



مؤسسه فرهنگی هنری
دیباگران تهران

به نام خدا

راهنمای جامع

CCNA 200-301

جلد دوم

آموزش جامع عملی و کاربردی سیسکو به همراه

آموزش نمونه ساز EVE-ng

مؤلف:

ایمان فرهی پرشگفتی



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: راهنمای جامع CCNA 200-301 – جلد دوم

آموزش جامع عملی و کاربردی سیسکو به همراه آموزش نمونه ساز EVE-ng

◀ مولف: ایمان فرهی پرشگفتی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرای: نازنین نصیری

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۴۰۴

◀ چاپ و صحافی: صدف

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۵۲۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۹۳۶-۵

نشانی واحد فروش: تهران - خیابان انقلاب -

خ شهدای ژاندارمری - بین خ فخر رازی و ۱۲ فروردین -

پلاک ۸۸ طبقه دوم - واحد ۴ تلفن ها: ۶۶۴۸۳۷۶۳-۶۶۴۸۳۷۶۲

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagaran-tehran.com

سرشناسه: فرهی پرشگفتی، ایمان، ۱۳۶۵-
عنوان و نام پدیدآور: راهنمای جامع CCNA200-301
/مولف: ایمان فرهی پرشگفتی.
مشخصات نشر: تهران: دیباگران تهران: ۱۴۰۴
مشخصات ظاهری: ۴۱۰ ص: جدول
شابک: ۹۷۸-۶۲۲-۲۱۸-۹۳۶-۵ ج ۱: ۹۷۸-۶۲۲-۲۱۸-۹۳۶-۵ ج ۲.
وضعیت فهرست نویسی: فیبا
مدرجات: ج ۱. آموزش جامع عملی و کاربردی سیسکو به همراه نمونه ساز EVE-ng
ج ۲. آموزش جامع عملی و کاربردی سیسکو به همراه نمونه ساز EVE-ng
موضوع: سیستم عامل اینترنتی سیسکو
موضوع: Cisco IOS
موضوع: مسیر یاب ها (شبکه کامپیوتری)
موضوع: Routers (computer networks)
موضوع: ارتباط بین شبکه ای
موضوع: Internetworking (telecommunication)
رده بندی کنگره: ۵۱۰/۵۴۳ TK
رده بندی دیویی: ۰۴/۶۲
شماره کتابشناسی ملی: ۱۰۱۰۰۳۳۹

نشانی تلگرام: @mftbook نشانی اینستاگرام دیبا dibagaran_publishing

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هرگوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

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 معماری های بی سیم سیسکو	۱۸
-----------	-------------------------------------	----

سوالات اول فصل	۱۸
معماری Autonomous AP	۲۰
معماری AP مبتنی بر Cloud	۲۱
معماری های Split-MAC	۲۳
مقایسه روش های پیاده سازی کنترل کننده شبکه بی سیم	۲۵
حالت های نقطه دسترسی سیسکو	۲۸
پاسخ سوالات ابتدای فصل ۲۰	۲۹

فصل بیست و یکم	امنیت شبکه های بی سیم	۳۱
----------------	-----------------------------	----

سوالات اول فصل	۳۱
آناتومی یک اتصال امن	۳۳
احراز هویت	۳۳
محرمانگی پیام	۳۵
یکپارچگی پیام	۳۶
روش های احراز هویت کلاینت بی سیم	۳۷
Open Authentication	۳۷

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

فصل بیست‌ودوم ساخت یک شبکه محلی بی‌سیم ۴۷

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

پاسخ سوالات ابتدای فصل ۲۲ 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

چندپختی (Multiplexing) با استفاده از شماره‌های پورت TCP ۷۳

برنامه‌های محبوب TCP/IP ۷۵

برقراری و خاتمه اتصال ۷۶

بازایی 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 کاربردی دریافتی صحیح را شناسایی می‌کند ۸۶

پاسخ سوالات ابتدای فصل ۲۳ ۸۷

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

سوالات ابتدای فصل ۸۹

مبانی لیست کنترل دسترسی IPv4 ۹۰

مکان و جهت ACL 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 در ACL‌های IP ۹۴

