

راهنمای کاربردی
CompTIA Network+

Exam N10-009

به همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی

ویرایش ششم



Todd Lammle

Jon Buhagiar

ترجمه: سید محمد متین روحانی راد

انتشارات پندار پارس

سرشناسه	: لامل، تاد - Lammle, Todd
عنوان و نام پدیدآور	: آموزش کاربردی CompTIA Network+ به همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی / تاد لامل، جان باهیگیر] :
	ترجمه سیدمحمدمتین روحانی‌راد.
مشخصات نشر	: تهران : پندار پارس ، ۱۴۰۴.
مشخصات ظاهری	: ۱۲۵۴ ص: مصور.
شابک	: 978-622-7785-45-6
وضعیت فهرست نویسی	: فیپا
یادداشت	: عنوان اصلی: (exam : N10-009) Comptia Network+ deluxe study guide, sixth edition
موضوع	: شبکه‌های کامپیوتری - Computer networks: داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها Electronic data processing personnel - Certification - مهندسان مخابرات -- گواهی و گواهی‌نامه‌ها - Telecommunications engineers -- Certification
شناسه افزوده	: باهیگیر، جان
شناسه افزوده	: Buhagiar, Jon
شناسه افزوده	: روحانی‌راد، سید محمدمتین، ۱۳۷۶-، مترجم
رده بندی کنگره	: ۳ / QA۷۶
رده بندی دیویی	: ۶ / ۰۰۴
شماره کتابشناسی ملی	: ۱۰۰۲۲۶۵۲
اطلاعات رکورد کتابشناسی	: فیپا

انتشارات پندارپارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸

ایمیل: info@pendarepars.com

نام کتاب : آموزش کاربردی CompTIA Network+ (ویرایش ششم)، به همراه ۸۰۰ سوال تمرینی با پاسخ تشریحی

ناشر : انتشارات پندار پارس

تالیف : تد لامل، جان باهیگیر

ترجمه : سید محمد متین روحانی راد

چاپ نخست : اردیبهشت ۱۴۰۴

شمارگان : ۲۰۰ نسخه

طرح جلد : رامین شکرالهی

چاپ، صحافی : روز

شابک : ۹۷۸-۶۲۲-۷۷۸۵-۴۵-۶

قیمت : ۹۷۰.۰۰۰ تومان

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

۳۱	مقدمه.....
۳۲	گواهینامه Network+ چیست؟.....
۳۲	چرا باید گواهینامه Network+ را دریافت کنیم؟.....
۳۳	نحوه دریافت گواهینامه Network+.....
۳۴	نکاتی برای شرکت در آزمون Network+.....
۳۴	چه کسی باید این کتاب را بخواند؟.....
۳۵	این کتاب چه چیزی را پوشش می‌دهد؟.....
۳۷	آنچه در این کتاب گنجانده شده است.....
۳۷	محیط یادگیری آنلاین تعاملی و بانک نمونه سؤالات.....
۳۸	نحوه استفاده از این کتاب.....
۳۹	اهداف امتحان N10-009.....
۴۰	نقشه هدف.....
۴۲	نحوه تماس با ناشر.....
۴۲	آزمون ارزیابی.....
۵۳	پاسخ آزمون سنجش.....
۶۳	فصل ۱؛ مقدمه‌ای بر شبکه‌ها.....
۶۴	اول از همه: شبکه چیست؟.....
۶۵	شبکه محلی.....
۶۷	اجزای شبکه مشترک.....
۶۷	ایستگاه‌های کاری.....
۶۸	سرورها.....
۷۰	هاست‌ها.....
۷۰	انواع شبکه.....
۷۰	شبکه بین شهری.....
۷۱	شبکه گسترده.....
۷۲	شبکه شخصی.....
۷۳	شبکه دانشگاهی.....
۷۳	شبکه ذخیره سازی.....
۷۳	رویکرد نرم‌افزاری در شبکه‌ی گسترده.....
۷۴	سوئیچینگ برجسب چند پروتکلی (MPLS).....
۷۵	کپسوله‌سازی مسیریابی عمومی چند نقطه‌ای (mGRE).....
۷۵	معماری شبکه: همتابه‌همتا یا کلاینت-سرور؟.....
۷۵	شبکه‌های همتا به همتا.....
۷۶	شبکه‌های کلاینت-سرور.....
۷۸	توپولوژی‌های شبکه فیزیکی.....

۷۸	توپولوژی باس (Bus).....
۷۹	توپولوژی ستاره‌ای (Star).....
۸۱	توپولوژی حلقه‌ای (Ring).....
۸۲	توپولوژی مش (Mesh).....
۸۳	توپولوژی نقطه به نقطه.....
۸۴	توپولوژی نقطه به چند نقطه.....
۸۵	توپولوژی ترکیبی.....
۸۵	انتخاب توپولوژی، ستون فقرات و بخش‌ها.....
۸۶	انتخاب توپولوژی مناسب.....
۸۷	ستون فقرات شبکه.....
۸۸	بخش‌های شبکه.....
۸۸	نقاط ورودی مرتبط با سرویس.....
۸۸	لینک‌های ارائه دهنده سرویس.....
۸۹	شبکه‌های مجازی.....
۸۹	مدل سه لایه.....
۹۱	طراحی Spine and Leaf.....
۹۲	جریان ترافیک.....
۹۳	خلاصه.....
۹۳	ملزومات امتحان.....
۹۴	آزمایشگاه نوشتاری.....
۹۵	مروری بر سؤالات.....
۹۹	فصل ۲؛ مدل مرجع اتصال سیستم‌های باز (OSI).....
۱۰۰	مدل‌های اینترنت‌ورک.....
۱۰۰	رویکرد لایه‌ای.....
۱۰۱	مزایای مدل‌های مرجع.....
۱۰۴	لایه اپلیکیشن.....
۱۰۵	لایه نمایش (Presentation Layer).....
۱۰۵	لایه جلسه (Session Layer).....
۱۰۶	لایه حمل و نقل (Transport Layer).....
۱۰۶	اتصال‌گرا.....
۱۰۸	کنترل جریان.....
۱۱۰	سیستم Windowing.....
۱۱۱	سیستم Acknowledgment.....
۱۱۲	لایه شبکه.....
۱۱۵	لایه پیوند داده (Data-link Layer).....
۱۱۸	لایه فیزیکی.....
۱۱۹	مقدمه‌ای بر کپسوله‌سازی.....
۱۲۰	تکنیک‌های مدولاسیون.....

۱۲۱.....	خلاصه
۱۲۲.....	ملزومات امتحان
۱۲۲.....	آزمایشگاه نوشتاری
۱۲۳.....	بررسی سؤالات
۱۲۷.....	فصل ۳: اتصالات شبکه و استانداردهای سیم کشی
۱۲۸.....	رسانه فیزیکی
۱۲۹.....	کابل کواکسیال
۱۳۱.....	کانکتور نوع F
۱۳۱.....	کابل زوج به هم تاییده (Twisted-Pair Cable)
۱۳۲.....	کابل Twinaxial
۱۳۲.....	توضیحات کابل اترنت
۱۳۴.....	اتصال UTP
۱۳۶.....	کابل فیبر نوری
۱۳۷.....	فیبر تک حالت
۱۳۷.....	فیبر چند حالت
۱۳۷.....	کانکتور فیبر
۱۳۸.....	کانکتور Straight Tip
۱۳۸.....	اینترفیس مشترک (SC)
۱۳۹.....	کانکتورهای فیبر نوری فرم کوچک
۱۴۱.....	APC در مقابل UPC
۱۴۲.....	از مس استفاده کنم یا فیبر؟
۱۴۲.....	پنل توزیع فیبر
۱۴۲.....	فرستنده و گیرنده فیبر نوری
۱۴۳.....	فرستنده و گیرنده (Transceivers)
۱۴۴.....	کانکتورهای رسانه‌ای
۱۴۵.....	کابل‌های سریال
۱۴۵.....	RS-232
۱۴۶.....	DB-25
۱۴۶.....	گذرگاه سریال عمومی (USB)
۱۴۷.....	ویژگی‌های کابل
۱۴۷.....	سرعت انتقال
۱۴۷.....	فاصله
۱۴۸.....	دوبلکس
۱۴۸.....	ایمنی در برابر نویز (امنیت، EMI)
۱۴۹.....	فرکانس
۱۴۹.....	استانداردهای سیم کشی
۱۵۰.....	T568A در مقابل T568B
۱۵۱.....	کابل مستقیم

۱۵۲.....	کابل کراس اور.....
۱۵۳.....	سیم کشی گیگابیتی UTP (1000BaseT).....
۱۵۴.....	کابل رول شده / رولور (Rolled/Rollover).....
۱۵۴.....	کابل کراس اور T1.....
۱۵۵.....	درک آزمایش کابل.....
۱۵۷.....	نصب توزیع‌های سیم کشی.....
۱۵۷.....	MDF/IDF.....
۱۵۷.....	کابل ۲۵ زوج.....
۱۵۸.....	کابل بلوک ۶۶.....
۱۵۸.....	کابل بلوک ۱۱۰.....
۱۵۹.....	کابل بلوک BIX.....
۱۵۹.....	پسوند Demarc/Demarc.....
۱۵۹.....	جک هوشمند.....
۱۵۹.....	خلاصه.....
۱۶۰.....	ملزومات امتحان.....
۱۶۰.....	آزمایشگاه نوشتاری.....
۱۶۱.....	بررسی سؤالات.....
۱۶۵.....	فصل ۴؛ مشخصات اترنت فعلی.....
۱۶۵.....	میانی شبکه.....
۱۶۷.....	میانی اترنت.....
۱۶۸.....	دامنه برخورد (Collision Domain).....
۱۶۸.....	دامنه برودکست.....
۱۶۹.....	CSMA/CD.....
۱۷۰.....	پهنای باند/باند پایه (Broadband/Baseband).....
۱۷۱.....	نرخ بیت در مقابل نرخ Baud.....
۱۷۱.....	طول موج.....
۱۷۲.....	اترنت دوپلکس نیمه و دوپلکس کامل.....
۱۷۴.....	اترنت در لایه پیوند داده.....
۱۷۴.....	تبدیل باینری به اعشاری و هگزادسیمال.....
۱۷۸.....	آدرس‌دهی اترنت.....
۱۷۹.....	فریم‌های اترنت.....
۱۸۲.....	اترنت در لایه فیزیکی.....
۱۸۹.....	استاندارد اتصال سیمی مناسب را اجرا کنید.....
۱۹۰.....	اترنت بر روی سایر استانداردها (IEEE 1905.1-2013).....
۱۹۰.....	اترنت از طریق خط برق.....
۱۹۱.....	اترنت از طریق HDMI.....
۱۹۳.....	خلاصه.....
۱۹۳.....	ملزومات امتحان.....

۱۹۴.....	آزمایشگاه نوشتاری
۱۹۴.....	بررسی سؤالات
۱۹۹.....	فصل ۵: دستگاه‌های شبکه
۲۰۱.....	دستگاه‌های اتصال دهنده مشترک شبکه
۲۰۲.....	کارت اینترفیس شبکه
۲۰۳.....	هاب
۲۰۴.....	دستگاه پل (Bridge)
۲۰۵.....	سوئیچ
۲۰۶.....	روتر
۲۰۷.....	تنظیمات اینترفیس
۲۱۰.....	فایروال
۲۱۱.....	IDS/IPS
۲۱۲.....	HIDS
۲۱۲.....	نقطه دسترسی (Access Point)
۲۱۳.....	توسعه دهنده برد بی سیم
۲۱۳.....	کنترلر شبکه بی سیم
۲۱۴.....	متعادل کننده بار (Load Balancer)
۲۱۵.....	روش‌های رقابت
۲۱۵.....	CSMA/CA
۲۱۵.....	توصیف عملیات CSMA/CA
۲۱۶.....	CSMA/CD
۲۱۷.....	شرح عملکرد CSMA/CD
۲۱۸.....	سرور پروتکل پیکربندی هاست پویا
۲۲۳.....	DHCP Relay
۲۲۴.....	IPAM
۲۲۴.....	سایر دستگاه‌های تخصصی
۲۲۵.....	سوئیچ چند لایه (MLS)
۲۲۵.....	سرور سیستم نام دامنه (DNS Server)
۲۳۳.....	DNS پویا
۲۳۳.....	DNS داخلی و خارجی
۲۳۴.....	پسوندهای امنیتی سیستم نام دامنه (DNSSEC)
۲۳۴.....	DNS روی HTTPS (DoH) و DNS روی TLS (DoT)
۲۳۵.....	پروتکل‌های زمان شبکه
۲۳۶.....	امنیت زمان شبکه (NTS)
۲۳۶.....	پراکسی سرور
۲۳۸.....	رمز گذاری و فیلتر محتوا
۲۳۹.....	مودم آنالوگ
۲۴۰.....	شکل دهی Packet

۲۴۰	VPN Concentrator/Headend
۲۴۱	میدل رسانه
۲۴۱	VoIP PBX
۲۴۱	VoIP Endpoint
۲۴۲	NGFW / فایروال لایه ۷
۲۴۲	VoIP Gateway
۲۴۲	مودم کابلی
۲۴۳	DSL مودم
۲۴۳	دستگاه‌های تحت شبکه
۲۴۳	تلفن‌های VoIP
۲۴۳	پرینترها
۲۴۳	دستگاه‌های کنترل دسترسی فیزیکی
۲۴۴	دوربین‌ها
۲۴۴	سنسورهای تهویه گرمایش و تهویه مطبوع (HVAC)
۲۴۴	اینترنت اشیا (IoT)
۲۴۵	سیستم‌های کنترل صنعتی
۲۴۵	برنامه‌ریزی و پیاده‌سازی یک شبکه پایه SOHO با استفاده از تقسیم‌بندی شبکه
۲۴۵	تعیین نیازها
۲۵۱	آیا باید همه هاب‌ها را با سوئیچ‌ها جایگزین کنیم؟
۲۵۳	سوئیچ‌ها و پل‌ها در لایه پیوند داده
۲۵۴	هاب‌ها در لایه فیزیکی
۲۵۵	ملاحظه‌های محیطی
۲۵۶	خلاصه
۲۵۶	ملزومات امتحان
۲۵۷	آزمایشگاه نوشتاری
۲۵۸	بررسی سؤالات
۲۶۳	فصل ۶: مقدمه‌ای بر پروتکل اینترنت
۲۶۵	معرفی TCP/IP
۲۶۵	تاریخچه مختصری از TCP/IP
۲۶۶	مدل TCP/IP و DoD
۲۶۸	پروتکل‌های لایه Process/Application
۲۶۸	پروتکل انتقال فایل (TCP 20, 21)
۲۶۹	پروتکل Secure Shell (TCP 22)
۲۷۰	پروتکل انتقال امن فایل (TCP 22)
۲۷۰	پروتکل Telnet (TCP 23)
۲۷۱	پروتکل انتقال ایمیل ساده (TCP 25)
۲۷۱	سیستم نام دامنه (TCP و UDP 53)
۲۷۵	پروتکل انتقال فایل بی‌اهمیت (TFTP/UDP 69)

۲۷۶.....	چه زمانی باید از FTP استفاده کرد؟
۲۷۶.....	پروتکل انتقال ابرمتن HTTP(TCP 80)
۲۷۷.....	پروتکل Post Office نسخه ۳ (TCP 110)
۲۷۷.....	پروتکل زمان شبکه NTP(UDP 123)
۲۷۸.....	پروتکل دسترسی به پیام اینترنتی (TCP 143)
۲۷۸.....	پروتکل ساده مدیریت شبکه (UDP 161/162)
۲۷۹.....	پروتکل دسترسی دایرکتوری سبک (TCP 389)
۲۸۰.....	پروتکل انتقال امن ابرمتن (TCP 443)
۲۸۰.....	امنیت لایه انتقال / لایه سوکت‌های امن (TCP 995/465)
۲۸۰.....	پروتکل Server Message Block (TCP 445)
۲۸۰.....	پروتکل Syslog (UDP 514)
۲۸۲.....	پروتکل SMTPS (TCP 587)
۲۸۲.....	پروتکل دسترسی دایرکتوری سبک روی SSL (TCP 636)
۲۸۲.....	IMAP از طریق SSL (TCP 993)
۲۸۲.....	POP3 از طریق SSL (TCP 995)
۲۸۲.....	سرور زبان کوثری ساختاریافته (TCP 1433)
۲۸۳.....	SQLnet (TCP 1521)
۲۸۳.....	MySQL (TCP 3306)
۲۸۳.....	پروتکل Remote Desktop (TCP 3389)
۲۸۴.....	SIP (VoIP) (TCP یا UDP 5060/TCP 5061)
۲۸۴.....	RTP (VoIP) (UDP 5004/TCP 5005)
۲۸۴.....	MGCP (چند رسانه‌ای) (TCP 2427/2727)
۲۸۴.....	H.323 (ویدیو) (TCP 1720)
۲۸۴.....	پروتکل Internet Group Management
۲۸۵.....	NetBIOS (UDP 137-139 و TCP)
۲۸۵.....	پروتکل‌های لایه Host-to-Host
۲۸۵.....	پروتکل کنترل انتقال
۲۸۶.....	فرمت بخش TCP
۲۸۸.....	پروتکل User Datagram
۲۸۹.....	مفاهیم کلیدی پروتکل‌های Host-to-Host
۲۹۰.....	شماره پورت‌ها
۲۹۲.....	پروتکل‌های لایه اینترنت
۲۹۳.....	پروتکل اینترنت
۲۹۶.....	پروتکل کنترل پیام اینترنت
۲۹۸.....	پروتکل Address Resolution
۲۹۹.....	پروتکل معکوس تشخیص آدرس (RARP)
۳۰۰.....	کپسوله‌سازی مسیریابی عمومی (GRE)
۳۰۱.....	امنیت پروتکل اینترنت (IPSec)

