مهندسی اینترنت

با رویکرد مباحث امنیتی

مولف:

دکتر محمد علی ترکمانی

سرشناسه	:	ترکمانی، محمدعلی، ۱۳۵۴ -
عنوان و نام پدیدآور	:	مهندسی اینترنت [کتاب]/ مولف محمدعلی ترکمانی.
مشخصات نشر	:	مشهد: ارسطو، ۱۳۹۵.
مشخصات ظاهری	:	۲۳۳ ص.: مصور، جدول، نمودار.
شابک	:	978-600-432-079-5
وضعیت فهرست نویسی	:	فیپا
موضوع	:	اینترنت
موضوع	:	Internet
موضوع	:	اینترنت -- برنامه‌نویسی
موضوع	:	Internet programming
موضوع	:	شبکه‌های کامپیوتری
موضوع	:	Computer networks
موضوع	:	پروتکل‌های شبکه کامپیوتری
موضوع	:	Computer network protocols
رده بندی کنگره	:	TK۵۱۰۵/۸۷۵ /الف۹ت۴۷ ۱۳۹۵
رده بندی دیویی	:	۰۰۴/۶۷۸
شماره کتابشناسی ملی	:	۴۳۵۸۰۸۵

نام کتاب : مهندسی اینترنت

مولف : دکتر محمدعلی ترکمانی

ناشر : ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)

صفحه آرایی ، تنظیم و طرح جلد : علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : دوم – ۱۴۰۱

تعداد صفحات: ۳۹۵ صفحه

چاپ : مدیران

قیمت : ۲۵۰۰۰۰ تومان

شابک : ۰ -۱۰۲- ۴۳۲ –۶۰۰ – ۹۷۸

تلفن های مرکز پخش : ۵۰۹۶۱۴۵ – ۵۰۹۶۱۴۶ – ۰۵۱۱ -۰۹۱۷۷۱۶۴۹۴۰

فهرست مطالب

فصل اول: اصول شبکه‌های کامپیوتری و اینترنت ۲۱

۱-۱-تعریف شبکه ۲۱

۱-۲- اهداف و مزایای شبکه ۲۱

۱-۳-خدمات معمول در شبکه ۲۲

۱-۴-دسته بندی سخت افزار شبکه‌های کامپیوتری ۲۳

۱-۴- تاریخچه مختصری از اینترنت ۲۳

۱-۵-تعریف پروتکل ۲۴

۱-۶- استانداردها ۲۵

۱-۷-سازمان های استانداردسازی ۲۵

۱-۸- استانداردهای اینترنت ۲۶

۱-۹-اجزای شبکه های کامپیوتری ۲۶

۱-۱۰-تقسیم بندی شبکه ها از نظر تکنولوژی انتقال ۲۷

۱-۱۱-TOPOLOGY یا همبندی یا ریخت شناسی ۲۹

۱-۱۱-۱-انواع توپولوژی ۲۹

۱-۱۲-نرم افزار شبکه ۳۲

۱-۱۲-۱-مدل Client/ Server ۳۳

۱-۱۲-۱-مدل نظیر به نظیر(همتا به همتا) (peer to peer) ۳۳

۱-۱۲-۱-۱-برخی کاربردهای شبکه نظیر به نظیر(P2P) ۳۳

۱-۱۳-سیستم انتقال داده ۳۴

۱-۱۴-انواع شبکه از لحاظ جغرافیایی ۳۴

۱-۱۴-۱-شبکه محلی ۳۴
۱-۱۴-۱- شبکه کلان شهری ۳۵
۱-۱۴-۱-شبکه گسترده ۳۶
۱-۱۵- شبکه های بی سیم ۳۷
۱-۱۵-۱-دلایل استفاده از شبکه بی سیم ۳۸
۱-۱۶-سه مفهوم مهم شبکه: لایه، معماری و آدرس ۳۸
۱-۱۷-مدل مرجع OSI ۳۹
۱-۱۷-۱- وظایف لایه‌های استاندارد OSI ۴۱
۱-۱-۱۷-۱- Physical Layer (لایه فیزیکی) ٤١
۱-۱-۱۷-۲- Data Link Layer (لایه پیوند داده یا لایه پیوند) ٤٣
۱-۱-۱۷-۳- Network Layer (لایه شبکه) ٤٤
۱-۱-۱۷-۴- Transport Layer (لایه انتقال یا حمل) ٤٥
۱-۱-۱۷-۵- Section Layer (لایه نشست یا جلسه) ٤٦
۱-۱-۱۷-۶- Presentation Layer (لایه ارائه یا نمایش) ٤٦
۱-۱-۱۷-۷- Application Layer (لایه کاربرد) ٤٧
۱-۱۸-پشته پروتکلی TCP/IP ۴۷
۱-۱۸-۱-لایه ی کاربرد ۴۹
۱-۱۸-۲-لایه ی انتقال ۴۹
۱-۱۸-۳-لایه ی شبکه ۵۰
۱-۱۸-۴-لایه ی پیوند ۵۰
۱-۱۸-۵-لایه فیزیکی ۵۱
۱-۱۹-تفاوت ها و شباهت های ما بین OSI و TCP/IP ۵۱
۱-۲۰-دلایل جهانی نشدن مدل OSI ۵۲
۱-۲۱-تعاریف مهم ۵۳