۹۵.....	منطق تطبیق و نحوه نگارش دستورات (Syntax)
۹۶.....	تطبیق دقیق آدرس IP
۹۶.....	تطبیق یک زیرمجموعه از آدرس با استفاده از Wildcard ها
۹۸.....	Wildcard masks باینری
۹۸.....	یافتن ماسک Wildcard مناسب برای تطبیق با یک زیرشبکه
۹۹.....	تطبیق با هر/تمام آدرس ها
۹۹.....	اجرای استاندارد IP ACL ها
۱۰۰.....	مثال ۱ از ACL استاندارد شماره گذاری شده
۱۰۲.....	مثال ۲ از ACL استاندارد شماره گذاری شده
۱۰۴.....	نکات عیب یابی و تأیید
۱۰۵.....	تمرین به کارگیری ACL های استاندارد IP
۱۰۵.....	تمرین ساخت دستورات access-list
۱۰۶.....	مهندسی معکوس از ACL به محدوده آدرس
۱۰۷.....	پاسخ سوالات ابتدای فصل ۲۴

فصل بیست و پنجم لیست های کنترل دسترسی پیشرفته IPv4..... ۱۰۸

۱۰۸.....	سوالات ابتدای فصل
۱۱۰.....	ACL های شماره گذاری شده توسعه یافته IP
۱۱۰.....	تطابق پروتکل، آدرس IP مبدأ و آدرس IP مقصد
۱۱۲.....	تطبیق شماره های پورت TCP و UDP
۱۱۵.....	پیکربندی ACL پیشرفته IP
۱۱۶.....	Extended IP Access Lists: مثال اول
۱۱۹.....	Extended IP Access Lists: مثال دوم
۱۲۰.....	ACL های نام گذاری شده و ویرایش ACL
۱۲۱.....	Named IP ACLs
۱۲۳.....	ویرایش ACL ها با استفاده از شماره های ترتیب (Sequence Numbers)
۱۲۵.....	مقایسه پیکربندی ACL شماره دار با پیکربندی ACL نام گذاری شده
۱۲۶.....	نکاتی که در پیاده سازی ACL باید در نظر گرفت
۱۲۷.....	پاسخ سوالات ابتدای فصل ۲۵

بخش نهم

۱۲۹..... سرویس‌های امن‌سازی

فصل بیست‌وششم ساختار امنیت ۱۳۰.....

- ۱۳۰ سوالات ابتدای فصل
- ۱۳۱ اصطلاحات کاربردی در مفاهیم امنیت
- ۱۳۴ انواع حملات در Spoofing Attacks
- ۱۳۵ حملات Denial of Service
- ۱۳۷ حملات Amplification و Reflection
- ۱۳۸ حملات Man In The Middle
- ۱۳۹ حملات در Reconnaissance Attack
- ۱۴۰ حملات در Buffer overflow Attacks
- ۱۴۰ آشنایی با Malware
- ۱۴۱ آشنایی با برخی از آسیب‌پذیری‌های انسانی
- ۱۴۲ آشنایی با آسیب‌پذیری در رمز عبورها
- ۱۴۵ کنترل و نظارت بر دسترسی کاربران
- ۱۴۷ آموزش نکات امنیتی به کاربران
- ۱۴۸ پاسخ سوالات ابتدای فصل ۲۶

فصل بیست‌وهفتم امن‌سازی دستگاه‌های شبکه ۱۵۰.....

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

۱۶۲	 Security Zone ها
۱۶۴	 سیستم‌های جلوگیری از نفوذ (IPS)
۱۶۵	 Cisco Next-Generation Firewalls
۱۶۸	 Cisco Next-Generation IPS
۱۷۰	 پاسخ سوالات ابتدای فصل ۲۷

فصل بیست و هشتم پیاده‌سازی Port-Security در سویچ‌ها ۱۷۲

۱۷۲	 سوالات ابتدای فصل
۱۷۴	 Port-Security مفاهیم و کانفیگ
۱۷۶	 Port-Security پیکربندی
۱۷۸	 Verifying Port-Security
۱۸۰	 Port Security MAC Addresses
۱۸۱	 Port-security violation modes
۱۸۲	 Port-security shutdown mode
۱۸۵	 Port Security Protect and Restrict Modes
۱۸۷	 پاسخ سوالات ابتدای فصل ۲۸

فصل بیست و نهم پیاده‌سازی DHCP ۱۸۹

۱۸۹	 سوالات ابتدای فصل
۱۹۱	 Dynamic Host Configuration Protocol
۱۹۱	 DHCP مفاهیم
۱۹۳	 پشتیبانی از DHCP برای subnet های راه دور با استفاده از DHCP Relay
۱۹۵	 DHCP Server اطلاعات ذخیره شده در
۱۹۷	 کانفیگ DHCP روی روترها و سویچ‌ها
۱۹۷	 DHCP Relay کانفیگ
۱۹۸	 DHCP client کانفیگ سوئیچ به عنوان
۲۰۰	 DHCP client کانفیگ روتر به عنوان یک
۲۰۱	 شناسایی تنظیمات IPv4 هاست
۲۰۹	 پاسخ سوالات ابتدای فصل ۲۹

