



۱. آشنایی با روتر.....	۲۳
۱.۱. خلاصه فصل.....	۲۴
۱.۲. مقدمه.....	۲۴
۱.۳. آشنایی اولیه با روتر.....	۲۵
۱.۴. انواع روترها.....	۲۵
۱.۴.۱. روترهای سخت افزاری.....	۲۶
۱.۴.۲. روترهای نرم افزاری.....	۲۶
۱.۴.۳. روتر به منظور اتصال دو شبکه.....	۲۷
۱.۴.۴. روتر در یک شبکه LAN.....	۲۷
۱.۴.۵. روتر به منظور اتصال دو دفتر کار.....	۲۸
۱.۵. ویژگی‌های یک روتر.....	۲۹
۱.۶. عناصر داخلی روتر.....	۲۹
۱.۶.۱. پردازنده.....	۲۹
۱.۶.۲. حافظه اصلی.....	۲۹
۱.۶.۳. حافظه فلش.....	۳۰
۱.۶.۴. حافظه NVRAM.....	۳۰
۱.۶.۵. گذرگاه‌ها.....	۳۰
۱.۶.۶. حافظه ROM.....	۳۱
۱.۶.۷. منبع تغذیه.....	۳۱
۱.۷. آشنایی با اینترنت‌های روتر.....	۳۱
۱.۷.۱. انواع اینترنت‌های روتر.....	۳۳
۱.۸. انواع کابل در شبکه‌های کامپیوتری.....	۳۴

۱۸.۱	کابل های چهار زوجی	۳۴
۱۸.۲	مشخصه های کابل UTP	۳۵
۱۸.۳	کابل کواکسیال	۳۶
۱۸.۴	فیبر نوری	۳۷
۱.۹	پیکربندی روتر با پورت های مدیریت	۳۷
۱.۹.۱	نحوه اتصال به پورت کنسول روتر	۳۷
۱.۱۰	راه اندازی اولیه روتر	۳۹
۱.۱۱	چراغ های Leds	۴۱
۱.۱۲	راه اندازی سیستم و نمایش پیام ها	۴۱
۱.۱۲.۱	نمایش پیام عدم پیکربندی	۴۱
۱.۱۳	سری ها و مدل های مسیراب های سیسکو	۴۲
۱.۱۳.۱	معرفی روتر ۵۳۰۰ سیسکو	۴۲
۱.۱۳.۲	مدل Cisco36XX	۴۵
۱.۱۳.۳	مدل Cisco5350	۴۵
۱.۱۳.۴	مدل Cisco1750	۴۶
۱.۱۳.۵	مدل Ciscovg200	۴۶
۱.۱۴	نتیجه گیری	۴۸
۱.۱۵	پرسش و تحقیق	۴۸
۱.۱۶	منابع و مراجع	۴۹
۲	پیکربندی روترهای سیسکو	۵۲
۲.۱	خلاصه بخش	۵۲
۲.۲	مقدمه	۵۲
۲.۳	پیکربندی اولیه روتر	۵۳
۲.۳.۱	اجرای برنامه Hyperterminal	۵۴
۲.۳.۲	انتخاب یک نام برای Hyperterminal Session	۵۴
۲.۳.۳	انتخاب اینترفیس ارتباطی کامپیوتر	۵۴
۲.۳.۴	مشخص نمودن خصایص اینترفیس ارتباطی	۵۵
۲.۴	اتصال به روتر	۵۶
۲.۴.۱	پورت Console	۵۶
۲.۴.۲	پورت Auxiliary	۵۷

