فهرست مطالب

مقدمه ناشر ۱۴

مقدمه ۱۵

ساختار و اهداف کتاب ۱۵

مخاطبان این کتاب چه کسانی هستند؟ ۱۵

راهنمای استفاده از کتاب ۱۶

بخش هفتم

Wireless LANs ۱۷

فصل بیستم **تحلیل معماری‌های بی‌سیم سیسکو** ۱۸

سوالات اول فصل ۱۸

معماری Autonomous AP ۲۰

معماری AP مبتنی بر Cloud ۲۱

معماری‌های Split-MAC ۲۳

مقایسه روش‌های پیاده‌سازی کنترل‌کننده شبکه بی‌سیم ۲۵

حالت‌های نقطه دسترسی سیسکو ۲۸

پاسخ سوالات ابتدای فصل ۲۰ ..... ۲۹

فصل بیست‌ویکم **امنیت شبکه‌های بی‌سیم** ۳۱

سوالات اول فصل ۳۱

آناتومی یک اتصال امن ۳۳

احراز هویت ۳۳

محرمانگی پیام ۳۵

یکپارچگی پیام ۳۶

روش‌های احراز هویت کلاینت بی‌سیم ۳۷

Open Authentication ۳۷

WEP (Wired Equivalent Privacy) ۳۷
802.1x/EAP ۳۸
روش‌های احراز هویت EAP ۳۹
LEAP (Lightweight EAP) ۳۹
EAP-FAST (EAP Flexible Authentication by Secure Tunneling) ۴۰
PEAP (Protected EAP) ۴۰
EAP-TLS (EAP Transport Layer Security) ۴۰
روش‌های حفظ حریم خصوصی و یکپارچگی بی‌سیم ۴۱
TKIP (Temporal Key Integrity Protocol) ۴۱
CCMP (Counter/CBC-MAC Protocol) ۴۲
GCMP (Galois/Counter Mode Protocol) ۴۲
WPA، WPA2 و WPA3 ..... ۴۲
حالت‌های احراز هویت WPA ۴۳
پاسخ سوالات ۴۵

فصل بیست‌ودوم **ساخت یک شبکه محلی بی‌سیم ۴۷**

سوالات اول فصل ۴۷
اتصال یک نقطه دسترسی سیسکو ۴۹
دسترسی به Cisco WLC ۵۰
اتصال یک Cisco WLC ۵۲
استفاده از پورت‌های WLC ۵۲
استفاده از رابط‌های WLC ۵۴
پیکربندی یک WLAN ۵۶
پیکربندی یک WLAN ۵۸
گام ۱. پیکربندی یک سرور RADIUS ۵۸
گام ۲. ایجاد یک رابط داینامیک ۵۹
گام ۳. ایجاد یک WLAN جدید ۶۱
پیکربندی امنیت WLAN ۶۲
پیکربندی QoS در WLAN ۶۴
پیکربندی تنظیمات پیشرفته WLAN ۶۵
نهایی کردن پیکربندی WLAN ۶۶

پاسخ سوالات ابتدای فصل۲۲ ..... ۶۷

بخش هشتم

لیست‌های کنترل دسترسی IP ۶۹

فصل بیست‌وسوم آشنایی با لایه انتقال و پروتکل‌های کاربردی TCP/IP ۷۰

سوالات ابتدای فصل ۷۰
پروتکل‌های لایه‌ی چهارم از مجموعه پروتکل‌های TCP/IP: پروتکل TCP و پروتکل UDP ۷۱
پروتکل کنترل انتقال (TCP) ۷۲
چندپخشی (Multiplexing) با استفاده از شماره‌های پورتTCP ۷۳
برنامه‌های محبوب TCP/IP ۷۵
برقراری و خاتمه اتصال ۷۶
بازیابی خطا و قابلیت اطمینان ۷۷
کنترل جریان با استفاده از Windowing ۷۹
پروتکل دیتاگرام کاربر (UDP) ۸۰
برنامه‌های TCP/IP ۸۱
شناسه‌های منبع یکتا (URI) ۸۱
یافتن سرور وب با استفاده از DNS ۸۳
انتقال فایل‌ها با HTTP ۸۵
چگونه هاست دریافت‌کننده، برنامه‌ی کاربردیِ دریافتی صحیح را شناسایی می‌کند ۸۶
پاسخ سوالات ابتدای فصل۲۳ ..... ۸۷