۲۲-۱-کیفیت سرویس در شبکه های کامپیوتری ۵۴
۲۳-۱-سئوالات تشریحی ۵۷
فصل دوم: لایه فیزیکی ۵۹
۱-۲-پدیده های رسانه انتقال ۵۹
۲-۲- انواع رسانه انتقال ۶۱
۱-۲-۲-زوج سیم به هم تابیده (Twisted Pair) ۶۱
۲-۲-۲-کابل کواکس(Coaxial Cable) ۶۲
۳-۲-۲-فیبر نوری ۶۳
۴-۲-۲-بی سیم ۶۵
۲-۴-۲-۲-طیف الکترومغناطیسی ٦٦
۳-۲-مفاهیم داده و سیگنال ۶۶
۱-۳-۲-سیگنال دیجیتال ۶۸
۲-۳-۲-تبدیل داده دیجیتال به سیگنال آنالوگ ۶۹
۳-۳-۲-مدولاسیون ASK، FSK، PSK ۶۹
۱-۳-۳-۲-انواع مدولاسیون PSK ۷۰
۴-۳-۲-دیاگرام فلکی ۷۱
۵-۳-۲-مدولاسیون ترکیبی QAM ۷۱
۶-۳-۲-نرخ بیتی و نرخ باود ۷۲
۷-۳-۲-مالتی پلکسینگ (Multiplexing) یا MUX ۷۲
۴-۲-سئوالات تشریحی ۷۵
فصل سوم :لایه پیوند داده ۷۷
۱-۳-مقدمه ۷۷

۲-۳-وظایف لایه پیوند داده ۷۸
۱-۲-۳- ارائه سرویس به لایه بالاتر ۷۸
۲-۲-۳- قرار دادن آدرس فیزیکی در فریم اطلاعاتی در شبکه های LAN ۷۹
۳-۲-۳ - فریم بندی (Framing) ۸۰
۴-۲-۳- کنترل خطا (Error Control) ۸۰
۱-۴-۲-۳- بیت توازن ۸۰
۲-۴-۲-۳-جمع مقابله ای (Checksum) ۸۱
۳-۴-۲-۳- CRC ۸۱
۵-۲-۳- کنترل جریان (Flow Control) ۸۱
۱-۵-۲- ۳-کنترل جریان نرم افزاری XON-XOFF ۸۲
۲-۵-۲-۳-کنترل جریان سخت افزاری RTS-CTS ۸۲
۳-۵-۲-۳-روش کنترل جریان نرم افزاری در لایه انتقال ۸۲
۶-۲-۳- مدیریت کانال ۸۳
۱-۶-۲-۳-مدیریت کانال نقطه به نقطه ۸۳
۱-۱-۶-۲-۳-روش ایست و انتظار یا Stop & Wait ۸۳
۲-۱-۶-۲-۳-روش عدم پذیرش انتخابی (Selective Reject ARQ) ۸٤
۳-۱-۶-۲-۳-روش بازگشت به عقب اندازه N (Go Back N ARQ) ۸٤
۴-۱-۶-۲-۳-مقایسه سه روش مدیریت کانال نقطه به نقطه ۸٤
۲-۶-۲-۳-مدیریت کانال پخش همگانی (کانال مشترک) ۸۵
۱-۲-۶-۲-۳-روش ایستا (static) ۸۵
۲-۲-۶-۲-۳-روش پویا (dynamic) ۸٦
۳-۳-شبکه های LAN ۹۰
۱-۳-۳- IEEE 802.3 ..... ۹۰
۱-۱-۳-۳-الگوریتم بدست آوردن زمان تصادفی ۹۱
۲-۱-۳-۳-فریم داده در اترنت ۹۱
۳-۱-۲-۳-انواع پیاده سازی اترنت ۹۳
۱-۳-۱-۳-۳-کابل کشی اترنت ۹۵

۲-۳-۳- Token Bus یا IEEE 802.4 ..... ۹۶
۳-۳-۳-Token Ring یا IEEE 802.5 ..... ۹۷
۴-۳-۳-مقایسه سه استاندارد 802.3 و 802.4 و 802.5 ..... ۹۸
۵-۳-۳-مروری بر شبکه بی سیم محلی IEEE 802.11 ..... ۹۹
۱-۵-۳-۳-معماری پروتکل IEEE 802.11 ..... ۹۹
۲-۵-۳-۳-مدل معماری و مولفه‌های شبکه IEEE 802.11 ..... ۱۰۳
۳-۵-۳-۳-سرویس های IEEE 802.11 ..... ۱۰٤
۴-۳-سئوالات تشریحی ۱۰۷

فصل چهارم :لایه شبکه ۱۰۹

۱-۴-مفهوم شبکه بندی ۱۰۹
۱-۱-۴-تکرارگر (Repeater) ۱۰۹
۲-۱-۴- پل (bridge) ۱۱۰
۳-۱-۴- Hub ۱۱۱
۴-۱-۴-مسیریاب (Router) ۱۱۲
۵-۱-۴-دروازه (Gateway) ۱۱۲
۲-۴-پیام ها ، قطعه ها ، داده گرام ها و قاب ها ۱۱۴
۳-۴-سوییچینگ ۱۱۶
۱-۳-۴-سوییچینگ مداری ۱۱۷
۲-۳-۴-سوییچینگ پیغام ۱۱۸
۳-۳-۴-سوییچینگ بسته ای ۱۱۹
۱-۳-۳-۴-سوییچینگ بسته ای مدار مجازی ۱۱۹
۲-۳-۳-۴-سوییچینگ بسته ای داده گرام ۱۲۰
۴-۴-تاخیر تضعیف و بازدهی در شبکه های سوئیچینک بسته ای(PSN) ۱۲۱

