۳۱ روز تا آزمون CCNA

آلن جانسون

ترجمه: مهندس مهران تاجبخش

انتشارات پندار پارس

سرشناسه	:	جانسون، آلن، ۱۹۶۳ - م. Johnson, Allan
عنوان و نام پدیدآور	:	۳۱ روز تا آزمون CCNA/آلن جانسون ؛ ترجمه مهران تاجبخش.
مشخصات نشر	:	تهران : پندار پارس ، ۱۳۹۶.
مشخصات ظاهری	:	۵۳۲ ص.: مصور ،جدول.
شابک	:	978-600-8201-58-8 : ۴۵۰۰۰۰ ریال
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی: 31 days before your ccna routing & switching exam : a day-by-day review guide for the icnd1 (100-105), icnd2 (200-105), and ccna (200-125) certification exams,2017.
عنوان گسترده	:	سی و یک روز تا آزمون CCNA.
موضوع	:	داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها -- راهنمای مطالعه
موضوع	:	Electronic data processing personnel -- Certification -- Study guides
موضوع	:	شبکه‌های کامپیوتری -- آزمون‌ها -- راهنمای مطالعه
موضوع	:	Computer networks -- Examinations -- Study guides
شناسه افزوده	:	تاجبخش، مهران، ۱۳۴۷ -، مترجم
رده بندی کنگره	:	QA۷۶/۳/ج۱۷س۹ ۱۳۹۶
رده بندی دیویی	:	۰۰۴/۶۰۷۶
شماره کتابشناسی ملی	:	۵۰۰۵۷۶۳

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ – تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

www.pendarepars.com **info@pendarepars.com**

نام کتاب : **۳۱ روز تا آزمون CCNA**

ناشر : **انتشارات پندار پارس**

تألیف : **آلن جانسون**

برگردان : **مهران تاجبخش**

چاپ نخست : **بهمن ماه ۹۶**

شمارگان : **۵۰۰ نسخه**

طرح جلد : **رامین شکرالهی**

چاپ، صحافی : **روز**

قیمت : **۴۵۰۰۰ تومان** **شابک : ۹۷۸-۶۰۰-۸۲۰۱-۵۸-۸**

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

تقدیم به رامتین،

پسر عزیزم، تلاش و پشت‌کارت باعث موفقیت، و مایه افتخار من است.
بدون حضور و همراهی تو، طی این مسیر امکان‌پذیر نبود.

فهرست

پیش‌گفتار ۱

روز ۳۱ ؛ مدل‌های شبکه و تجهیزات و اجزا ۷

سرفصل‌های مربوط به آزمون CCNA 200-125

مدل‌های OSI و TCP/IP ۸

لایه‌های OSI ۸

پروتکل‌ها و لایه‌های مدل TCP/IP ۹

PDU و بسته‌بندی داده‌ها ۱۱

لایه کاربردی مدل TCP/IP ۱۲

لایه انتقال در مدل TCP/IP ۱۲

عنوان TCP ۱۴

شماره‌های گذرگاه ۱۴

بازیابی خطا ۱۵

کنترل جریان ترافیک ۱۶

برقراری و قطع ارتباط ۱۶

UDP ۱۷

لایه اینترنت در مدل TCP/IP ۱۸

لایه دسترسی شبکه در مدل TCP/IP ۱۸

خلاصه بسته‌بندی داده ۲۰

تجهیزات ۲۱

سوئیچ‌ها ۲۱

سوئیچ‌های لایه دسترسی ۲۲

سوئیچ‌های لایه ارتباط ۲۲

سوئیچ‌های لایه مرکزی ۲۲

مسیریاب‌ها ۲۳

تجهیزات خاص ۲۴

فایروال‌ها ۲۴

فناوری‌های IDS و IPS ۲۵

نقاط دسترسی و کنترل کننده‌های شبکه‌های بی‌سیم ۲۶

لایه فیزیکی ۲۸

استانداردها و انواع رسانه شبکه ۲۸

راهنمای برقراری ارتباط تجهیزات شبکه محلی ۳۰

شبکه‌های محلی (LANs) و شبکه‌های گسترده (WANs) ۳۰

نمایه‌های شبکه ۳۲

توپولوژی های فیزیکی و منطقی ۳۲

طراحی ساختار سلسله مراتبی شبکه سازمانی ۳۳

منابع مطالعه ۳۵

روز ۳۰ ؛ سوئیچینگ اترنت ۳۷

سرفصل آزمون CCNA 200-125

تحول سوئیچینگ ۳۷

منطق سوئیچینگ ۳۸

دامنه‌های برخورد و فراگیر ۴۰

ارسال پیام‌ها ٤٠
روش های ارسال پیام‌ها در سوئیچ ٤١
سوئیچینگ متقارن و نامتقارن ٤١
حافظه میانگیر ٤١
سوئیچینگ لایه دو و سه ٤٢
مروری بر اترنت (Ethernet) ٤٢
فناوری‌های ابتدایی اترنت ٤٣
CSMA/CD ٤٤
خلاصه‌ای از فناوری شبکه اترنت اولیه ٤٥
فناوری حال حاضر در شبکه اترنت ٤٥
کابل‌های UTP ٤٥
مزایای استفاده از سوئیچ‌ها ٤٧
آدرس‌دهی اترنت ٤٨
ساختار پیام‌ها در شبکه اترنت ٤٨
نقش لایه فیزیکی ٥٠
منابع مطالعه ٥٠
روز ۲۹ ؛ مبانی پیکربندی سوئیچ ۵۳
سرفصل آزمون ICND1 100-101
دسترسی و مشاهده سیستم‌عامل IOS سیسکو ٥٣
اتصال به تجهیزات سیسکو ٥٣
نشست‌های CLI EXEC ٥٤
استفاده از راهنمای سیستم ٥٤
کلیدهای میانبر (shortcuts) برای مرور و ویرایش دستورات ٥٥
تاریخچه دستورات ٥٧
دستورات بررسی و آزمایش در IOS ٥٧
وضعیت‌های پیکربندی جزئی ٥٨
دستورات پیکربندی مقدماتی سوئیچ ٥٨
ارتباط یک طرفه، دوطرفه و سرعت پورت ٦٠
فناوری auto-MDIX ٦١
کنترل ارتباط‌های شبکه ٦١
رفع اشکال کابل و رابط شبکه ٦٥
موارد مربوط به رسانه ارتباطی ٦٥
وضعیت رابط شبکه و پیکربندی سوئیچ ٦٦
کدهای وضعیت رابط شبکه ٦٦
عدم هماهنگی سرعت (speed) و جهت انتقال ترافیک(duplex) ٦٧
موارد اشکال متداول لایه اول در درگاه ارتباطی فعال ٦٩
منابع مطالعه ٦٩
روز ۲۸ ؛ مفاهیم و پیکربندی ترانک و شبکه مجازی ۷۱
سرفصل آزمون CCENT 100-101 ICDN1
مفاهیم شبکه مجازی محلی (VLAN) ٧٢
انواع ترافیک ٧٣

انواع شبکه‌های مجازی محلی (VLANs) ۷٤
مثالی از شبکه مجازی صدا (Voice VLAN) ۷۵
ارتباط شبکه‌های مجازی (Trunking) ۷۵
پروتکل DTP ۷۷
پیکربندی و کنترل VLAN ۷۸
شبکه‌های مجازی توسعه یافته ۸۲
پیکربندی و کنترل ترانک ۸۵
رفع اشکال شبکه مجازی ۸۸
شبکه‌های مجازی غیرفعال ۸۹
رفع اشکال ترانک ۹۰
کنترل دو سر انتهایی ترانک ۹۰
کنترل وضعیت‌های عملیاتی ترانک ۹۲
منابع مطالعه ۹۲
روز ۲۷ ؛ آدرس‌دهی IP ۹۵
سرفصل آزمون CCENT 100-101 ICDN1
آدرس‌دهی IPv4 ..... ۹٦
قالب و ساختار عنوان ۹٦
کلاس‌های آدرس‌ها ۹٦
دلیل استفاده از الگوی زیرشبکه ۹۷
آدرس‌دهی IP عمومی و خصوصی ۹۸
تعریف زیرشبکه‌ها در ٤ مرحله ۹۹
تعیین تعداد بیت‌های قرضی برای زیرشبکه ۱۰۰
تعیین الگوی جدید زیرشبکه ۱۰۱
تعیین ضرب کننده زیرشبکه ۱۰۱
فهرست زیرشبکه‌ها، محدوده آدرس میزبان‌ها و آدرس‌های فراگیر ۱۰۱
زیرشبکه مثال ۱ ..... ۱۰۲
زیرشبکه مثال ۲ ..... ۱۰۲
زیرشبکه مثال ۳ ..... ۱۰۳
VLSM ۱۰۳
منابع مطالعه ۱۰٦
روز ۲٦ ؛ آدرس‌دهی IPV6 ..... ۱۰۷
سرفصل آزمون CCNA 200-125
مرور و مزایای آدرس‌دهی IPv6 ..... ۱۰۷
پروتکل IPv6 ..... ۱۰۸
انواع آدرس‌های IPv6 ..... ۱۰۹
یک‌به‌یک (Unicast) ۱۱۰
آدرس Global Unicast ۱۱۰
آدرس Link-Local ۱۱۳
آدرس Loopback ۱۱۳
آدرس‌های نامشخص (Unspecified) ۱۱٤
آدرس محلی منحصر به فرد (Unique Local) ۱۱٤

آدرس IPv4 Embedded ۱۱۵
Multicast ۱۱۵
Assigned Multicast ۱۱۶
Solicited-Node Multicast ۱۱۶
Anycast ۱۱۸
نمایش آدرس IPv6 ..... ۱۱۸
قوانین نوشتن آدرس‌های IPv6 ..... ۱۱۸
قوانین پیشوندها در IPv6 ..... ۱۱۹
زیرشبکه IPv6 ..... ۱۲۰
زیرشبکه با استفاده از بخش شناسایی زیرشبکه ۱۲۱
زیرشبکه با استفاده از بخش شناسایی درگاه ارتباطی ۱۲۱
مفهوم EUI-64 ..... ۱۲۲
پیکربندی خودکار آدرس Stateless ۱۲۳
انتقال به IPv6 ..... ۱۲۳
منابع مطالعه ۱۲۴