۳۰۲.....	پروتکل (AH) Authentication Header
۳۰۲.....	پروتکل (ESP) Encapsulating Security Payload
۳۰۳.....	تبادل کلید اینترنت (IKE)
۳۰۴.....	کپسوله‌سازی داده‌ها
۳۰۸.....	خلاصه
۳۰۹.....	ملزومات امتحان
۳۰۹.....	آزمایشگاه نوشتاری
۳۱۰.....	بررسی سؤالات
۳۱۵.....	فصل ۷: آدرس‌دهی IP
۳۱۷.....	اصطلاحات IP
۳۱۷.....	طرح آدرس‌دهی IP سلسله مراتبی
۳۱۸.....	آدرس‌دهی شبکه
۳۱۹.....	آدرس‌های کلاس A
۳۲۱.....	آدرس‌های کلاس B
۳۲۲.....	آدرس‌های کلاس C
۳۲۳.....	آدرس‌های کلاس D و E
۳۲۳.....	اهداف ویژه آدرس‌های شبکه
۳۲۳.....	آدرس‌های IP خصوصی (RFC 1918)
۳۲۴.....	از چه آدرس IP خصوصی باید استفاده کنیم؟
۳۲۵.....	IP مجازی (VIP)
۳۲۵.....	APIPA
۳۲۶.....	انواع آدرس IPv4
۳۲۶.....	Broadcast لایه ۲
۳۲۷.....	Broadcast لایه ۳
۳۲۷.....	آدرس Unicast
۳۲۷.....	آدرس Multicast (کلاس D)
۳۲۸.....	پروتکل اینترنت نسخه ۶ (IPv6)
۳۲۸.....	چرا به IPv6 نیاز داریم؟
۳۲۹.....	مزایا و کاربردهای IPv6
۳۳۱.....	آدرس‌دهی و عبارات IPv6
۳۳۲.....	عبارت کوتاه شده
۳۳۳.....	انواع آدرس
۳۳۴.....	آدرس‌های خاص
۳۳۵.....	پیگیربندی خودکار آدرس بدون وضعیت (SLAAC)
۳۳۷.....	DHCPv6 (Stateful)
۳۳۷.....	مهاجرت به IPv6
۳۳۸.....	انباشته شدن دو گانه
۳۳۸.....	تونل‌سازی 6to4

۳۴۰	خلاصه
۳۴۰	ملزومات امتحان
۳۴۱	آزمایشگاه نوشتاری
۳۴۳	بررسی سؤالات
۳۴۷	فصل ۸: زیر شبکه IP، عیب یابی IP و مقدمه‌ای بر NAT
۳۴۸	مبانی زیر شبکه
۳۴۹	نحوه ایجاد زیر شبکه
۳۵۰	درک توان‌های ۲
۳۵۱	ساب‌نت ماسک‌ها
۳۵۱	مسیریابی بین دامنه‌ای بدون کلاس (CIDR)
۳۵۴	زیر شبکه‌سازی آدرس‌های کلاس C
۳۵۵	زیر شبکه‌سازی یک آدرس کلاس C: راه سریع!
۳۵۶	نمونه‌های تمرین زیر شبکه: آدرس‌های کلاس C
۳۶۲	زیر شبکه در ذهن شما: آدرس‌های کلاس C
۳۶۴	اکنون چه می‌دانید؟
۳۶۶	زیر شبکه‌سازی آدرس‌های کلاس B
۳۶۷	نمونه‌های تمرین زیر شبکه: آدرس‌های کلاس B
۳۷۳	زیر شبکه در ذهن شما: آدرس‌های کلاس B
۳۷۴	عیب‌یابی آدرس‌دهی IP
۳۷۷	تعیین مشکلات آدرس IP
۳۸۲	مقدمه‌ای بر ترجمه آدرس شبکه (NAT)
۳۸۴	انواع ترجمه آدرس شبکه
۳۸۴	نام‌های NAT
۳۸۵	NAT چگونه کار می‌کند
۳۸۷	خلاصه
۳۸۷	ملزومات امتحان
۳۸۸	آزمایشگاه نوشتاری
۳۸۹	بررسی سؤالات
۳۹۵	فصل ۹: مقدمه‌ای بر مسیریابی IP
۳۹۶	مبانی مسیریابی
۳۹۹	فرآیند مسیریابی IP
۴۰۶	تست مسیریابی IP
۴۰۸	مسیریابی ایستا و پویا
۴۱۱	خلاصه
۴۱۱	ملزومات امتحان
۴۱۲	آزمایشگاه نوشتاری
۴۱۳	بررسی سؤالات
۴۱۷	فصل ۱۰: پروتکل‌های مسیریابی

۴۱۸.....	میانی پروتکل مسیریابی
۴۱۹.....	فاصله‌های اداری
۴۲۰.....	چرا همه پروتکل‌های مسیریابی را روشن نمی‌کنیم؟
۴۲۱.....	کلاس‌های پروتکل‌های مسیریابی
۴۲۲.....	پروتکل‌های مسیریابی بردار فاصله
۴۲۴.....	پروتکل اطلاعات مسیریابی (RIP)
۴۲۵.....	RIP نسخه ۲ (RIPv2)
۴۲۶.....	VLSM ها و شبکه‌های ناپیوسته
۴۲۹.....	EIGRP
۴۳۱.....	پروتکل گیت‌وی مرزی (BGP)
۴۳۳.....	پروتکل‌های مسیریابی Link-State
۴۳۴.....	پروتکل OSPF
۴۳۷.....	سامانه حد واسط-به-سامانه حد واسط (IS-IS)
۴۳۹.....	مسیرهای High Available
۴۴۰.....	مفاهیم پیشرفته IPv6
۴۴۱.....	Router Advertisement
۴۴۲.....	پروتکل Neighbor Discovery
۴۴۴.....	پروتکل تونل‌زنی
۴۴۴.....	تونل‌های GRE
۴۴۴.....	تونل‌زنی 6to4
۴۴۵.....	تونل‌زنی دستی IPv6
۴۴۵.....	6to4 (اتوماتیک)
۴۴۶.....	تونل‌زنی ISATAP
۴۴۷.....	Teredo
۴۴۷.....	دو پشته
۴۴۸.....	پروتکل‌های مسیریابی IPv6
۴۴۸.....	RIPng
۴۴۹.....	EIGRPv6
۴۴۹.....	OSPFv3
۴۵۰.....	خلاصه
۴۵۰.....	ملزومات امتحان
۴۵۱.....	آزمایشگاه نوشتاری
۴۵۳.....	بررسی سوالات
۴۵۷.....	فصل ۱۱؛ سوئیچینگ و LAN‌های مجازی
۴۵۹.....	شبکه‌سازی پیش از سوئیچینگ لایه ۲
۴۶۲.....	سرویس‌های سوئیچینگ
۴۶۳.....	محدودیت‌های سوئیچینگ لایه ۲
۴۶۴.....	پل‌زدن در مقابل سوئیچینگ LAN

۴۶۴	سه تابع سوئیچ در لایه ۲
۴۶۵	یادگیری آدرس
۴۶۷	تصمیمات فوروارد/فیلتر
۴۶۸	اجتناب از حلقه
۴۷۰	سوئیچینگ توزیع شده
۴۷۰	پروتکل درخت پوشا
۴۷۲	حالت پورت درخت پوشا
۴۷۳	هم‌گرایی STP
۴۷۴	پروتکل درخت پوشای سریع 802.1w
۴۷۵	LANهای مجازی
۴۷۶	مبانی VLAN
۴۸۰	کیفیت سرویس
۴۸۱	عضویت‌های VLAN
۴۸۱	VLANهای ایستا
۴۸۲	VLANهای پویا
۴۸۲	شناسایی VLANها
۴۸۳	پورت‌های دسترسی
۴۸۳	پورت‌های دسترسی صوتی
۴۸۳	پورت‌های ترانک
۴۸۵	روش‌های شناسایی VLAN
۴۸۵	پیوند بین سوئیچ (ISL)
۴۸۵	برچسب‌گذاری پورت/IEEE 802.1Q
۴۸۶	مسیریابی بین VLANها
۴۸۹	پروتکل ترانکینگ VLAN
۴۹۰	حالت‌های عملکرد VTP
۴۹۱	آیا واقعاً نیاز داریم که یک آدرس IP روی سوئیچ قرار دهیم؟
۴۹۳	محافظت سوئیچ پورت
۴۹۴	امنیت پورت
۴۹۵	شنود DHCP
۴۹۵	بازرسی ARP
۴۹۵	Flood Guard
۴۹۶	BPDUGuard
۴۹۷	Root Guard
۴۹۷	اتصال پورت‌ها (Port Bonding)
۴۹۹	سخت شدن دستگاه
۴۹۹	ویژگی‌های پیشرفته سوئیچ‌ها
۴۹۹	توان از طریق اترنت (802.3af, 802.3at)
۵۰۰	PoE

۵۰۲.....	(SPAN/RSPAN) Port Mirroring/Spanning
۵۰۴.....	Jumbo های فریم‌های
۵۰۴.....	خلاصه
۵۰۵.....	ملزومات امتحان
۵۰۵.....	آزمایشگاه نوشتاری
۵۰۶.....	بررسی سوالات
۵۱۱.....	فصل ۱۲؛ شبکه‌های بی‌سیم
۵۱۳.....	مقدمه‌ای بر فناوری بی‌سیم
۵۱۶.....	فناوری‌های سلولی (Cellular Technologies)
۵۱۸.....	استانداردهای ۸۰۲.۱۱ (تأثیرات نظارتی)
۵۲۰.....	2.4 GHz (802.11b)
۵۲۱.....	2.4 GHz (802.11g)
۵۲۲.....	5 GHz (802.11a)
۵۲۳.....	5 GHz (802.11h)
۵۲۴.....	2.4 GHz/5 GHz (802.11n)
۵۲۵.....	پس Wi-Fi چیست؟
۵۲۵.....	5 GHz (802.11ac)
۵۲۶.....	Wi-Fi 6 (802.11ax)
۵۲۷.....	مقایسه استانداردهای ۸۰۲.۱۱
۵۲۸.....	مقایسه برد و سرعت
۵۲۸.....	اجزای شبکه بی‌سیم
۵۲۸.....	نقاط دسترسی بی‌سیم
۵۲۹.....	کارت اینترفیس شبکه بی‌سیم
۵۳۰.....	آنتن‌های بی‌سیم
۵۳۲.....	نصب شبکه بی‌سیم
۵۳۲.....	حالت Ad Hoc: مجموعه سرویس پایه مستقل
۵۳۳.....	حالت Infrastructure: شناسه مجموعه سرویس پایه (BSSID)
۵۳۵.....	کنترلرهای بی‌سیم
۵۳۷.....	شبکه‌های مهمان
۵۳۷.....	پورتال‌های Captive
۵۳۸.....	نقطه اتصال موبایل
۵۳۹.....	تضعیف سیگنال
۵۴۰.....	سایر پیاده‌سازی‌های زیرساخت شبکه
۵۴۱.....	نسخه‌های ۴.۰ و ۵.۰: بلوتوث کم انرژی
۵۴۲.....	فناوری‌هایی که اینترنت اشیا (IoT) را تسهیل می‌کنند
۵۴۳.....	نصب و پیکربندی سخت‌افزار WLAN
۵۴۴.....	پیکربندی NIC
۵۴۵.....	پیکربندی AP

۵۴۹.....	بررسی سایت
۵۵۱.....	تأمین ظرفیت
۵۵۲.....	طبقه‌های چندگانه
۵۵۳.....	WLAN مبتنی بر مکان
۵۵۴.....	ابزارهای بررسی سایت (Site Survey Tools)
۵۵۴.....	امنیت بی‌سیم (وایرلس)
۵۵۵.....	تهدیدات بی‌سیم
۵۵۵.....	APهای متقلب
۵۵۵.....	کاهش
۵۵۶.....	شبکه‌های Ad Hoc
۵۵۶.....	کاهش
۵۵۶.....	انکار سرویس
۵۵۶.....	کاهش
۵۵۷.....	حالت زیرساخت
۵۵۷.....	حالت کلاینت
۵۵۷.....	حملات غیرفعال
۵۵۷.....	کاهش
۵۵۸.....	جست‌وجوی شبکه‌ها حین رانندگی (war driving)
۵۵۹.....	دسترسی آزاد (Open Access)
۵۵۹.....	شناسه‌های مجموعه سرویس، حریم خصوصی معادل سیمی و احراز هویت آدرس کنترل دسترسی به رسانه
۵۶۱.....	ژئوفنسینگ (Geofencing)
۵۶۱.....	سیستم تأیید هویت کاربران جهت ورود از راه دور (802.1X)
۵۶۲.....	پروتکل جامع کلید موقت
۵۶۴.....	WPA2 Pre-Shared Key یا Wi-Fi Protected Access
۵۶۵.....	گواهینامه‌ها و PKI
۵۶۷.....	خلاصه
۵۶۷.....	ملزومات امتحان
۵۶۹.....	آزمایشگاه نوشتاری
۵۷۰.....	بررسی سؤالات
۵۷۵.....	فصل ۱۳؛ دسترسی به شبکه از راه دور
۵۷۶.....	VPN̄ سایت به سایت
۵۷۷.....	VPN کلاینت به سایت
۵۷۷.....	VPN بدون کلاینت
۵۷۷.....	Split Tunnel در مقابل Full Tunnel
۵۷۸.....	اتصال دسکتاپ از راه دور (Remote Desktop Connection)
۵۷۹.....	Remote Desktop پروتکل
۵۸۱.....	RDP گیتوی
۵۸۲.....	محاسبه شبکه مجازی

۵۸۲.....	دسکتاپ مجازی
۵۸۳.....	روش‌های اتصال
۵۸۳.....	پوسته امن (Secure Shell)
۵۸۴.....	اینترفیس کاربری گرافیکی
۵۸۴.....	اینترفیس برنامه‌نویسی کاربردی
۵۸۶.....	کنسول/کابل سریال رول شده
۵۸۸.....	جامپ باکس/هاست
۵۸۹.....	جامپ باکس/هاست را کجا باید پیاده‌سازی کنید؟
۵۸۹.....	مقایسه مدیریت In-Band و Out of Band
۵۹۰.....	خلاصه
۵۹۰.....	ملزومات امتحان
۵۹۰.....	آزمایشگاه نوشتاری
۵۹۱.....	بررسی سؤالات
۵۹۵.....	فصل ۱۴؛ استفاده از آمار و حسگرها برای اطمینان از در دسترس بودن شبکه
۵۹۶.....	عملکرد نظارت/متریک/حسگرها
۵۹۷.....	دستگاه / شاسی
۵۹۷.....	دما
۵۹۸.....	استفاده از واحد پردازش مرکزی
۵۹۸.....	حافظه (Memory)
۵۹۹.....	متریک‌های شبکه
۵۹۹.....	پهنای باند
۶۰۰.....	تأخیر (Latency)
۶۰۰.....	Jitter
۶۰۱.....	Loss
۶۰۱.....	راه حل‌های نظارتی اضافی
۶۰۱.....	پویش شبکه (Network Discovery)
۶۰۱.....	Ad Hoc
۶۰۱.....	برنامه‌ریزی شده (Scheduled)
۶۰۱.....	متریک‌های خط مینا
۶۰۲.....	هشدار/اعلان ناهنجاری
۶۰۲.....	تجزیه و تحلیل ترافیک
۶۰۲.....	نظارت بر عملکرد
۶۰۳.....	نظارت بر دردسترس بودن
۶۰۴.....	نظارت بر پیکربندی
۶۰۵.....	SNMP
۶۰۵.....	عامل (Agent)
۶۰۶.....	NMS
۶۰۶.....	فرمان‌ها

۶۰۸.....	نام جامعه.....
۶۰۸.....	نسخه‌ها.....
۶۰۹.....	MIB و OID.....
۶۱۰.....	احراز هویت.....
۶۱۱.....	یکپارچه‌سازی اینترفیس برنامه‌نویسی کاربردی (API).....
۶۱۱.....	تحلیل‌گر پروتکل / ضبط بسته.....
۶۱۲.....	Port Mirroring.....
۶۱۳.....	جریان داده.....
۶۱۴.....	جمع‌آوری لاگ (Log Aggregation).....
۶۱۴.....	لاگ‌های دستگاه شبکه.....
۶۱۵.....	بررسی لاگ‌ها.....
۶۱۵.....	ترافیک لاگ‌ها.....
۶۱۵.....	حسابرسی لاگ‌ها.....
۶۱۶.....	Syslog.....
۶۱۷.....	جمع‌آوری کننده Syslog.....
۶۱۸.....	پیام‌های Syslog.....
۶۱۸.....	سطوح ورود/سطوح Severity.....
۶۱۹.....	SIEM.....
۶۲۰.....	اعلان‌ها.....
۶۲۰.....	خلاصه.....
۶۲۰.....	ملزومات امتحان.....
۶۲۱.....	آزمایشگاه نوشتاری.....
۶۲۱.....	بررسی سؤالات.....
۶۲۵.....	فصل ۱۵؛ اسناد و خط‌مشی‌های سازمانی.....
۶۲۷.....	طرح‌ها و رویه‌ها.....
۶۲۸.....	مدیریت تغییر.....
۶۲۸.....	سند دلیل تغییر.....
۶۲۸.....	درخواست تغییر.....
۶۲۸.....	رویه‌های پیکربندی.....
۶۲۸.....	فرآیند بازگشت.....
۶۲۹.....	تأثیر بالقوه.....
۶۲۹.....	اطلاع‌رسانی.....
۶۲۹.....	فرآیند تأیید.....
۶۲۹.....	پنجره تعمیر و نگهداری.....
۶۲۹.....	توقف مجاز.....
۶۳۰.....	اطلاعیه تغییر.....
۶۳۰.....	مستندات.....
۶۳۰.....	طرح واکنش به حادثه.....