۱-۴-۴-تاخیر پردازش ۱۲۲
۲-۴-۴-تاخیر صف ۱۲۲
۳-۴-۴-تاخیر انتقال ۱۲۳
۴-۴-۴-تاخیر انتشار ۱۲۳
۵-۴-تاخیر صف و اتلاف بسته ها ۱۲۵
۶-۴-تاخیر دو نقطه انتهایی ۱۲۸
۷-۴- بازدهی شبکه های کامپیوتری ۱۲۹
۸-۴- الگوی خدمات شبکه ۱۳۱
۹-۴-آدرس دهی در لایه شبکه ۱۳۳
۱-۹-۴-آدرس IP ۱۳۳
۱-۱-۹-۴-آدرس های IP خصوصی یا نامعتبر (invalid) ۱۳٤
۲-۱-۹-۴-زیرشبکه سازی (Subnet working) ۱۳۵
۱-۲-۱-۹-۴-ماسک زیرشبکه (Subnet Mask) ۱۳۵
۱۰-۴-آدرسهای IP خاص ۱۳۶
۱۱-۴-پروتکل های لایه شبکه ۱۳۷
۱-۱۱-۴- ARP ۱۳۸
۲-۱۱-۴-پروتکل IP ۱۳۸
۱-۲-۱۱-۴-قالب بسته IP نسخه چهار (IPv4) ۱۳۹
۲-۲-۱۱-۴-پروتکل آدرس دهی IP نسخه ی 6(IPV6) ۱٤۱
۱-۲-۲-۱۱-۴-قالب بندی داده گرام IPV6 ..... ۱٤۱
۳-۱۱-۴- IP سیار یا mobile IP یا MIP ۱۴۵
۱-۳-۱۱-۴-مفاهیم اولیه در IP سیار ۱٤٦
۲-۳-۱۱-۴-طرز کار IP سیار ۱٤۷
۳-۳-۱۱-۴-نسخه ششم IP سیار ۱٤۸
۴-۱۱-۴-ICMP (Internet Control Message Protocol) ۱۴۹

۴-۱۲-مسیریابی (ROUTING) ۱۴۹
۴-۱۲-۱-اصطلاحات مهم ۱۵۰
۴-۱۲-۲- معیارهای تصمیم گیری مسیریاب ها ۱۵۰
۴-۱۲-۳-انواع الگوریتم‌های مسیریابی ۱۵۱
۴-۱۲-۴-مدلسازی زیر شبکه با Graph ۱۵۲
۴-۱۲-۵-الگوریتم سیل آسا (flooding) ۱۵۳
۴-۱۲-۶-الگوریتم مسیریابی حالت لینک (Link State Routing) ۱۵۴
۴-۱۲-۷-الگوریتم بردار فاصله (Distance Vector Routing) ۱۵۸
۴-۱۲-۸- مقایسه دو الگوریتم مسیریابی DV و LS ۱۶۸
۴-۱۲-۹-مسیریابی سلسله مراتبی (Hierachial Routing) ۱۶۹
۴-۱۲-۹-۱-مسیریابی درونی و بیرونی ۱۷۰
۴-۱۳-مسیریابی در اینترنت ۱۷۱
۴-۱۳-۱-مسیریابی درون سیستم‌های خودمختار در اینترنت (RIP) ۱۷۱
۴-۱۳-۲-پروتکل مسیریابی درونی OSPF ۱۷۵
۴-۱۳-۳-پروتکل بیرونی BGP ۱۷۸
۴-۱۳-۴-پروتکل IBGP ۱۷۹
۴-۱۳-۵-پروتکل EBGP ۱۸۰
۴-۱۳-۶-دلایل پروتکل‌های متفاوت مسیریابی درونی و بیرونی (AS) ۱۸۰
۴-۱۴-مسیریابی فراپخش و چند پخش ۱۸۱
۴-۱۴-۱-الگوریتم های فراپخش ۱۸۲
۴-۱۴-۲-چندپخش ۱۸۷
۴-۱۵-سئوالات تشریحی ۱۹۲
۴-۱۶-پاسخ سئوالات ۲۰۵

فصل پنجم :لایه انتقال ۲۱۹

۱-۵-کلیات ۲۱۹

۲-۵-انواع آدرس دهی ۲۲۰

۳-۵-کیفیت سرویس(QOS) ۲۲۱

۴-۵-پروتکل های لایه انتقال ۲۲۲

۱-۴-۵-TCP (Transmission Control Protocol) ۲۲۲

۱-۱-۴-۵-هدر TCP ۲۲۲

۲-۱-۴-۵-روش برقراری ارتباط در پروتکل TCP ۲۲٤

۱-۲-۱-۴-۵-کنترل جریان و کنترل ازدحام در پروتکل TCP ۲۲٦

۲-۲-۱-۴-۵-پنجره ی ازدحام ۲۲۷

۳-۲-۱-۴-۵-کنترل خطا و زمانسنجها در پروتکل TCP ۲۲۸

۲-۴-۵- UDP (User Datagram Protocol) ۲۳۱

۱-۲-۴-۵-هدر UDP ۲۳۱

۳-۴-۵-مقایسه TCP و UDP ۲۳۲

۵-۵-سئوالات تشریحی ۲۳۳

۶-۵-پاسخ ها ۲۳۴

فصل ششم :شبکه اینترنت و لایه کاربرد ۲۳۷

۱-۶- تقسیم بندی شبکه از نظر جغرافیایی ۲۳۷

۲-۶-شبکه اینترنت ، اینترانت و اکسرانت ۲۳۷

۱-۲-۶-اینترنت(INTERNET) ۲۳۷

۲-۲-۶-اینترانت(Intranet) ۲۳۸

۳-۲-۶-اکسترانت (Extranet) ۲۳۸

۳-۶-صفحات وب ۲۳۸

۱-۳-۶-آشنایی با URL ۲۳۹
۴-۶-انواع روشهای اتصال به ISP ۲۴۰
۵-۶-تاریخچه وب جهانی ۲۴۱
۶-۶- تفاوت بین اینترنت و وب جهان گستر (www) ۲۴۲
۷-۶-معماری وب ۲۴۴
۱-۷-۶-جنبه سرویس گیرنده و سرویس دهنده ۲۴۴
۸-۶-پروتکل های لایه کاربرد اینترنت ۲۴۵
۱-۸-۶- FTP ۲۴۵
۱-۱-۸-۶-روش های برقراری یک نشست FTP ۲٤٦
۲-۸-۶- پروتکل HTTP ۲۴۷
۳-۸-۶- HTTPS ۲۵۲
۱-۳-۸-۶-تفاوت Https و Http ۲۵۳
۲-۳-۸-۶- SSL چیست؟ ۲٥٤
۴-۸-۶-پروتکل IMAP ۲۵۴
۵-۸-۶-پروتکل pop3 ..... ۲۵۵
۱-۵-۸-۶-مزیت استفاده از pop3 ..... ۲٥٥
۶-۸-۶- SMTP ۲۵۶
۷-۸-۶-پروتکل MIME ۲۵۸
۱-۷-۸-۶-مثالي از MIME ۲٥۹
۸-۸-۶- DNS ۲۶۰
۱-۸-۸-۶-نامگذاری دامنه ۲٦۱
۲-۸-۸-۶-پرس و جوها ۲٦۲
۱-۲-۸-۸-۶-پرس و جوی تکراری ۲٦۳
۲-۲-۸-۸-۶-پرس و جوهای بازگشتی ۲٦٤
۳-۲-۸-۸-۶-پرس و جوهای معکوس ۲٦٦