روز ۲۵ ؛ مفاهیم اولیه مسیریابی ۱۲۷

سرفصل آزمون CCNA 200-125
انتقال بسته ۱۲۷
مثال تعیین مسیر و عملیات سوئیچینگ ۱۲۸
روش‌های مسیریابی ۱۳۰
طبقه بندی انواع پروتکل‌های مسیریابی پویا ۱۳۱
IGP and EGP ۱۳۲
پروتکل‌های تعیین مسیر بر حسب بردار مسافت ۱۳۲
پروتکل‌های مسیریابی مبتنی بر وضعیت مسیر (Link-State) ۱۳۳
پروتکل‌های مسیریابی Classful ۱۳۳
پروتکل‌های مسیریابی Classless ۱۳۴
مقیاس‌های مسیریابی پویا ۱۳۴
مسافت انتخاب راهبر ۱۳۶
مقایسه کلی پروتکل‌های IGP ۱۳۷
جلوگیری از مسیرهای حلقه(Routing loops) ۱۳۸
ویژگی‌های پروتکل‌های مسیریابی مبتنی بر وضعیت مسیر ۱۳۹
ساختن LSDB ۱۳۹
محاسبه الگوریتم دیجسترا ۱۴۰
همگرایی با استفاده از پروتکل‌های مبتنی بر وضعیت مسیر ۱۴۱
منابع مطالعه ۱۴۲

روز ۲۴ ؛ پیکربندی اولیه روتر ۱۴۳

عناوین آزمون CCNA 200-125
پیکربندی اولیه روترها با استفاده از IPV4 ..... ۱۴۳
قالب دستور ۱۴۴
مثال پیکربندی ۱۴۵
مثال کنترل تنظیمات و پیکربندی روتر ۱۴۷

پیکربندی اولیه روتر با IPv6 ..... ۱۵۶
قالب و ساختار دستور ۱۵۶
مثالی از پیکربندی ۱۵۷
کنترل ارتباط شبکه در IPv4 و IPv6 ..... ۱۶۰
رفع اشکال‌های مقدماتی آدرس‌دهی IP ۱۶۳
درگاه ارتباطی شبکه (Default gateway) ۱۶۳
IP آدرس‌های تکراری ۱۶۳
منابع مطالعه ۱۶۴
روز ۲۳ ؛ پیکربندی مسیر ثابت و پیش‌فرض ۱۶۵
سرفصل آزمون CCNA 200-125
مروری بر مسیرهای ثابت و پیش‌فرض ۱۶۵
پیکربندی مسیر ثابت IPv4 ..... ۱۶۶
تنظیم مسیر ثابت IPv4 با استفاده از پارامتر Next-Hop ۱۶۸
مسیرهای ثابت IPv4 با استفاده از پارامتر Exit Interface ۱۶۹
پیکربندی مسیر پیش‌فرض IPv4 ..... ۱۷۰
پیکربندی مسیر ثابت IPv4 خلاصه شده ۱۷۳
مسیر ثابت IPv6 ..... ۱۷۵
پیکربندی آدرس ثابت IPv6 ..... ۱۷۶
پیکربندی مسیر پیش‌فرض IPv6 ..... ۱۷۷
پیکربندی مسیر ثابت IPv6 خلاصه شده ۱۷۸
منابع مطالعه ۱۸۰
روز ۲۲ ؛ پیاده‌سازی RIPV2 ..... ۱۸۱
سرفصل آزمون CCNA 200-125
مفاهیم RIP ۱۸۲
ساختار پیام RIPv1 ..... ۱۸۲
عملکرد RIPv1 ..... ۱۸۲
پیکربندی RIPv1 ..... ۱۸۳
RIPv1 Verification and Troubleshooting ۱۸۴
درگاه‌های ارتباطی غیر فعال (passive) ۱۸۸
خلاصه کردن خودکار ۱۸۹
مسیر پیش‌فرض و RIPv1 ..... ۱۹۱
پیکربندی RIPv2 ..... ۱۹۳
غیرفعال‌سازی خلاصه کردن خودکار ۱۹۴
کنترل و رفع اشکال RIPv2 ..... ۱۹۴
منابع مطالعه ۱۹۵
روز ۲۱ ؛ VTP و پیکربندی مسیریابی INTER-VLAN ۱۹۷
سرفصل‌های آزمون CCNA 200-125
مفاهیم VTP ۱۹۷
پیکربندی و کنترل پروتکل VTP ۲۰۰
مفاهیم مسیریابی Inter-VLAN ۲۰۵
مسیریابی سنتی بین شبکه‌های مجازی (legacy Inter-VLAN routing) ۲۰۵

روتر به عنوان پیوند دهنده (Router on a stick) ۲۰۶
سوئیچ چند لایه (Multilayer Switch) ۲۰۶
پیکربندی و کنترل روتر به عنوان پیوند دهنده (Router on a stick) ۲۰۷
کنترل و پیکربندی سوئیچ چند لایه برای مسیریابی بین شبکه‌های مجازی ۲۱۰
ایجاد درگاه‌های ارتباطی SVI اضافی ۲۱۰
Configuring a Layer 3 Routed Port ۲۱۲
پیکربندی پورت مسیریابی شده لایه سه (L3 Routed port) ۲۱۲
منابع مطالعه ۲۱۳
روز ۲۰ ؛ عملکرد OSPF ۲۱۵
سرفصل آزمون CCNA 200-125
عملکرد OSPF در یک ناحیه ۲۱۵
قالب پیام OSPF ۲۱۵
انواع بسته OSPF ۲۱۶
شناسایی روترهای مجاور(Neighbors) ۲۱۷
اعلان وضعیت مسیر (LSA) ۲۱۸
بسته‌های OSPF DR و BDR ۲۱۹
الگوریتم OSPF ۲۱۹
روند مسیریابی بر اساس وضعیت مسیر (Link-State) ۲۲۱
مقایسه OSPFv2 و OSPFv3 ..... ۲۲۱
تشابه بین OSPFv2 و OSPFv3 ..... ۲۲۲
تفاوت‌های بین OSPFv2 و OSPFv3 ..... ۲۲۲
عملکرد OSPF در چند ناحیه ۲۲۲
طراحی OSPF چندناحیه ۲۲۳
افزایش کارآیی OSPF چند ناحیه ۲۲۴
منابع مطالعه ۲۲۵
روز ۱۹ ؛ پیاده‌سازی OSPF در یک ناحیه ۲۲۷
سرفصل آزمون 200-125
پیکربندی OSPFv2 در یک ناحیه ۲۲۷
دستور router ospf ۲۲۸
پارامتر Router ID ۲۲۸
دستور network ۲۲۹
درگاه‌های غیرفعال ۲۳۰
تغییر مقیاس‌های سنجش OSPF (metrics) ۲۳۱
کنترل OSPFv2 ..... ۲۳۳
پیکربندی OSPFv3 برای یک ناحیه ۲۳۷
دستور router ID در OSPFv3 ..... ۲۳۸
کنترل OSPFv3 ..... ۲۴۰
منابع مطالعه ۲۴۳
روز ۱۸ ؛ پیاده‌سازی OSPF در چند ناحیه ۲۴۵
سرفصل آزمون CCNA 200-125
پیاده‌سازی OSPFv2 در چند ناحیه ۲۴۵

پیاده‌سازی OSPFv3 در چند ناحیه ۲۴۹
منابع مطالعه ۲۵۳
روز ۱۷ ؛ بهینه‌سازی و رفع اشکال OSPF ۲۵۵
سرفصل آزمون CCNA 200-125
مثالی از پیکربندی OSPFv2 ..... ۲۵۵
تغییر در پیکربندی پروتکل OSPFv2 ..... ۲۵۷
انتشار مجدد مسیر پیش‌فرض ۲۵۷
تغییر تایمرهای مربوط به ارسال پیام‌های Hello و Dead ۲۵۸
انواع شبکه OSPF ۲۵۹
انتخاب DR/BDR ۲۵۹
کنترل انتخاب DR/BDR ۲۶۰
مثالی از پیکربندی OSPFv3 ..... ۲۶۲
ایجاد تغییرات در OSPFv3 ..... ۲۶۴
انتشار مسیر پیش‌فرض ۲۶۵
تغییر تایمرها ۲۶۶
رفع اشکال OSPF ۲۶۶
وضعیت‌های OSPF ۲۶۷
مجاورت در OSPF ۲۶۷
دستورات رفع اشکال OSPF ۲۶۷
منابع مطالعه ۲۶۹
روز ۱۶ ؛ عملکرد EIGRP ۲۷۱
سرفصل آزمون CCNA 200-125
مروری بر EIGRP ۲۷۱
مشخصات پروتکل EIGRP ۲۷۲
پیمانه‌های وابسته به پروتکل (PDMs) ۲۷۲
پروتکل انتقال مطمئن (RTP) ۲۷۳
انواع بسته‌های EIGRP ۲۷۳
قالب پیام EIGRP ۲۷۴
روند عملیات در EIGRP ۲۷۶
همگرایی در EIGRP ۲۷۶
مقیاس ترکیبی EIGRP ۲۷۶
مسیر AD ۲۷۷
DUAL ۲۷۸
مفاهیم DUAL ۲۷۸
DUAL FSM ۲۷۹
منابع مطالعه ۲۷۹
روز ۱۵ ؛ پیاده‌سازی EIGRP ۲۸۱
سرفصل آزمون CCNA 200-125
پیکربندی EIGRP برای IPv4 ..... ۲۸۱
الگوی آدرس‌دهی و توپولوژی EIGRP ۲۸۱
دستور network ۲۸۲