۶۳۰	طرح بازیابی فاجعه
۶۳۱	طرح تداوم کسب‌وکار
۶۳۱	مدیریت موجودی
۶۳۲	چرخه حیات سیستم
۶۳۳	رویه‌های عملیاتی استاندارد
۶۳۴	سخت‌سازی و خط‌مشی‌های امنیتی
۶۳۴	خط‌مشی‌های استفاده صحیح
۶۳۵	خط‌مشی‌رمز عبور
۶۳۵	خط‌مشی دستگاه خود را بیاورید
۶۳۶	خط‌مشی دسترسی از راه دور
۶۳۶	خط‌مشی Onboarding و Offboarding
۶۳۷	مدیریت Patch
۶۳۷	به‌روزرسانی درایور / فریمویر
۶۳۸	خط‌مشی امنیتی (Security Policy)
۶۳۸	ممیزی امنیتی
۶۳۸	خط‌مشی میز تمیز (Clean-Desk)
۶۳۹	تجهیزات ضبط
۶۳۹	سایر خط‌مشی‌های امنیتی مشترک
۶۴۳	شکستن خط‌مشی
۶۴۳	پیشگیری از فقدان داده (Data Loss Prevention)
۶۴۴	اسناد مشترک
۶۴۵	نمودار شبکه فیزیکی
۶۴۵	اجتناب از سردرگمی
۶۴۷	پلن طبقه
۶۴۸	نمودار رک
۶۴۹	مستندات چارچوب توزیع میانی / فریم توزیع اصلی
۶۵۰	نمودار شبکه منطقی
۶۵۱	نمودار سیم‌کشی
۶۵۱	نقشه‌های کابل
۶۵۲	نمودار شبکه لایه‌ای
۶۵۳	گزارش بررسی سایت (Site Survey)
۶۵۴	گزارش حسابرسی و ارزیابی
۶۵۴	ممیزی امنیتی
۶۵۴	قدم بزیند
۶۵۵	تنظیمات خط مینا
۶۵۶	پیکربندی طلایی
۶۵۶	مدیریت آدرس IP
۶۵۶	توافقنامه‌های مشترک

۶۵۷	توافق نامه عدم افشای اطلاعات
۶۵۷	توافق نامه سطح سرویس
۶۵۸	تفاهم نامه
۶۵۸	خلاصه
۶۵۹	ملزومات امتحان
۶۵۹	آزمایشگاه نوشتاری
۶۶۰	بررسی سؤالات
۶۶۵	فصل ۱۶؛ دسترس پذیری بالا و بازیابی فاجعه
۶۶۷	تقسیم بار (Load Balancing)
۶۶۷	چند مسیری (Multipathing)
۶۶۸	تیم سازی کارت اینترفیس شبکه (NIC)
۶۶۹	سخت افزار/کلاسترهای اضافی
۶۶۹	سوئیچ ها
۶۷۲	کلاسترینگ سوئیچ
۶۷۲	روتورها
۶۷۴	فایروال ها
۶۷۴	سرورها
۶۷۴	افزودگی منبع تغذیه
۶۷۵	افزودگی ذخیره سازی
۶۷۷	کلاسترها
۶۷۷	میانگین زمان برای تعمیر
۶۷۸	میانگین زمان بین خرابی
۶۷۸	پشتیبانی تأسیسات و زیرساخت ها
۶۷۸	منبع تغذیه بدون وقفه
۶۷۹	واحدهای توزیع نیروی برق
۶۷۹	ژنراتور
۶۸۰	HVAC
۶۸۱	اطفاء حریق
۶۸۳	مفاهیم افزودگی و دسترس پذیری بالا
۶۸۳	سایت های بازیابی فاجعه
۶۸۳	سایت سرد
۶۸۳	سایت گرم (warm)
۶۸۳	سایت داغ (Hot)
۶۸۴	سایت ابری
۶۸۴	فعال/فعال در مقابل فعال/غیرفعال
۶۸۵	چندین ارائه دهنده سرویس اینترنتی/مسیرهای متنوع
۶۸۶	پروتکل افزودگی First-Hop
۶۸۶	پروتکل Hot Standby Router

۶۸۸.....	مک آدرس مجازی
۶۸۹.....	تایمرهای HSRP
۶۹۰.....	قطع شدن شبکه سازمانی بزرگ با FHRP
۶۹۰.....	پروتکل Virtual Router Redundancy
۶۹۱.....	مقایسه HSRP و VRRP
۶۹۱.....	ویژگی‌های افزونگی VRRP
۶۹۱.....	پشتیبان‌گیری
۶۹۲.....	پشتیبان‌گیری/بازیابی دستگاه شبکه
۶۹۳.....	بازیابی
۶۹۳.....	آزمایش
۶۹۴.....	تمرینات رومیزی
۶۹۴.....	آزمایش‌های اعتبارسنجی
۶۹۵.....	خلاصه
۶۹۶.....	ملزومات امتحان
۶۹۶.....	آزمایشگاه نوشتاری
۶۹۷.....	بررسی سؤالات
۷۰۱.....	فصل ۱۷؛ معماری دیتاستر و مفاهیم ابری
۷۰۴.....	رایانش ابری
۷۰۵.....	ویژگی‌های ابر
۷۰۶.....	مدل‌های تحویل ابری
۷۰۶.....	خصوصی
۷۰۷.....	عمومی
۷۰۸.....	هیبرید (ترکیبی)
۷۰۹.....	انواع سرویس‌ها
۷۱۰.....	SaaS
۷۱۰.....	PaaS
۷۱۱.....	IaaS
۷۱۱.....	DaaS
۷۱۲.....	مجازی‌سازی عملکرد شبکه
۷۱۲.....	فایروال مجازی
۷۱۳.....	روتر مجازی
۷۱۳.....	سوئیچ مجازی
۷۱۳.....	ابر خصوصی مجازی
۷۱۳.....	گزینه‌های اتصال
۷۱۴.....	شبکه خصوصی مجازی
۷۱۴.....	اتصال مستقیم خصوصی
۷۱۵.....	گیت‌وی‌های ابری
۷۱۵.....	گیت‌وی اینترنت

۷۱۵.....	گیتوی ترجمه آدرس شبکه
۷۱۶.....	چند مستأجری
۷۱۷.....	کشسانی (Elasticity)
۷۱۷.....	مقیاس پذیری
۷۱۸.....	گروه‌های امنیتی شبکه
۷۱۸.....	لیست‌های امنیتی شبکه
۷۱۸.....	مفاهیم / ملاحظات امنیتی
۷۱۸.....	ارتباط بین منابع محلی و ابری
۷۱۹.....	زیرساخت مبتنی بر کد
۷۲۰.....	اتوماسیون / ارکستراسیون
۷۲۰.....	کتاب‌های راهنما/الگوها/کارهای قابل استفاده مجدد
۷۲۲.....	پیکر بندی Drift/Compliance
۷۲۲.....	ارتقاء
۷۲۲.....	موجودی‌های پویا
۷۲۲.....	کنترل منبع
۷۲۳.....	کنترل نسخه
۷۲۳.....	مخزن مرکزی
۷۲۳.....	شناسایی تعارض
۷۲۳.....	انشعاب
۷۲۳.....	شبکه‌های نرم‌افزاری تعریف شده
۷۲۴.....	مزایای شبکه‌های نرم‌افزاری تعریف شده
۷۲۴.....	کاربردی-آگاه (Application-Aware)
۷۲۴.....	پروسه Zero-Touch Provisioning
۷۲۴.....	انتقال آگنوستیک
۷۲۴.....	مدیریت خط مشی مرکزی
۷۲۵.....	اجزای شبکه‌های تعریف شده با نرم افزار
۷۲۵.....	لایه اپلیکیشن
۷۲۵.....	لایه کنترل
۷۲۶.....	لایه زیرساخت
۷۲۶.....	سطوح SDN
۷۲۶.....	اینترفیس‌های برنامه‌نویسی کاربردی
۷۲۷.....	API های Southbound
۷۲۸.....	API های Northbound
۷۲۹.....	شبکه محلی قابل توسعه مجازی
۷۲۹.....	محدودیت‌های کپسوله‌سازی لایه ۲ آدرس‌دهی شده توسط VXLAN
۷۲۹.....	اتصال بین دیتاستر
۷۳۰.....	معماری Zero Trust
۷۳۰.....	احراز هویت مبتنی بر خط مشی

۷۳۰	مجوز
۷۳۰	حداقل دسترسی به امتیاز
۷۳۱	Secure Access Secure Edge/Security Service Edge
۷۳۱	SASE
۷۳۱	SSE
۷۳۲	خلاصه
۷۳۲	ملزومات امتحان
۷۳۳	آزمایشگاه نوشتاری
۷۳۴	بررسی سوالات
۷۳۹	فصل ۱۸؛ روش عیب‌یابی شبکه
۷۴۲	محدود کردن مشکل
۷۴۳	آیا چیزهای بسیار ساده را بررسی کردید؟
۷۴۳	روش ورود صحیح و حقوق دسترسی
۷۴۴	آیا می‌توان مشکل را بازتولید کرد؟
۷۴۵	نشانه‌های وضعیت LED اتصال شبکه
۷۴۶	سوئیچ پاور
۷۴۶	خطای اپراتور
۷۴۷	آیا سخت‌افزار یا نرم‌افزار باعث ایجاد مشکل می‌شود؟
۷۴۸	آیا مشکل از ایستگاه کاری است یا سرور؟
۷۴۹	کدام بخش‌های شبکه تحت تأثیر قرار می‌گیرند؟
۷۵۰	آیا کابل کشی بد است؟
۷۵۰	ملاحظات کابل
۷۵۱	شیلددار و بدون شیلد
۷۵۱	Riser-Rated و Plenum
۷۵۲	کاربردهای کابل
۷۵۲	کابل رول‌اور/کابل کنسول
۷۵۳	کابل کراس‌اور
۷۵۴	سایر مشکلات مهم کابل که باعث مشکلات عملکرد می‌شود
۷۵۷	مشکلات کابل فیبر
۷۵۹	مشکلات رسانه‌ای نامحدود (بی‌سیم)
۷۶۵	مراحل عیب‌یابی
۷۶۶	مرحله ۱: مشکل را شناسایی کنید
۷۶۶	جمع‌آوری اطلاعات با پرسش از کاربران
۷۶۷	در صورت امکان مشکل را تکرار کنید
۷۶۷	تعیین کنید که آیا چیزی تغییر کرده است
۷۶۸	علائم را شناسایی کنید
۷۷۰	به مشکلات متعدد به صورت جداگانه نزدیک شوید
۷۷۰	مرحله ۲: تئوری علت احتمالی را ایجاد کنید

۷۷۱.....	سؤالات آشکار بپرسید
۷۸۷.....	چند رویکرد را در نظر بگیرید
۷۸۸.....	مرحله ۳: تئوری را برای تعیین علت آزمایش کنید
۷۹۰.....	مرحله ۴: ایجاد یک برنامه اقدام برای حل مشکل و شناسایی اثرات بالقوه
۷۹۲.....	مرحله ۵: راه حل را اجرا کنید یا در صورت لزوم افزایش دهید
۷۹۶.....	مرحله ۶: بررسی عملکرد کامل سیستم و اجرای اقدامات پیشگیرانه در صورت وجود
۷۹۶.....	مرحله ۷: مستندسازی یافته‌ها، اقدامات، نتایج و درس‌های آموخته شده در طول فرآیند
۷۹۶.....	مستندات شبکه
۷۹۷.....	نکات عیب یابی
۷۹۷.....	چیزهای کوچک را نادیده نگیرید
۷۹۷.....	مشکلات خود را اولویت‌بندی کنید
۷۹۸.....	تنظیمات نرم‌افزار را بررسی کنید
۷۹۹.....	شرایط فیزیکی را نادیده نگیرید
۸۰۰.....	مشکلات کابل را نادیده نگیرید
۸۰۱.....	ویروس‌ها را بررسی کنید
۸۰۱.....	خلاصه
۸۰۱.....	ملزومات امتحان
۸۰۲.....	آزمایشگاه نوشتاری
۸۰۳.....	بررسی سؤالات
۸۰۹.....	فصل ۱۹؛ ابزارها و فرمان‌های نرم‌افزار شبکه
۸۱۰.....	ابزارهای نرم‌افزاری
۸۱۰.....	تحلیل‌گر پروتکل / ضبط بسته
۸۱۲.....	تسترهای سرعت پهنای باند
۸۱۳.....	اسکنرهای پورت
۸۱۴.....	تحلیل‌گرهای NetFlow
۸۱۴.....	سرور پروتکل انتقال فایل بی‌اهمیت
۸۱۵.....	نرم‌افزار اتصال
۸۱۶.....	اسکنر IP
۸۱۶.....	استفاده از Traceroute
۸۲۰.....	استفاده از ipconfig و ifconfig و ip
۸۲۰.....	استفاده از ابزار ipconfig
۸۲۳.....	استفاده از ابزار ifconfig
۸۲۴.....	استفاده از ابزار ip
۸۲۵.....	استفاده از ابزار iptables
۸۲۵.....	نمونه‌هایی از iptables
۸۲۶.....	استفاده از ابزار ping
۸۲۹.....	پروتکل Address Resolution
۸۳۰.....	جدول ARP ویندوز

۸۳۰	استفاده از ابزار arp
۸۳۴	استفاده از ابزار nslookup
۸۳۵	حل نام‌ها با فایل هاست
۸۳۷	استفاده از فرمان mtr (pathping)
۸۳۸	استفاده از ابزار Nmap
۸۳۹	استفاده از فرمان route
۸۴۱	استفاده از گزینه‌های فرمان route
۸۴۲	چند نمونه از فرمان route
۸۴۳	استفاده از ابزار netstat
۸۴۶	سوئیچ -e
۸۴۸	سوئیچ -r
۸۴۸	سوئیچ -s
۸۴۸	سوئیچ -p
۸۵۰	سوئیچ -n
۸۵۱	موارد استفاده از netstat
۸۵۲	استفاده از tcpdump
۸۵۲	نمونه‌های استفاده از tcpdump
۸۵۲	فرمان‌های اصلی دستگاه شبکه
۸۵۲	فرمان show running-config (Show Run)
۸۵۴	فرمان show config
۸۵۴	Cisco Discovery Protocol
۸۵۴	فرمان show cdp neighbors
۸۵۷	پروتکل شناسایی لایه پیوند
۸۵۷	فرمان show ip route (فرمان route در ویندوز)
۸۵۸	فرمان show version
۸۵۹	فرمان show inventory
۸۶۰	فرمان show switch
۸۶۱	فرمان show mac-address-table
۸۶۲	فرمان show interface
۸۶۴	عیب‌یابی با فرمان show interfaces
۸۶۵	فرمان show ip interface brief
۸۶۶	تأیید با فرمان show ip interface
۸۶۶	فرمان show arp
۸۶۷	فرمان show vlan
۸۶۹	فرمان show power
۸۶۹	ابزارهای سخت‌افزار
۸۶۹	ابزار Toner/Toner Probe
۸۷۱	تستر کابل