۹-۸-۶-DHCP ۲۶۷
۹-۶-سئوالات تشریحی ۲۷۰
۱۰-۶-پاسخ برخی از سئوالات ۲۷۱

فصل هفتم :برنامه نویسی شبکه به زبانC#.NET ۲۷۳

۱-۷-مقدمه ۲۷۳
۲-۷-بررسی چند کلاس ۲۷۳
۱-۲-۷-کلاس IPAddress ۲۷۳
۱-۱-۲-۷-متد Equals ۲۷٤
۲-۱-۲-۷-متدهای HostToNetworkOrder و NetworkToHostOrder ۲۷٤
۲-۲-۷-کلاس IPHostEntry ۲۷۵
۳-۲-۷-کلاس DNS ۲۷۶
۱-۳-۲-۷-متدهای مربوط به dns: ۲۷٦
۳-۷-سوکت TCP ۲۷۸
۱-۳-۷-سرویس گیرنده Tcp ۲۷۸
۱-۱-۳-۷-کلاس TcpClient ۲۷۹
۲-۱-۳-۷-متدهای کلاس TCPClient ۲۷۹
٤-۱-۳-۷-کلاس IpEndPoint ۲۸۰
۲-۳-۷-سرویس دهنده Tcp ۲۸۰
۱-۲-۳-۷-کلاس TcpListener ۲۸۱
۴-۷-سوکت های UDP ۲۸۴
۱-۴-۷-سرویس گیرنده UDP ۲۸۵
۱-۱-٤-۷-کلاس UdpClient ۲۸۵
۵-۷-مقدمه ای بر سوکت ۲۸۶
۱-۵-۷-سرویس گیرنده TCP با کلاس Socket ۲۸۶

۶-۷- I/O بدون وقفه ۲۹۲
۱-۶-۷-بررسی وضعیت I/O ۲۹۳
۲-۶-۷-فراخوانی مسدود کننده با مهلت زمانی ۲۹۵
۳-۶-۷-متد Poll ۲۹۵

فصل هشتم :مفاهیم و اصول امنیت اطلاعات ۲۹۷

۱-۸-امنیت اطلاعات چیست؟ ۲۹۷
۱-۱-۸-خصوصیات سیستم امن ۲۹۸
۲-۸-اصطلاحات امنیتی ۲۹۸
۱-۲-۸-آسیب‌پذیری ۲۹۸
۲-۲-۸-حمله ۲۹۹
۳-۲-۸-تهدید ۲۹۹
۴-۲-۸-مفهوم AAA در امنیت اطلاعات ۲۹۹
۵-۲-۸-عدم انکار (سندیت) ۳۰۱
۳-۸-نفوذگر یا هکر ۳۰۱
۱-۳-۸- نفوذگران کلاه سفید ۳۰۱
۲-۳-۸-نفوذگران کلاه سیاه ۳۰۱
۳-۳-۸- نفوذگران کلاه خاکستری ۳۰۲
۴-۳-۸-نفوذگران کلاه صورتی ۳۰۲
۴-۸-دسته‌بندی کلی حملات ۳۰۲
۱-۴- ۸-دسته بندی از نظر تغییر دادن اطلاعات ۳۰۲
۲-۴-۸-دسته‌بندی از نظر به چالش کشیدن اصول امنیت ۳۰۲

۸-۸- سئوالات تشریحی ۳۰۳
۸-۹-سئوالات چهارگزینه‌ای ۳۰۴
پاسخنامه: ۳۰۵

فصل نهم :کاربردهای رمزنگاری در امنیت شبکه ۳۰۷

۹-۱-مفاهیم و اصطلاحات رمزنگاری ۳۰۷
۹-۲- سیستم‌های رمزنگاری ۳۰۸
۹-۲-۱-رمزنگاری متقارن ۳۰۸
۹-۲-۲-رمزنگاری نامتقارن ۳۰۹
۹-۳-تکنیک‌های رمزگذاری ۳۰۹
۹-۳-۱-رمزنگاری سزار ۳۱۰
۹-۳-۲-رمزنگاری ورنام ۳۱۱
۹-۳-۳-ترکیب جایگشتی و جایگزینی ۳۱۲
۹-۳-۴-تکنیک‌های رمزنگاری متقارن ۳۱۲
۹-۳-۴-۱-رمز رشته‌ای یا دنباله‌ای ۳۱۲
۹-۳-۴-۲-رمز بلاکی ۳۱۲
۹-۴-رمزنگاری DES ۳۱۳
۹-۵-الگوریتم 2DES ۳۱۳
۹-۶-الگوریتم 3DES ۳۱۴
۹-۷- امنیت DES ۳۱۴
۹-۸-رمزنگاری با کلید عمومی ۳۱۵
۹-۹-الگوریتم RSA ۳۱۸