فصل بیست‌وچهارم فهرست‌های کنترل دسترسی (ACL) پایه در IPv4 ..... ۸۹

سوالات ابتدای فصل ۸۹
مبانی لیست کنترل دسترسیIPv4 ..... ۹۰
مکان و جهتACL ها ۹۱
تطبیق بسته‌ها (Matching Packets) ۹۲
اقدامات هنگام تطبیق یک بسته ۹۳
انواع IP ACL ۹۳
ACLهای شماره‌گذاری شده‌ی استاندارد برای IPv4 ..... ۹۴
منطق لیست درACL های IP ۹۴

منطق تطبیق و نحوه نگارش دستورات (Syntax) ۹۵
تطبیق دقیق آدرس IP ۹۶
تطبیق یک زیرمجموعه از آدرس با استفاده از Wildcardها ۹۶
Wildcard masks باینری ۹۸
یافتن ماسک Wildcard مناسب برای تطبیق با یک زیرشبکه ۹۸
تطبیق با هر/تمام آدرس‌ها ۹۹
اجرای استاندارد IP ACLها ۹۹
مثال ۱ از ACL استاندارد شماره‌گذاری شده ۱۰۰
مثال ۲ از ACL استاندارد شماره‌گذاری شده ۱۰۲
نکات عیب‌یابی و تأیید ۱۰۴
تمرین به‌کارگیری ACLهای استاندارد IP ۱۰۵
تمرین ساخت دستورات access-list ۱۰۵
مهندسی معکوس از ACL به محدوده آدرس ۱۰۶
پاسخ سوالات ابتدای فصل۲۴ ..... ۱۰۷

فصل بیست‌وپنجم لیست‌های کنترل دسترسی پیشرفته IPv4 ..... ۱۰۸

سوالات ابتدای فصل ۱۰۸
ACLهای شماره‌گذاری شده توسعه‌یافته IP ۱۱۰
تطابق پروتکل، آدرس IP مبدأ و آدرس IP مقصد ۱۱۰
تطبیق شماره‌های پورت TCP و UDP ۱۱۲
پیکربندی ACL پیشرفته IP ۱۱۵
Extended IP Access Lists: مثال اول ۱۱۶
Extended IP Access Lists: مثال دوم ۱۱۹
ACLهای نام‌گذاری‌شده و ویرایش ACL ۱۲۰
Named IP ACLs ۱۲۱
ویرایش ACLها با استفاده از شماره‌های ترتیب (Sequence Numbers) ۱۲۳
مقایسه پیکربندی ACL شماره‌دار با پیکربندی ACL نام گذاری شده ۱۲۵
نکاتی که در پیاده‌سازی ACL باید در نظر گرفت ۱۲۶
پاسخ سوالات ابتدای فصل۲۵ ..... ۱۲۷

بخش نهم

سرویس‌های امن‌سازی ۱۲۹

فصل بیست‌وششم ساختار امنیت ۱۳۰

سوالات ابتدای فصل ۱۳۰
اصطلاحات کاربردی در مفاهیم امنیت ۱۳۱
انواع حملات در Spoofing Attacks ۱۳۴
حملات Denial of Service ۱۳۵
حملات Reflection و Amplification ۱۳۷
حملات Man In The Middle ۱۳۸
حملات در Reconnaissance Attack ۱۳۹
حملات در Buffer overflow Attacks ۱۴۰
آشنایی با Malware ۱۴۰
آشنایی با برخی از آسیب‌پذیری‌های انسانی ۱۴۱
آشنایی با آسیب‌پذیری در رمز عبورها ۱۴۲
کنترل و نظارت بر دسترسی کاربران ۱۴۵
آموزش نکات امنیتی به کاربران ۱۴۷
پاسخ سوالات ابتدای فصل۲۶ ..... ۱۴۸