۸۷۲	Tapها
۸۷۲	تحلیل گرهای WI-FI
۸۷۳	قلم فیبر نوری
۸۷۳	خلاصه
۸۷۴	ملزومات امتحان
۸۷۵	آزمایشگاه نوشتاری
۸۷۶	بررسی سؤالات
۸۸۱	فصل ۲۰؛ مفاهیم امنیت شبکه
۸۸۳	اصطلاحات امنیتی رایج
۸۸۳	تهدیدها و ریسک
۸۸۴	تهدیدهای خارجی
۸۸۴	تهدیدهای داخلی
۸۸۴	تهدیدهای غیرعمدی
۸۸۵	آسیب پذیری
۸۸۵	آسیب پذیری ها و تهدیدهای رایج
۸۸۶	آسیب پذیری Zero-Day
۸۸۷	اکسپلویت (Exploit)
۸۸۸	عدم افشا، یکپارچگی و در دسترس بودن
۸۸۹	رمز گذاری
۸۹۱	رمز گذاری متقارن
۸۹۱	رمز گذاری نامتقارن
۸۹۲	گواهی ها
۸۹۲	زیرساخت کلید عمومی
۸۹۵	CA عمومی در مقابل CA خصوصی
۸۹۶	گواهینامه Self-Signed
۸۹۷	مدل AAA
۸۹۷	احراز هویت
۸۹۸	احراز هویت چند عاملی
۹۰۰	روش های احراز هویت چند عاملی
۹۰۲	شناسایی یگانه (Single Sign-On)
۹۰۳	سرویس احراز هویت از راه دور
	Terminal Access Controller Access Control System Plus پروتکل
۹۰۴	
۹۰۵	LDAP
۹۰۶	مجوز
۹۰۷	مدیریت هویت و دسترسی
۹۰۷	حداقل امتیاز
۹۰۸	کنترل دسترسی مبتنی بر نقش

۹۰۸.....	حصار جغرافیایی (Geofencing)
۹۰۹.....	حسابداری
۹۱۰.....	رعایت مقررات
۹۱۳.....	خط مشی ها، فرآیندها و رویه‌ها
۹۱۴.....	حسابرسی (ممیزی)
۹۱۵.....	خلاصه
۹۱۶.....	ملزومات امتحان
۹۱۶.....	آزمایشگاه نوشتاری
۹۱۷.....	بررسی سؤالات
۹۲۱.....	فصل ۲۱: انواع رایج حملات
۹۲۴.....	حملات مبتنی بر فناوری
۹۲۴.....	انکار سرویس / انکار سرویس توزیع شده
۹۲۶.....	DoS دوستانه/غیر عمدی
۹۲۶.....	DoS فیزیکی
۹۲۷.....	DoS دائمی
۹۲۷.....	حمله On-Path (که قبلاً به عنوان حمله مرد میانی شناخته می‌شد)
۹۲۷.....	مسمومیت / جعل DNS
۹۲۸.....	VLAN Hopping
۹۲۹.....	جعل / مسمومیت ARP
۹۲۹.....	دستگاه‌ها و سرویس‌های متقلب (سرکش)
۹۲۹.....	DHCP متقلب
۹۳۰.....	اکسس پوینت متقلب
۹۳۱.....	حمله دوقلوهای شیطانی (Evil Twin)
۹۳۲.....	حمله Deauthentication
۹۳۲.....	حملات رمز عبور
۹۳۳.....	حمله MAC Spoofing
۹۳۴.....	حمله IP Spoofing
۹۳۴.....	حمله غرق کردن مک (MAC Flooding)
۹۳۴.....	بدافزار
۹۳۵.....	باچ‌افزار
۹۳۶.....	تروجان‌ها
۹۳۶.....	کی‌لاگرها
۹۳۶.....	روت‌کیت‌ها
۹۳۷.....	جاسوس‌افزار
۹۳۷.....	بدافزار Cryptominers
۹۳۷.....	ویروس‌ها
۹۳۸.....	انسان و محیط زیست
۹۳۸.....	مهندسی اجتماعی

۹۳۸.....	فیشینگ (Phishing)
۹۳۹.....	محیطزیست
۹۳۹.....	حمله دنبالرویی (Tailgating)
۹۳۹.....	حمله سواری گرفتن (Piggybacking)
۹۳۹.....	حمله Dumpster Diving
۹۳۹.....	حمله Shoulder Surfing
۹۴۰.....	سخت‌سازی امنیت
۹۴۱.....	باغبانی دستگاه (Device Gardening)
۹۴۱.....	تغییر اعتبار پیش‌فرض
۹۴۱.....	اجتناب از رمزهای عبور رایج
۹۴۱.....	غیرفعال کردن سرویس‌های غیر ضروری
۹۴۲.....	استفاده از پروتکل‌های امن
۹۴۳.....	غیرفعال کردن پورت‌های استفاده نشده
۹۴۳.....	پورت‌های IP
۹۴۳.....	پورت‌های دستگاه (فیزیکی و مجازی)
۹۴۴.....	مدیریت کلید
۹۴۴.....	لیست‌های کنترل دسترسی
۹۴۶.....	فیلتر کردن محتوا
۹۴۷.....	پیاده‌سازی بخش‌بندی شبکه
۹۴۷.....	اجرای بخش‌بندی شبکه
۹۴۸.....	زیرشبکه غربال شده
۹۴۹.....	802.1X
۹۵۰.....	NAC
۹۵۱.....	فیلتر MAC
۹۵۱.....	امنیت پورت
۹۵۳.....	اینترنت اشياء
۹۵۴.....	سیستم‌های کنترل صنعتی/کنترل نظارتی و جمع‌آوری داده‌ها
۹۵۵.....	سیستم نظارتی
۹۵۵.....	فناوری عملیاتی
۹۵۶.....	زیرساخت‌های ارتباطی
۹۵۶.....	شبکه‌های خصوصی/عمومی مجزا
۹۵۶.....	هانی‌پات / هانی‌نت (Honeypot/Honeynet)
۹۵۷.....	دستگاه خود را بیاورید
۹۵۷.....	جداسازی شبکه مهمان
۹۵۷.....	پورتال Captive
۹۵۸.....	مفاهیم امنیت فیزیکی
۹۵۸.....	نظارت تصویری
۹۶۰.....	قفل درب

۹۶۰	قفل تجهیزات
۹۶۱	قفل کابل
۹۶۲	قفل سرور
۹۶۲	قفل USB
۹۶۲	خلاصه
۹۶۳	ملزومات امتحان
۹۶۳	آزمایشگاه نوشتاری
۹۶۴	بررسی سؤالات
۹۶۹	پیوست الف؛ پاسخ آزمایشگاه‌های نوشتاری
۹۶۹	فصل ۱: مقدمه‌ای بر شبکه‌ها
۹۶۹	فصل ۲: مدل مرجع اتصال سیستم‌های باز (OSI)
۹۷۰	فصل ۳: اتصالات شبکه و استانداردهای سیم کشی
۹۷۰	فصل ۴: مشخصات اترنت فعلی
۹۷۱	فصل ۵: دستگاه‌های شبکه
۹۷۲	فصل ۶: مقدمه‌ای بر پروتکل اینترنت
۹۷۲	فصل ۷: آدرس دهی IP
۹۷۳	فصل ۸: زیرشبکه IP، عیب‌یابی IP و مقدمه‌ای بر NAT
۹۷۴	فصل نهم: مقدمه‌ای بر مسیریابی IP
۹۷۴	فصل ۱۰: پروتکل‌های مسیریابی
۹۷۶	فصل ۱۱: سوئیچینگ و LAN‌های مجازی
۹۷۷	فصل ۱۲: شبکه‌های بی سیم
۹۷۷	فصل ۱۳: دسترسی به شبکه از راه دور
۹۷۷	فصل ۱۴: استفاده از آمار و حسگرها برای اطمینان از در دسترس بودن شبکه
۹۷۸	فصل ۱۵: اسناد و خط مشی‌های سازمانی
۹۷۹	فصل ۱۶: دسترس پذیری بالا و بازیابی بلایا
۹۷۹	فصل ۱۷: معماری دیتاستر و مفاهیم ابر
۹۸۰	فصل ۱۸: روش عیب‌یابی شبکه
۹۸۰	فصل ۱۹: ابزارها و فرمان‌های نرم‌افزار شبکه
۹۸۰	فصل ۲۰: مفاهیم امنیت شبکه
۹۸۱	فصل ۲۱: انواع رایج حملات
۹۸۳	پیوست ب؛ پاسخ به بررسی سؤالات
۹۸۳	فصل ۱: مقدمه‌ای بر شبکه‌ها
۹۸۶	فصل ۲: مدل مرجع اتصال سیستم‌های باز (OSI)
۹۸۸	فصل ۳: اتصالات شبکه و استانداردهای سیم کشی
۹۹۱	فصل ۴: مشخصات اترنت فعلی
۹۹۴	فصل ۵: دستگاه‌های شبکه
۹۹۷	فصل ششم: مقدمه‌ای بر پروتکل اینترنت
۱۰۰۰	فصل ۷: آدرس دهی IP

۱۰۰۲	فصل ۸: زیرشبکه IP، عیب‌یابی IP و مقدمه‌ای بر NAT
۱۰۰۵	فصل ۹: مقدمه‌ای بر مسیریابی IP
۱۰۰۸	فصل ۱۰: پروتکل‌های مسیریابی
۱۰۱۲	فصل ۱۱: سوئیچینگ و LAN‌های مجازی
۱۰۱۵	فصل ۱۲: شبکه‌های بی‌سیم
۱۰۱۸	فصل ۱۳: دسترسی به شبکه از راه دور
۱۰۲۲	فصل ۱۴: استفاده از آمار و حسگرها برای اطمینان از در دسترس بودن شبکه
۱۰۲۵	فصل ۱۵: اسناد و خط‌مشی‌های سازمانی
۱۰۲۷	فصل ۱۶: دسترس‌پذیری بالا و بازیابی بلایا
۱۰۳۰	فصل ۱۷: معماری دیتاستر و مفاهیم ابری
۱۰۳۴	فصل ۱۸: روش عیب‌یابی شبکه
۱۰۳۶	فصل ۱۹: ابزارها و فرمان‌های نرم‌افزار شبکه
۱۰۳۹	فصل ۲۰: مفاهیم امنیت شبکه
۱۰۴۲	فصل ۲۱: انواع رایج حملات
۱۰۴۷	پیوست C؛ زیرشبکه کلاس A
۱۰۴۷	مثال‌های تمرین زیرشبکه: آدرس‌های کلاس A
۱۰۴۸	تمرین #1A: 255.255.0.0 (/16)
۱۰۴۸	تمرین #2A: 255.255.240.0 (/20)
۱۰۴۹	تمرین #3A: 255.255.255.192 (/26)
۱۰۵۰	زیرشبکه در ذهن شما: آدرس‌های کلاس A
۱۰۵۰	آزمایشگاه نوشتاری C.1
۱۰۵۱	آزمایشگاه نوشتاری C.2
۱۰۵۲	پاسخ آزمایشگاه نوشتاری C.1
۱۰۵۲	پاسخ آزمایشگاه نوشتاری C.2

مقدمه

اگر مانند بسیاری از ما در جامعه شبکه هستید، احتمالاً یک یا چند گواهینامه شبکه دارید. اگر این چنین است، بسیار عاقلانه است که گواهینامه (N10-009) CompTIA Network+ را با افتخار به کارنامه خود اضافه کنید؛ زیرا این دستاورد، جایگاه شما را به عنوان یک شبکه‌کار، ارزشمندتر می‌کند.

در این دوران چالش برانگیز اقتصادی، پیشی گرفتن از رقبا (حتی در میان همکاران فعلی‌تان) می‌تواند تفاوت بزرگی در کسب ترفیع یا حفظ شغل‌تان ایجاد کند! یا شاید این اولین تلاش شما برای دریافت گواهینامه باشد؛ زیرا تصمیم گرفته‌اید وارد یک حرفه جدید در فناوری اطلاعات (IT) شوید. متوجه شده‌اید که ورود به حوزه فناوری اطلاعات راه خوبی برای پیمایش است؛ زیرا با پیشرفت عصر اطلاعات، تقاضا برای متخصصان آگاه در این زمینه پویا به طور چشمگیری افزایش می‌یابد.

در هر صورت، اگر در حرفه شبکه کار می‌کنید یا می‌خواهید وارد آن شوید، گرفتن گواهینامه یکی از بهترین کارهایی است که می‌توانید برای حرفه خود انجام دهید. زیرا ثابت می‌کند در مورد موضوعاتی که در مورد آن صحبت می‌کنید، اطلاعات کافی دارید. همچنین شما را به عنوان یک حرفه‌ای تأیید می‌کند، مانند پزشکی که در یک حوزه تخصصی خاص دارای مورد تخصصی است.

در این کتاب متوجه خواهید شد که آزمون CompTIA Network+ چیست؛ هر فصل بخشی از آزمون را پوشش می‌دهد. در پایان هر فصل "بررسی سوالات" را گنجانده‌ایم تا به یادگیری بیشتر اطلاعاتی که آموخته‌اید کمک کند و شما را برای آزمون آماده کند.

یک نکته جالب در مورد کار در حوزه IT این است که دائماً در حال تکامل است، بنابراین همیشه چیزهای جدیدی برای یادگیری وجود دارد و چالش‌های جدیدی برای تسلط بر آن وجود دارد. هنگامی که گواهینامه Network+ خود را دریافت کردید و متوجه شدید که به آن علاقه‌مندید، با وارد شدن به شبکه‌های پیچیده‌تر (و کسب درآمد بیشتر) پیش بروید، گواهینامه Cisco CCNA قطعاً گام بعدی شما خواهد بود. می‌توانید اطلاعاتی در مورد آن و حتی گواهینامه‌های دیگر در وبلاگ من (www.lammle.com) دریافت کنید.

توجه: برای آموزش Network+ با Todd Lammle، چه توسط مربی و چه آنلاین، لطفاً به www.lammle.com مراجعه کنید.

گواهینامه +Network چیست؟

گواهینامه +Network توسط انجمن صنعت فناوری رایانه‌ای (CompTIA) ایجاد شده است که برای ارائه منابع و آموزش برای جامعه رایانه و فناوری وجود دارد. این همان ارگانی است که آزمون A+ را برای تکنسین‌های کامپیوتر توسعه داده است.

آزمون +Network برای محک‌زدن مهارت تکنسین‌های شبکه با ۹ تا ۱۲ ماه سابقه در زمینه شبکه‌های فناوری اطلاعات طراحی شده است. این آزمون حوزه‌هایی از فناوری‌های شبکه، مانند تعریف یک پروتکل، مدل اتصال سامانه‌های باز^۲ (OSI) و لایه‌های آن و مفاهیم طراحی و پیاده‌سازی شبکه (حداقل دانش مورد نیاز برای کار بر روی یک شبکه و برخی از پیش‌نیازهای اساسی برای طراحی و پیاده‌سازی شبکه) را آزمایش می‌کند.

چرا باید گواهینامه +Network را دریافت کنیم؟

از آنجایی که CompTIA یک توسعه‌دهنده معتبر گواهینامه‌های بی‌طرف صنعت شبکه است، دریافت گواهینامه +Network نشان می‌دهد که شما در زمینه‌های خاص تحت پوشش اهداف آزمون +Network مهارت دارید.

چهار مزیت عمده که با دریافت گواهینامه +Network مرتبط است:

اثبات موفقیت حرفه‌ای: متخصصان شبکه در جمع‌آوری گواهینامه‌های بیشتر نسبت به هم‌تایان خود در رقابت هستند. از آنجایی که گواهینامه +Network به طور گسترده تمام حوزه شبکه را پوشش می‌دهد، تکنسین‌ها این گواهینامه را بسیار بیشتر از گواهینامه‌های میکروسافت قبول دارند (+Network بسیار معتبرتر و ارزشمندتر است). از آنجایی که به ندرت می‌توان با تلاش اندک چیزی به دست آورد که ارزش زیادی داشته باشد، صادقانه می‌گوییم آماده شدن برای آزمون +Network دقیقاً مانند روزی توام با بی‌حالی در ساحل نیست. (با این حال، سواحل واقعاً در لیست شخصی من از مکان‌های عالی برای مطالعه قرار دارند!) افرادی که در حوزه IT هستند می‌دانند که قبولی در آزمون +Network کار آسانی نیست، بنابراین قطعاً به شما احترام بیشتری می‌گذارند و می‌دانند که شما به سطح مشخصی از تخصص در مورد موضوعات مرتبط با شبکه و مستقل از فروشنده دست یافته‌اید.

فرصتی برای پیشرفت: همه ما دوست داریم در شغل خود پیشرفت کنیم که مسئولیت و اعتبار بیشتری را به همراه دارد و این معمولاً به معنای حقوق بیشتر، فرصت‌های بیشتر و گزینه‌های اضافی است. در حوزه فناوری اطلاعات، یک راه عالی برای اطمینان از اینکه اتفاق‌های خوبی می‌افتد، کسب گواهینامه‌های فناوری زیاد از جمله +Network است.

¹ Computing Technology Industry Association

² Open Systems Interconnection

برآورده کردن نیازهای آموزشی: Network+ به دلیل پشتیبانی گسترده در صنعت، به عنوان پایه اطلاعات شبکه شناخته می‌شود. در واقع برخی از شرکت‌ها داشتن گواهینامه Network+ را به عنوان یک شرط شغلی قبل از اینکه حتی به فکر استخدام شما باشند، مشخص می‌کنند، یا ممکن است به عنوان هدفی مشخص شود که باید پیش از بررسی شغلی بعدی شما محقق شود.