۹-۹-۱-انتخاب کلید ۳۱۸
۹-۹-۲-روش رمزگذاری و رمزگشایی ۳۱۹
۹-۱۰-تبادل کلید نشست با استفاده از رمزنگاری RSA ۳۲۰
۹-۱۰-۱-پروتکل توزیع کلید متقارن با استفاده از کلید عمومی ۳۲۱
۹-۱۱-صحت پیام با استفاده از MAC ۳۲۳
۹-۱۲-الگوریتم‌های MAC ۳۲۵
۹-۱۳-امضای دیجیتال ۳۲۶
۹-۱۴-گواهینامه ۳۲۷
۹-۱۵-سئوالات تشریحی ۳۲۹
۹-۱۶-سئوالات چهارگزینه‌ای ۳۳۰
پاسخنامه: ۳۳۴
فصل دهم:امنیت پست الکترونیکی ۳۳۵
۱۰-۱-۱-سیستم اول ۳۳۵
۱۰-۱-۲-سیستم دوم ۳۳۶
۱۰-۱-۳-سیستم سوم ۳۳۷
۱۰-۲-استانداردPGP ۳۳۸
۱۰-۳- پست الکترونیکی چند منظوره امن S/MIME ۳۳۹
۱۰-۴-سئوالات تشریحی ۳۴۱
۱۰-۵-سئوالات چهارگزینه‌ای ۳۴۱
پاسخنامه: ۳۴۲
فصل یازدهم :امنیت IP ۳۴۳

۱-۱۱-مقدمه ۳۴۳
۲-۱۱-معماری IPSEC ۳۴۳
۳-۱۱-سرویس‌های IPSEC ..... ۳۴۴÷
۴-۱۱-مدهای کاری IPSEC ۳۴۴
۵-۱۱-مزایای IPSEC VPN ۳۴۶
۶-۱۱-پروتکل‌های IPSEC ۳۴۷
۱-۶-۱۱- پروتکل AH ۳۴۸
۲-۶-۱۱- پروتکل ESP ۳۴۸
۷-۱۱-ترکیب مد و پروتکل IPSEC ۳۴۹
۸-۱۱- مجمع امنیتی(SA) و سیاست امنیتی(SP) ۳۴۹
۹-۱۱- پروتکل تبادل کلید در اینترنت(IKE) ۳۵۲
۱۰-۱۱-سئوالات تشریحی ۳۵۲
۱۱-۱۱-سئوالات چهارگزینه‌ای ۳۵۳
پاسخنامه: ۳۵۵

فصل دوازدهم :امنیت وب ۳۵۷

۱-۱۲- مقدمه ۳۵۷
۲-۱۲- محل قرار گرفتن SSL ۳۵۸
۳-۱۲-پروتکل SSL ۳۵۸
۴-۱۲- پروتکل TLS ۳۵۹
۵-۱۲- نحوه عملکرد SSL ۳۵۹
۱-۵-۱۲-صحت پیام SSL درهم ساز ۳۶۱

۱۲-۶- اثبات هویت سرویس دهنده ۳۶۲
۱۲-۷- حملات ۳۶۳
۱۲-۸- نتیجه گیری ۳۶۴
۱۲-۹-سئوالات تشریحی ۳۶۴
۱۲-۱۰-سئوالات چهارگزینه‌ای ۳۶۴
پاسخنامه: ۳۶۵
فصل سیزدهم :امنیت تجارت الکترونیک ۳۶۷
۱۳-۱-مقدمه ۳۶۷
۱۳-۲-تراکنش الکترونیکی امن (SET) ۳۶۷
۱۳-۲-۱-مراحل تراکنش مالی توسط SET ۳۷۰
۱۳-۲-۲-پردازش پرداخت در SET ۳۷۱
۱۳-۲-۲-۱-درخواست خرید ۳۷۱
۱۳-۲-۲-۲-اجازه پرداخت ۳۷۲
۱۳-۲-۲-۳-اخذ پرداختی ۳۷٤
۱۳-۳ -تجارت الکترونیک امن ۳۷۴
۱۳-۳-۱ -مراجع صدور گواهی ۳۷۵
۱۳-۳-۲ -کارت‌های هوشمند ۳۷۶
۱۳-۴- اعتماد به وب ۳۷۶
۱۳-۵- پول الکترونیکی ۳۷۶
۱۳-۶- امنیت مرورگر وب ۳۷۷
۱۳-۷-امنیت اسکریپت ۳۷۸
۱۳-۸-امنیت پروتکل وب ۳۷۹

۹-۱۳-سئوالات چهارگزینه‌ای ۳۸۰

۱۰-۱۳-سئوالات چهارگزینه‌ای ۳۸۰

پاسخنامه: ۳۸۲

فصل چهاردهم :امنیت در مدیریت شبکه ۳۸۳

۱-۱۴-مقدمه ۳۸۳

۲-۱۴-عناصر کلیدی در مدل مدیریت شبکه SNMP ۳۸۴

۳-۱۴-معماری پروتکل مدیریتی شبکه ۳۸۶

۴-۱۴ -پروکسی‌ها ۳۸۶

۵-۱۴-امکانات (وسایل) موجود در جماعت ایجاد شده در نسخهٔ اول پروتکل SNMP ۳۸۷

۶-۱۴-نسخهٔ سوم پروتکل SNMP ۳۸۸

۷-۱۴-سئوالات تشریحی ۳۸۹

۸-۱۴-سئوالات چهارگزینه‌ای ۳۸۹

پاسخنامه: ۳۹۳

منابع: ۳۹۴

مقدمه:

امروزه اینترنت نقش مهمی در زندگی بشر بازی می‌کنند و مانند جاده ها که نقاط مختلف یک کشور را به یکدیگر متصل می‌کنند، کاربران مختلف را به یکدیگر متصل می‌نماید و به نوعی زیر ساخت اصلی فناوری اطلاعات یک سازمان و یا کشور اینترنت است. بنابراین دانشجویان رشته های مختلف خصوصا رشته های کامپیوتر، IT و ICT باید دانش مورد نیاز در این حوزه را کسب نمایند. در این کتاب، مهندسی اینترنت مورد بررسی قرار می‌گیرد. در این کتاب به مباحث امنیتی در شبکه اینترنت توجه خاصی شده است. در پایان هر فصل سئوالات تشریحی و چهارگزینه ای آورده شده است تا مخاطبین محترم بتوانند از آن به عنوان حود آزمایی استفاده نمایند و دانشجویان گرامی بتوانند خود را برای آزمونهای پیش رو آماده نمایند. از اساتید و دانشجویان گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با مولف در میان بگذارند تا انشالله در ویرایش‌های بعدی اشکالات یا کاستی‌های احتمالی کتاب مورد تجدید نظر قرار گیرد. در پایان وظیفه خود می‌دانم مدیریت انتشارات ارسطو و سامانه اطلاع رسانی چاپ و نشر ایران جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.