فصل سی ام ARP Inspection و DHCP Snooping ۲۱۱

۲۱۲	 سوالات ابتدای فصل
-----	-------------------------

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

بخش دهم

۲۳۷..... سرویس‌های IP

۲۳۸..... پروتکل‌های مدیریتی دستگاه‌ها فصل سی و یکم

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

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

۲۶۷..... Network Address Translation **فصل سی‌ودوم**

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

۲۹۰	سوالات ابتدای فصل
۲۹۲	مقدمه‌ای بر QoS
۲۹۲	QoS: مدیریت پهنای باند، تأخیر، لرزش و از دست دادن
۲۹۳	انواع ترافیک
۲۹۳	برنامه‌های کاربردی داده
۲۹۴	برنامه‌های صوتی و تصویری
۲۹۵	QoS در این کتاب
۲۹۵	QoS روی سوئیچ‌ها و روترها
۲۹۵	طبقه‌بندی و نشانه‌گذاری
۲۹۶	اصول طبقه‌بندی
۲۹۶	اصول تطبیق (طبقه‌بندی)
۲۹۷	طبقه‌بندی روی روترها با ACLها و NBAR
۲۹۹	نشانه‌گذاری DSCP IP و CoS اترنت
۲۹۹	نشانه‌گذاری هدر IP
۳۰۰	نشانه‌گذاری هدر اترنت Q.۸۰۲.۱
۳۰۱	سایر فیلدهای نشانه‌گذاری
۳۰۱	تعریف مرزهای اعتماد
۳۰۳	مقادیر نشانه‌گذاری پیشنهادی DiffServ
۳۰۳	ارسال تسریع شده (EF)
۳۰۳	ارسال تضمین شده (AF)
۳۰۴	انتخاب‌کننده کلاس (CS)
۳۰۵	دستورالعمل‌هایی برای مقادیر نشانه‌گذاری DSCP
۳۰۶	صف‌بندی
۳۰۷	زمان‌بندی Round-Robin (اولویت‌بندی)
۳۰۸	صف‌بندی با تأخیر کم
۳۱۰	یک استراتژی اولویت‌بندی برای داده، صدا و تصویر
۳۱۰	نظارت (Policing)
۳۱۱	کجا از نظارت استفاده کنیم
۳۱۳	شکل‌دهی (Shaping)

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 سی و چهارم خدمات متفرقه IP ۳۲۰

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

بخش یازدهم

آزمایشگاه مجازی: از دواپس تا سناریوی OSPF ۳۴۹

فصل سی و پنجم مقدمه‌ای بر DevOps ۳۵۰

بررسی مفهوم infrastructure as a code	۳۵۱
declarative و Imperative مقایسه	۳۵۱

۳۵۲	مزایای ایجاد Iac
۳۵۲	اهمیت Iac در دواپس
۳۵۲	CI چیست؟
۳۵۳	مزایای CI
۳۵۳	CD چیست؟
۳۵۴	مزایای CI/CD

۳۵۵..... آشنایی با Network Emulator ها **فصل سی و هشتم**

۳۵۵	نصب و راه اندازی EVE-NG
۳۵۶	راه اندازی EVE-NG به عنوان یک ماشین مجازی
۳۶۲	نصب EVE-NG
۳۶۹	اضافه کردن دستگاه های مختلف به پلتفرم EVE-NG
۳۷۱	اضافه کردن RouterOS به EVE-NG
۳۷۵	اضافه کردن روتر سیسکو به EVE-NG
۳۷۶	اضافه کردن سویچ سیسکو به EVE-NG
۳۷۹	استفاده از ابزار ishare2
۳۸۰	نصب ishare2 بر روی EVE-NG
۳۸۱	آموزش کار با ishare2

۳۸۴..... پیاده سازی سناریو OSPF **فصل سی و نهم**

۳۸۵	توضیح سناریو OSPF
۳۸۵	کانفیگ Cisco Switches
۳۹۴	کانفیگ Cisco Routers

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که بتواند
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست‌دارید تألیف "جناب آقای ایمان فرهی پرشگفتی" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

dibagaran@mftplus.com

مقدمه

در عصر حاضر، شبکه‌های کامپیوتری به عنوان زیرساختی حیاتی، نقشی بی‌بدیل در تبادل اطلاعات و ارتباطات ایفا می‌کنند. تسلط بر مفاهیم و مهارت‌های مرتبط با شبکه، نه تنها برای متخصصان این حوزه، بلکه برای طیف وسیعی از مشاغل و صنایع، امری ضروری و اجتناب‌ناپذیر است.