اعتماد مشتری: همانطور که شرکت‌ها مزیت CompTIA را کشف می‌کنند، بدون شک برای دستیابی به این گواهینامه‌ها به کارکنان واجد شرایط نیاز دارند. بسیاری از شرکت‌ها کار خود را به شرکت‌های مشاوره با تجربه کار با امنیت می‌سپارند. شرکت‌هایی که دارای کارکنان دارای گواهینامه هستند، نسبت به شرکت‌هایی که کارکنان بدون گواهینامه دارند، برتری قطعی دارند.

نحوه دریافت گواهینامه Network+

حین انتشار این کتاب، Pearson VUE تنها ارائه‌دهنده آزمون Network+ است. در اینجا اطلاعات تماس و مشخصات لازم ویژه آزمون جهت ثبت نام آمده است. قیمت آزمون ممکن است با توجه به کشور یا عضویت CompTIA متفاوت باشد.

فروشنده: Pearson VUE

وب سایت: www.pearsonvue.com/comptia

شماره تلفن (آمریکا و کانادا): 877-551-PLUS (7587)

وقتی برای آزمون برنامه‌ریزی می‌کنید، دستورالعمل‌های مربوط به وقت ملاقات و انصراف، شناسایی الزامات و اطلاعات مربوط به محل مرکز آزمون را دریافت خواهید کرد. علاوه بر این، یک نامه تأیید ثبت نام و پرداخت دریافت خواهید کرد. آزمون‌ها می‌توانند تا شش هفته یا در روز بعد (یا در برخی موارد حتی در همان روز) برنامه‌ریزی شوند.

توجه: قیمت‌ها و کدهای آزمون ممکن است بر اساس کشوری که آزمون در آن برگزار می‌شود متفاوت باشد. برای اطلاع از قیمت دقیق و مراحل ثبت نام آزمون، به وب سایت CompTIA (www.comptia.org) مراجعه کنید.

پس از اینکه آزمون Network+ خود را با موفقیت گذرانید، CompTIA به شما گواهینامه می‌دهد. در عرض چهار تا شش هفته پس از قبولی در آزمون، گواهینامه رسمی Network+ CompTIA و کارت شناسایی خود را دریافت خواهید کرد. (اگر این موارد را ظرف هشت هفته پس از انجام آزمون دریافت نکردید، مستقیماً با استفاده از اطلاعات موجود در بسته ثبت نام خود با CompTIA تماس بگیرید.)

نکاتی برای شرکت در آزمون Network+

در اینجا چند نکته کلی برای شرکت و موفقیت در آزمون آورده شده است:

- دو فرم شناسایی همراه خود داشته باشید. یکی باید کارت شناسایی عکس دار باشد، مانند گواهینامه رانندگی، دیگری می تواند کارت اعتباری اصلی یا پاسپورت باشد. هر دو فرم باید دارای امضاء باشند.
- زودتر در مرکز آزمون حاضر شوید تا بتوانید استراحت کنید و مطالب درسی خود، به ویژه جدول ها و لیست های اطلاعات مربوط به آزمون را مرور کنید. پس از آماده شدن برای ورود به اتاق آزمون، باید همه چیز را بیرون بگذارید. شما نمی توانید هیچ وسیله ای را به محل آزمون بیاورید.
- سؤالات را با دقت بخوانید. وسوسه نشوید که زود به نتیجه برسید. مطمئن شوید که دقیقاً می دانید هر سؤال چه چیزی می پرسد.
- هیچ سؤالی را بی پاسخ نگذارید. سؤالات بی پاسخ امتیاز منفی دارند. سؤالاتی با چندین پاسخ صحیح وجود خواهد داشت. هنگامی که بیش از یک پاسخ صحیح وجود دارد، یک پیام در پایین صفحه از شما می خواهد که "دو مورد را انتخاب کنید" یا "همه مواردی که اعمال می شود را انتخاب کنید". حتماً پیام های نمایش داده شده را بخوانید تا بدانید چه تعداد پاسخ صحیح را باید انتخاب کنید.
- هنگام پاسخ دادن به سؤالات چند گزینه ای که در مورد آنها مطمئن نیستید، از فرآیند حذف کردن استفاده کنید تا ابتدا از شر پاسخ هایی که آشکارا نادرست هستند خلاص شوید. اگر نیاز به حدس زدن دارید، انجام این کار شانس شما را بهبود می بخشد.
- در آزمون های مبتنی بر فرم (غیر انطباقی)، چون سؤالات سخت بیشترین زمان را خواهند گرفت، آنها را برای آخر نگه دارید. می توانید در طول آزمون به جلو و عقب بروید.

چه کسی باید این کتاب را بخواند؟

شما! اگر می خواهید در آزمون Network+ قبول شوید و آن را با اطمینان پشت سر بگذارید! این کتاب مملو از اطلاعات دقیقی است که نیاز دارید و مستقیماً اهداف آزمون Network+ را ترسیم می کند، بنابراین اگر از آن برای مطالعه در آزمون استفاده کنید، احتمال موفقیت شما افزایش می یابد.

علاوه بر گنجاندن هر ذره دانشی که برای گذراندن آزمون نیاز دارید، نکات بسیار عالی و محکمی برای مجهز کردن شما برای موفقیت در دنیای واقعی فناوری اطلاعات ارائه کرده ایم.

این کتاب چه چیزی را پوشش می‌دهد؟

این کتاب همه چیزهایی را که برای قبولی در آزمون CompTIA Network+ باید بدانید را پوشش می‌دهد. اما علاوه بر مطالعه کتاب، اگر می‌توانید، ایده خوبی است که در واقعیت در حوزه شبکه تمرین کنید.

در اینجا لیستی از ۲۱ فصل این کتاب آمده است:

فصل ۱، "مقدمه‌ای بر شبکه‌ها": این فصل شامل مقدمه‌ای بر شبکه‌ها و مروری بر رایج‌ترین توپولوژی‌های فیزیکی شبکه در شبکه‌های امروزی است.

فصل ۲، "مدل مرجع اتصال سامانه‌های باز (OSI)": این فصل مدل OSI، چپستی آن، آنچه در هر یک از لایه‌های آن اتفاق می‌افتد و نحوه عملکرد هر لایه را پوشش می‌دهد.

فصل ۳، "کانکتورهای شبکه و استانداردهای سیم‌کشی": این فصل رسانه‌ها و توپولوژی‌های مختلف شبکه، به علاوه انواع و ویژگی‌های کابل مورد استفاده در شبکه‌های امروزی را پوشش می‌دهد.

فصل ۴، "مشخصات اترنت فعلی": این فصل نحوه عملکرد یک شبکه اترنت پایه را پوشش می‌دهد و مشخصات مختلف اترنت را توصیف و دسته‌بندی می‌کند.

فصل ۵، "دستگاه‌های شبکه": شما باید تمام دستگاه‌های مختلف مورد استفاده در شبکه‌های امروزی را بشناسید. این فصل نحوه عملکرد هاب‌ها، روترها، و سوئیچ‌ها و برخی دستگاه‌های دیگر در یک شبکه را شرح می‌دهد.

فصل ۶، "مقدمه‌ای بر پروتکل اینترنت": این مقدمه برای پشته پروتکل IP بسیار مهم است.

فصل ۷، "آدرس دهی IP": این فصل پس از پایان فصل ۶، ادامه خواهد یافت و به آدرس دهی IP منتقل می‌شود. همچنین حاوی اطلاعاتی در مورد آدرس دهی عمومی در مقابل خصوصی و DHCP است.

فصل ۸، "زیر شبکه IP، عیب‌یابی IP، و مقدمه‌ای بر NAT": پس از پایان فصل ۷ شروع می‌شود، در این فصل به زیرشبکه IP می‌پردازیم. اما جای نگرانی نیست (سخت تلاش کرده‌ایم تا این موضوع نه چندان محبوب و در عین حال حیاتی را تا حد امکان آسان کنیم).

فصل ۹، "مقدمه‌ای بر مسیریابی IP": این مقدمه اساساً برای مسیریابی آنچه روترها انجام می‌دهند و چگونگی انجام آنرا پوشش می‌دهد. این فصل، همراه با فصل‌های ۱۰ و ۱۱، مسیریابی و سوئیچینگ را با جزئیات بسیار بیشتر از آنچه برای دستیابی به اهداف CompTIA Network+ لازم است پوشش می‌دهد، زیرا درک این دانش هنگام کار با شبکه‌های امروزی بسیار حیاتی است.

فصل ۱۰، "پروتکل‌های مسیریابی": این فصل پروتکل‌هایی را که روی روترها اجرا می‌شوند و نحوه به‌روزرسانی جدول‌های مسیریابی برای ایجاد یک نقشه شبکه کارآمد را شرح می‌دهد.

فصل ۱۱، "سوئیچینگ و شبکه‌های محلی مجازی": این فصل سوئیچینگ در لایه ۲، پروتکل درخت پوشا (STP) و شبکه‌های محلی مجازی (vLANS) را پوشش می‌دهد. با فصل‌های مسیریابی، بیشتر از آنچه برای آزمون لازم است پیش رفتیم و سوئیچینگ و شبکه‌های محلی مجازی (که در شبکه‌های شرکتی امروزی نیز حیاتی هستند) را به طور کامل تر پوشش خواهیم داد.

فصل ۱۲، "شبکه بی‌سیم": از آنجایی که وایرلس امروزه برای شبکه‌های خانگی و تجاری بسیار ضروری است، در این فصل تمام اطلاعاتی که برای موفقیت در شبکه‌های بی‌سیم در خانه و محل کار نیاز دارید بارگذاری شده است.

فصل ۱۳، "دسترسی به شبکه از راه دور": در این فصل، با اهمیت فراهم کردن تحمل خطا و نیز دسترسی‌پذیری سطح بالا آشنا خواهید شد. همچنین با معماری VPN آشنا خواهید شد که عبارتند از: VPN‌های سایت به سایت، VPN‌های کلاینت به سایت، VPN‌های بدون کلاینت، تونل تقسیم در مقابل VPN کامل، و VPN‌های SSH.

فصل ۱۴، "استفاده از آمار و حسگرها برای اطمینان از در دسترس بودن شبکه": در این فصل، نوع داده‌هایی را که باید نظارت کنید و برخی از راه‌های انجام این کار را خواهید آموخت.

فصل ۱۵، "اسناد و خط مشی‌های سازمانی": در این فصل، خواهید آموخت که برنامه‌ها و رویه‌ها باید برای مدیریت مسائل عملیاتی مانند مدیریت تغییر، واکنش به حادثه، بازیابی فاجعه، تداوم کسب‌وکار و چرخه حیات سیستم، توسعه داده شوند. همچنین رویه‌های عملیاتی استاندارد را که باید برای هدایت هر یک از این فرآیندها ایجاد شوند، خواهید آموخت.

فصل ۱۶، "دسترسی سطح بالا و بازیابی حادثه": در این فصل، با مفاهیم افزونگی، تحمل خطا و فرآیند بازیابی حادثه آشنا خواهید شد.

فصل ۱۷، "معماری دیتاستر و مفاهیم ابری": در این فصل، در مورد جنبه‌های مستندسازی مدیریت شبکه صحبت خواهیم کرد. این فصل به طور منطقی به بحث در مورد نمودارهای فیزیکی و شماتیک‌ها و همچنین به مستندات مدیریت پیکربندی می‌پردازد. در مورد اهمیت این نمودارها، اشکال ساده تا پیچیده‌ای که می‌توانند داشته باشند و ابزارهای مورد استفاده برای ایجاد آنها (از مداد و کاغذ گرفته تا شماتیک‌های اتوکد با فناوری پیشرفته)، آشنا خواهید شد. همچنین چیزهای زیادی در مورد ایجاد و عملکرد خطوط مبنا خواهید یافت.

فصل ۱۸، "روش عیب‌یابی شبکه": در این فصل، در مورد همه موارد عیب‌یابی، مانند نحوه ردیابی و حل بسیاری از مشکلات شبکه، آشنا خواهید شد.

فصل ۱۹، "ابزارها و فرمان‌های نرم‌افزار شبکه": این فصل ابزارهای شبکه‌ای را که برای کمک به اجرای شبکه‌های خود استفاده خواهید کرد، معرفی می‌کند. کارهای تخصصی نیاز به ابزارهای تخصصی دارند و نصب اجزای شبکه نیز از این قاعده مستثنی نیست. ما هر روز از برخی از این ابزارها مانند اسکنرهای شبکه استفاده می‌کنیم.

فصل ۲۰، "مفاهیم امنیت شبکه": در این فصل، مفاهیم اساسی، اصطلاحات و اصولی را که همه متخصصان شبکه باید برای ایمن‌سازی شبکه سازمانی بدانند، خواهید آموخت.

فصل ۲۱، "انواع رایج حملات": در این فصل انواع رایج حملات را که همه متخصصان شبکه باید برای ایمن‌سازی شبکه سازمانی بدانند، خواهید آموخت.

آنچه در این کتاب گنجانده شده است

در سراسر کتاب چندین ابزار مطالعه را گنجانده‌ایم:

آزمون ارزیابی: در پایان این مقدمه یک آزمون سنجش وجود دارد که می‌توانید از آن برای بررسی آمادگی خود برای آزمون استفاده کنید. پیش از خواندن کتاب این تست را انجام دهید. این کار به شما کمک می‌کند تا بخش‌هایی را که ممکن است نیاز به تجدید معلومات خود داشته باشید، تعیین کنید. پاسخ سؤالات آزمون سنجش در صفحه‌ای جداگانه پس از آخرین سؤال آزمون قرار می‌گیرد. هر پاسخ شامل توضیح کاملی می‌باشد.

نقشه هدف و فهرست آغازین اهداف: در بخش‌های بعد این مقدمه یک نقشه هدف ارائه شده است که به شما نشان می‌دهد هر هدف برای امتحان در کجای این کتاب پوشش داده شده است. افزون بر این، هر فصل با فهرستی از اهداف امتحانی خود شروع می‌شود. از اینها برای مشاهده دقیق محل پوشش هر یک از مباحث امتحانی استفاده کنید.

الزامات امتحان: هر فصل شامل چندین مورد ضروری امتحان است. اینها موضوعات کلیدی هستند که باید از فصل مربوط به بخش‌هایی که هنگام آماده شدن برای امتحان روی آنها تمرکز کنید، استفاده کنید.

آزمایشگاه نوشتاری: هر فصل شامل یک آزمایشگاه نوشتاری است. اینها تمرینات کوتاهی هستند که با اهداف امتحانی هماهنگ است. پاسخ به این موارد را می‌توان در پیوست الف یافت.

بررسی سؤالات فصل: برای آزمایش دانش خود در حین پیشروی در کتاب، بررسی سؤالات در پایان هر فصل قرار دارند. همانطور که هر فصل را تمام می‌کنید، به بررسی سؤالات پاسخ دهید و سپس پاسخ‌های خود را بررسی کنید (پاسخ‌ها و توضیحات صحیح در پیوست ب آمده است). می‌توانید هر بخشی را با سؤالی که اشتباه کرده‌اید، بازخوانی کنید تا مطمئن شوید که دفعه بعد که مطالب را خواندید، به درستی پاسخ دهید.

محیط یادگیری آنلاین تعاملی و بانک نمونه سؤالات

محیط یادگیری آنلاین تعاملی همراه با CompTIA Network+ Study Guide: Exam N10-009 ویرایش ششم یک بانک نمونه سؤالات با ابزارهای مطالعه را فراهم می‌کند تا به شما کمک کند برای امتحان این گواهینامه آماده شوید و شانس خود را برای قبولی در اولین بار افزایش دهید! بانک نمونه سؤالات شامل ابزارهای زیر است:

نمونه سؤالات: تمام سؤالات این کتاب، از جمله آزمون سنجش که در پایان این مقدمه خواهید یافت و تست‌های فصل که شامل بررسی سؤالات در پایان هر فصل می‌شود ارائه شده است. علاوه بر این، دو آزمون عملی وجود دارد. از این سؤالات برای آزمایش دانش خود در مورد مطالب راهنمای مطالعه استفاده کنید. بانک نمونه سؤالات آنلاین بر روی چندین دستگاه اجرا می‌شود.

فلش کارت: تقریباً ۲۰۰ سؤال در فرمت فلش کارت دیجیتال ارائه شده است (یک سؤال و پاسخ صحیح آن). می‌توانید از فلش کارت‌ها برای تقویت یادگیری خود استفاده کنید و پیش از امتحان آمادگی تست لحظه آخری را انجام دهید.

واژه نامه: واژه نامه‌ای از اصطلاحات کلیدی این کتاب و تعاریف آنها به صورت PDF قابل جستجو در سایت انتشارات پندارپارس قابل دسترس است.

توجه: برای ثبت نام و دسترسی به این محیط یادگیری آنلاین تعاملی و بانک نمونه سؤالات با ابزارهای مطالعه، به www.wiley.com/go/netplustestprep بروید.