محمد علی ترکمانی

پاییز ۱۳۹۵

فصل اول

اصول شبکه‌های کامپیوتری و اینترنت

۱-۱-تعریف شبکه

به مجموعه ای از چند کامپیوتر مستقل یا اجزای کامپیوتری که با یکدیگر ارتباط دا شته با شند و ما بین آنها انتقال داده انجام شود یک شبکه کامپیوتری می گویند.

در این تعریف چند نکته وجود دارد:

- مستقل بودن کامپیوترها: هر کامپیوتر به تنهایی و بدون حضور در شبکه بتواند عملکرد عادی خود را داشته باشد
- اجزای کامپیوتر می توانند چاپگرها، اسکنرها و... باشند.
- هدف اصلی شبکه های کامپیوتری، عمل انتقال داده است.

بنابراین در شبکه علاوه بر این که کامپیوترها متصل به یکدیگرند از همدیگر مستقل هستند.

۱-۲- اهداف و مزایای شبکه

- سهولت انتقال داده ها
- اشتراک منابع نرم افزاری مانند پایگاه داده و فایل ها و منابع سخت افزاری مانند چاپگرها و اسکنرها و...
- صرفه جویی در هزینه ها: اشتراک منابع باعث صرفه جویی در هزینه می شود.
- افزایش قابلیت اطمینان(reliability) به دلیل تعدد منابع: قرار دادن چندین نسخه یکسان از یک نرم افزار یا فایل بر روی چندین کامپیوتر درون شبکه موجب افزایش قابلیت اطمینان می شود.

- از بین رفتن بعد فاصله
- مشکل شبکه امنیت آن است.

۳-۱-خدمات معمول در شبکه

برخی از خدمات متداول شبکه های کامپیوتری عبارتند از:

- دسترسی به بانکهای اطلاعاتی راه دور
- پست الکترونیکی
- خدمات انتقال فایل
- ورود به سیستم از راه دور
- گروههای خبری
- جستجوی اطلاعات مورد نیاز
- تبلیغات
- تجارت الکترونیکی
- بانکداری الکترونیکی
- سرگرمی و محاوره
- مجلات و روزنامه‌های الکترونیکی
- محاوره مستقیم و چهره به چهره از راه دور
- کنفرانس از راه دور
- یافتن اشخاص مورد نظر در جهان
- تلفن ودورنگار از طریق شبکه
- رادیو از طریق شبکه
- آموزش از راه دور
- ارائه مدون اطلاعات فنی و علمی
- اخبار مربوط به هنر ، ورزش ، سیاست ، تجارت و...
- کاریابی و اشتغال
- درمان از راه دور

- خرید و فروش روزمره با استفاده از کارت اعتباری
- انجمن‌های خیریه
- مشاوره از راه دور

۴-۱-دسته بندی سخت افزار شبکه‌های کامپیوتری

سخت افزار شبکه‌های کامپیوتری را میتوان از دیدگاه های مختلف دسته بندی نمود. یک مورد از این تسیم بندی به شرح ذیل است:

۱-از دیدگاه تکنولوژی انتقال

- شبکه‌های پخش فراگیر
- شبکه‌های نقطه به نقطه

۲- از دیدگاه مقیاس بزرگی

- شبکه های LAN
- شبکه های MAN
- شبکه های WAN

۴-۱- تاریخچه مختصری از اینترنت

نقطه شروع و عامل اصلی ایجاد شبکه اینترنت به سال ۱۹۵۷ میلادی باز می‌گردد. در آن سال اتحاد جماهیر شوروی سابق سفینه Sputnik را به فضا فرستاد و موفقیت پروژه Sputnik سبب ایجاد آژانس پروژه‌های پیشرفته(ARPA)۱ در وزارت دفاع ایالات متحده آمریکا گردید. بعد از ایجاد آرپا در سال ۱۹۵۷ میلادی، این سازمان هسته‌های پژوهشی متعددی را در دانشگاه های مختلف در سرتاسر آمریکا پدید آورد. پس از ایجاد هسته‌های پژوهشی، نیاز به تبادل اطلاعات بین دانشمندان دانشگاه‌ها در هر یک از این گروه‌های پژوهشی احساس می‌شد و سازمان آرپا به این نتیجه رسید که باید این مراکز پژوهشی را به نحوی به یکدیگر متصل نماید. چنین موضوعی زمینه ساز ایجاد ساختار اتصال شبکه‌ها گردید. در ابتدا کامپیوترهای دانشگاه لس‌آنجلس درکالیفرنیا،

1 Advanced Research Projects Agency

انستیتو پژوهشی دانشگاه استنفرد، دانشگاه یوتا، و دانشگاه سانتا باربارا درکالیفرنیا به یکدیگر متصل گردیدند و اولین شبکه راه دور به نام ARPANET (شبکه آژانس پروژه‌های پژوهشی پیشرفته) در سال ۱۹۶۸ میلادی پدید آمد. با نگرش به نظامی بودن پروژه‌های مراکز پژوهشی، تمام اطلاعات در این کامپیوترها سری بودند. وزارت دفاع آمریکا ابتدا پروژه آرپانت را پیاده‌سازی نمود تا دانشمندان دانشگاه‌ها را در سرتاسر ایالات متحده آمریکا به هم مرتبط سازد تا بتوانند به آسانی، به سرعت و بطور امن در اطلاعات سهیم باشند. در سال ۱۹۸۴ میلادی و درحالی که تقریباً ۵۰۰ دانشگاه به طور فعال از آرپانت استفاده می‌نمودند، نام ARPANET به Internet که اختصار Internet network است تبدیل گردید و مسئولیت اداره آن در سه سال بعد به عهده بنیاد علوم ملی[1] واگذار گردید. با اجرای موفق طرح ARPANET، مراکز تجاری در استفاده از زیرساخت شبکه تشویق شده و شبکه اینترنت کنونی به وجود آمد. درنتیجه آرپانت از یک شبکه آزمایشی چهار سایتی شروع به رشد نمود تا به یک شبکه جهان گستر شبکه‌ها یا اینترنت متشکل از میلیون‌ها کامپیوتر تبدیل گردید.