دستور Router ID ۲۸۳
کنترل IPv4 در پروتکل EIGRP ۲۸۳
بررسی جزئیات پروتکل ۲۸۳
بررسی جدول مجاورت ۲۸۵
بررسی جدول‌های توپولوژی ۲۸۵
بررسی جدول مسیریابی ۲۸۷
مفاهیم EIGRP برای IPv6 ..... ۲۸۸
پیکربندی EIGRP برای IPv6 ..... ۲۸۹
کنترل پروتکل EIGRP برای IPv6 ..... ۲۹۰
بررسی جزئیات پروتکل ۲۹۰
بررسی جدول مجاورت ۲۹۱
بررسی جدول مسیریابی ۲۹۲
منابع مطالعه ۲۹۳
روز ۱۴ ؛ بهینه‌سازی و رفع اشکال EIGRP ۲۹۵
سرفصل آزمون CCNA 200-125
تغییر پیکربندی EIGRP برای IPv4 ..... ۲۹۵
خلاصه‌سازی خودکار ۲۹۵
پروتکل EIGRP برای توپولوژی IPv4 ..... ۲۹۶
انتشار مسیر پیش‌فرض IPv4 ..... ۲۹۷
تغییر معیار تعیین مسیر (Metric) در EIGRP ۲۹۸
تغییر بازه زمانی ارسال پیام hello و زمان انتظار(Hold time) ۲۹۸
تغییر پروتکل EIGRP برای IPv6 ..... ۲۹۹
توپولوژی شبکه EIGRP برای IPv6 ..... ۲۹۹
انتشار مسیر پیش‌فرض IPv6 ..... ۳۰۰
تغییر مقدار پهنای باند ۳۰۰
تغییر بازه زمانی ارسال پیام hello و زمان انتظار (hold time) ۳۰۱
دستورات رفع اشکال EIGRP ۳۰۱
شبکه‌های ناپیوسته ۳۰۳
منابع مطالعه ۳۰۳
روز ۱۳ ؛ CDP و LLDP ۳۰۵
سرفصل آزمون CCNA 200-125
مروری بر CDP ۳۰۵
پیکربندی CDP ۳۰۶
کنترل CDP ۳۰۹
مروری بر LLDP ۳۱۲
پیکربندی LLDP ۳۱۳
کنترل LLDP ۳۱۴
منابع مطالعه ۳۱۶
روز ۱۲ ؛ امنیت شبکه LAN و ایمن سازی تجهیزات ۳۱۹
سرفصل آزمون CCNA 200-125
پیکربندی امنیت پورت ۳۱۹

بازیابی پورت پس از شناسایی تهدید ۳۲۲
کاهش تهدید در شبکه LAN ۳۲٤
DHCP snooping ۳۲٤
تغییر VLAN بومی و مدیریتی ۳۲۵
ایمن سازی پورت سوئیچ ۳۲٦
AAA ۳۲۷
802.1X ۳۲۸
پیکربندی SSH ۳۲۹
منابع مطالعه ۳۳۱
روز ۱۱ ؛ STP ۳۳۳
سرفصل آزمون CCNA 200-125
مفاهیم و عملکرد پروتکل STP ۳۳۳
الگوریتم STP ۳۳٤
همگرایی STP ۳۳۵
ویرایش‌های مختلف STP ۳۳۷
عملکرد PVST ۳۳۸
وضعیت‌های پورت ۳۳۸
کد شناسایی توسعه یافته سیستم ۳۳۹
عملکرد Rapid PVST+ ۳٤۰
شرایط درگاه RSTP ۳٤۰
نقش‌های پورت در پروتکل RSTP ۳٤۱
پورت‌های Edge ۳٤۲
پیکربندی و کنترل انواع ویرایش‌های پروتکل STP ۳٤۳
مروری بر پیکربندی STP ۳٤۳
پیکربندی و کنترل BID ۳٤٤
پیکربندی PortFast و BPDU Guard ۳٤٦
پیکربندی Rapid PVST+ ۳٤۷
کنترل STP ۳٤۷
سوئیچ‌های دسته‌ای(Switch Stacking) ۳٤۸
منابع مطالعه ۳٤۹
روز ۱۰ ؛ ETHERCHANNEL و HSRP ۳۵۱
سرفصل آزمون CCNA 200-125
عملکرد فناوری EtherChannel ۳۵۱
مزایای فناوری EtherChannel ۳۵۲
محدودیت‌های پیاده‌سازی ۳۵۲
پروتکل‌های EtherChannel ۳۵۳
پروتکل PAgP: ۳۵۳
پروتکل LACP: ۳۵٤
پیکربندی EtherChannel ۳۵۵
کنترل EtherChannel ۳۵٦
رفع اشکال EtherChannel ۳۵۸

مفاهیم پروتکل FHRP ۳۵۸
پروتکل‌های FHRP ۳۵۹
عملیات HSRP ۳۶۰
ویرایش‌های HSRP ۳۶۱
اولویت و حق تگام در پروتکل HSRP ۳۶۱
پیکربندی و کنترل پروتکل HSRP ۳۶۱
تنظیم بار ترافیک در پروتکل HSRP ۳۶۳
رفع اشکال HSRP ۳۶۵
منابع مطالعه ۳۶۶
روز ۹ ؛ مفاهیم لیست کنترل دسترسی (ACL) ۳۶۷
سرفصل آزمون CCNA 200-125
عملیات ACL ۳۶۷
تعریف یک ACL ۳۶۸
روند عملیات ACL در درگاه ارتباطی ۳۶۸
منطق لیست دستورات IP ACLs ۳۶۹
برنامه‌ریزی برای استفاده از ACL ۳۷۰
انواع ACLs ۳۷۰
شناسایی ACL ۳۷۱
راهنمای طراحی ACL ۳۷۲
منابع مطالعه ۳۷۲
..... ۳۷۲
روز ۸ ؛ پیاده‌سازی ACL ۳۷۳
سرفصل آزمون CCNA 200-125
پیکربندی IPv4 ACL استاندارد شماره‌گذاری شده ۳۷۳
IPv4 ACL استاندارد شماره‌گذاری شده: اجازه ورود برای شبکه مشخص ۳۷۴
IPv4 ACL استاندارد شماره‌گذاری شده: مسدود کردن ترافیک مربوط به میزبان مشخص ۳۷۵
IPv4 ACL استاندارد شماره‌گذاری شده: مسدود کردن ترافیک زیرشبکه مشخص ۳۷۵
IPv4 ACL استاندارد شماره‌گذاری شده: جلوگیری از ترافیک مربوط به Telnet و SSH برای دسترسی به روتر ۳۷۶
پیکربندی IPv4 ACL استاندارد توسعه یافته شماره‌گذاری شده ۳۷۶
IPv4 ACL توسعه یافته شماره‌گذاری شده: جلوگیری از ترافیک FTP از یک شبکه مشخص ۳۷۷
IPv4 ACL توسعه یافته شماره‌گذاری شده: مسدود کردن ترافیک Telnet از یک زیرشبکه ۳۷۸
پیکربندی IP ACLهای نام‌گذاری شده ۳۷۸
مراحل پیکربندی و قالب IPv4 ACL استاندارد نام‌گذاری شده ۳۷۹
IPv4 ACL استاندارد نام‌گذاری شده: مسدود کردن ترافیک یک میزبان از یک زیرشبکه مشخص ۳۷۹
مراحل پیکربندی و قالب دستورات IPv4 ACL توسعه‌یافته و نام‌گذاری شده ۳۸۰
افزودن عبارات توضیحی (comments) در IPv4 ACLهای شماره‌گذاری و نام‌گذاری شده ۳۸۰
کنترل IPv4 ACL ۳۸۱
مقایسه ACL برای IPv4 و IPv6 ..... ۳۸۳
پیکربندی IPv6 ACL ۳۸۳

گام ۱. نام‌گذاری IPv6 ACL ۳۸٤
گام ۲. ایجاد IPv6 ACL ۳۸٤
گام ۳. فعال کردن ACL ۳۸٤
IPv6 ACL استاندارد: اجازه دسترسی راه‌دور SSH ۳۸۵
IPv6 ACL توسعه یافته: مجوز عبور ترافیک وب ۳۸۵
کنترل IPv6 ACL ۳۸٦
رفع اشکال ACL ۳۸۹
منابع مطالعه ۳۸۹
روز ۷؛ DHCP و DNS ۳۹۱
سرفصل آزمون CCNA 200-125
پروتکل DHCPv4 ..... ۳۹۱
گزینه‌های پیکربندی DHCPv4 ..... ۳۹۲
پیکر بندی یک روتر به عنوان سرور DHCPv4 ..... ۳۹۲
پیکربندی روتر برای انتقال درخواست‌های DHCPv4 (relay agent) ۳۹٦
پیکربندی روتر به عنوان کاربر سرور DHCP ۳۹۸
پروتکل DHCPv6 ..... ۳۹۹
SLAAC ۳۹۹
Stateless DHCPv6 ..... ٤۰۱
Stateful DHCPv6 ..... ٤۰۱
عملیات Stateless DHCPv6 و stateful DHCPv6 ..... ٤۰۱
گزینه‌های پیکربندی DHCPv6 ..... ٤۰۲
پیکربندی روتر به عنوان سرور stateless DHCPv6 ..... ٤۰۳
پیکربندی روتر به عنوان سرور stateful DHCPv6 ..... ٤۰٤
رفع اشکال DHCP ٤۰۵
برطرف کردن تداخل آدرس‌های IPv4 ..... ٤۰۵
تست ارتباط با استفاده از IP آدرس ثابت ٤۰٦
کنترل پیکربندی پورت‌های سوئیچ ٤۰٦
تست عملکرد DHCPv4 در همان زیرشبکه و یا شبکه مجازی (VLAN) ٤۰٦
عملکرد DNS ٤۰٦
رفع اشکال DNS ٤۰۸
منابع مطالعه ٤۰۹
روز ٦؛ NAT ٤۱۱
سرفصل آزمون CCNA 200-125
مفاهیم NAT ٤۱۱
یک مثال از NAT ٤۱۳
فناوری NAT ایستا و پویا ٤۱٤
سربارگذاری NAT ٤۱٤
مزایای NAT ٤۱۵
محدودیت‌های NAT ٤۱۵
پیکربندی Static NAT ٤۱٦
پیکربندی Dynamic NAT ٤۱۷