کتاب حاضر، با هدف ارائه دانش و مهارت‌های لازم برای موفقیت در دو آزمون معتبر Network+ و CCNA، تدوین شده است. این دو آزمون، به عنوان استانداردهایی بین‌المللی در حوزه شبکه شناخته می‌شوند و می‌توانند مسیر حرفه‌ای علاقه‌مندان و متخصصان این حوزه را به طور چشمگیری ارتقا بخشند.

✓ **آزمون Network+:** این آزمون، به عنوان نقطه شروعی ایده‌آل، مبانی و مفاهیم کلیدی شبکه‌های کامپیوتری را در بر می‌گیرد. داوطلبان با گذراندن این آزمون، درک جامعی از عملکرد شبکه‌ها، پروتکل‌ها، سخت‌افزارها و نرم‌افزارهای مرتبط به دست می‌آورند و توانایی نصب، پیکربندی، عیب‌یابی و مدیریت شبکه‌های در مقیاس کوچک و متوسط را کسب می‌کنند.

✓ **آزمون CCNA:** این آزمون، به طور تخصصی بر دانش و مهارت‌های مرتبط با تجهیزات و فناوری‌های شرکت سیسکو (Cisco) متمرکز است. سیسکو، به عنوان یکی از پیشگامان صنعت شبکه، نقشی محوری در توسعه و پیشرفت این حوزه ایفا می‌کند. مدرک CCNA، به عنوان گواهینامه‌ای معتبر و شناخته‌شده در سطح جهانی، توانایی دارندگان آن را در طراحی، پیاده‌سازی، نگهداری و عیب‌یابی شبکه‌های مبتنی بر تجهیزات سیسکو، به اثبات می‌رساند.

CCNA

ساختار و اهداف کتاب

این کتاب، با رویکردی نظام‌مند و منسجم، مفاهیم نظری و مهارت‌های عملی مورد نیاز برای موفقیت در آزمون‌های مذکور را ارائه می‌دهد. ساختار کتاب به گونه‌ای طراحی شده است که خواننده را از مباحث پایه به سمت موضوعات پیشرفته‌تر هدایت کند. هر فصل شامل توضیحات دقیق، مثال‌های کاربردی، تصاویر و نمودارهای گویا، و تمرین‌های متنوع برای تثبیت یادگیری است.

CCNA

مخاطبان این کتاب چه کسانی هستند؟

- دانشجویان رشته‌های مهندسی کامپیوتر، فناوری اطلاعات و سایر رشته‌های مرتبط
- متخصصان شبکه که قصد ارتقاء دانش و دریافت مدارک معتبر بین‌المللی را دارند
- افرادی که علاقه‌مند به ورود به حوزه شبکه و کسب مهارت‌های تخصصی هستند

این کتاب، با ارائه محتوایی جامع و به‌روز، منبعی ارزشمند برای تمامی افرادی است که به دنبال کسب دانش و مهارت‌های تخصصی در حوزه شبکه‌های کامپیوتری و آمادگی برای آزمون‌های Network+ و CCNA هستند.

راهنمای استفاده از کتاب

❖ در ابتدای هر فصل، تعدادی سوال مرتبط با مباحث آورده شده است؛

- اگر به تمام سوالات پاسخ صحیح دادید، درک مفاهیم پیش‌رو برایتان راحت و سریع خواهد بود
- اما اگر در انتخاب جواب صحیح مردد بودید و یا حتی سوالی را اشتباه پاسخ دادید، جای هیچ نگرانی نیست! پرداختن به سوالات، ذهن شما را نسب به موضوعات مطرح شده در فصل آماده خواهد کرد که این امر، به یادگیری هرچه بیشتر شما کمک می‌کند.

❖ برای درک بیشتر مفاهیم اصلی، شکل‌ها و مثال‌هایی در هر فصل گنجانده شده است. شناخت نمادهای به کار رفته، ذهن شما را برای دریافت و تثبیت مطالب، آماده می‌سازد.



Access Point



PC



Laptop



Server



IP Phone



Router



Switch



Layer 3 Switch



Hub



Bridge



Cable (Various)



Serial Line



Virtual Circuit



Ethernet WAN



Wireless



SDN Controller



vSwitch



IPS



ASA



Firewall



Network Cloud



Cable Modem



DSLAM