در حال حاضر اینترنت در تملک کسی نمی‌باشد، بلکه در عوض یک شبکه‌ای متشکل از بسیاری از سازمان‌ها درسرتاسر جهان است که در دسترسی به کامپیوترهایشان بادیگران سهیم می‌باشند. آنچه که در ابتدا صرفاً به عنوان یک وسیله ارتباطی جهت تبادل اطلاعات درمورد پژوهش‌های نظامی و دفاعی آغاز به کار نمود، برای یک جامعه جهانی شکوفا گردید.

۵-۱-تعریف پروتکل

پروتکل مترادف با قاعده (rule) است. به منظور آن که مخابره ای صورت بگیرد باید دو سیستم مخابره کننده داده از یک پروتکل مورد توافق طرفین استفاده کنند. پروتکل، مجموعه قواعد حاکم بر یک سیستم مخابراتی است. پروتکل می گوید که چه چیزی مخابره می شود، چگونه مخابره می شود و چه زمانی مخابره می شود. المان های کلیدی یک پروتکل عبارتند از: ساختار (syntax)، معنا (semantic) و زمان بندی (timing).

1 National Science Foundation

- ساختار: به فرمت(قالب) داده اشاره می کند و ترتیب فیلدهای سازنده پروتکل را نشان می دهد
- معنا: به معنای هر فیلد از پروتکل اشاره می کند.
- هر فیلد مشخص می کند چه کار می کند و بر اساس تفسیر مربوطه چه عملی باید انجام شود.
- به عنوان مثال آیا یک آدرس مسیری که باید طی شود را مشخص می کند و یا مقصد نهایی پیغام را نشان می دهد.
- زمان بندی: زمان بندی به دو مشخصه اشاره می کند: چه زمانی باید داده را ارسال کرد و سرعت ارسال آن باید چه قدر باشد.
- به عنوان مثال اگر فرستنده با سرعت ۱۰۰Mbps داده تولید کند اما سرعت پردازش گیرنده فقط ۱Mbps باشد گیرنده از داده لبریز می شود.

۱-۶- استانداردها

استانداردها برای ایجاد رقابت میان تولیدکنندگان تجهیزات و نیز برای این که سیستم های مخابراتی ملی و بین المللی بتوانند به درستی به مبادله اطلاعات بپردازند، ضروری هستند. آنها خط مشی هایی برای تولید کنندگان، نمایندگی های دولتی و سایر سرویس دهندگان قرار می دهند تا تضمینی بر عملکرد صحیح سیستم های مخابراتی به وجود آید. استانداردهای سیستم های مخابره داده به دو گروه تقسیم می شوند:

- استانداردهای طبق واقعیت (de facto standard) : استانداردهایی هستند که توسط یک سازمان استاندارد سازی ارائه نشده اند اما استفاده گسترده ای دارند، به نام استانداردهای طبق واقعیت موسومند. مانند پروتکل TCP/IP.
- استاندارد طبق قانون (de jure standard)" این استانداردها توسط یک سازمان استانداردسازی اعلام شده اند. مانند پروتکل OSI.

۱-۷-سازمان های استانداردسازی

در اثر همکاری کمیته های تولید استاندارد، گردهمایی ها و نمایندگی های تنظیم کننده دولتی، استانداردها تولید می شوند. کمیته های تولید استاندارد عبارتند از:

- سازمان استاندارد های بین المللی (ISO)
- اتحادیه بین المللی مخابره از راه دور (ITU)
- انستیتوی استانداردهای ملی آمریکا (ANSI)
- انستیتوی مهندسین برق و الکترونیک (IEEE)
- انجمن صنایع الکترونیک (EAI)

۸-۱- استانداردهای اینترنت

روند تولید یک استاندارد برای اینترنت یک روند مشخص است و باید روال معینی را طی کند. هر مشخصه ای با یک طرح اولیه اینترنتی (internet draft) آغاز می شود. یک طرح اولیه اینترنتی یک مشخصه در حال اجرا در اینترنت است که هنوز به صورت رسمی در نیامده و طول عمر آن شش ماه است. با گرفتن تاییدیه می توان طرح اولیه را به صورت یک نظرخواهی (Request For Comment:RFC) منتشر کرد. RFCها سطوح تکامل دارند (شش سطح).

۹-۱-اجزای شبکه های کامپیوتری

هر شبکه کامپیوتری از دو قسمت سخت افزار و نرم افزار تشکیل شده است. سخت افزار یک شبکه کامپیوتری (LAN یا WAN) از سه قسمت تشکیل شده:

۱-میزبان (host): به کامپیوترها یا اجزای کامپیوتری متصل به شبکه host یا گره (node) یا ایستگاه کاری (workstation) گفته می شود.

۲-وا سطه میانی: د ستگاهی برای اتصال شبکه ها به یکدیگر و یا میزبان ها به شبکه ا ست. مانند کارت شبکه، مودم و روتر و ...

۳-کانال (link): ارتباط میزبان ها از طریق کانال ها امکان پذیر است. به کانال رسانه انتقال و محیط فیزیکی نیز گفته می شود.

به مجموعه واسطه میانی و کانال که عمل انتقال داده ما بین ایستگاه ها را فراهم می کنند **زیر شبکه یا subnet** می گویند.

