می‌دهد.

۱۰. SMTP از پورت 25، TCP و POP3 از پورت 110، TCP و RDP از پورت 3389، TCP و IMAP4 از پورت 143، TCP استفاده می‌کند.

فصل ۷: آدرس‌دهی IP

۱. محدوده‌ی اختصاصی کلاس C از 192.168.0.0 تا 192.168.255.255 می‌باشد.
۲. IPv6 دارای مشخصات زیر است، که آن را در مقایسه با IPv4 برتر می‌کند؛ آدرس‌های بیشتر، سرآیند ساده‌تر، گزینه‌هایی برای احراز هویت و سایر امور امنیتی است.
۳. آدرس‌دهی IP اختصاصی خودکار (APIPA) فناوری است که سبب می‌شود میزبان‌ها به طور خودکار خودشان را با آدرس‌هایی که با 169.254 شروع می‌شوند پیکربندی نمایند.
۴. برای یک رابط یک آدرس IP تعیین می‌شود.
۵. یک – به – چند آدرس
۶. یک آدرس MAC، گاهی‌اوقات یک آدرس سخت‌افزاری یا حتی یک آدرس burned-in نامیده می‌شود.
۷. حقیقت این‌است‌که آن دارای آدرس‌های 128 بیتی (16-octet) در مقایسه با IPv4 که دارای آدرس‌های 32 بیت (4-octet) است می‌باشد.
۸. 172.16.0.0 تا 172.31.255.255
۹. 192 – 223، *xxxxx*110
۱۰. حلقه‌ی برگشتی یا تشخیص معایب

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

۱. 192.168.100.25/30. /30 A برابر 255.255.255.252 است. زیرشبکه‌ی معتبر 192.168.100.24 و پخش 192.168.100.27 می‌باشد و میزبان‌های معتبر عبارتند از 192.168.100.25 و 26.
۲. 192.168.100.37/28. /28 A برابر 255.255.255.240 است. چهارمین octet یک بلوک با اندازه‌ی 16 است. تا 16 ثانیه بشمارید تا از 0, 16, 32, 48 .37 عبور کنید. میزبان در 32 زیرشبکه با آدرس پخش 47 است. میزبان‌های معتبر 46 – 33 است.
۳. 192.168.100.66/27. /27 A برابر 255.255.255.224 است. چهارمین octet دارای بلوکی به اندازه‌ی 32 است. 32 ثانیه بشمارید تا از آدرس میزبان 0, 32, 64 .66 عبور کنید. میزبان در 64 زیرشبکه و آدرس پخش 95 قرار دارد محدوده‌ی میزبان معتبر 94 – 65 است.
۴. 192.168.100.17/29. /29 A برابر 255.255.255.248 است. چهارمین octet دارای بلوکی به اندازه‌ی 8 است یعنی 0، 8، 16، 24. میزبان در 16 زیرشبکه و پخش 23 قرار دارد. میزبان‌های معتبر 22 – 17 هستند.
۵. 192.168.100.99/26. /26 A برابر 255.255.255.192 است. چهارمین octet دارای بلوکی به اندازه‌ی 64 است یعنی 0، 64، و 128. میزبان در 64 زیرشبکه و پخش 127 قرار دارد. میزبان‌های معتبر 126 – 65 هستند.
۶. 192.168.100.99/25. /25 A برابر 255.255.255.128 است. چهارمین octet دارای بلوک به اندازه‌ی 128 است یعنی 0 و 128. میزبان در زیرشبکه‌ی 0 و پخش 127 قرار دارد. میزبان معتبر 126 – 1.
۷. یک کلاس B پیش‌فرض 255.255.0.0 است. یک ماسک کلاس B 255.255.255.0 برابر 256 زیرشبکه است. که هر یک با 254 میزبان می‌باشد. ما به زیرشبکه‌های کمتر نیاز داریم. اگر ما 255.255.240.0 را به کار ببریم این انتخاب 16 زیرشبکه را فراهم می‌کند. حال یک بیت زیرشبکه‌ی دیگر به بیت‌ها اضافه کنید. 255.255.248.0. این معادل 5 بیت برای زیرشبکه‌سازی است که 32 زیرشبکه را تأمین می‌کند. بهترین پاسخ a /21 است.