فصل بیست‌وهفتم امن‌سازی دستگاه‌های شبکه ۱۵۰

سوالات ابتدای فصل ۱۵۰
امن‌سازی پسوردهای IOS ۱۵۲
رمزگذاری پسوردهای قدیمی IOS با دستور service password-encryption ۱۵۲
رمزگذاری enable password با استفاده از Hashها ۱۵۴
Enable password و Enable Secret ۱۵۴
مخفی کردن حقیقی Enable password با استفاده از Hash ۱۵۵
بهبود Hashها برای Enable secret سیسکو ۱۵۷
رمزگذاری پسوردها برای usernameهای لوکال ۱۵۸
کنترل Password Attackها با استفاده از ACLها ۱۵۹
فایروال‌ها و سیستم‌های جلوگیری از نفوذ ۱۶۰
فایروال‌های سنتی ۱۶۰

Security Zoneها ۱۶۲
سیستم‌های جلوگیری از نفوذ (IPS) ۱۶۴
Cisco Next-Generation Firewalls ۱۶۵
Cisco Next-Generation IPS ۱۶۸
پاسخ سوالات ابتدای فصل۲۷ ..... ۱۷۰

فصل بیست‌وهشتم **پیاده‌سازی Port-Security در سوییچ‌ها ۱۷۲**

سوالات ابتدای فصل ۱۷۲
مفاهیم و کانفیگ Port-Security ۱۷۴
پیکربندی Port-Security ۱۷۶
Verifying Port-Security ۱۷۸
Port Security MAC Addresses ۱۸۰
Port-security violation modes ۱۸۱
Port-security shutdown mode ۱۸۲
Port Security Protect and Restrict Modes ۱۸۵
پاسخ سوالات ابتدای فصل۲۸ ..... ۱۸۷

فصل بیست‌ونهم **پیاده‌سازی DHCP ۱۸۹**

سوالات ابتدای فصل ۱۸۹
Dynamic Host Configuration Protocol ۱۹۱
مفاهیم DHCP ۱۹۱
پشتیبانی از DHCP برای subnetهای راه دور با استفاده از DHCP Relay ۱۹۳
اطلاعات ذخیره شده در DHCP Server ۱۹۵
کانفیگ DHCP روی روترها و سوییچ‌ها ۱۹۷
کانفیگ DHCP Relay ۱۹۷
کانفیگ سوئیچ به عنوان DHCP client ۱۹۸
کانفیگ روتر به عنوان یک DHCP client ۲۰۰
شناسایی تنظیمات IPv4 هاست ۲۰۱
پاسخ سوالات ابتدای فصل۲۹ ..... ۲۰۹

فصل سی‌ام **DHCP Snooping و ARP Inspection ۲۱۱**

سوالات ابتدای فصل ۲۱۲

DHCP Snooping ۲۱۳
مفاهیم DHCP Snooping ۲۱۳
یک حمله نمونه: DHCP server جعلی ۲۱۴
منطق DHCP Snooping ۲۱۶
فیلتر کردن پیام‌های DISCOVER بر اساس آدرس MAC ۲۱۷
فیلتر کردن پیام‌هایی که آدرس‌های IP را release می‌کنند ۲۱۸
کانفیگ DHCP Snooping ۲۲۰
کانفیگ DHCP Snooping بر روی یک سوییچ لایه ۲ ..... ۲۲۰
محدود کردن نرخ پیام‌های DHCP ۲۲۲
Dynamic ARP Inspection ۲۲۴
مفاهیم DAI ۲۲۴
مروری بر ARP ۲۲۴
ARP gratuitous به عنوان ARP Vector ۲۲۵
منطق Dynamic ARP Inspection ۲۲۷
کانفیگ Dynamic ARP Inspection ۲۲۹
کانفیگ بازرسی ARP بر روی یک سوییچ لایه ۲ ..... ۲۲۹
محدود کردن DAI message rates ۲۳۲
کانفیگ بررسی پیام اختیاری DAI ۲۳۴
پاسخ سوالات ابتدای فصل ۳۰ ..... ۲۳۴