پیکربندی NAT Overload ٤١٨
کنترل NAT ٤١٩
رفع اشکال NAT ٤٢٠
NAT برای IPv6 ..... ٤٢٢
محدوده آدرس‌های خصوصی IPv6 ..... ٤٢٢
موارد کاربرد NAT برای IPv6 ..... ٤٢٣
منابع مطالعه ٤٢٣
روز ٥؛ مروری بر شبکه گسترده (WAN) ٤٢٥
سرفصل آزمون CCNA 200-125
توپولوژی‌های WAN ٤٢٥
گزینه‌های ارتباطی WAN ٤٢٧
گزینه‌های ارتباط اختصاصی (dedicated) ٤٢٧
گزینه‌های ارتباطی از طریق شبکه‌های سوئیچینگ ٤٢٨
گزینه‌های ارتباطی در شبکه‌های سوئچینگ انتقال بسته ٤٢٩
Metro Ethernet ٤٢٩
MPLS ٤٣٠
گزینه‌های ارتباط به اینترنت ٤٣٠
DSL ٤٣١
Cable Modem ٤٣١
Wireless ٤٣٢
انتخاب گزینه‌های ارتباطی شبکه WAN ٤٣٢
فناوری VPN ٤٣٣
مزایای VPN ٤٣٣
انواع دسترسی VPN ٤٣٣
منابع مطالعه ٤٣٥
روز ٤؛ پیاده‌سازی WAN ٤٣٧
سرفصل آزمون
مفاهیم PPP ٤٣٧
قالب بسته پروتکل PPP ٤٣٨
PPP LCP ٤٣٩
تشخیص مسیر حلقه (looped-link detection) ٤٣٩
تشخیص خطای بهینه شده ٤٣٩
PPP Multilink ٤٤٠
تأیید هویت PPP ٤٤٠
پیکربندی و کنترل PPP ٤٤٠
پیکربندی مقدماتی PPP ٤٤١
CHAP ٤٤٢
PAP ٤٤٣
رفع اشکال PPP ٤٤٣
مفاهیم PPPoE ٤٤٤
پیکربندی PPPoE ٤٤٥

مثال پیکربندی بندی PPPoE ٤٤٥
رفع اشکال PPPoE ٤٤٦
GRE Tunneling ٤٤٦
مشخصات GRE ٤٤٧
پیکربندی و کنترل GRE ٤٤٧
رفع اشکال GRE ٤٤٩
مفاهیم BGP ٤٥٠
کنترل و پیکربندی eBGP ٤٥١
منابع مطالعه ٤٥٤
روز ۳؛ QOS و فضای ابری و شبکه SDN ٤٥٧
سرفصل آزمون CCNA 200-125
کیفیت ارائه خدمات (QoS) ٤٥٨
طبقه‌بندی و نشانه‌گذاری ٤٥٩
بیت‌های DSCP و IPP ٤٦٠
بیت‌های EF و AF ٤٦١
مدیریت تراکم ترافیک ٤٦٢
سیاست‌گذاری، تغییر شکل و حذف TCP ٤٦٣
کیفیت ارائه خدمات (QoS) و TCP ٤٦٤
پردازش ابری ٤٦٥
مجازی‌سازی سرور ٤٦٦
سرویس‌های فضای پردازش ابری ٤٦٧
ساختار شبکه مجازی ٤٦٩
شبکه‌های نرم‌افزاری تعریف شده (SDNs) ٤٦٩
سطوح داده، کنترل و مدیریت ٤٧٠
کنترل کننده‌ها ٤٧١
مثال‌های SDN ٤٧٢
پروتکل‌های Open SDN و OpenFlow ٤٧٢
ساختار متمرکز بر کاربرد سیسکو ٤٧٣
فناوری Cisco APIC-EM ٤٧٣
فناوری APIC-EM و ACL ٤٧٤
منابع مطالعه ٤٧٦
روز ۲؛ کنترل، مدیریت و نگهداری تجهیزات ٤٧٧
سرفصل آزمون CCNA 200-125
عملیات SNMP ٤٧٧
اجزای SNMP ٤٧٧
پیام‌های SNMP ٤٧٨
ویرایش‌های SNMP ٤٧٨
بانک اطلاعات MIB ٤٧٩
پیکربندی SNMP ٤٨٠
کنترل SNMP ٤٨١
Syslog ٤٨٢

عملکرد syslog ٤٨٣
کنترل و پیکربندی syslog ٤٨٥
پروتکل NTP ٤٨٨
سیستم فایل IOS سیسکو و تجهیزات شبکه ٤٨٩
دستورات IFS ٤٨٩
استفاده از پیشوندهای URL برای تعیین محل فایل‌ها ٤٩٢
دستورات مدیریت فایل‌های پیکربندی ٤٩٢
مدیریت Cisco IOS images ٤٩٤
تهیه پشتیبان از Cisco IOS image ٤٩٤
بازیابی Csico IOS image ٤٩٥
مدیریت لایسنس‌های Cisco IOS ٤٩٧
بازیابی رمزعبور ٥٠٠
منابع مطالعه ٥٠١

روز ۱؛ متدولوژی و ابزارهای رفع اشکال ۵۰۳

سرفصل آزمون CCNA 200-125
مستندسازی رفع اشکال ٥٠٣
فایل‌های پیکربندی ٥٠٣
نمودارهای توپولوژی شبکه ٥٠٤
داده‌های حدنصاب (مرجع) ٥٠٦
روش‌های رفع اشکال ٥٠٦
رفع اشکال در هر لایه ٥٠٨
روش پایین به بالا و لایه‌ها ٥١٠
رفع اشکال بر اساس IP SLA ٥١١
منابع مطالعه ٥١٤

پیش‌گفتار

زمانی که این مقدمه را می‌خوانید، به این معنی است که زمان و انرژی قابل ملاحظه‌ای را برای دریافت مدرک CCNA صرف کرده‌اید. برای گرفتن مدرک CCNA دو راه در پیش رو دارید. یا باید در دو آزمون ICDN1 (Interconnecting Cisco Network Devices) 100-105 و ICDN2 200-105 شرکت کنید و یا اینکه مستقیما در یک آزمون Cisco Certified Network Associate (CCNA 200-125) شرکت کنید. ورای اینکه کدام مسیر را برای رسیدن به مدرک CCNA انتخاب کرده‌اید، این کتاب می‌تواند به عنوان آخرین گام شما در جهت رسیدن به هدف مورد نظر باشد. البته باید توجه داشته باشید که این کتاب در شرایطی که دارای دانش و تجربه کافی در پیکربندی و رفع اشکال تجهیزات سیسکو باشید، مؤثر و کارآمد می‌باشد. به دیگر سخن، این کتاب نمی‌تواند به عنوان تنها مرجع آماده‌سازی برای آزمون CCNA مورد استفاده قرار گیرد. به همین دلیل در این بخش سعی خواهم کرد تا توصیه‌هایی را برای استفاده از منابع آموزشی مربوط به آزمون CCNA ارائه دهم.

منابع آموزشی

انتشارات سیسکو و پیرسون (Pearson IT) کتاب‌ها و منابع آموزشی متعددی را برای آماده‌سازی آزمون CCNA ارائه داده‌اند. این منابع در زمینه‌های مختلف نصب، پیکربندی، راه‌اندازی و رفع اشکال شبکه‌های سوئیچینگ کوچک تا متوسط می‌باشند.

سایت Safari Books

همه منابع مطالعاتی که در این بخش به آنها اشاره می‌شود را می‌توانید با عضویت در سایت Safaribooksonline.com در اختیار داشته باشید و یا به صورت آنلاین آنها را مطالعه و یا مشاهده کنید.

منابع اصلی

نخستین عنوان در لیست مورد نظر، بدون تردید کتاب Wendell Odom’s CCNA Routing and Switching 200-125 Official Cert Guide and Network Simulator Library (ISBN: 9781587206108) می‌باشد. اگر قصد خرید کتاب زیادی را ندارید، تنها این کتاب را خریداری کنید. نویسنده کتاب سعی کرده است تا با دانش و تجربه تخصصی خود، مفاهیم و مطالب مورد نیاز آزمون CCNA را با جزئیات کامل و به شکلی مطلوب ارائه کند. با توجه به لوح فشرده همراه کتاب و امکان دسترسی به منابع آنلاین مربوط به کتاب، قیمت کتاب بسیار مناسب می‌باشد. بدون شک منبعی مناسب‌تر و کامل‌تر از این کتاب را نمی‌توان برای آماده‌سازی آزمون CCNA پیدا کرد.

در صورتی‌که در آکادمی آموزشی سیسکو (Cisco Networking Academy) عضو هستید، امکان دسترسی به منابع آموزشی آنلاین سیسکو و همچنین شبیه‌ساز شبکه Packet Tracer را خواهید داشت. برنامه آموزشی آکادمی سیسکو از چهار دوره آموزشی تشکیل شده است. برای دریافت اطلاعات بیشتر می‌توانید به سایت www.netcad.com مراجعه کنید.

چنانچه عضو آکادمی سیسکو نباشید، امکان خریداری منابع آموزشی ارائه شده برای دوره‌های آموزشی فوق را با عناوین CCNA Routing and Switching Companion Guides (CGs) و Labs & Study

(LSGs) Guides را دارید. البته در این وضعیت امکان دسترسی به فایل‌های شبیه‌سازی شبکه مربوط به نرم افزار Packet Tracer را نخواهید داشت. عناوین کتب و منابع آموزشی CGs و LSGs در زیر آورده شده‌اند:

- Introduction to Networks v6 Companion Guide (ISBN: 9781587133602)
- *Introduction to Networks v6 Labs & Study Guide* (ISBN: 9781587133619)
- *Routing and Switching Essentials v6 Companion Guide* (ISBN: 9781587134289)
- *Routing and Switching Essentials v6 Labs & Study Guide* (ISBN: 9781587134265)
- *Scaling Networks v6 Companion Guide* (ISBN: 9781587134340)
- *Scaling Networks v6 Labs & Study Guide* (ISBN: 9781587134333)
- *Connecting Networks v6 Companion Guide* (ISBN: 9781587134326)
- *Connecting Networks v6 Labs & Study Guide* (ISBN: 9781587134296)

امکان دسترسی به منابع فوق از طریق سایت www.ciscopress.com و انتخاب لینک Cisco Networking Academy وجود دارد.

منابع تکمیلی

افزون بر منابع فوق، توصیه می‌شود که در ۳۱ روز پایانی باقیمانده تا آزمون CCNA از منابع تکمیلی که در زیر اشاره می‌شود، نیز استفاده کنید.

کتاب Scott Empson’s CCNA Routing and Switching Portable Command Guide (ISBN:97815872005880) که بسیار معروف و شناخته شده می‌باشد. این کتاب تنها فهرستی از فرمان‌ها و دستورات مورد استفاده در آزمون CCNA نمی‌باشد، برای هر یک از دستورات مثال‌ها و موارد کاربردی نیز ارائه شده است. مثال‌های پیکربندی ارائه شده در کتاب مورد نظر برای طراحی ساده یک شبکه سیسکو کافی می‌باشند.