۵۷	پورت Telnet	۲.۴.۳
۵۷	پروتکل TFTP	۲.۴.۴
۵۷	مرورگر وب	۲.۴.۵
۵۸	حالات متفاوت رابط کاربر روتر	۲.۵
۵۸	انواع مدهای دسترسی	۲.۶
۵۸	مد کاربر	۲.۶.۱
۵۸	Router >	۲.۶.۲
۵۸	دستور HELP	۲.۶.۳
۵۹	Router> ?	۲.۶.۴
۵۹	مد دسترسی	۲.۶.۵
۵۹	Router > Enable	۲.۶.۶
۶۰	Router#	۲.۶.۷
۶۰	Router # Exit	۲.۶.۸
۶۰	مد پیکربندی	۲.۶.۹
۶۰	Router# Configure Terminal	۲.۶.۱۰
۶۱	پیکربندی نام برای روتر	۲.۶.۱۱
۶۱	ذخیره کردن تنظیمات	۲.۷
۶۱	پیکربندی رمز عبور روتر	۲.۸
۶۲	پسورد دسترسی	۲.۸.۱
۶۲	پسورد امنیتی	۲.۸.۲
۶۲	پسورد Telnet	۲.۸.۳
۶۳	پسورد پورت Console	۲.۸.۴
۶۳	پسورد پورت AUX	۲.۸.۵
۶۴	ویژگیهای یک شبکه WAN	۲.۹
۶۴	اتصال اینترنتیهای WAN	۲.۹.۱
۶۵	استفاده از اینترنتی WAN	۲.۹.۲
۶۵	اتصال روتر به شبکه LAN	۲.۱۰
۶۶	تنظیمات اینترنتی Serial	۲.۱۱
۶۷	تنظیمات Ethernet و Fast Ethernet	۲.۱۲
۶۷	فعال و غیرفعال کردن یک اینترنتی	۲.۱۳
۶۸	معرفی IP Address	۲.۱۴

۶۸	۲.۱۴.۱ آدرس دهی به اینترنت روتر
۶۹	۲.۱۵. متداولترین دستورات Show
۷۰	۲.۱۶. مسیریابی
۷۱	۲.۱۶.۱. مسیریابی چیست؟
۷۲	۲.۱۶.۲. معرفی Static Routing و Dynamic Routin
۷۳	۲.۱۷. پروتکل های مسیریابی
۷۴	۲.۱۷.۱. مسیریابی بردار خطی
۷۴	۲.۱۷.۲. مسیریابی شناخت کلی
۷۵	۲.۱۷.۳. مسیریابی ترکیبی
۷۵	۲.۱۸. پروتکل RIP
۷۷	۲.۱۸.۱. راه اندازی پروتکل RIP
۷۷	۲.۱۸.۲. پیکربندی RIP بر روی روتر Router1
۷۸	۲.۱۸.۳. پیکربندی RIP بر روی روتر Router2
۷۸	۲.۱۸.۴. پیکربندی RIP بر روی روتر ROUTER3
۷۸	۲.۱۸.۵. مشاهده جدول Routing Table روترها
۷۹	۲.۱۸.۶. متریک
۸۰	۲.۱۹. پروتکل مسیریابی IGRP
۸۱	۲.۱۹.۱. پیکربندی IGRP
۸۲	۲.۱۹.۲. پیکربندی IGRP در یک مثال
۸۲	۲.۱۹.۳. پیکربندی IGRP بر روی ROUTER 1
۸۲	۲.۱۹.۴. پیکربندی IGRP بر روی ROUTER 2
۸۲	۲.۱۹.۵. پیکربندی IGRP بر روی ROUTER 3
۸۲	۲.۲۰. پروتکل HDLC
۸۳	۲.۲۰.۱. پیکربندی پروتکل HDLC
۸۴	۲.۲۱. پروتکل PPP
۸۵	۲.۲۲. اجزای پروتکل لایه ای
۸۵	۲.۲۳. برقراری یک PPP Session
۸۷	۲.۲۴. تنظیم PPP روی لینک نقطه به نقطه
۸۷	۲.۲۴.۱. پیکربندی پروتکل PPP
۸۷	۲.۲۴.۲. تنظیم Authentication در پروتکل PPP
۸۸	۲.۲۴.۳. مشخص کردن یک نام برای روتر