توجه: مانند همه امتحانات، گواهینامه +CompTIA Network به طور دوره‌ای به‌روز می‌شود و ممکن است در نهایت از دور خارج شده یا جایگزین شود. در مقطعی پس از اینکه CompTIA دیگر این آزمون را ارائه ندهد، نسخه‌های قدیمی کتاب‌ها و ابزارهای آنلاین ما از رده خارج می‌شوند. اگر این کتاب را پس از از رده خارج شدن آزمون خریداری کرده‌اید یا می‌خواهید پس از آن آزمون، در محیط یادگیری آنلاین Sybex ثبت‌نام کنید، لطفاً بدانید که پس از در دسترس نبودن آزمون، ما هیچ تضمینی نمی‌دهیم که ابزارهای آنلاین Sybex این آزمون در دسترس باشد.

نحوه استفاده از این کتاب

اگر می‌خواهید برای آزمون +Network تلاشی جدی کرده و آماده شوید، دیگر به دنبال آن نباشید، زیرا ما ساعت‌های بی‌شماری را صرف جمع‌آوری این کتاب کرده‌ایم تا به شما کمک کنیم در آن موفق شوید!

این کتاب مملو از اطلاعات ارزشمند است و اگر درک کنید که چگونه کتاب را کنار هم قرار داده‌ایم، بیشترین استفاده را از زمان مطالعه خود خواهید برد. در اینجا لیستی وجود دارد که نحوه مطالعه را شرح می‌دهد:

(۱) بلافاصله پس از این مقدمه در آزمون ارزیابی شرکت کنید. (پاسخ‌ها در پایان آزمون هستند، اما به آنها نگاه نکنید!) اگر هیچ یک از پاسخ‌ها را نمی‌دانید اشکالی ندارد. این کتاب برای همین است. توضیح هر پاسخ اشتباه را با دقت بخوانید و فصلی را که در آن مطالب پوشش داده شده است را یادداشت کنید.

۲) هر فصل را با دقت مطالعه کنید و مطمئن شوید که اطلاعات و اهداف امتحانی که در ابتدای هر فصل ذکر شده است را کاملاً درک کرده‌اید. دوباره به فصلی که سؤالات آزمون ارزیابی‌اش را از دست داده‌اید، توجه ویژه‌ای داشته باشید.

۳) آزمایشگاه نوشتاری در پایان هر فصل را کامل کنید. این تمرین‌های نوشتاری را نادیده نگیرید، زیرا آنها مستقیماً اهداف CompTIA و آنچه که برای رسیدن به آنها نیاز دارید را نشان می‌دهند.

۴) به تمام بررسی سؤالات مربوط به هر فصل پاسخ دهید. به طور خاص هر سؤالی که شما را گیج می‌کند یادداشت کنید و بخش‌های مربوطه کتاب را دوباره مطالعه کنید و از این سؤالات عبور نکنید. مطمئن شوید که هر پاسخ را کاملاً درک کرده‌اید.

۵) توانایی خود را در امتحانات تمرینی محک بزنید. پیش از شرکت در آزمون، حتماً از وب سایت ما برای سؤالات، ویدیوها، فایل‌های صوتی و سایر اطلاعات مفید دیدن کنید.

۶) خود را با استفاده از تمام فلش کارت‌های الکترونیکی آزمایش کنید. این یک برنامه فلش کارت کاملاً جدید و به‌روز است که به شما کمک می‌کند برای آخرین امتحان CompTIA Network+ آماده شوید و یک ابزار مطالعه واقعاً عالی است.

ما با شما صادق هستیم! یادگیری تک تک مطالب این کتاب مستلزم آن است که خودتان را با معیارهای خوبی از نظم و انضباط به کار بگیرید. بنابراین سعی کنید هر روز یک بازه زمانی یکسان را برای مطالعه در نظر بگیرید و مکانی راحت و آرام را برای این کار انتخاب کنید. اگر سخت کار کنید، از سرعت یادگیری این مطالب شگفت‌زده خواهید شد.

اگر مراحل ذکر شده در اینجا را دنبال کنید و با بررسی سؤالات، امتحانات تمرینی، فلش کارت‌های الکترونیکی و تمام آزمایشگاه‌های نوشتاری را مطالعه کنید، مردود شدن در آزمون CompTIA Network+ کار سختی خواهد بود. با این حال، مطالعه برای آزمون Network+ مانند آموزش برای یک ماراتن است. اگر هر روز برای دوییدن خوب تمرین نکنید، احتمالاً خیلی خوب به پایان نخواهید رسید.

اهداف امتحان N10-009

در مورد اهداف صحبت می‌کنیم، احتمالاً در مورد آنها بسیار کنجکاو هستید، درست است؟ CompTIA از گروه‌هایی از متخصصان فناوری اطلاعات خواست تا مهارت‌هایی را که احساس می‌کنند در شغل‌شان مهم است، رتبه‌بندی کنند و نتایج در اهداف امتحان گروه‌بندی و به پنج حوزه تقسیم شدند.

این جدول میزانی را بر حسب درصد به شما نشان می‌دهد که هر دامنه در بررسی واقعی نشان داده شده است.

هدف	درصد امتحان
مفاهیم شبکه	۲۳٪
پیاده سازی شبکه	۲۰٪
عملیات شبکه	۱۹٪
امنیت شبکه	۱۴٪
عیب یابی شبکه	۲۴٪

نقشه هدف

جدول زیر نشان می‌دهد که هر هدف در کدام بخش کتاب پوشش داده شده است.

شماره هدف	هدف	فصل
۱.۰	مفاهیم شبکه	
۱.۱	مفاهیم مربوط به مدل مرجع اتصال سامانه‌های باز (OSI).	فصل ۲، فصل ۶
۱.۲	مقایسه لوازم شبکه، برنامه‌های کاربردی و توابع.	فصل ۱۰
۱.۳	مفاهیم ابری و گزینه‌های اتصال.	فصل ۱۷
۱.۴	پورت‌های رایج شبکه، پروتکل‌ها، سرویس‌ها و انواع ترافیک.	فصل ۶، فصل ۸
۱.۵	مقایسه رسانه‌های انتقال و فرستنده و گیرنده.	فصل ۳، فصل ۴، فصل ۱۲
۱.۶	مقایسه توپولوژی‌ها، معماری‌ها و انواع شبکه.	فصل ۱
۱.۷	استفاده از آدرس‌دهی شبکه IPv4 مناسب با توجه به یک سناریو.	فصل ۷، فصل ۸
۱.۸	مورد کاربردی (Use case) درحال تکامل برای محیط‌های شبکه مدرن.	فصل ۷، فصل ۱۰، فصل ۱۷
۲.۰	پیاده سازی شبکه	
۲.۱	ویژگی‌های فناوری‌های مسیریابی.	فصل ۸، فصل ۹، فصل ۱۰
۲.۲	فناوری‌ها و ویژگی‌های سوئیچینگ با توجه به یک سناریو.	فصل ۱۱

شماره هدف	هدف	فصل
۲.۳	انتخاب پیکربندی دستگاه‌ها و فناوری‌های بی‌سیم با توجه به یک سناریو.	فصل ۵، فصل ۱۲
۲.۴	عوامل مهم تأسیسات فیزیکی.	فصل ۱۶
۳.۰	عملیات شبکه	
۳.۱	هدف فرآیندها و رویه‌های سازمانی را توضیح دهید.	فصل ۱۵
۳.۲	استفاده از فناوری‌های نظارت شبکه با توجه به یک سناریو.	فصل ۱۴
۳.۳	مفاهیم بازیابی از حادثه (DR) را توضیح دهید.	فصل ۱۶
۳.۴	با توجه به یک سناریو، سرویس شبکه IPv4 و IPv6 را پیاده‌سازی کنید.	فصل ۵، فصل ۷
۳.۵	مقایسه روش‌های مدیریت و دسترسی به شبکه.	فصل ۱۳
۴.۰	امنیت شبکه	
۴.۱	اهمیت مفاهیم مبنای امنیت شبکه را توضیح دهید.	فصل ۲۰، فصل ۲۱
۴.۲	انواع مختلف حملات و تأثیر آنها بر شبکه.	فصل ۲۱
۴.۳	با توجه به یک سناریو، ویژگی‌های امنیتی شبکه، تکنیک‌های دفاعی و راه حل‌ها را اعمال کنید.	فصل ۲۱
۵.۰	عیب‌یابی شبکه	
۵.۱	روش عیب‌یابی را توضیح دهید.	فصل ۱۸
۵.۲	با توجه به یک سناریو، مشکلات رایج کابل‌کشی و اینترفیس فیزیکی را عیب‌یابی کنید.	فصل ۳، فصل ۱۸
۵.۳	با توجه به یک سناریو، مشکلات رایج سرویس شبکه را عیب‌یابی کنید.	فصل ۱۱، فصل ۱۸
۵.۴	با توجه به یک سناریو، مشکلات رایج عملکرد را عیب‌یابی کنید.	فصل ۱۱، فصل ۱۸

شماره هدف	هدف	فصل
۵.۵	با توجه به یک سناریو، از ابزار یا پروتکل مناسب برای حل مشکلات شبکه استفاده کنید.	فصل ۱۹

نحوه تماس با ناشر

اگر فکر می‌کنید اشتباهی در این کتاب پیدا کرده‌اید، لطفاً آن را به ما اطلاع دهید. در John Wiley & Sons ما می‌دانیم که ارائه محتوای دقیق به مشتریانمان چقدر مهم است، اما با وجود تلاش زیاد ممکن است خطایی رخ دهد.

برای ارسال اشتباه احتمالی پیش آمده، لطفاً آن را با عنوان "ارسال اشتباه احتمالی کتاب" به تیم سرویس مشتری ما به آدرس wileysupport@wiley.com ایمیل کنید.

آزمون ارزیابی

(۱) کدام معماری شبکه یک روش دسترسی دقیق را برای هاست‌های مختلف تعریف می‌کند؟

(۱) همتا به همتا

(۲) کلاینت سرور

(۳) LAN

(۴) توپولوژی ترکیبی

(۲) برای اتصال دو مکان اداری باید یک توپولوژی را انتخاب کنید و انتظار ندارید در آینده مکان‌هایی را اضافه کنید. کدام توپولوژی را باید انتخاب کنید؟

(۱) نقطه به نقطه

(۲) نقطه به چند نقطه

(۳) حلقه‌ای

(۴) باس

(۳) کدام پروتکل واحد داده (PDU) برای توصیف نوع داده‌ای که در لایه نمایش منتقل می‌شود، استفاده می‌شود؟

(۱) بیت‌ها

- (۲) دیتاگرام‌های کاربر
- (۳) فریم‌ها
- (۴) قطعه‌ها
- (۴) کدام لایه وظیفه رمزگذاری و رمزگشایی را بر عهده دارد؟
- (۱) لایه اپلیکیشن
- (۲) لایه فیزیکی
- (۳) لایه جلسه
- (۴) لایه نمایش یا ارائه
- (۵) اگر بخواهید کابل UTP را با سرعت ۱۰ گیگابیت بر ثانیه با فاصله ۴۰ متر اجرا کنید، از کدام دسته‌بندی کابل باید استفاده کنید؟
- (۱) دسته ۵
- (۲) دسته 5e
- (۳) دسته ۶
- (۴) دسته ۳
- (۶) کدام عبارت، مسیر سیگنال‌دهی در کابل شبکه را توصیف می‌کند؟
- (۱) تضعیف (Attenuation)
- (۲) دوبلکس (Duplex)
- (۳) علامت‌گذاری (Demarcation)
- (۴) EMI
- (۷) با یک پیمانکار کار می‌کنید؛ آنها در حال کشیدن و تکمیل خطوط فیبر نوری هستند. خطوط فیبر نوری در مرکز خط تولید شما قرار خواهد گرفت. کدام انتهای کابل را توصیه می‌کنید که احتمال شل شدن کابل‌ها در اثر لرزش در کف تولیدی را کاهش دهد؟
- (۱) کانکتورهای SC
- (۲) کانکتورهای ST

- ۳ کانکتورهای LC
- ۴ کانکتورهای MTRJ
- ۸ کدام یک از گزینه‌های زیر دلیل رایج برای ازدحام LAN نیست؟
- ۱) برودکست^۱
 - ۲) مولتی کست^۲
 - ۳) اضافه کردن سوئیچ برای اتصال
 - ۴) هاب‌های متعدد برای اتصال
- ۹ رایانه دریافت‌کننده، یک فریم Checksum را بررسی کرد. در حین انتقال آسیب دیده بود، بنابراین باید دور انداخته شود. در کدام لایه از OSI این اتفاق افتاده است؟
- ۱) لایه فیزیکی
 - ۲) لایه پیوند داده
 - ۳) لایه شبکه
 - ۴) لایه جلسه
- ۱۰ دلیل اینکه یک مدیر شبکه، شبکه را با یک سوئیچ بخش‌بندی می‌کند چیست؟
- ۱) ایجاد دامنه‌های برودکست بیشتر
 - ۲) ایجاد جداسازی از پیام‌های ARP
 - ۳) ایجاد دامنه‌های برخورد کمتر
 - ۴) جداسازی ترافیک بین قطعه‌ها
- ۱۱ بر اساس بهترین روش‌ها، محل قراردادن مناسب فایروال به چه صورت است؟
- ۱) فقط بین شبکه داخلی و اینترنت
 - ۲) در مرزهای امنیتی کلیدی
 - ۳) در DMZ

^۱ Broadcast

^۲ Multicast

۴) فقط بین DMZ و اینترنت

۱۲) روش مناقشه ۸۰۲.۱۱ شبکه بی سیم کدام است؟

(۱) CSMA/CA

(۲) CSMA/CD

(۳) DSSS

(۴) OFDM

۱۳) یک سرویس گیرنده DHCP از چه شکلی از ارتباط برای به دست آوردن یک آدرس IP در ابتدا استفاده می کند؟

(۱) لایه ۳ برودکست

(۲) لایه ۳ مولتی کست

(۳) لایه ۳ از 802.1Q

(۴) لایه ۳ یونیکست^۱

۱۴) کدام روش دسترسی مدیریت باید در دستگاه های شبکه برای رمزگذاری یک جلسه پیکربندی شود؟

(۱) RADIUS

(۲) HTTP

(۳) SSH

(۴) SFTP

۱۵) کدام پروتکل دسترسی از راه دور مایکروسافت اجازه می دهد تا درایوهای محلی به سیستم راه دور ارائه شوند؟

(۱) VNC

(۲) RDP

(۳) SSH

(۴) Telnet

۱۶) سیستم Syslog از کدام پروتکل و شماره پورت استفاده می کند؟

¹ Unicast

(۱) UDP/161

(۲) TCP/162

(۳) UDP/162

(۴) UDP/514

(۱۷) کدام یک از موارد زیر محدوده IP شبکه کلاس B است؟

(۱) ۱۲۶-۱

(۲) ۱۲۷-۱

(۳) ۱۹۱-۱۲۸

(۴) ۲۲۴-۱۹۲

(۱۸) کدام یک در مورد آدرس IP 135.20.255.255 درست است؟

(۱) یک آدرس کلاس A است.

(۲) آدرس پرودکست است.

(۳) آدرس Gateway پیش فرض است.

(۴) دارای ماسک پیش فرض ۲۵۵.۰.۰.۰ است.

(۱۹) دلیل اصلی استفاده از آدرس IP خصوصی چیست؟

(۱) اجازه می‌دهد تا آدرس‌های IP عمومی را حفظ کنید.

(۲) از آنجایی که آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند، ایمن هستند.

(۳) ارتباطات را خصوصی نگه می‌دارد.

(۴) راه‌اندازی آن آسان‌تر از آدرس‌های IP عمومی است.

(۲۰) هنگام استفاده از آدرس‌های IP خصوصی برای برقراری ارتباط با هاست اینترنت چه چیزی لازم است؟

(۱) روتر اینترنت

(۲) تونل IPv4

(۳) تونل VPN

(۴) ترجمه آدرس شبکه

(۲۱) کدام پروتکل مسیریابی یک پروتکل حالت پیوند^۱ واقعی است؟

- (۱) RIP
- (۲) OSPF
- (۳) RIPv2
- (۴) EIGRP

(۲۲) چرا در قسمت Age خروجی زیر خط تیره وجود دارد؟

```
Lab_A#sh ip arp
Protocol Address Age(min) Hardware Addr Type Interface
Internet 172.16.20.1 - 00d0.58ad.05f4 ARPA Ethernet1
Internet 172.16.20.2 3 0030.9492.a5dd ARPA Ethernet1
Internet 172.16.10.1 - 0015.0506.31b0 ARPA Ethernet0
```

- (۱) ورودی ARP کهنه است.
- (۲) ورودی ARP نامعتبر است.
- (۳) اینترفیس‌های فیزیکی هستند.
- (۴) اینترفیس‌های مجازی وجود دارد.