کتاب Kevin Wallace’s CCNA routing and Switching 200-125 Premium Edition Complete Video Course (ISBN: 97813480708) به صورت ویدیویی سعی دارد تا با طرح مفاد آموزشی به صورت سناریوهای واقعی، همه مواردی را که برای آزمون CCNA نیاز دارید در اختیارتان قرار دهد. این منبع آموزشی شامل بیش از ۳۰۰ فیلم و با زمان بیش از ۲۵ ساعت می‌باشد. این منبع آموزشی به همراه یک مجموعه ارزشمند از تست‌های آمادگی آزمون می‌باشد.

کتاب Wendell Odom and Sean Wilkins شامل بیش از ۴۰۰ مورد سناریوی آزمایشگاهی مربوط به آزمون CCNA Routing and Switching 2001-125 Network Simulator (ISBN: 9780789757760) می‌باشد. سناریوهای ارائه شده به طور کامل و دقیق در فصل‌های مختلف کتاب ارائه شده‌اند.

شبکه آموزشی سیسکو

اگر هیچیک از موارد فوق را مورد استفاده قرار نداده‌اید، می‌توانید در شبکه آموزشی سیسکو در آدرس http://learningnetwork.cisco.com ثبت نام کنید. حامی این سایت سیسکو می‌باشد. این شبکه

آموزشی به صورت یک شبکه اجتماعی رایگان در اختیار افراد متخصص و کسانی است که می‌خواهند دانش خود را در زمینه فناوری‌های مربوط به سیسکو ارتقا دهند.

اکنون پرسش مهم این است که کدامیک از این منابع را باید تهیه کرد؟ پاسخ به این پرسش بستگی به میزان بودجه در نظر گرفته شده برای آن دارد. اگر محدودیتی ندارید توصیه من این است که همه منابع را تهیه کنید. اما اگر محدودیت بودجه دارید بهتر است که یکی از منابع اصلی و یکی از منابع کمکی (مانند Wendell Odom's Certification library and Scott Empson's command guide) را تهیه کنید.

اهداف و روش‌ها

هدف اصلی از این کتاب ارائه یک خلاصه کامل از موضوعات مربوط به آزمون CCNA می‌باشد. در عناوین در نظر گرفته شده برای هر روز سعی شده است که هر یک از مفاهیم مورد نظر با قالب و ساختار زیر ارائه شود:

- برای مطالب هر روز از کتاب عنوانی دقیق و جامع مبتنی بر مطالب همان روز در نظر گرفته شده است.
- هر روز، یک یا چند عنوان از مفاد آزمون CCNA 200-101 را پوشش می‌دهد.
- در پایان هر روز با ارائه منابع آموزشی مرتبط با محتوای آن سعی شده است تا در صورت نیاز، امکان دسترسی به محتوای کامل و جامع مورد نظر برای خواننده فراهم شود.

کتاب در ۳۱ روز پیکربندی شده است که از روز سی و یکم به سمت روز یکم که در نزدیکی زمان آزمون CCNA قرار دارد، کاهش می‌یابد.

چه کسی باید این کتاب را مطالعه کند؟

هر کسی که خود را آماده شرکت در آزمون CCNA 200-125 کرده است و کسانی که قصد مرور بر مفاد آزمون CCNA را دارند؛ این افراد یا قصد شرکت مجدد و دریافت مجدد مدرک به‌روز شده CCNA را دارند و یا آزمون CCNA یکی از پیش‌نیازهای مدرکی است که قصد دریافت آن را دارند.

آشنایی با آزمون CCNA 200-125

آزمون کنونی CCNA تغییراتی کرده است که در ماه می سال ۲۰۱۶ اعلان شده است، سیسکو آزمون CCNA را در دو بخش (100-105) ICDN1 و (200-105) ICDN2 و یا یک آزمون جامع (200-125) CCNA ارائه کرده است. برای گذراندن آزمون و دریافت مدرک آن، یا باید در آزمون ICDN1 و ICDN2 شرکت کنید و یا اینکه تنها در آزمون CCNA شرکت نمایید. با گذراندن موفق آزمون‌های ذکر شده می‌توانید مدرک CCNA Routing and Switching (R & S) را دریافت کنید. شرکت در دو آزمون، امکان آماده‌سازی ساده‌تر را برای متقاضیان مدرک CCNA فراهم می‌کند. افرادی که دارای تجربه و توانایی کافی می‌باشند، می‌توانند با شرکت و کسب موفقیت در آزمون CCNA (200-125) مدرک مربوط به آن را سریع‌تر و با هزینه کمتر کسب کنند. به همین دلیل تمرکز مطالب و مباحث در نظر گرفته شده در این کتاب، بر روی عناوین و سرفصل‌های آزمون CCNA 200-125 می‌باشد.

در حال حاضر آزمون CCNA از ۵۰ تا ۶۰ سؤال تشکیل شده است که متقاضی باید آن‌ها را در مدت ۹۰ دقیقه پاسخ دهد. با استفاده از مراحل زیر می‌توانید به خودآموز آزمون و همچنین شرحی در بیان شرایط و نحوه برگزاری آزمون مورد نظر دسترسی پیدا کنید:

مرحله نخست: به سایت http://www.vue.com.cisco مراجعه کنید.
مرحله دوم: در این سایت به دنبال لینکی مربوط به خودآموز آزمون (certification tutorial) بگردید. این لینک هم اینک در سمت راست سایت و در بخشی با عنوان "Related Links" قرار دارد.
مرحله سوم: بر روی لینک "Certification Tutorial" کلیک کنید.

در آزمون CCNA با سؤال‌های متنوعی روبرو خواهید شد. هر یک از آنها به صورت انفرادی نمایش داده می‌شوند و باید پیش از مشاهده سؤال بعدی به آن پاسخ دهید. در آزمون CCNA امکان بازگشت به سؤالات پیشین و تغییر در پاسخ آنها داده نمی‌شود. سؤالات آزمون از انواع قالب‌های زیر تشکیل شده است:

- Multiple choice
- Fill in the blank
- Drag and drop
- Testlet
- Simlet
- Simulation

سؤالات چند گزینه‌ای (multiple-choice) از یک سؤال به همراه چند گزینه به عنوان پاسخ آن تشکیل شده است، تعداد پاسخ‌های صحیح برای هر سؤال در آزمون مشخص می‌شود و از انتخاب گزینه‌های کمتر و یا بیشتر از تعداد تعیین شده جلوگیری می‌شود.

در سؤال پر کردن جای خالی (Fill-in-the-blank) باید جای خالی موجود در متن سؤال را با یک عدد و یا واژه پر کنید، جز در مواردی که پاسخ مربوط به دستورات سیسکو نباشد (الزاما باید با حروف کوچک وارد شوند)، ورود عبارت با حروف کوچک و یا بزرگ فرقی نمی‌کند.

سؤالات انتقال و جابجایی (Drag-and-drop) به گونه‌ای طراحی شده‌اند که باید گزینه مورد نظر را از بین گزینه‌های ارائه شده با استفاده از ماوس به محل مورد نظر منتقل کنید. در برخی موارد این نوع سؤال به شکلی طراحی می‌شود که باید پنج گزینه ارائه شده را به ترتیب صحیح مرتب کنید.

سؤالات Testlets از یک سناریوی کلی و چندین سؤال چند گزینه‌ای در ارتباط با همان سناریو تشکیل شده‌اند. در صورتی‌که با موضوع و مفهوم سناریوی مطرح شده آشنایی کامل داشته باشید، می‌توانید چندین سؤال را به راحتی پاسخ داده و امتیاز مربوط به آنها را کسب کنید.

سؤالات Simlets شبیه به سؤالات Testlets می‌باشند، در این نوع سؤالات یک سناریو به همراه چندین سؤال چند گزینه‌ای ارائه می‌شوند. در اینها از یک محیط شبیه‌ساز استفاده می‌شود که با استفاده از آن می‌توانید اجرای دستورات سیسکو را شبیه‌سازی کنید. همچنین از فرمان show برای مشاهده نتیجه دستورات وارد شده استفاده می‌شود.

در سؤالات شبیه‌سازی شده، از یک شبیه‌ساز شبکه نیز استفاده می‌شود که با استفاده از آن عملیاتی نظیر پیاده‌سازی شبکه و یا رفع اشکال شبکه موجود مطرح می‌شود. در این نوع، هدف تنظیم و پیکربندی سوئیچ‌ها و یا روترهای موجود در ساختار شبکه موجود می‌باشند. سپس بر اساس تنظیمات و پیکربندی‌های انجام شده از سؤال مزبور امتیاز کسب خواهید کرد. نوع جدیدتر سؤالات در این گروه از رابط کاربری گرافیکی برای ارائه

محیط شبیه‌سازی شده استفاده می‌شود. این رابط گرافیکی شبیه به آنچه که در روترهای Linksys و یا Cisco Security Device Manager وجود دارند، می‌باشد.

عناوین و سرفصل های آزمون CCNA

در جدول زیر عناوین و ارزش وزنی (تعداد تست) هر یک از موضوعات مربوط به آزمون CCNA 200-125 نشان داده شده است:

Domain	% of Examination
1.0 Network Fundamentals	15%
2.0 LAN Switching Technologies	21%
3.0 Routing Technologies	23%
4.0 WAN Technologies	10%
5.0 Infrastructure Services	10%
6.0 Infrastructure Security	11%
7.0 Infrastructure Management	10%

درباره مترجم

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در حدود ۱۰ سال است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و فضای مجازی و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت دارم که حاصل آن مدارک بین المللی متعددی در حوزه شبکه، امنیت شبکه و تست نفوذ به شرح زیر می‌باشد:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW Security Professional, ISO27001 Lead Auditor, MCP - Microsoft Certified Professional (2016), MCT – Microsoft Certified Trainer

در صورت نیاز به برقراری ارتباط با من می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com

روز ۳۱

مدل‌های شبکه و تجهیزات و اجزا

سرفصل‌های مربوط به آزمون CCNA 200-125

- مشخصات و مقایسه مدل‌های OSI و TCP/IP
- مشخصات و مقایسه پروتکل‌های TCP و UDP
- تأثیر اجزای ساختاری شبکه در شبکه سازمانی
- مشخصات و مقایسه معماری گسترده و سه لایه
- مشخصات و مقایسه توپولوژی‌های شبکه
- انتخاب نوع مناسب کابل شبکه بر اساس نیازهای پیاده‌سازی

نکات کلیدی

هر دو ساختار OSI[1] و TCP/IP[2] برای درک مفاهیم و عملکرد شبکه از اهمیت زیادی برخوردار می‌باشند. امروز قصد داریم تا عملکرد لایه‌های موجود در ساختارهای مورد نظر را برای پردازش داده‌ها به منظور انتقال بین مبدأ و مقصد بررسی کنیم. همچنین، زمانی را نیز برای بررسی پروتکل‌های TCP[3] و UDP[4] اختصاص خواهیم داد. در انتهای روز نیز به تجهیزاتی که در شبکه‌های امروزی مورد استفاده قرار می‌گیرند و رسانه‌های ارتباطی آنها و انواع توپولوژی‌های شبکه می‌پردازیم.