۸۸	۲.۲۴.۴. مشخص کردن Username و Password
۸۸	۲.۲۴.۵. تنظیمات مربوط به روتر Hamadan
۸۹	۲.۲۴.۶. تنظیمات مربوط به روتر Tehran
۸۹	۲.۲۵. نتیجه گیری
۸۹	۲.۲۶. منابع و مراجع
۹۲	۳. امنیت تجهیزات شبکه
۹۲	۳.۱. خلاصه بخش
	۳.۲. مقدمه ۹۲
۹۳	۳.۳. تدوین سیاست
۹۴	۳.۴. استانداردها و روال‌های امنیتی
۹۴	۳.۵. ساختار سیاست امنیتی
۹۴	۳.۶. امنیت تجهیزات شبکه
۹۵	۳.۷. امنیت فیزیکی
	۳.۷.۱. افزودنی در محل استقرار شبکه ۹۶
	۳.۷.۲. توپولوژی شبکه ۹۶
	۳.۷.۳. محل‌های امن برای تجهیزات ۹۷
	۳.۷.۴. انتخاب لایه کانال ارتباطی امن ۹۷
	۳.۷.۵. منابع تغذیه ۹۸
	۳.۷.۶. عوامل محیط ۹۹
۹۹	۳.۸. امنیت منطقی
	۳.۸.۱. امنیت مسیربازها ۹۹
	۳.۸.۲. مدیریت پیکربندی ۱۰۰
	۳.۸.۳. کنترل دسترسی به تجهیزات ۱۰۰
	۳.۸.۴. امن سازی دسترسی ۱۰۱
	۳.۸.۵. مدیریت رمزهای عبور ۱۰۱
۱۰۱	۳.۹. ملزومات و مشکلات امنیتی ارائه دهندگان خدمات
	۳.۹.۱. قابلیت‌های امنیتی ۱۰۲
	۳.۹.۲. مشکلات اعمال ملزومات امنیتی ۱۰۲
۱۰۲	۳.۱۰. امنیت روترها از طریق پیکربندی
	۳.۱۰.۱. ساخت یک سیاست امنیتی برای یک روتر ۱۰۵

۳.۱۰.۲	ایجاد ارتباط بین شبکه محلی و شبکه خارجی	۱۰۷
۳.۱۰.۳	تغییرات در سیاست‌های شبکه مادر یا شبکه محلی	۱۰۷
۳.۱۰.۴	چک لیست سیاست‌های کلی برای یک روتر	۱۰۷
۳.۱۰.۵	امنیت فیزیکی	۱۰۸
۳.۱۰.۶	امنیت پیکربندی ساکن	۱۰۹
۳.۱۰.۷	امنیت برای پیکربندیهای دینامیک	۱۱۰
۳.۱۰.۸	امنیت در سرویسهای شبکه	۱۱۱
۳.۱۰.۹	توپولوژی شبکه	۱۱۱
۳.۱۱	اقدامات عملی امن کردن روتر	۱۱۳
۳.۱۱.۱	امنیت سخت افزاری یا فیزیکی	۱۱۴
۳.۱۲	نسخه‌های نرم افزاری روترها	۱۱۸
۳.۱۳	پیکربندی روتر و فرمان IOS	۱۲۰
۳.۱۴	نتیجه گیری	۱۲۰
۳.۱۵	پرسش و تحقیق	۱۲۱
۳.۱۶	منابع و مراجع	۱۲۲
۴	امنیت اطلاعات	۱۲۴
۴.۱	خلاصه بخش	۱۲۴
۴.۲	مقدمه ۱۲۴	
۴.۳	اهمیت امنیت اطلاعات و کامپیوترها	۱۲۵
۴.۴	امنیت اطلاعات چیست؟	۱۲۵
۴.۵	سیستم مدیریت امنیت اطلاعات	۱۲۶
۴.۶	چرا به امنیت اطلاعات نیاز داریم؟	۱۲۸
۴.۷	آسیب پذیری سیستم اطلاعاتی و جرایم کامپیوتری	۱۲۸
۴.۸	لایه‌های شبکه‌های نوین	۱۲۹
۴.۸.۱	شبکه بیرونی	۱۳۰
۴.۸.۲	شبکه داخلی	۱۳۰
۴.۸.۳	فاکتور انسانی	۱۳۱
۴.۹	شرایط امنیتی شبکه بیرونی	۱۳۲
۴.۹.۱	Routerهای مرزی	۱۳۲
۴.۹.۲	فایروال	۱۳۲