(۲۳) تعریف مسیر AD چیست؟

- (۱) AD معیاری است که پروتکل‌های مسیریابی از آن برای انتخاب بهترین مسیر استفاده می‌کنند.
- (۲) AD مقداری است که توسط مدیران شبکه برای انتخاب مسیر اختصاص داده شده است.
- (۳) AD رتبه‌بندی اعتماد زمانی است که چندین مسیر به یک مقصد وجود داشته باشد.
- (۴) AD مقداری است که با هزینه رسیدن به مقصد مرتبط است.

(۲۴) فرض کنید یک مسیر نمایش آی پی روی روتر انجام می‌دهید و چندین مسیر را با AD 90 می‌بینید. کدام پروتکل مسیریابی این فرمان‌های مسیر را ایجاد کرده است؟

- (۱) IGRP
- (۲) OSPF
- (۳) EIGRP
- (۴) RIP

¹ Link State

۲۵) کدام پروتکل مسیریابی از معیارهای بردار مسیر (Path-Vector) استفاده می‌کند؟

BGP (۱)

RIP (۲)

OSPF (۳)

EIGRP (۴)

۲۶) کدام پروتکل جایگزین ARP در IPv6 می‌شود؟

NDP (۱)

ARIPv6 (۲)

GRE (۳)

RA (۴)

۲۷) کدام حالت VTP اجازه نمی‌دهد سوئیچ در ترافیک VTP شرکت کند اما ترافیک VTP را ارسال می‌کند؟

حالت سرور (۱)

حالت شفاف (Transparent) (۲)

حالت پراکسی (۳)

حالت کلاینت (۴)

۲۸) کدام پروتکل از پروتکل اختصاصی سیسکو برای سوئیچ‌های ترانک استفاده می‌شود؟

ISL (۱)

802.1Q (۲)

VTP (۳)

CDP (۴)

۲۹) کدام فناوری بر اساس احراز هویت، به شبکه، دسترسی انتخابی می‌دهد؟

802.1Q (۱)

ACL (۲)

802.1X (۳)

فایروال (۴)

۳۰) چند کانال غیر همپوشانی با 802.11a موجود است؟

(۱) ۳

(۲) ۱۲

(۳) ۲۳

(۴) ۴۰

(۳۱) حداکثر نرخ داده برای استاندارد 802.11a چقدر است؟

(۱) ۶ مگابیت بر ثانیه

(۲) ۱۱ مگابیت بر ثانیه

(۳) ۲۲ مگابیت بر ثانیه

(۴) ۵۴ مگابیت بر ثانیه

(۳۲) مزایای VPN های سایت به سایت IPsec چیست؟

(۱) نیاز به پهنای باند کمتر

(۲) تأخیر کمتر

(۳) مقیاس پذیری

(۴) پشتیبانی از مولتی کست

(۳۳) برای اتصال به پورت سریال روتر از چه کابلی باید استفاده کرد؟

(۱) Cat 5e

(۲) کابل رول شده

(۳) PuTTY کابل

(۴) SMF

(۳۴) چه نوع پیام SNMP از NMS برای درخواست اطلاعات به عامل ارسال می شود؟

(۱) پیام Get-request

(۲) پیام Get-response

(۳) پیام Set-request

(۴) پیام Trap

۳۵) چه پروتکلی اطلاعات دقیقی در مورد جریان ترافیک بین نقاط پایانی ارائه می‌دهد؟

(۱) Syslog

(۲) SNMP

(۳) NetFlow

(۴) SPAN

۳۶) با یک ارائه دهنده سرویس جدید قرارداد بسته‌اید و در حال بررسی قرارداد سطح سرویس آنها (SLA) هستید. SLA بیان می‌کند که تعهد آنها به زمان کار ۹۹٪ است. زمان توقف مورد انتظار در سال چقدر است؟

(۱) ۳.۶۵ روز

(۲) ۸.۷۶ ساعت

(۳) ۵۲.۵۶ دقیقه

(۴) ۵.۲۹ دقیقه

۳۷) آیا باید مطمئن شوید که کاربران زمانی که رمز عبور آنها منقضی می‌شود و مجبور به تغییر آن هستند، از رمزهای عبور مجدد استفاده نمی‌کنند؟ در کدام یک از موارد زیر نیاز به تغییر دارید؟

(۱) BYOD

(۲) خط‌مشی رمز عبور

(۳) DLP

(۴) AUP

۳۸) کدام یک از موارد زیر معیاری است برای اینکه چقدر طول می‌کشد تا داده‌های شما قبل از حذف یا خرابی بازیابی شود؟

(۱) RTO

(۲) MTBF

(۳) RPO

(۴) MTTR

۳۹) بازیابی از نوار ۴ ساعت طول می‌کشد. این نمونه چیست؟

(۱) هدف نقطه بازیابی (RPO)

۲) هدف زمان بازیابی (RTO)

۳) چرخش GFS

۴) پنجره پشتیبان‌گیری

۴۰) کدام سرویس ابری برای توسعه نرم‌افزار استفاده می‌شود؟

۱) SaaS

۲) IaaS

۳) PaaS

۴) DRaaS

۴۱) پروتکل مسیریابی در کدام سطح شبکه اجرا می‌شود؟

۱) سطح داده

۲) سطح کنترل

۳) سطح مدیریت

۴) سطح مسیریابی

۴۲) پس از تأیید یک نظریه، مرحله بعدی در حل مسئله چیست؟

۱) یک فرضیه ایجاد کنید.

۲) چندین رویکرد را در نظر بگیرید.

۳) یک برنامه اقدام تنظیم کنید.

۴) با مشکلات متعدد به صورت جداگانه برخورد کنید.

۴۳) مرحله نهایی برای حل یک مشکل در روش عیب‌یابی چیست؟

۱) راه حلی را اجرا کنید.

۲) اعتبار یک نظریه.

۳) یک برنامه اقدام تنظیم کنید.

۴) سند.

۴۴) کدام ابزار نرم‌افزاری به شما اجازه می‌دهد تا بررسی کنید که آیا یک برنامه وب در حال اجرا بر روی سرور آنلاین است؟

(۱) ping

(۲) nslookup

(۳) Tracert/Traceroute

(۴) Port scanner

۴۵) برای بررسی حداکثر واحد انتقال پیکربندی شده (MTU) در اینترنتفیس یک هاست لینوکس، از کدام فرمان باید استفاده کرد؟

(۱) ipconfig

(۲) ifconfig

(۳) mtuconfig

(۴) iptables

۴۶) کدام ابزار اجازه می‌دهد تا در سطح بسته^۱ برای ترافیک مربوط به یک اپلیکیشن بررسی شود؟

(۱) آنالیزگر پروتکل

(۲) dig

(۳) اسپکتروم آنالایزر (Spectrum analyzer)

(۴) Nslookup

۴۷) کدام پروتکل، احراز هویت و حسابداری را در یک بسته TCP در پورت ۴۹ ترکیب می‌کند؟

(۱) TACACS+

(۲) RADIUS

(۳) TLS

(۴) LDAP

۴۸) کدام عامل احراز هویت، شما را ملزم به ارائه چیزی می‌کند که دارید؟

(۱) رمز عبور

(۲) امضاء

¹ Packet

۳) اثر انگشت

۴) توکن

۴۹) یک مدیر جوان با وحشت نزد شما می‌آید. پس از مشاهده فایل‌های گزارش، او متقاعد شده است که یک مهاجم تلاش می‌کند از یک آدرس IP قانونی برای ایجاد اختلال در دسترسی به نقاط دیگر شبکه استفاده کند. این کدام نوع حمله است؟

۱) جعل

۲) مهندسی اجتماعی

۳) کرم

۴) رمز عبور

۵۰) فرض کنید که مدیر یک شرکت بزرگ بطری‌سازی هستید. در پایان هر ماه، شما به طور معمول همه گزارش‌ها را مشاهده می‌کنید و به دنبال مغایرت می‌گردید. در این ماه، گزارش خطای سیستم ایمیل شما تعداد زیادی تلاش ناموفق برای ورود به سیستم را گزارش می‌دهد. واضح است که سرور ایمیل هدف قرار گرفته است. کدام نوع حمله به احتمال زیاد رخ می‌دهد؟

۱) بی رحمانه (Brute-force)

۲) درب پستی (Backdoor)

۳) کرم

۴) جعل IP

پاسخ آزمون سنجش

۱) گزینه ۲. معماری شبکه کلاینت-سرور به طور دقیق هاست‌ها را تعریف می‌کند. کلاینت‌ها به اطلاعات دسترسی دارند و سرورها اطلاعات را به اشتراک می‌گذارند. همتابه‌همتا (Peer-to-Peer) یک معماری شبکه است که به یک هاست اجازه می‌دهد تا هم به منابع یک شبکه دسترسی داشته باشد و هم آنرا به اشتراک بگذارد. شبکه محلی (LAN) یک نوع شبکه است و به اشتراک‌گذاری اطلاعات مربوط نمی‌شود. توپولوژی ترکیبی، توپولوژی را توصیف می‌کند که دو یا چند توپولوژی را در خود جای داده است.

۲) گزینه ۱. اتصال نقطه‌به‌نقطه معمولاً برای اتصال دو اداره استفاده می‌شود که در آن گسترش مکان‌ها نگران‌کننده نیست. اگر یک اداره نیاز به اتصال به چندین مکان اداری دیگر داشته باشد، باید توپولوژی

نقطه به چند نقطه انتخاب شود. حلقه و باس، توپولوژی هستند و برای توصیف روش‌های اتصال WAN استفاده نمی‌شوند.

۳) گزینه ۲. دیتاگرام‌های کاربر، پروتکل واحدهای داده (PDU) هستند که داده‌ها را در لایه نمایش توصیف می‌کنند. بیت‌ها، داده‌ها را در لایه فیزیکی توصیف می‌کنند. فریم‌ها داده‌ها را در لایه پیوند داده توصیف می‌کنند. قطعه‌ها داده‌ها را در لایه حمل توصیف می‌کنند.

۴) گزینه ۴. لایه نمایش، وظیفه رمزگذاری و رمزگشایی و همچنین فشرده‌سازی و رفع فشرده‌سازی را بر عهده دارد. لایه اپلیکیشن، مسئول دسترسی به اینترفیس برنامه‌نویسی کاربردی (API) و شروع فرآیند ارتباط شبکه است. لایه فیزیکی وظیفه انتقال داده‌ها از طریق نور، الکتریسیته و امواج هوا را بر عهده دارد. لایه جلسه، وظیفه تنظیم گفتگو بین دو هاست را بر عهده دارد.

۵) گزینه ۳. دسته ۶ قابلیت سرعت ۱۰ گیگابیت بر ثانیه تا حداکثر فاصله ۵۵ متری را دارد. دسته ۵، توانایی سرعت ۱۰۰ مگابیت بر ثانیه در فاصله ۱۰۰ متری را دارد. دسته 5e قادر به سرعت ۱ گیگابیت بر ثانیه در فاصله ۱۰۰ متری است. دسته ۳ تنها قادر به حداکثر سرعت ۱۰ مگابیت بر ثانیه است.

۶) گزینه ۲. Duplex به مسیر سیگنال‌دهی در کابل شبکه اشاره دارد. Attenuation، کاهش سیگنال با افزایش طول کابل است. Demarcation یا مرزبندی به نقطه مسئولیت یک ارائه دهنده شبکه اشاره دارد. تداخل الکترومغناطیسی (EMI) تداخلی است که از یک منبع خارجی به کابل شبکه القا می‌شود.

۷) گزینه ۲. کانکتور ST بهترین انتخاب برای نصب در نزدیکی منابع ارتعاش است. کانکتور SC یک کانکتور مربعی است که اغلب برای کابل چند حالت استفاده می‌شود. کانکتور ST دارای یک مهار فبری است که در برابر لرزش مقاومت می‌کند و به طور مثبت قفل می‌شود. اگرچه کانکتورهای LC و MTRJ دارای مکانیسم‌های مهارکننده هستند، ST دارای یک مهار فبری است تا از شل نشدن آن اطمینان حاصل کند.

۸) گزینه ۳. برودکست، مولتی‌کست و هاب‌های متعدد برای اتصال، همگی از علل شایع تراکم شبکه LAN هستند. افزودن سوئیچ برای اتصال، ارتباط مستقیمی با تراکم LAN ندارد، زیرا سوئیچ‌ها دامنه‌های برخورد ایجاد می‌کنند و پهنای باند مؤثر را افزایش می‌دهند.

۹) گزینه ۲. لایه پیوند داده، مسئول بررسی دنباله چک فریم (FCS) است که Checksum فریم است. لایه فیزیکی مسئول انتقال داده‌ها از طریق برق، نور یا هوا است. لایه شبکه مسئول آدرس‌دهی منطقی و مسیریابی داده‌ها است. لایه جلسه وظیفه کنترل گفتگو را بر عهده دارد.

۱۰) گزینه ۴. یک سوئیچ، تقسیم‌بندی میکرو ایجاد می‌کند که به نوبه خود ترافیک بین دو رایانه مکالمه را از رایانه‌های دیگری که بخشی از ارتباطات نیستند جدا می‌کند. این به نوبه خود پهنای باند را برای رایانه‌هایی

¹ Frame Check Sequence

که بخشی از ارتباطات بین مکالمه دو رایانه نیستند افزایش می‌دهد. ایجاد دامنه‌های برودکست تنها با افزودن VLAN و روتر امکان‌پذیر است. جداسازی پیام‌های پروتکل حل آدرس (ARP) تنها با ایجاد دامنه‌های برودکست امکان‌پذیر است. تقسیم‌بندی با سوئیچ، دامنه‌های برخورد بیشتری ایجاد می‌کند، نه دامنه‌های برخورد کمتر.

(۱۱) گزینه ۲. فایروال‌ها باید همیشه در مرزهای امنیتی کلیدی قرار گیرند که می‌تواند اینترنت و شبکه داخلی شما باشد. با این حال، قراردادن مناسب، منحصر به مرزهای اینترنت و شبکه‌های داخلی نیست. به عنوان مثال، می‌تواند بین دو شبکه داخلی مانند R&D و شبکه‌های مهمان قرار گیرد. شبکه منطقه غیرنظامی (DMZ^۱) که اکنون به عنوان یک زیرشبکه غربال شده نیز نامیده می‌شود، بخشی از فایروال است که در آن سرویس‌ها رو به روی اینترنت قرار می‌گیرند. فایروال‌ها معمولاً فقط بین DMZ و اینترنت قرار نمی‌گیرند زیرا اکثر شبکه‌ها دارای یک شبکه داخلی هستند.

(۱۲) گزینه ۱. ۸۰۲.۱۱ از روش مناقشه‌ای استفاده می‌کند که شامل دسترسی چندگانه با قابلیت شنود سیگنال حامل/پیشگیری از حادثه (CSMA/CA^۲) است. ۸۰۲.۱۱ سازوکار Request-to-Send/Clear-to-Send را پیاده‌سازی می‌کند که از برخورد جلوگیری می‌کند. اترنت از یک روش مناقشه‌ای استفاده می‌کند که تشخیص برخورد/دسترسی چندگانه (CSMA/CD^۳) است. هر دو، طیف گسترده توالی مستقیم^۴ (DSSS) و تقسیم فرکانس عمود برهم^۵ (OFDM) مدولاسیون‌های بی‌سیم هستند که برای انتقال داده‌ها استفاده می‌شوند.

(۱۳) گزینه ۱. DHCP از برودکست‌های لایه ۳ با ارسال بسته‌ها به ۲۵۵.۲۵۵.۲۵۵.۲۵۵ برای کشف اولیه DHCP استفاده می‌کند. مولتی‌کست لایه ۳ برای کلاینت‌های DHCP استفاده نمی‌شود. لایه ۳، 802.1Q پاسخ نادرستی است؛ زیرا 802.1Q برای سوئیچ ترانک استفاده می‌شود. یونیکست‌های لایه ۳ شکل ارتباطی است که کلاینت‌ها پس از به‌دست‌آوردن آدرس IP استفاده می‌کنند.

(۱۴) گزینه ۳. پوسته امن^۶ (SSH) یک روش شبیه‌سازی کنسول ایمن برای مدیریت دستگاه‌های شبکه است. این امکان را به فرستنده و گیرنده می‌دهد تا یک جلسه رمزگذاری شده ایجاد کنند تا داده‌ها قابل رهگیری نباشند. سیستم تأیید هویت کاربران جهت ورود از راه دور (RADIUS^۷) پروتکلی است که کاربران را احراز

¹ demilitarized zone

² Carrier Sense Multiple Access/Collision Avoidance

³ Carrier Sense Multiple Access/Collision Detection

⁴ Direct Sequence Spread Spectrum

⁵ Orthogonal Frequency Division Multiplexing

⁶ Secure Shell

⁷ Remote Authentication Dial-In User Service

هویت می‌کند و رمزگذاری را ارائه نمی‌دهد. پروتکل انتقال ابرمتن (HTTP) روشی برای انتقال زبان نشانه‌گذاری ابرمتن (HTML) از سرور به هاست درخواست‌کننده است. رمزگذاری را ارائه نمی‌دهد. پروتکل انتقال فایل SSH (SFTP^۱) پروتکلی است که برای انتقال فایل رمزگذاری می‌کند، اما دسترسی مدیریتی را فراهم نمی‌کند.