نکته: برنامه امروز کمی بلند به نظر خواهد آمد. البته با توجه به شناخت مبانی شبکه، امروز با اغلب موارد آشنایی قبلی دارید. بنابراین توصیه می‌کنیم مطالب امروز را مرور کنید و به مواردی تمرکز کنید که نیاز به مطالعه بیشتر دارند.

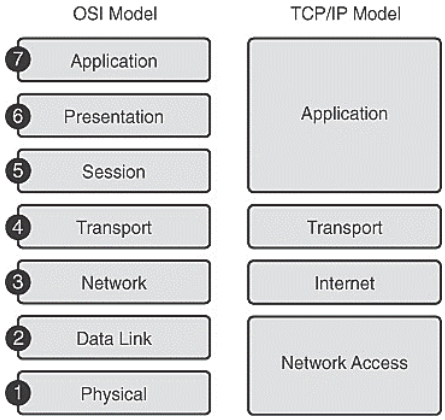
---

[1] Open System Interconnection
[2] Transport Control Protocol/Internet Protocol
[3] Transport Control Protocol
[4] User Datagram Protocol

مدل‌های OSI و TCP/IP

برای درک دقیق چگونگی انتقال داده‌ها در شبکه، از مدل‌های ساختاری لایه‌ای در شبکه برای بیان مفاهیم و فناوری‌های موجود استفاده می‌شود. مدل‌های لایه‌ای نظیر OSI و TCP/IP از جمله مواردی هستند که در برندهای مختلف برای تبادل ترافیک شبکه مورد استفاده قرار می‌گیرند.

مدل OSI در اصل به عنوان ابزاری برای شرح مفاهیم شبکه و اشکال‌یابی آن مورد استفاده قرار می‌گیرد و پروتکل‌های موجود در مدل TCP/IP به منظور تعیین نوع و چگونگی عملکرد شبکه، مورد استفاده قرار می‌گیرند. با توجه به اینکه هر دو مدل از اهمیت زیادی برخوردار می‌باشند، بنابراین باید با لایه‌های مختلف موجود و عملکرد آنها و همچنین انطباق بین لایه‌های موجود در آنها آشنایی کامل داشته باشید. در شکل زیر لایه‌های مورد نظر به‌طور خلاصه نمایش داده شده‌اند.



موارد زیر از بروز تداخل در استفاده از مدل‌های بالا جلوگیری می‌کنند:

- زمانی‌که در مورد عملکرد لایه‌های موجود در مدل شبکه صحبت می‌کنیم، منظورمان مدل OSI می‌باشد.
- زمانی که در مورد پروتکل‌های شبکه صحبت می‌کنیم، منظورمان مدل TCP/IP می‌باشد.

در ادامه به شرح مختصر لایه‌های OSI و همچنین پروتکل‌های TCP/IP می‌پردازیم.

لایه‌های OSI

در جدول زیر لایه‌های OSI به صورت خلاصه نشان داده شده‌اند و در مورد هر یک توضیحات مختصری ارائه شده است.

لایه	شرح عملکرد
کاربرد (Application) (۷)	رابط میان شبکه و نرم‌افزارهای کاربردی می‌باشد. در این لایه، سرویس‌های تائید هویت نیز قرار دارند.
ارائه (Presentation) (٦)	ساختار و قالب ارائه اطلاعات مشخص می‌شوند. عملیات رمزنگاری نیز در این لایه انجام می‌شوند.
دیدگاه (Session) (۵)	ایجاد و نگهداری نشست ارتباطی بین دو نقطه در شبکه را بر عهده دارد. در این بخش مدیریت تبادل پیام‌ها انجام می‌شود.
انتقال (Transport) (۴)	در این لایه خدمات ارتباطی مختلف بین ایستگاه‌های کاری در شبکه ارائه می‌شود. در این لایه عملیات ایجاد و خاتمه ارتباط کنترل جریان ترافیک و تشخیص خطا و تقسیم‌بندی داده‌های بزرگ انجام می‌شود.
شبکه (Network) (۳)	آدرس‌دهی منطقی و مسیریابی و تشخیص مسیر
انتقال داده (Data link) (۲)	بر اساس نوع رسانه ارتباطی، بسته‌های ترافیکی با قالب مورد نظر آماده می‌شوند. قوانین استفاده از رسانه مورد نظر تعریف و مدیریت می‌شوند. در این بخش ابزارهای مورد نیاز برای شناسایی و مدیریت خطاها نیز قرار دارند.
فیزیکی (Physical) (۱)	در بخش تبدیل بسته‌های ترافیکی به سیگنال‌های الکتریکی و یا امواج نوری و یا امواج رادیویی، بر حسب نوع رسانه مورد استفاده در شبکه انجام می‌شود.

عبارت زیر که کلمات آن از حروف ابتدای نام هر یک از لایه‌های موجود در مدل OSI تشکیل شده‌است، می‌تواند در به خاطر سپردن نام لایه‌های مدل OSI بسیار مفید باشد:

All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing

پروتکل‌ها و لایه‌های مدل TCP/IP

مدل TCP/IP چهار عمکرد اصلی که در انتقال ترافیک در شبکه باید انجام شود را شرح می‌دهد. اغلب مدل‌های پروتکل‌های موجود در آن با توجه به برند مشخصی تعریف می‌شوند، زیرا مدل TCP/IP دارای استاندارد باز بوده و یک شرکت نمی‌تواند تعریف پروتکل‌های موجود در آن مدل را در کنترل خود درآورد.

در جدول زیر لایه‌های TCP/IP و عملکرد هر یک از آنها به همراه پروتکل‌های متداول در هر یک از لایه‌ها نشان داده شده است.

لایه TCP/IP	عملکرد	پروتکل های نمونه
برنامه کاربردی (Application)	ارائه داده‌های مورد نیاز کاربر و کنترل ارتباط کاربر	DNS, Telnet, SMTP, POP3, IMAP, DHCP, HTTP, FTP, SNMP
انتقال (Transport)	پشتیبانی ارتباط بین تجهیزات مختلف در شبکه‌های گوناگون را بر عهده دارد.	TCP, UDP
اینترنت (Internet)	ارائه بهترین مسیر ارتباطی در شبکه را بر عهده دارد.	IP, ARP, ICMP
دسترسی شبکه (Network access)	کنترل تجهیزات سخت‌افزاری و رسانه‌های ارتباطی در شبکه را بر عهده دارد.	Ethernet, Frame Relay

در روزهای آینده به جزئیات بیشتری از هر یک از پروتکل‌ها خواهیم پرداخت، اکنون شرح مختصری از پروتکل‌های اصلی TCP/IP را ارائه می‌دهیم:

- **Domain Name System (DNS):** آدرس متناظر با یک وب سایت و یا نام دامنه را برای برقراری ارتباط با آن در اختیار قرار می‌دهد.
- **Telnet:** به راهبران امکان برقراری ارتباط از راه‌دور به میزبان مورد نظر را می‌دهد.
- **Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3), Internet Message Access Protocol (IMAP):** با استفاده از این پروتکل‌ها، عملیات مربوط به ارسال و دریافت و مدیریت ایمیل‌ها انجام می‌شوند.
- **Dynamic Host Configuration Protocol (DHCP):** به کاربران آدرس‌های مورد نیازشان را به صورت پویا تخصیص می‌دهد.
- **Hypertext Transfer Protocol (HTTP):** این پروتکل برای انتقال ترافیک بین کاربران و سرویس دهنده‌های شبکه وب مورد استفاده قرار می‌گیرد.
- **File Transfer Protocol (FTP):** با استفاده از این پروتکل عملیات ارسال و دریافت فایل بین سرویس دهنده و سرویس گیرنده انتقال فایل (FTP) مدیریت می‌شود.
- **Simple Network Management Protocol (SNMP):** با استفاده از این پروتکل، سیستم‌های مدیریت شبکه امکان برقراری ارتباط با تجهیزات موجود در شبکه را خواهند داشت.
- **Transmission Control Protocol (TCP):** این پروتکل با پشتیبانی از ارتباط‌های مجازی بین ایستگاه‌های کاری در شبکه، انتقال مطمئن داده‌ها بین آنها را تضمین می‌کند.

- **User Datagram Protocol (UDP):** با استفاده از این پروتکل انتقال سریع و غیر مطمئن داده‌ها بین میزبان‌ها در شرایطی که زمان انتقال اهمیت داشته باشد، انجام می‌شود.
- **Internet Protocol (IP):** برای تبادل ترافیک بین ایستگاه‌های موجود در شبکه، به آنها یک آدرس منحصر به فرد تخصیص می‌دهد.
- **Address Resolution Protocol (ARP):** با استفاده از IP آدرس، امکان دسترسی به آدرس فیزیکی (Mac Address) میزبان مورد نظر را فراهم می‌سازد.
- **Internet Control Message Protocol (ICMP):** برای ارسال پیام‌های کنترل و خطا و همچنین تست ارتباط و در دسترس بودن سرویس‌های شبکه مورد استفاده قرار می‌گیرد.
- **Ethernet:** با استفاده از پروتکل‌های موجود در آن، امکان استفاده از اغلب استانداردهای بسته‌بندی و انتقال بسته‌های ترافیکی در رسانه‌های ارتباطی شبکه را خواهیم داشت.

فعالیت: تناظر لایه‌های موجود در مدل‌های OSI و TCP/IP را مشخص کنید.