۴.۹.۳	سنسور IDS	۱۳۲
۴.۹.۴	سرور VPN	۱۳۳
۴.۹.۵	روتر و سویچ	۱۳۳
۴.۱۰	شرایط امنیت شبکه داخلی	۱۳۴
۴.۱۱	نرم افزارهای مهاجمان	۱۳۴
۴.۱۱.۱	ویروس ها	۱۳۴
۴.۱۱.۲	برنامه های اسب تروا	۱۳۵
۴.۱۱.۳	ویرانگران	۱۳۵
۴.۱۱.۴	ره گیری داده	۱۳۶
۴.۱۱.۵	کلاهبرداری	۱۳۶
۴.۱۱.۶	نامه های الکترونیکی ناخواسته	۱۳۶
۴.۱۲	شرایط امنیت فاکتور انسانی	۱۳۷
۴.۱۲.۱	آموزش کاربران	۱۳۷
۴.۱۲.۲	ساختار عملیات	۱۳۸
۴.۱۲.۳	سیاست های قابل اجرا	۱۳۸
۴.۱۳	سیاست امنیتی	۱۳۸
۴.۱۳.۱	بخشهای سند سیاست امنیت اطلاعات	۱۳۹
۴.۱۳.۲	نیاز به امنیت اطلاعات و محدودهی آن	۱۳۹
۴.۱۳.۳	هدف امنیت اطلاعات	۱۴۰
۴.۱۳.۴	تعریف امنیت اطلاعات	۱۴۰
۴.۱۳.۵	تعهد مدیریت در امنیت اطلاعات	۱۴۰
۴.۱۳.۶	تأییدیه سیاست امنیت اطلاعات	۱۴۰
۴.۱۳.۷	هدف سیاست امنیت اطلاعات	۱۴۰
۴.۱۳.۸	اصول امنیت اطلاعات	۱۴۱
۴.۱۳.۹	نقشها و مسئولیتها	۱۴۱
۴.۱۳.۱۰	اقدامات انضباطی	۱۴۱
۴.۱۳.۱۱	بازبینی و کنترل	۱۴۲
۴.۱۳.۱۲	اعلامیه کاربر و تأیید آن	۱۴۲
۴.۱۳.۱۳	ارجاعات	۱۴۲
۴.۱۳.۱۴	عناصر عمومی	۱۴۲
۴.۱۴	پیاده سازی سیاست امنیتی	۱۴۳

۴.۱۴.۱	سیستم‌های عامل و برنامه‌های کاربردی	۱۴۴
۴.۱۴.۲	آنتی ویروس	۱۴۵
۴.۱۴.۳	مقاوم سازی Host	۱۴۵
۴.۱۴.۴	رمزهای عبور	۱۴۵
۴.۱۴.۵	استاندارد سازی	۱۴۶
۴.۱۴.۶	بازبینی امنیت شبکه	۱۴۶
۴.۱۴.۷	روتر و سوئیچ	۱۴۶
۴.۱۴.۸	فایروال	۱۴۶
۴.۱۴.۹	فایروال شخصی	۱۴۷
۴.۱۵	پروتکل SNMP	۱۴۷
۴.۱۶	حملات	۱۴۸
۴.۱۶.۱	حملات شناسائی	۱۴۸
۴.۱۶.۲	حملات دستیابی	۱۴۸
۴.۱۶.۳	حملات از کار انداختن سرویس‌ها	۱۴۹
۴.۱۷	انواع دفاع در شبکه	۱۴۹
۴.۱۷.۱	جلوگیری از IP Spoofing	۱۵۰
۴.۱۷.۲	پیشگیری از Dos	۱۵۰
۴.۱۷.۳	متوقف کردن IP Spoofing خارج شونده	۱۵۱
۴.۱۷.۴	استفاده از Anti Spoofing بر روی Gateway	۱۵۱
۴.۱۷.۵	جلوگیری از حمله Smurf	۱۵۲
۴.۱۷.۶	جلوگیری از طوفان TCP SYN	۱۵۳
۴.۱۷.۷	جلوگیری از حمله LAND Attack	۱۵۳
۴.۱۷.۸	غیر فعال کردن ARP Proxy	۱۵۳
۴.۱۷.۹	جلوگیری از حمله ARP	۱۵۴
۴.۱۷.۱۰	جلوگیری از استفاده ICMP	۱۵۴
۴.۱۷.۱۱	محدود کردن Broadcast	۱۵۵
۴.۱۷.۱۲	جلوگیری از Fragmentation	۱۵۵
۴.۱۷.۱۳	چگونه کار می‌کند Fragmentation	۱۵۶
۴.۱۷.۱۴	مثال Fragmentation	۱۵۶
۴.۱۸	اجرای سیاست امنیت اطلاعات	۱۵۶
۴.۱۸.۱	برنامه آگاه سازی امنیتی	۱۵۷