۸. /29 A برابر 255.255.255.248 است. این چهارمین octet دارای بلوک با اندازه‌ی 8 است یعنی 0، 8، 16. میزبان در 8 زیرشبکه و پخش 15 قرار دارد.
۹. /29 A برابر 255.255.255.248 است که 5 بیت مربوط به زیرشبکه و 3 بیت برای میزبان است. این فقط 6 میزبان به ازای هر زیرشبکه می‌باشد.
۱۰. /23 A برابر 255.255.254.0 است. سومین octet دارای بلوک به اندازه‌ی 2 است یعنی 0، 2، 4. میزبان در زیرشبکه‌ی 16.2.0 و آدرس پخش 16.3.255 است.

فصل ۹: مقدمه‌ای بر مسیردهی IP

۱. غلط. RIP و RIPv2 هر دو پروتکل‌های بردار فاصله هستند.
۲. غلط. RIP و RIPv2 هر دو پروتکل‌های بردار فاصله هستند.
۳. غلط. EIGRP یک پروتکل مسیردهی اختصاصی شرکت Cisco می‌باشد.
۴. سیستم خودگردان
۵. RIP در شبکه‌های بزرگ کار نمی‌کند، بنابراین OSPF بهترین پاسخ خواهد بود و RIP و OSPF هر دو غیر اختصاصی هستند.
۶. مسیردهی استاتیک
۷. آدرس MAC گیت‌وی پیش‌فرض
۸. آدرس IP سرور
۹. آدرس MAC مسیریاب ارسال کننده‌ی فریم به سرور
۱۰. آدرس IP سرور

فصل ۱۰: پروتکل‌های مسیردهی

۱. 120
۲. 90
۳. 120
۴. 1
۵. RIPng (نسل بعدی). تعجب می‌کنم. چند نفر از شما پاسخ‌تان RIPv3 است.
۶. OSPFv3
۷. EIGRPv6
۸. وقتی که نیاز دارید دو سیستم خودگردان را (ASs) را به هم متصل کنید.
۹. وقتی که تمام مسیریاب‌های شما مسیریاب‌های سیسکو باشند.
۱۰. بردار فاصله

فصل ۱۱: سوئیچینگ و LANهای مجازی

۱. پخش
۲. تصادم
۳. استفاده از ترانک (Trunk) به شما امکان می‌دهد تا اطلاعات چند یا همه‌ی VLANها را از یک لینک ارسال کنید. پورت‌های دسترسی به اطلاعات ارسال شده توسط فقط یک VLAN می‌باشد.

۴. ارسال انرژی الکتریکی از طریق اترنت (PoE)
۵. عضویت پورت VLAN نادرست تنظیم شده است.
۶. فریم از تمام پورت‌ها به جز پورتی که از آن دریافت شد سرریز کرد.
۷. یادگیری و فیلترینگ آدرس و اجتناب از بروز حلقه
۸. آدرس MAC منبع به جدول ارسال/فیلتر اضافه خواهد شد.
۹. پروتکل درخت پوشا (STP)
۱۰. برای پیمان‌کاران یک VLAN و VLAN دیگر برای میزبان‌ها ایجاد کنید.

فصل ۱۲: شبکه‌سازی بی‌سیم

۱. 11Mbps
۲. 54Mbps
۳. 54Mbps
۴. 2.4GHz
۵. 2.4GHz
۶. 5GHz
۷. هیچ‌کدام
۸. مقادیر کلیدهای WPA وقتی از سیستم استفاده می‌شود می‌تواند به طور پویا تغییر کنند.
۹. استاندارد IEEE 802.11i به وسیله‌ی WPA استفاده می‌شود و نسخه‌ی 2، WPA نامیده می‌شود.
۱۰. سه

فصل ۱۳: احراز هویت و کنترل دسترسی

۱. آدرس‌های IP و آدرس‌های MAC
۲. IPSec
۳. SSL VPN
۴. PKI
۵. فقط دارنده‌ی کلید
۶. Kerberos
۷. احراز هویت، ارائه‌ی مجوز و حساب کاربری
۸. 802.1x
۹. MS-CHAP
۱۰. TACACS+

فصل ۱۴: تهدیدهای شبکه و کاهش خطرات

۱. امتناع از سرویس (DoS)
۲. هر هفته یک‌بار
۳. سرریز بافر
۴. یک ویروس فایل
۵. استراق سمع ترافیک شبکه
۶. یک ویروس macro