PDU و بسته‌بندی داده‌ها

پس از اینکه هر یک از کاربردهای موجود در شبکه، ترافیک خود را به لایه‌های موجود در مدل OSI ارسال کردند تا توسط رسانه شبکه منتقل شود، در هر یک از لایه‌های موجود در مدل موردنظر، پروتکل‌ها و اطلاعات مشخصی بر روی ترافیک مورد نظر اعمال می‌شوند که به آن‌ها بسته‌بندی (Encapsulation) می‌گویند. ساختار داده‌ای که در هر یک از لایه‌ها ایجاد می‌شود را PDU (Protocol Data Unit) می‌نامند. در جدول زیر PDU مربوط به هر یک از لایه‌های مدل OSI نشان داده شده‌اند:

OSI Layer	PDU
Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data link	Frame
Physical	Bits

در زیر مراحل کلی در روند انتقال ترافیک بین مبدأ و مقصد مورد نظر در شبکه ارائه شده است:

۱- در ایستگاه مبدأ و در لایه کاربردی، داده مورد نظر توسط برنامه کاربردی ایجاد می‌شود.
۲- داده مورد نظر در حین عبور از لایه‌ها و پروتکل‌های موجود در ایستگاه مبدا، تقسیم و بسته‌بندی می‌شود.
۳- داده مورد نظر در پایین‌ترین بخش و لایه مدل OSI، با استفاده از رسانه شبکه منتقل می‌شود.
٤- با استفاده از رسانه و تجهیزات ارتباطی موجود در شبکه مورد نظر، داده مورد نظر در شبکه منتقل می‌شود.

۵- ایستگاه مقصد، ترافیک ارسالی را توسط پایین‌ترین لایه در مدل OSI دریافت می‌کند.
٦- بسته‌های ترافیکی دریافتی در حین حرکت در لایه‌های بالاتر، از حالت بسته‌بندی خارج شده و به شکل اولیه خود تبدیل می‌شوند.
۷- در نهایت ترافیک دریافتی در بالاترین لایه به برنامه کاربردی مورد نظر در ایستگاه مقصد منتقل می‌شود.

لایه کاربردی مدل TCP/IP

لایه کاربردی (Application) در مدل TCP/IP رابطی بین برنامه‌های کاربردی نظیر مرورگر وب و شبکه می‌باشد. مراحل ارسال درخواست و دریافت پاسخ مربوط به یک صفحه وب در زیر آورده شده است:

۱. درخواست HTTP ارسال می‌شود، این درخواست شامل دستورالعمل "get" برای فایل مورد نظر (به‌طور معمول صفحه اول وب‌سایت مورد نظر می‌باشد) است.
۲. پاسخ درخواست از طریق وب سرور به صورت بسته‌ای که در عنوان آن کد مشخصی قرار دارد، نظیر ۲۰۰ (درخواست موفقیت‌آمیز بود و پاسخ آن ارسال شد) و یا ۴۰۴ (صفحه مورد نظر یافت نشد)، ارسال می‌شود.

درخواست‌ها و پاسخ‌های HTTP در عنوان بسته‌های ترافیکی قرار می‌گیرند. محتوای عنوان بسته‌ها به لایه‌های برنامه کاربردی در مبدأ و مقصد ترافیک امکان برقراری ارتباط و تبادل اطلاعات مورد نیاز را می‌دهند. صرف‌نظر از پروتکل‌های لایه کاربردی (... ,HTTP, FTP, DNS)، عملیاتی که برای برقراری ارتباط و تبادل ترافیک در این لایه انجام می‌شود، مشابه و یکسان می‌باشند.

لایه انتقال در مدل TCP/IP

لایه انتقال، با استفاده از پروتکل TCP، مکانیزمی را برای تبادل مطمئن داده‌ها در شبکه فراهم می‌سازد. پروتکل TCP از امکان بازیابی خطا در لایه کاربردی پشتیبانی می‌کند. این پروتکل برای ایجاد اطمینان در ارسال درخواست، مراحل زیر را در مرحله درخواست داده‌های مربوط به صفحه وب مثال بالا اضافه می‌کند:

۱. کاربر وب درخواست HTTP خود را برای وب سرور مورد نظر به لایه انتقال (Transport) ارسال می‌کند.
۲. در این لایه بخش عنوان درخواست HTTP با محتوای مربوط به پروتکل TCP مقدارگذاری می‌شود. در این محتوا شماره گذرگاه مقصد برای پروتکل HTTP نیز مشخص شده‌است.
۳. لایه‌های پایین‌تر، بسته ترافیکی مورد نظر را پردازش کرده و آن را به وب‌سرور ارسال می‌کنند.
۴. وب‌سرور درخواست مورد نظر را دریافت می‌کند و اعلان دریافت (TCP Acknowledgement) آن را به کاربر وب ارسال می‌کند.
۵. وب سرور پاسخ HTTP را به لایه انتقال مربوط به خود ارسال می‌کند.
۶. در این لایه در بخش عنوان بسته ترافیکی، محتوای مربوط به پروتکل TCP مقدارگذاری می‌شود.

۷. لایه‌های پایین‌تر، بسته مورد نظر را پردازش کرده و آن را به کاربر وب درخواست کننده ارسال می‌کنند.
۸. کاربر وب، اعلان دریافت پاسخ را به وب سرور ارسال می‌کند.

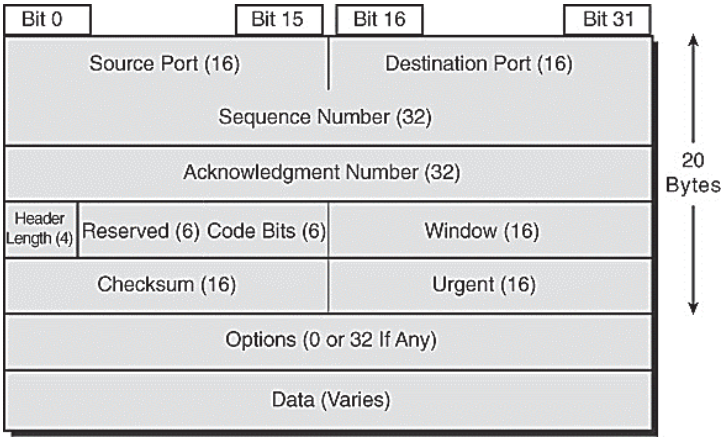
اگر بسته ترافیکی در یکی از مراحل ارائه شده بالا گم شود، پروتکل TCP وظیفه بازیابی آن را بر عهده دارد. در این شرایط پروتکل HTTP در لایه کاربردی، هیچگونه نقشی در بازیابی خطا ندارد.

افزون بر پروتکل TCP، در لایه انتقال از پروتکل UDP نیز استفاده می‌شود، این پروتکل بدون کنترل برقراری ارتباط و به صورت غیرقابل اعتماد داده‌های مورد نظر را منتقل می‌کند و معمولا در شرایطی استفاده می‌شود که نیازی به بازیابی خطا نداشته باشیم. در جدول زیر ویژگی‌های اصلی پروتکل‌های لایه انتقال آورده شده است. هر دو پروتکل TCP و UDP از نخستین کارآیی پشتیبانی می‌کنند، و تنها پروتکل TCP بقیه موارد ارائه شده در جدول را پشتیبانی می‌کند.

عملیات	شرح
تسهیم با استفاده از پورت	با استفاده از پورت مقصد، نرم‌افزار کاربردی مورد نظر برای دریافت ترافیک را مشخص می‌کند.
تشخیص خطا (اعتمادسازی)	با استفاده از فیلدهای اطلاعاتی موجود در عنوان بسته‌های ترافیکی عملیات شماره‌گذاری و کنترل دریافت بسته‌های ترافیکی در مقصد را انجام می‌دهد.
کنترل جریان ترافیک با استفاده از پنجره‌های لغزنده	با استفاده از فناوری پنجره‌های لغزنده و تعیین اندازه آن بین فرستنده و گیرنده، کنترل و مدیریت جریان ترافیک را از طریق ارتباط‌های مجازی بین آنها انجام می‌دهد. اندازه پنجره لغزنده، میزان حداکثر داده‌ای که فرستنده تا پیش از دریافت اعلام وصول می‌تواند ارسال کند را تعیین می‌کند.
ایحاد و خاتمه ارتباط	در این بخش عملیات تعیین و شناسایی پورت‌های ارتباطی و شماره‌گذاری بسته‌های ترافیکی و اعلام وصول آنها در مبدا و مقصد انجام می‌شود.
بسته‌بندی و انتقال داده‌های درخواستی	جریان پیوسته داده‌های ترافیکی را از لایه‌های بالاتر دریافت می‌کند و آنها را به بسته‌های ترافیکی تبدیل می‌کند و بسته‌های ترافیکی دریافتی را به جریانی پیوسته از بایت‌ها تبدیل می‌کند و آنها را به لایه‌های بالاتر ارسال می کند.

عنوان TCP

پروتکل TCP قابلیت بازیابی خطا را دارد، اما برای انجام این کار نیاز به ارسال بسته‌های ترافیکی و انجام مراحل بیشتر نسبت به پروتکل UDP دارد. هر دو پروتکل TCP و UDP قابلیت انتقال ترافیک مبتنی بر IP را بین مبدأ و مقصد مورد نظر دارند. پروتکل TCP امکان انتقال بسته‌های ترافیکی مربوط به برنامه‌های کاربردی موجود در لایه کاربردی را بین فرستنده و گیرنده مورد نظر فراهم می‌کند. برای ارائه همه خدمات مربوط به TCP، این پروتکل از فیلدهای مختلفی در بخش عنوان بسته ترافیکی استفاده می‌کند (شکل زیر):



شماره‌های گذرگاه

دوفیلد نخست در عنوان TCP مربوط به شماره گذرگاه‌های مبدأ و مقصد ترافیک مورد نظر می‌باشند، این دوفیلد هم‌چنانکه در ادامه فصل به آن اشاره خواهد شد، برای پروتکل UDP نیز مورد استفاده قرار می‌گیرند. با استفاده از شماره گذرگاه می‌توانیم گذرگاه‌های موجود را برای انتقال ترافیک مربوط به چندین برنامه کاربردی تسهیم کنیم. هم‌اکنون مرورگرهای وب امکان مرور چندین صفحه وب را به‌طور همزمان پشتیبانی می‌کنند. زمانی که یک صفحه وب جدید را در مرورگر باز می‌کنید، پروتکل TCP در عنوان بسته ترافیکی از یک یا چند گذرگاه جدید استفاده می‌کند. به عنوان مثال، در صورتی‌که پنج صفحه وب را در مرورگر وب باز کرده باشید، شماره گذرگاه مبدأ مربوط به هر یک متفاوت خواهد بود، البته معمولا برای شماره گذرگاه مقصد هر پنج صفحه وب از شماره ۸۰ استفاده می‌شود. بنابراین به این ترتیب پروتکل‌های TCP و UDP امکان برقراری ارتباط و انتقال ترافیک همزمان چندین برنامه کاربردی را از طریق ایستگاه‌کاری مورد نظر فراهم می‌کنند.