۱۵۷	هدف از برنامه. ۴.۱۸.۲
۱۵۸	شناخت مخاطبان. ۴.۱۸.۳
۱۵۸	سنجش سطح دانش امنیتی کارکنان. ۴.۱۸.۴
۱۵۸	تشویق کارکنان به رعایت نکات ایمنی. ۴.۱۸.۵
۱۵۹	انتخاب شیوه آموزش. ۴.۱۸.۶
۱۵۹	کاغذ اخبار امنیت اطلاعات. ۴.۱۸.۷
۱۶۰	وب سایت امنیت اطلاعات. ۴.۱۸.۸
۱۶۰	تکنیک "ما به کمک شما نیازمندیم". ۴.۱۸.۹
۱۶۰	جدال‌های آموزشی. ۴.۱۸.۱۰
۱۶۰	مدیریت تهدیدات امنیتی. ۴.۱۸.۱۱
۱۶۱	ارزیابی سیاست امنیتی. ۴.۱۹
۱۶۱	محصول VPC. ۴.۱۹.۱
۱۶۱	محصول Intel Integrated Security Software. ۴.۱۹.۲
۱۶۲	عوامل موفقیت برنامه امنیت اطلاعات. ۴.۲۰
۱۶۳	نتیجه گیری. ۴.۲۱
۱۶۴	پرسش و تحقیق. ۴.۲۲
۱۶۴	منابع و مراجع. ۴.۲۳
۱۶۶	 ۵. پروتکل NAT و VPN
۱۶۶	۵.۱ خلاصه بخش
	۵.۲ مقدمه ۱۶۶
۱۶۷	۵.۳ قابلیت‌های NAT
۱۶۹	۵.۴ مفاهیم اولیه NAT و انواع آن
۱۷۱	۵.۵ انواع NAT
۱۷۱	۵.۵.۱ Static NAT
۱۷۲	۵.۵.۲ Dynamic NAT
۱۷۲	۵.۵.۳ Dynamic NAT With Overload
۱۷۳	۵.۵.۴ Overlapping
۱۷۴	۵.۶ جدول NAT
۱۷۴	۵.۷ نحوه ترجمه آدرس مبدا در NAT
۱۷۵	۵.۸ نحوه پیکربندی Static NAT