بخش دهم

سرویس‌های IP ۲۳۷

فصل سی‌ویکم پروتکل‌های مدیریتی دستگاه‌ها ۲۳۸

سوالات ابتدای فصل ۲۳۸
ثبت پیام‌های سیستمی (Syslog) ۲۳۹
ارسال پیام به کاربران آنلاین در لحظه ۲۳۹
ذخیره پیام‌های لاگ برای بررسی‌های بعدی ۲۴۰
قالب پیام‌های Log ۲۴۱
سطوح اهمیت پیام‌های Log ۲۴۲
پیکربندی و تأیید System Logging ۲۴۳

دستور debug و پیام‌های Log ۲۴۵
پروتکل زمان شبکه (NTP) ۲۴۷
تنظیم زمان و منطقه زمانی ۲۴۸
پیکربندی پایه NTP ۲۴۹
ساعت مرجع NTP و Stratum ۲۵۱
مقدار پیش‌فرض و تنظیمات Stratum در NTP ۲۵۲
پیکربندی NTP با قابلیت افزونگی ۲۵۳
استفاده از اینترفیس Loopback در NTP برای دسترسی بهتر ۲۵۵
تحلیل توپولوژی با استفاده از CDP و LLDP ۲۵۶
بررسی اطلاعاتی که توسط CDP آموخته می‌شود ۲۵۶
پیکربندی و تأیید CDP ۲۶۰
بررسی اطلاعات به‌دست‌آمده توسط LLDP ۲۶۱
پیکربندی و تأیید LLDP ۲۶۴
پاسخ سوالات ابتدای فصل ۳۱ ..... ۲۶۶

فصل سی‌ودوم Network Address Translation ۲۶۷

سوالات ابتدای فصل ۲۶۷
دیدگاه‌های مقیاس‌پذیری آدرس IPv4 ..... ۲۶۹
CIDR ۲۷۰
آدرس‌دهی خصوصی (Private Addressing) ۲۷۱
مفاهیم ترجمه آدرس شبکه (NAT) ۲۷۲
NAT استاتیک ۲۷۳
NAT پویا (Dynamic NAT) ۲۷۵
NAT Overload با ترجمه آدرس پورت (PAT) ۲۷۶
پیکربندی و عیب‌یابی NAT ۲۷۸
پیکربندی NAT استاتیک ۲۷۸
پیکربندی NAT داینامیک ۲۸۰
تأیید NAT داینامیک ۲۸۱
پیکربندی NAT Overload (PAT) ۲۸۴
عیب‌یابی NAT ۲۸۷
پاسخ سوالات ابتدای فصل ۳۲ ..... ۲۸۹

سوالات ابتدای فصل ۲۹۰
مقدمه‌ای بر QoS ۲۹۲
QoS: مدیریت پهنای باند، تأخیر، لرزش و از دست دادن ۲۹۲
انواع ترافیک ۲۹۳
برنامه‌های کاربردی داده ۲۹۳
برنامه‌های صوتی و تصویری ۲۹۴
QoS در این کتاب ۲۹۵
QoS روی سوئیچ‌ها و روترها ۲۹۵
طبقه‌بندی و نشانه‌گذاری ۲۹۵
اصول طبقه‌بندی ۲۹۶
اصول تطبیق (طبقه‌بندی) ۲۹۶
طبقه‌بندی روی روترها با ACLها و NBAR ۲۹۷
نشانه‌گذاری DSCP IP و CoS اترنت ۲۹۹
نشانه‌گذاری هدر IP ۲۹۹
نشانه‌گذاری هدر اترنت Q۸۰۲,۱ ..... ۳۰۰
سایر فیلدهای نشانه‌گذاری ۳۰۱
تعریف مرزهای اعتماد ۳۰۱
مقادیر نشانه‌گذاری پیشنهادی DiffServ ۳۰۳
ارسال تسریع شده (EF) ۳۰۳
ارسال تضمین شده (AF) ۳۰۳
انتخاب‌کننده کلاس (CS) ۳۰۴
دستورالعمل‌هایی برای مقادیر نشانه‌گذاری DSCP ۳۰۵
صف‌بندی ۳۰۶
زمان‌بندی Round-Robin (اولویت‌بندی) ۳۰۷
صف‌بندی با تأخیر کم ۳۰۸
یک استراتژی اولویت‌بندی برای داده، صدا و تصویر ۳۱۰
نظارت (Policing) ۳۱۰
کجا از نظارت استفاده کنیم ۳۱۱
شکل‌دهی (Shaping) ۳۱۳