۱۵) گزینه ۲. پروتکل ریموت دسکتاپ (RDP) اجازه می‌دهد تا درایوهای محلی در هنگام شروع جلسه RDP در دسترس دستگاه راه دور باشند. شبکه مجازی رایانه (VNC^۲)، پوسته امن (SSH) و Telnet قادر به تغییر مسیر درایوها نیستند.

۱۶) گزینه ۴. روتر یا سوئیچ پیام‌های Syslog را به سرور Syslog در پورت ۵۱۴ با UDP ارسال می‌کند. عوامل SNMP به UDP/161 گوش می‌دهند. SNMP از TCP برای پیام‌رسانی استفاده نمی‌کند. SNMP تله‌ها را روی UDP/162 ارسال می‌کند.

۱۷) گزینه ۳. محدوده IP برای شبکه کلاس B، ۱۹۱-۱۲۸ است. آدرس‌دهی کلاس B به طور پیش فرض ۱۶ بیت آدرس‌دهی شبکه و ۱۶ بیت آدرس‌دهی هاست را فراهم می‌کند.

۱۸) گزینه ۲. آدرس IP 135.20.255.255 یک آدرس برودکست کلاس B است. این یک آدرس کلاس A نیست و همچنین آدرس Gateway پیش فرض نیست. ماسک پیش فرض یک آدرس کلاس B، 255.255.0.0 است.

۱۹) گزینه ۱. فضای آدرس IP خصوصی برای حفظ تعداد آدرس‌های IP عمومی ایجاد شده است. آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند، اما این امر باعث امنیت آنها نمی‌شود. آدرس‌های IP خصوصی، همانطور که از نامشان پیداست، ارتباطات را عمومی بیان نمی‌کنند. آدرس‌های IP خصوصی به صورت عمومی برای ارتباطات قابل آدرس‌دهی نیستند. راه‌اندازی آدرس‌های IP خصوصی آسان‌تر از آدرس‌های IP عمومی نیست.

۲۰) گزینه ۴. ترجمه آدرس شبکه (NAT) برای برقراری ارتباط از طریق اینترنت عمومی با آدرس‌های IP خصوصی مورد نیاز است. اگرچه روترهای اینترنت برای مسیریابی مورد نیاز هستند، اما به طور پیش فرض آدرس‌های IP خصوصی را به آدرس‌های IP عمومی هدایت نمی‌کنند. تونل IPv4 یا تونل VPN برای ارتباطات در اینترنت با آدرس‌های IP خصوصی مورد نیاز نیست.

۲۱) گزینه ۲. پروتکل نخستین کوتاه‌ترین مسیر باز یا OSPF^۳ یک پروتکل حالت-پیوند است. پروتکل اطلاعات مسیریابی (RIP) و RIPv2 هر دو پروتکل‌های برداری فاصله هستند. پروتکل مسیریابی گیت‌وی داخلی

¹ SSH File Transfer Protocol

² Virtual Network Computing

³ Open Shortest Path First

پیشرفته (EIGRP^۲) یک پروتکل مسیریابی ترکیبی است که بهترین ویژگی‌های بردار فاصله و حالت-پیوند را ترکیب می‌کند.

(۲۲) گزینه ۳. هر ورودی پروتکل تفکیک آدرس (ARP^۳) یک زمان مشخص برای زندگی در حافظه پنهان ARP دارد. با این حال، اینترفیس‌های فیزیکی به طور دائم به حافظه پنهان ARP اضافه می‌شوند و با یک خط تیره زیر ستون Age مشخص می‌شوند. هنگامی که ورودی‌های ARP کهنه می‌شوند، ورودی از حافظه پنهان ARP حذف می‌شود. اگر ورودی ARP نامعتبر باشد، از حافظه پنهان ARP حذف خواهد شد.

(۲۳) گزینه ۳. فاصله ادمینی (AD^۴) رتبه‌بندی اعتماد بین پروتکل‌های مسیریابی مختلف و روش‌های مسیر است. این مقیاس اعتماد، زمانی مهم است که چندین مسیر به یک مقصد وجود داشته باشد. مسیرهای متصل مستقیم دارای فواصل ادمینی (AD) با بالاترین سطح اعتماد هستند. فرمان‌های مسیر پر شده توسط پروتکل مسیریابی پویا برای بهترین مسیر بر اساس اندازه‌های متریک و نه فاصله ادمینی آنها محاسبه می‌شود. فاصله ادمینی توسط مدیر برای انتخاب مسیر تعیین نشده است. مقدار فاصله ادمینی با هزینه تا مقصد مرتبط نیست، فقط اعتماد به یک بیانیه مسیر است.

(۲۴) گزینه ۳. فاصله ادمینی یا اداری (AD) پروتکل مسیریابی گیت‌وی داخلی پیشرفته (EIGRP^۵)، ۹۰ است. رایج‌ترین ADها ۹۰ برای EIGRP، ۱۰۰ برای IGRP، ۱۱۰ برای OSPF، و ۱۲۰ برای RIP هستند. یادداشت "۹۰ یا قوت بیضی هندی عجیب و غریب" به شما کمک می‌کند ترتیب را به خاطر بسپارید. سپس با شروع EIGRP با مقدار ۹۰، مقادیر زیر ۱۰ را افزایش دهید.

(۲۵) گزینه ۱. پروتکل گیت‌وی مرزی (BGP^۶) یک پروتکل مسیریابی بردار مسیر است. پروتکل اطلاعات مسیریابی (RIP^۷) یک پروتکل مسیریابی بردار فاصله است. OSPF یک پروتکل حالت-پیوند است. پروتکل مسیریابی گیت‌وی داخلی پیشرفته (EIGRP) یک پروتکل ترکیبی در نظر گرفته می‌شود که هم مکانیسم‌های بردار فاصله و هم سازوکار حالت پیوند را در بر می‌گیرد.

(۲۶) گزینه ۱. پروتکل تفکیک آدرس (ARP) در IPv6 با پروتکل کشف شبکه (NDP^۸) جایگزین شده است. پروتکل NDP از درخواست همسایه (NS^۱) و تبلیغات همسایه (NA^۲) برای یادگیری همسایگان به جای

¹ Routing Information Protocol

² Enhanced Interior Gateway Routing Protocol

³ Address Resolution Protocol

⁴ Administrative Distance

⁵ Enhanced Interior Gateway Routing Protocol

⁶ Border Gateway Protocol

⁷ Routing Information Protocol

⁸ Network Discovery Protocol

برودکست ARP استفاده می‌کند. ARPv6 یک پروتکل واقعی نیست بنابراین یک پاسخ نامعتبر است. کپسوله‌سازی روتر عمومی (GRE³) یک پروتکل تونل‌سازی برای سایر پروتکل‌های شبکه است. یک بسته تبلیغاتی روتر (RA) از گیت‌وی بازگردانده می‌شود تا هاست، آدرس گیت‌وی را یاد بگیرد.

(۲۷) گزینه ۲. سوئیچ در حالت شفاف VTP در VTP شرکت نخواهد کرد. با این حال، اگر VTP، v2 باشد، سوئیچ، تبلیغات VTP را ارسال و دریافت می‌کند. حالت سرور VTP به سوئیچ اجازه می‌دهد تا به عنوان یک Master برای دامنه VTP عمل کند. حالت پراکسی VTP یک حالت واقعی نیست. بنابراین، نادرست است. حالت سرویس‌گیرنده VTP به سوئیچ اجازه می‌دهد تا به عنوان یک Slave به سرور Master عمل کند.

(۲۸) گزینه ۱. پیوند بین سوئیچ (ISL⁴)، یک پروتکل اختصاصی است که برای ترانکینگ سوئیچ‌ها استفاده می‌شود. اگر نیاز به اتصال سوئیچ‌های غیر سیسکو به سوئیچ سیسکو دارید، باید از استاندارد IEEE 802.1Q استفاده کنید. VTP یک پروتکل ترانکینگ نیست. برای انطباق و سهولت در پیکربندی، به پرکردن VLANها در سوئیچ‌های سیسکو کمک می‌کند. پروتکل شناسایی سیسکو (CDP⁵) نیز یک پروتکل ترانکینگ نیست و از طریق قابلیت‌های قدرت برقراری ارتباط خود، با دستگاه‌های همسایه مذاکره می‌کند. همچنین امکان کشف همسایگان را فراهم می‌کند، اما CDP اختصاصی سیسکو است، بنابراین فقط با دستگاه‌های سیسکو می‌تواند ارتباط برقرار کند.

(۲۹) گزینه ۳. 802.1X اجازه دسترسی انتخابی به شبکه در لایه ۲ را می‌دهد. این امکان را در سوئیچ فراهم می‌کند؛ زیرا سوئیچ به عنوان یک تأییدکننده برای یک سرور AAA عمل می‌کند و فقط پس از احراز هویت کاربر یا دستگاه، اجازه دسترسی را می‌دهد. 802.1Q یک پروتکل ترانکینگ است که برای انتقال چندین VLAN بر روی یک اتصال لایه ۲ استفاده می‌شود و احراز هویت را ارائه نمی‌دهد. لیست کنترل دسترسی (ACL⁶) یک شرط و عبارت عملی است که برای اجازه‌دادن، رد کردن یا ثبت ترافیک استفاده می‌شود. فایروال‌ها حاوی ACL و خط‌مشی‌هایی برای اجازه‌دادن، رد کردن و ثبت ترافیک هستند، اما معمولاً ترافیک را تأیید نمی‌کنند.

(۳۰) گزینه ۲. استاندارد IEEE 802.11a تا ۱۲ کانال بدون همپوشانی یا اگر استاندارد 802.11h را اضافه کنید تا ۲۳ کانال را ارائه می‌دهد. همه پاسخ‌های دیگر نادرست است.

¹ neighbor solicitation

² neighbor advertisements

³ Generic Router Encapsulation

⁴ Inter-Switch Link

⁵ Cisco Discovery Protocol

⁶ Access Control List

(۳۱) گزینه ۴. استاندارد IEEE 802.11a حداکثر سرعت داده تا ۵۴ مگابیت بر ثانیه را فراهم می‌کند. همه پاسخ‌های دیگر نادرست است.

(۳۲) گزینه ۳. VPN‌های IPsec سایت به سایت، مقیاس‌پذیری را به عنوان یک مزیت ارائه می‌دهند. این به این دلیل است که هر اداره راه دور فقط به اتصال اینترنت برای ایجاد یک تونل VPN به اداره اصلی نیاز دارد. هنگام استفاده از VPN، سرپار خاصی وجود دارد. بنابراین، پس از استقرار VPN‌های IPsec سایت به سایت ممکن است به پهنای باند بالاتری نیاز باشد. تأخیر، تحت تأثیر قرار می‌گیرد و به دلیل سطح رمزگذاری که هر بسته هنگام عبور از VPN سایت به سایت باید متحمل شود، بیشتر خواهد بود. پشتیبانی از مولتی‌کست مزیت رایج VPN‌های IPsec سایت به سایت نیست.

(۳۳) گزینه ۲. یک کابل رول شده برای ایجاد یک اتصال سریال از رایانه به روتر برای پیکربندی استفاده می‌شود. برای اتصال اترنت از کابل Cat 5e استفاده می‌شود. چیزی به نام کابل PuTTY وجود ندارد، اما PuTTY یک برنامه شبیه‌سازی ترمینال است که با کابل سریال استفاده می‌شود. فیبر تک حالت (SMF)^۱ نوعی کابل فیبر نوری است که می‌تواند مسافت‌های طولانی را طی کند.

(۳۴) گزینه ۱. پیام Get-Request توسط یک ایستگاه مدیریت شبکه (NMS)^۲ برای درخواست اطلاعات از یک عامل SNMP استفاده می‌شود. پیام Get-Response پیامی است که پس از دریافت پیام Get-Request از کلاینت به NMS ارسال می‌شود. پیام Set-Request توسط NMS به سرویس‌گیرنده SNMP ارسال می‌شود و درخواست می‌کند یک شمارنده قابل نوشتن خاص روی مقدار مشخص شده تنظیم شود. پیام‌های Trap از دستگاه شبکه به ایستگاه مدیریت شبکه SNMP ارسال می‌شوند که رویدادی بیش از یک آستانه تعیین شده در دستگاه راه‌اندازی شود.

(۳۵) گزینه ۳. استاندارد NetFlow اطلاعات جلسه شامل آدرس مبدا و مقصد، برنامه‌ها و حجم ترافیک را ارائه می‌دهد. Syslog روشی برای جمع‌آوری پیام‌های سیستمی برای شناسایی مشکلات است یا می‌توان از آن برای تجزیه و تحلیل پس از مرگ (Post-Mortem) استفاده کرد. پروتکل ساده مدیریت شبکه (SNMP)^۳ پروتکلی است که برای ثبت آمار عملکرد سرورها، برنامه‌ها و دستگاه‌های شبکه استفاده می‌شود. آنالیزگر پورت سوئیچ (SPAN)^۴ برای بازتاب ترافیک پورت استفاده می‌شود.

(۳۶) گزینه ۱. یک SLA از دو نه ۳۶۵ روز در سال از زمان توقف مورد انتظار است. این معادل ۷.۲ ساعت در ماه است که سرویس می‌تواند قطع شود. همه پاسخ‌های دیگر نادرست است.

¹ Single-mode fiber

² network management station

³ Simple Network Management Protocol

⁴ Switched Port Analyzer

۳۷) گزینه ۲. خطامشی رمز عبور، عمر، پیچیدگی، تاریخچه و پیچیدگی رمزهای عبور را در سازمان تعریف می‌کند. خطامشی (BYOD) نحوه استفاده از دستگاه‌های شخصی را در سازمان تعریف می‌کند. نرم‌افزار جلوگیری از فقدان داده (DLP) سعی می‌کند از کمبود داده‌ها جلوگیری کند. این کار را با حفظ آگاهی از اقداماتی انجام می‌دهد که می‌تواند و نمی‌توان آن را در رابطه با یک سند انجام داد. یک خطامشی استفاده قابل قبول (AUP)^۱، استفاده قابل قبول از منابع سازمانی را تعریف می‌کند.

۳۸) گزینه ۱. هدف زمان بازیابی (RTO)^۲ مدت زمان لازم برای بازیابی اطلاعات شما به هدف نقطه بازیابی (RPO)^۳ است. RPO اندازه‌گیری زمان از یک شکست، فاجعه، یا یک رویداد زیان‌آور قابل مقایسه است. RPOها زمانی اندازه‌گیری می‌شوند که داده‌های شما در فرمت قابل استفاده معمولاً در آخرین نسخه پشتیبان ذخیره شده است. MTBF^۴، میانگین زمان بین خرابی‌ها است. MTTR^۵ به معنی میانگین زمانی است که یک فروشنده برای تعمیر خرابی لازم دارد.

۳۹) گزینه ۲. هدف زمان بازیابی (RTO) اندازه‌گیری سرعتی است که می‌توانید از دست‌دادن داده‌ها را با استفاده از پشتیبان‌گیری بازیابی کنید. هدف نقطه بازیابی (RPO) نقطه زمانی است که در صورت وقوع فاجعه می‌توانید به آن بازگردید. چرخش Grandfather-Father-Son (GFS) یک روش سیستماتیک برای بایگانی کردن رسانه‌های پشتیبان است. پنجره پشتیبان‌گیری پنجره زمانی است که در آن می‌توان پشتیبان‌گیری را انجام داد.

۴۰) گزینه ۳. پلت‌فرم به عنوان یک سرویس (PaaS) معمولاً توسط توسعه‌دهندگان نرم‌افزار استفاده می‌شود. این یک پلت‌فرم توسعه را فراهم می‌کند که توسعه‌دهنده نرم‌افزار می‌تواند از آن برای ایجاد برنامه‌های کاربردی استفاده کند. نمونه‌ای از آن، یک وب سرور با PHP و MySQL است که در فضای ابری میزبانی می‌شود. نرم‌افزار به عنوان سرویس (SaaS) یک محصول نرم‌افزاری مشابه ایمیل یا نرم‌افزار شبکه‌های اجتماعی است که در آن، از نرم‌افزار ارائه شده به عنوان سرویس استفاده می‌کنید. زیرساخت به عنوان یک سرویس (IaaS) به شما اجازه می‌دهد زیرساخت‌هایی مانند ماشین‌های مجازی (VM)، شبکه‌های مجازی یا حتی DNS را اجاره کنید. بازیابی فاجعه به عنوان یک سرویس (DRaaS)^۶ یکی دیگر از سرویس‌های محبوب است. شما می‌توانید فضای ذخیره‌سازی را اجاره کنید و قدرت را محاسبه کنید تا یک سایت بازیابی فاجعه را تسهیل کنید.

¹ Acceptable Use Policy

² Recovery Time Objective

³ Recovery Point Objective

⁴ Mean Time Between Failures

⁵ Mean Time To Repair

⁶ Disaster recovery as a service