۵.۸.۱	فعال کردن Static NAT	۱۷۵
۵.۸.۲	تعیین Inside Interface	۱۷۵
۵.۸.۳	تعیین Outside Interface	۱۷۵
۵.۸.۴	مثال Static NAT	۱۷۶
۵.۹	نحوه پیکربندی Dynamic NAT	۱۷۶
۵.۹.۱	لیست آدرس‌های Valid	۱۷۷
۵.۹.۲	فعال کردن Dynamic NAT	۱۷۷
۵.۹.۳	تعیین Inside Interface	۱۷۸
۵.۹.۴	تعیین Outside Interface	۱۷۸
۵.۹.۵	مثال Dynamic NAT	۱۷۸
۵.۱۰	Nat داینامیک با سر بار	۱۷۹
۵.۱۰.۱	پیکربندی Dynamic NAT With Overload	۱۸۰
۵.۱۰.۲	فعال کردن Dynamic NAT With Overload	۱۸۰
۵.۱۰.۳	تعیین Inside Interface	۱۸۰
۵.۱۰.۴	تعیین Outside Interface	۱۸۱
۵.۱۰.۵	مثال Dynamic NAT With Overload	۱۸۱
۵.۱۱	عملکرد روتر در Dynamic NAT With Overload	۱۸۲
۵.۱۲	پاک کردن رکورد در NAT Table	۱۸۲
۵.۱۳	نمایش اطلاعات مربوط به NAT	۱۸۳
۵.۱۴	عدم رکورد در NAT Table	۱۸۳
۵.۱۵	امنیت ۱۸۳	
۵.۱۶	پیاده سازی NAT در ویندوز سرور ۲۰۰۳	۱۸۴
۵.۱۶.۱	تنظیم NAT	۱۸۵
۵.۱۷	شبکه مجازی VPN	۱۸۶
۵.۱۸	معایب و مزایا	۱۸۹
۵.۱۹	تونل کشی	۱۹۰
۵.۱۹.۱	هویت شناسی	۱۹۲
۵.۱۹.۲	فایروال	۱۹۲
۵.۱۹.۳	رمزنگاری	۱۹۳
۵.۲۰	معماری VPN شبکه‌ی محلی به شبکه‌ی محلی	۱۹۵
۵.۲۰.۱	شبکه‌ی محلی به شبکه‌ی محلی مبتنی بر اینترنت	۱۹۶

۵.۲۰.۲	شبکه‌ی محلی به شبکه‌ی محلی مبتنی بر اکسترانت	۱۹۶
۵.۲۰.۳	میزبان به شبکه‌ی محلی	۱۹۶
۵.۲۰.۴	میزبان به میزبان	۱۹۷
۵.۲۰.۵	تکنولوژی‌های VPN	۱۹۸
۵.۲۱	قراردادهای پیاده‌سازی VPN	۱۹۹
۵.۲۱.۱	رده‌ی بسته‌گرا	۱۹۹
۵.۲۱.۲	رده‌ی کاربردگرا	۱۹۹
۵.۲۱.۳	قراردادهای SSH	۲۰۰
۵.۲۱.۴	قرارداد SOCKS	۲۰۰
۵.۲۲	نتیجه‌گیری	۲۰۱
۵.۲۳	پرسش و تحقیق	۲۰۱
۵.۲۴	منابع و مراجع	۲۰۲
۶	سرور امنیتی AAA	۲۰۴
۶.۱	خلاصه بخش	۲۰۴
۶.۲	مقدمه ۲۰۴	
۶.۳	تایید، شما چه کسی هستید؟	۲۰۵
۶.۳.۱	فعال نمودن Authentication	۲۰۶
۶.۴	مجوز، مجاز به انجام چه کاری هستید؟	۲۰۶
۶.۴.۱	فعال نمودن Authorization	۲۰۸
۶.۵	حسابداری: چه کارهایی را انجام داده‌اید؟	۲۰۸
۶.۵.۱	فعال نمودن Accounting	۲۰۸
۶.۶	مزایای استفاده از AAA	۲۰۹
۶.۷	مفهوم دسترسی	۲۰۹
۶.۸	روش‌های Authentication	۲۱۰
۶.۸.۱	پروتکل PAP	۲۱۰
۶.۸.۲	پروتکل CHAP	۲۱۰
۶.۸.۳	پروتکل MSCHAP	۲۱۱
۶.۸.۴	پروتکل EAP	۲۱۱
۶.۹	استانداردهای AAA سرور	۲۱۱
۶.۹.۱	استاندارد RADIUS	۲۱۱