تنظیم یک فاصله زمانی شکل‌دهی خوب برای صدا و تصویر ۳۱۴
جلوگیری از ازدحام ۳۱۶
اصول اولیه پنجره‌بندی TCP ۳۱۶
ابزارهای جلوگیری از ازدحام ۳۱۷
پاسخ سوالات ابتدای فصل ۳۳ ..... ۳۱۸

فصل سی‌وچهارم خدمات متفرقه IP ۳۲۰

سوالات ابتدای فصل ۳۲۰
پروتکل First Hop Redundancy ۳۲۲
نیاز به Redundancy در شبکه‌ها ۳۲۲
نیاز به پروتکل First Hop Redundancy ۳۲۴
سه راه‌حل برای First-Hop Redundancy ۳۲۵
مفاهیم HSRP ۳۲۵
پروتکل Simple Network Management (SNMP) ۳۲۷
خواندن و نوشتن متغیرهای SNMP : SNMP Get and Set ۳۲۸
اعلان‌های SNMP: Traps , Informs ۳۲۹
پایگاه اطلاعات مدیریتی (MIB) ۳۳۰
امنیت SNMP ۳۳۱
FTP و TFTP ۳۳۲
مدیریت تصاویر Cisco IOS با FTP/TFTP ۳۳۲
سیستم فایل IOS ۳۳۳
پروتکل‌های FTP و TFTP ۳۴۰
اصول اولیه پروتکل TFTP ۳۴۶
پاسخ سوالات ابتدای فصل ۳۴ ..... ۳۴۷

بخش یازدهم

آزمایشگاه مجازی: از دواپس تا سناریوی OSPF ۳۴۹

فصل سی‌وپنجم مقدمه‌ای بر DevOps ۳۵۰

بررسی مفهوم infrastructure as a code ۳۵۱
مقایسهٔ Imperactive و declarative ۳۵۱

مزایای ایجاد Iac ۳۵۲
اهمیت Iac در دواپس ۳۵۲
CI چیست؟ ۳۵۲
مزایای CI ۳۵۳
CD چیست؟ ۳۵۳
مزایای CI/CD ۳۵۴
فصل سی‌وششم آشنایی با Network Emulatorها ۳۵۵
نصب و راه‌اندازی EVE-NG ۳۵۵
راه‌اندازی EVE-NG به عنوان یک ماشین مجازی ۳۵۶
نصب EVE-NG ۳۶۲
اضافه کردن دستگاه‌های مختلف به پلتفورم EVE-NG ۳۶۹
اضافه‌کردن RouterOS به EVE-NG ۳۷۱
اضافه کردن روتر سیسکو به EVE-NG ۳۷۵
اضافه کردن سوییچ سیسکو به EVE-NG ۳۷۶
استفاده از ابزار ishare2 ..... ۳۷۹
نصب ishare2 بر روی EVE-NG ۳۸۰
آموزش کار با ishare2 ..... ۳۸۱
فصل سی‌وهفتم پیاده‌سازی سناریو OSPF ۳۸۴
توضیح سناریو OSPF ۳۸۵
کانفیگ Cisco Switches ۳۸۵
کانفیگ Cisco Routers ۳۹۴