۷. حمله‌ی Man-in-the-middle
۸. یک نقطه‌ی دسترسی نامناسب
۹. Windows Update
۱۰. اسکن برای ویروس بر طبق درخواست و پس از دسترسی

فصل ۱۵: امنیت فیزیکی و سخت‌افزاری

۱. سیستم جلوگیری از مزاحمت
۲. با حالت
۳. فیلتر کردن محتوا
۴. فهرست کنترل دسترسی (ACL)
۵. یک کانکتور VPN
۶. نواحی امنیتی
۷. امنیت پورت
۸. امتناع
۹. شبکه‌ی Honeynet
۱۰. عکس‌العمل‌های غیر فعال از یک IDS

فصل ۱۶: شبکه‌های WAN

۱. به آسانی موجود است.
۲. کابل. در یک شبکه‌ی مدرن، ترکیب فیبر و کواکسیال (HFC)، یک اصطلاح صنعت مخابرات برای شبکه‌ای است که از فیبرنوری و کابل کواکسیال هر دو برای ایجاد یک شبکه‌ی پهن‌باند استفاده می‌شود.
۳. Frame Relay. اگرچه امروزه Frame Relay در خیلی از فروشگاه‌ها موجود نیست، ولی به عنوان یک راه حل ممکن برای مشکل ایجاد شده مطرح است.
۴. 1.544Mbps
۵. خط مشترک دیجیتالی DSL
۶. Frame Relay و X.25
۷. LTE و WiMAX
۸. ATM
۹. HDSL، SDSL، VDSL، ADSL
۱۰. فیبر

فصل ۱۷: ابزار عیب‌یابی

۱. traceroute یا tracert
۲. آزمایش کننده‌ی توان عملیاتی
۳. Ipconfig /all
۴. Telnet
۵. Route

۶. FTP
۷. Nslookup
۸. –n
۹. Ifconfig
۱۰. Route print

فصل ۱۸: ابزار سخت‌افزاری و نرم‌افزاری

۱. غلط
۲. غلط
۳. درست
۴. درست
۵. غلط. یک تحلیل کننده‌ی شبکه‌ی معمولی می‌تواند در هر بار فقط یک سگمنت را ببیند.
۶. تأیید کننده‌ی کابل
۷. غلط. مگر این‌که منظور شما زندان نباشد.
۸. یک نشان دهنده‌ی درجه حرارت
۹. یک ثبت کننده‌ی تغییرات ولتاژ
۱۰. یک stripper/crimper کابل

فصل ۱۹: عیب‌یابی شبکه

۱. تئوری را بررسی کنید تا علت تعیین شود.
۲. مدارک به دست آمده، اقدامات و نتایج
۳. طراحان شبکه با تابیده شدن زوج سیم‌ها به یکدیگر و آن‌ها را با زاویه‌ی 90 درجه نسبت به یکدیگر در کنار هم قرار دادن، اثر هم‌پوشانی را در داخل شبکه به حداقل می‌رسانند.
۴. پورت دارای VLAN اشتباه است.
۵. زوج Split
۶. احراز هویت
۷. برقراری یک طرح اجرایی برای تحلیل مشکل و شناسایی اثرات پتانسیل.
۸. راه حل را اجرا کنید یا در صورت نیاز تلاش برای حل ادامه یابد.
۹. حلقه‌های سوئیچینگ، حلقه‌های مسیریابی، مشکلات مسیریابی، proxy ARP، توفان‌های پخش
۱۰. هم‌پوشانی، تضعیف، تصادم‌ها، اتصال کوتاه‌ها، عدم انطباق ناشی از امپدانس باز، تداخل

فصل ۲۰: مدیریت، نظارت و بهینه‌سازی

۱. منطقی
۲. شکل‌دهی ترافیک
۳. بهترین تلاش
۴. Jitter

۵. متعادل‌سازی بار
۶. یک خط مبنا
۷. متقاطع
۸. محاسبات ابری
۹. سرورهای مجازی، سوئیچ‌های مجازی، میزکارهای مجازی، نرم‌افزار به عنوان یک سرویس (SaaS) و شبکه به عنوان یک سرویس (NaaS).
۱۰. روال‌ها