۶.۹.۲. استاندارد TACACS	۲۱۴
۶.۱۰. نحوه عملکرد مدل AAA	۲۱۴
۶.۱۱. عملکرد پروتکل های TACACS و RADIUS	۲۱۵
۶.۱۲. تصدیق کاربر	۲۱۶
۶.۱۳. مجوز دسترسی	۲۱۶
۶.۱۴. فرآیند تصدیق کاربری AAA	۲۱۷
۶.۱۵. فرآیند اعطای مجوز AAA	۲۱۸
۶.۱۵.۱. مجوز دسترسی TACACS	۲۱۸
۶.۱۵.۲. اخذ مجوز دسترسی توسط پروتکل RADIUS	۲۱۹
۶.۱۶. فرآیند حسابداری AAA	۲۱۹
۶.۱۷. مقایسه TACACS و RADIUS	۲۲۰
۶.۱۸. صفات RADIUS	۲۲۱
۶.۱۹. کلید رمزگذاری	۲۲۲
۶.۲۰. گروه ها و توارث بین آنها	۲۲۲
۶.۲۱. بانک اطلاعاتی کاربران	۲۲۳
۶.۲۱.۱. بانک های اطلاعاتی با ساختار سلسله مراتبی	۲۲۳
۶.۲۲. کنترل دستی اضافه	۲۲۴
۶.۲۳. امکانات اضافی هنگام حالات مشکوک	۲۲۴
۶.۲۴. امکانات اضافی برای حساب کاربران	۲۲۵
۶.۲۴.۱. پیکر بندی AAA برای قطع ارتباط کاربر	۲۲۵
۶.۲۵. قطع ارتباط کاربر	۲۲۶
۶.۲۶. سرویس دهنده کمکی	۲۲۶
۶.۲۷. سیستم پشتیبان	۲۲۶
۶.۲۸. پیکربندی AAA بر روی روتر	۲۲۷
۶.۲۸.۱. هویت سنجی AAA با استفاده از TACACS و RADIUS	۲۲۸
۶.۲۸.۲. پیکر بندی TACACS +	۲۲۹
۶.۲۹. نتیجه گیری	۲۳۱
۶.۳۰. پرسش و تحقیق	۲۳۱
۶.۳۱. منابع و مراجع	۲۳۲
۷. دیوار آتش	۲۳۴

۲۳۴	۷.۱. خلاصه بخش
۲۳۴	۷.۲. مقدمه
۲۳۵	۷.۳. بخشهای شبکه به لحاظ امنیتی
۲۳۵	۷.۳.۱. تجهیزات غیر فعال
۲۳۵	۷.۳.۲. تجهیزات فعال
۲۳۶	۷.۴. قسمتهای شبکه به لحاظ حفاظت امنیتی
۲۳۶	۷.۵. نحوه تقسیم بندی شبکه و مفهوم Firewall
۲۳۷	۷.۵.۱. تعریف Firewalls
۲۳۸	۷.۵.۲. تاریخچه ی Firewalls
۲۳۹	۷.۵.۳. محل قرار گرفتن دیوار آتش
۲۳۹	۷.۶. دسته بندی فایر وال
۲۳۹	۷.۶.۱. فایروال سخت افزاری
۲۴۰	۷.۶.۲. فایروال نرم افزاری
۲۴۰	۷.۶.۳. مزایا و معایب فایروال نرم افزاری
۲۴۱	۷.۶.۴. ترکیب سخت افزار و نرم افزار فایروال
۲۴۱	۷.۶.۵. فایروال NAT ساده
۲۴۲	۷.۶.۶. فایروالهای با ویژگی Stateful Packet Inspection
۲۴۲	۷.۷. انواع Firewallها از نظر عملکرد
۲۴۲	۷.۷.۱. دیواره‌های آتشین فیلترینگ بسته ای
۲۴۴	۷.۷.۲. دیواره آتش فیلترینگ بسته مبتنی بر حالت
۲۴۴	۷.۷.۳. دیواره‌های آتشین پراکسی
۲۴۵	۷.۸. مبانی طراحی دیوار آتش
۲۴۷	۷.۸.۱. لایه اول دیوار آتش
۲۴۸	۷.۸.۲. لایه دوم دیوار آتش
۲۴۹	۷.۸.۳. لایه سوم دیوار آتش
۲۴۹	۷.۹. اجزای جانبی یک دیوار آتش
۲۵۰	۷.۹.۱. واسط محاوره‌ای و ساده ورودی / خروجی
۲۵۰	۷.۹.۲. فایروال NAT
۲۵۱	۷.۹.۳. فیلترینگ پورت‌ها
۲۵۲	۷.۹.۴. ناحیه غیرنظامی
۲۵۳	۷.۹.۵. فورواردینگ پورت‌ها