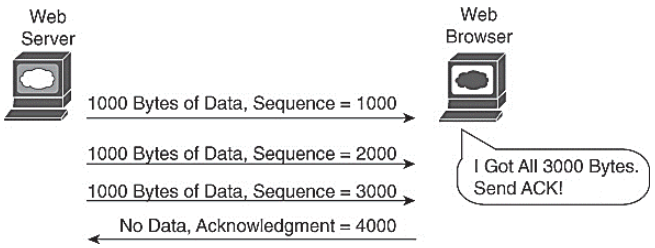
شماره گذرگاه‌های مبدأ که توسط پروتکل‌های TCP و UDP مورد استفاده قرار می‌گیرند، به‌طور پویا از اعداد بین ۱۰۲۴ تا ۶۵۵۳۵ انتخاب می‌شوند. شماره گذرگاه‌های کمتر از ۱۰۲۴ برای استفاده توسط پروتکل‌ها و برنامه‌های کاربردی شناخته شده در نظر گرفته شده‌اند. در جدول زیر اهم این برنامه‌های کاربردی نشان داده شده‌اند.

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	HTTPS (SSL)
16384–32767	UDP	RTP-based voice (VoIP) and video

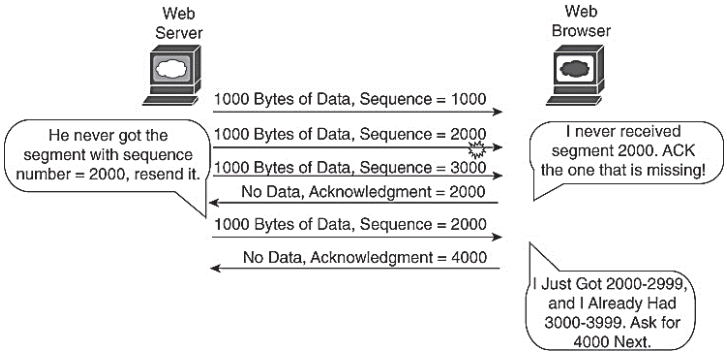
بازیابی خطا

این قابلیت معمولا با نام اطمینان‌پذیری (Reliability) نیز نامیده می‌شود، پروتکل TCP قادر است از امکان بازیابی خطا در نشست‌های ارتباطی بین مبدأ و مقصد ترافیک پشتیبانی کند. با استفاده از فیلدهای موجود در عنوان TCP که مراحل مختلف برقراری ارتباط را مشخص می‌کنند، مراحل مختلف برقراری ارتباط و تبادل ترافیک در این پروتکل رصد و کنترل می‌شود، و در صورت بروز خطا، بسته ترافیکی مورد نظر مجددا ارسال می‌شود.

در شکل زیر، فیلد اعلان ارسال شده توسط کاربر وب به سرور می‌گوید که ٤٠٠٠ بایت ارسال شده را دریافت کرده است، این مثال را اعلان مثبت می‌گویند.



در شکل زیر همان سناریوی فوق را در نظر می‌گیریم، اما با این فرض که در آن خطاهایی نیز رخ داده است. در بخش دوم انتقال ترافیک TCP خطایی رخ داده است و بسته ترافیکی گم شده است. بنابراین کاربر وب در بسته اعلان خود به سرور عدد ۲۰۰۰ را ارسال می‌کند. این مثال را اعلان مثبت به همراه درخواست ارسال مجدد بخشی از بسته‌های ترافیکی می‌گویند. در این حالت وب سرور اقدام به ارسال مجدد بسته‌های ترافیکی پس از ۲۰۰۰ می‌کند تا کاربر وب، بسته‌های گم شده را مجددا دریافت کند.



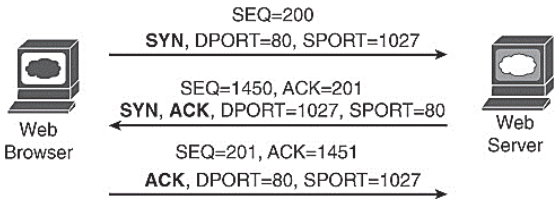
البته در شکل بالا نشان داده نشده است، وب سرور، تایمر انتقال مجدد ترافیک را تنظیم می‌کند و منتظر دریافت اعلان از طرق کاربر وب می‌ماند، این شرایط تنها در زمان گم شدن بسته ترافیکی و انتقال مجدد آن رخ می‌دهد. در صورتی‌که تایمر مورد نظر منقضی شود، وب سرور تمامی بسته‌های ترافیکی مربوط به نشست مورد نظر را مجددا ارسال می‌کند.

کنترل جریان ترافیک

پروتکل TCP با استفاده از فناوری پنجره‌های لغزان (Windowing)، جریان ترافیک را بین مبدأ و مقصد کنترل می‌کند. طرفین ارتباط در ابتدای نشست ارتباطی، اندازه پنجره را با یکدیگر مشخص می‌کنند، سپس در زمان ارتباط اندازه این پنجره می‌تواند با توافق طرفین ارتباط به صورت پویا مجددا تنظیم شود، اندازه این پنجره می‌تواند تا حداکثر ۶۵۵۳۵ بایت افزایش یابد. اندازه پنجره توسط فیلد مربوط به آن در عنوان TCP بسته ترافیکی تعیین می‌شود. پس از ارسال داده‌هایی به اندازه تعیین شده در اندازه پنجره، گیرنده باید اعلان دریافت آنها را به فرستنده ارسال کند تا فرستنده اقدام به ارسال داده‌های بعدی به اندازه پنجره تعیین شده کند.

برقراری و قطع ارتباط

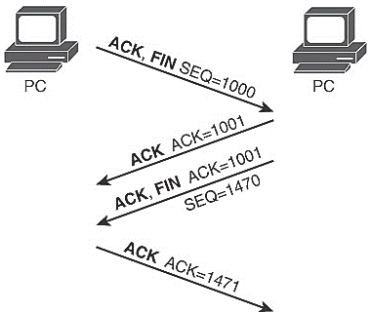
برقراری ارتباط شامل مراحل مربوط به آماده‌سازی فیلدهای ترتیب و اعلان در عنوان TCP بسته ترافیکی و توافق برای اندازه پنجره و گذرگاه‌های ارتباطی بین فرستنده و گیرنده می‌باشد. برقراری ارتباط سه مرحله‌ای، پیش از انتقال داده‌ها بین فرستنده و گیرنده انجام می‌شود (شکل زیر).



در شکل بالا، DPORT و SPORT به ترتیب مشخص کننده گذرگاه‌های مقصد و مبدأ می‌باشند. SEQ شماره ترتیب بسته‌های ترافیکی می‌باشد. عبارت‌های ACK و SYN که به صورت پررنگ‌تر نشان داده شده‌اند، مربوط به فیلدهایی در عنوان TCP بسته‌های ترافیکی می‌باشند که برای برقراری ارتباط مورد استفاده قرار می‌گیرند.

پروتکل TCP مقدار اولیه فیلدهای ترتیب (SEQ) و شماره اعلان (Acknowledgement) را به هر عددی که در اندازه ۴ بایت قرار گیرد، مقدارگذاری می‌کند. بنابراین شماره ترتیب می‌تواند هر عدد ۳۲ بیتی اتفاقی باشد که برای هر نشست جدید تعیین می‌شود. شماره اعلان نیز برای هر نشست از شماره ۱ آغاز می‌شود.

زمانی که انتقال داده‌های مورد نظر به اتمام رسید، مراحل قطع ارتباط در چهار مرحله‌ای که در شکل زیر نشان داده شده است، آغاز می‌شود. در این مرحله از یک flag جدید با نام FIN استفاده می‌شود.



UDP

پروتکل TCP برقراری و قطع ارتباط بین طرفین نشست ارتباطی را بر عهده دارد، این درحالی است که پروتکل UDP این کار را انجام نمی‌دهد. به همین دلیل UDP را پروتکل فاقد ارتباط (Conectionless) می‌نامند. این پروتکل فاقد اطمینان‌پذیری و فناوری پنجره‌های لغزنده برای کنترل جریان ترافیک و همچنین فاقد قابلیت مرتب‌سازی بسته‌های ترافیکی می‌باشد. افزون بر این موارد، پروتکل UDP نمی‌تواند با استفاده از شماره گذرگاه، عملیات تسهیم ترافیک مربوط به برنامه‌های کاربردی مختلف را انجام دهد، البته این پروتکل حجم بسیار کمتری ترافیک سربار بر روی بسته‌های ترافیکی اصلی ایجاد می‌کند و حجم عملیات کمتری در زمان انتقال ترافیک انجام می‌دهد. نرم‌افزارهای کاربردی که از پروتکل UDP استفاده می‌کنند، معمولا در زمان تبادل ترافیک با از دست دادن برخی از بسته‌های ترافیکی مواجه می‌شوند، نظیر ترافیک مربوط به VoIP. در شکل زیر عناوین بسته‌ها در دو پروتکل TCP و UDP با یکدیگر مقایسه شده‌اند.

2	2	4	4	4 bits	6 bits	6 bits	2	2	2	3	1
Source Port	Dest. Port	Sequence Number	Ack. Number	Offset	Reserved	Flags	Window Size	Checksum	Urgent	Options	PAD

TCP Header

2	2	2	2
Source Port	Dest. Port	Length	Checksum

UDP Header

* Unless Specified, Lengths Shown Are the Numbers of Bytes

فعالیت: مشخصات مربوط به پروتکل‌های TCP و UDP را بیان کنید.