۲۵۵	۷.۱۰. توپولوژی های فایروال
۲۵۵	۷.۱۰.۱. Dual-Homed فایروال
۲۵۶	۷.۱۰.۲. Two-Legged فایروال
۲۵۸	۷.۱۰.۳. Three-Legged فایروال
۲۵۹	۷.۱۱. فایروال و نحوه کنترل ترافیک
۲۵۹	۷.۱۱.۱. فیلتر نمودن بسته های اطلاعاتی
۲۵۹	۷.۱۱.۲. Proxy سرویس
۲۵۹	۷.۱۲. مشخصه های مهم یک فایروال قوی
۲۶۰	۷.۱۳. امنیت فایروال
۲۶۱	۷.۱۳.۱. امنیت سیستم عامل فایروال
۲۶۱	۷.۱۳.۲. دسترسی امن به فایروال جهت مقاصد مدیریتی
۲۶۱	۷.۱۴. معایب عمومی Firewallها
۲۶۲	۷.۱۵. پراکسی سرور
۲۶۲	۷.۱۵.۱. عملکردهای پراکسی سرور
۲۶۴	۷.۱۶. نتیجه گیری
۲۶۵	۷.۱۷. پرسش و تحقیق
۲۶۵	۷.۱۸. منابع و مراجع
۲۶۸	ضمیمه اول
۲۶۸	۸. استاندارد سیستم مدیریت امنیت اطلاعات
	۸.۱. مقدمه ۲۶۸
۲۶۸	۸.۲. سیاست ها و دستورالعمل های امنیتی
۲۶۸	۸.۳. تکنولوژی و محصولات امنیتی
۲۶۹	۸.۴. عوامل اجرایی
۲۶۹	۸.۵. خانواده استاندارد های ISO27000
۲۶۹	۸.۵.۱. موارد مطروحه در این استاندارد ها
۲۷۰	۸.۶. معرفی خانواده استاندارد های ISO27000
۲۷۱	۸.۷. استاندارد BS 7799
۲۷۲	۸.۸. استاندارد BS 7799
۲۷۳	۸.۹. استاندارد ISO/IEC 27006

۲۷۳		ISO/IEC 27005	۸.۱۰ استاندارد
۲۷۳		ISO/IEC 27011	۸.۱۱ استاندارد
۲۷۴		ISO/IEC 27004	۸.۱۲ استاندارد
۲۷۴		ISO/IEC 27003	۸.۱۳ استاندارد
۲۷۴		ISO/IEC 27007	۸.۱۴ استاندارد
۲۷۵		ISO 27001	۸.۱۵ استاندارد
۲۷۷		ISO/IEC 27001:2005	۸.۱۶ استاندارد
۲۷۷		۲۷۰۰۱	۸.۱۷ تاریخچه استاندارد
۲۷۸		۲۷۰۰۱	۸.۱۷.۱ بندهای استاندارد
۲۸۰		۹. ضمیمه دوم: منابع اینترنتی	
۲۸۱		۱۰. ضمیمه سوم: واژگان و عبارات (فارسی به انگلیسی)	
۳۰۲		۱۱. ضمیمه چهارم: واژگان و عبارات (انگلیسی به فارسی)	
۳۱۸		۱۲. ضمیمه پنجم: فهرست علائم اختصاری	

CHAPTER 1

فصل ۱

آشنایی با روتر

شناخت مسیر یاب
نحوه کار مسیر یاب
نصب و راه اندازی مسیر یاب
انواع مسیر یاب سیسکو