اگر بخواهیم به صورت کلی به شبکه نگاه کنیم، می‌توانیم آن را به سه قسمت اصلی تقسیم کنیم.

- Network edgeیا لبه شبکه : همان طور که از اسمش مشخص است، انتهایی ترین سیستم متصل به شبکه، لبه را تشکیل می‌دهد که در اصطلاح به آن End System می‌گویند .
- Network coreیا هسته شبکه: این بخش شامل مجموعه‌ای از مسیریاب‌ها (Router)، سوییچ‌ها و لینک‌ها است که میان اجزای مختلف سیستم ارتباط و هماهنگی به وجود می‌آورد .
- Accessیا دسترسی: این بخش انعطاف بیشتری دارد. در واقع مجموعه بخش‌هایی که به کاربران اجازه اتصال به شبکه را می‌دهد بخش دسترسی را تشکیل می‌دهند. به عنوان مثال کاری که مودم انجام می‌دهد زیر مجموعه بخش دسترسی است.

۱۰-۱-تقسیم بندی شبکه ها از نظر تکنولوژی انتقال

شبکه ها را از نظر تکنولوژی انتقال یعنی چگونگی دسترسی کامپیوترها به کانال یا رسانه انتقال به دو دسته تقسیم می کنند:

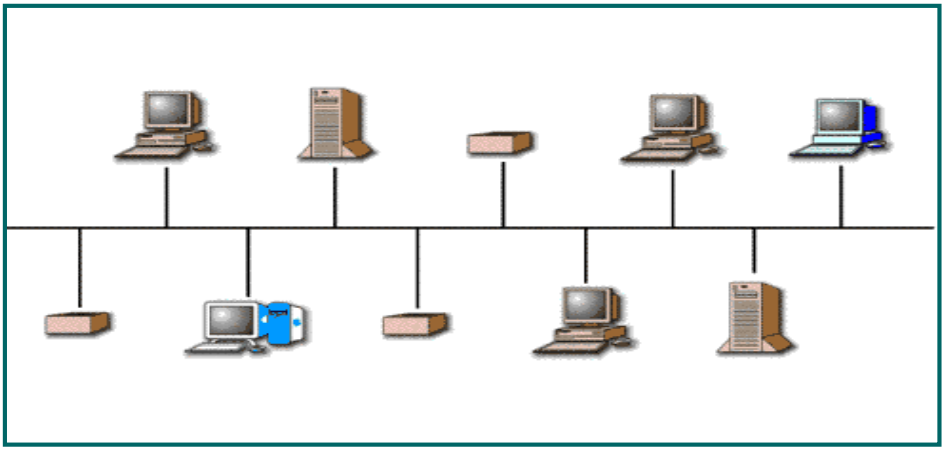
۱- پخش همگانی (broadcast) یا چند نقطه ای (multipoint) یا مشترک:

در این روش (شکل ۱-۱) همه ایستگاه ها به یک کانال مشترک متصلند و برای ارسال داده باید اطلاعات خود را بر روی این کانال قرار دهند و برای دریافت داده باید به کانال گوش دهند.

معایب کانال مشترک عبارتند از:

- امنیت پایین: دریافت اطلاعات توسط دیگر گره ها به علت مشترک بودن کانال. راه حل: رمزگذاری اطلاعات.
- کارایی نسبتا پایین: با توجه به مشترک بودن کانال برای ارسال اطلاعات، به هر کامپیوتر درصد کمی از پهنای باند کانال می رسد.

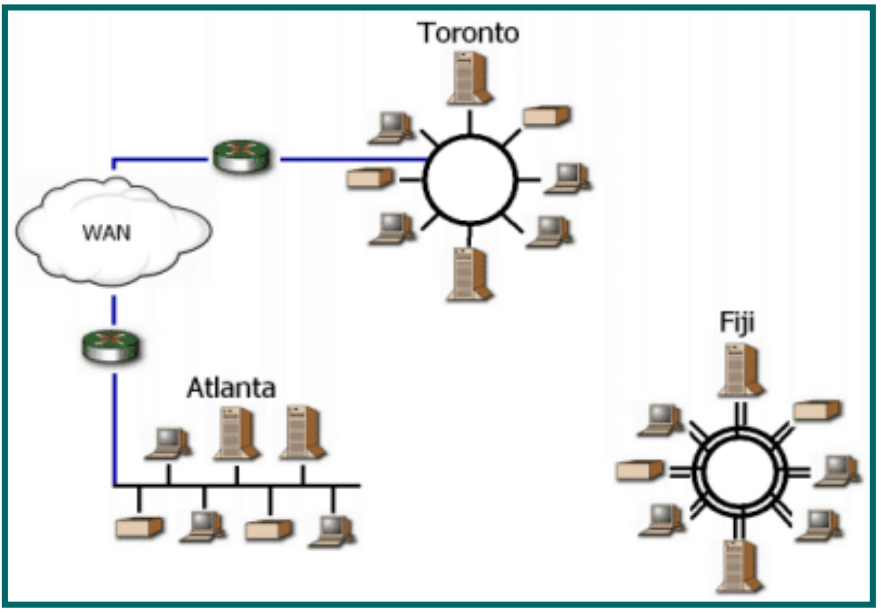
- مدیریت پیچیده کانال: باید قوانینی وضع شود تا به تمامی ایستگاه ها اجازه ارسال داده شود بنابراین به نرم افزاری پیچیده برای اداره این قوانین مانند کنترل برخورد اطلاعات، کنترل ترافیک و ... نیاز داریم.
- قابلیت اطمینان پایین کانال: با قطع یا خرابی کانال مشـــترک ارتباط تمامی گره ها با یکدیگر از بین می رود.



شکل ۱-۱: شبکه پخش فراگیر

۲- نقطه به نقطه (point-to-point)

در این شـبکه (شـکل ۱-۲) بین هر دو گره درون شـبکه یک کانال وجود دارد که این کانال فقط مختص آن دو ایستگاه است. ما بین ایستگاه های مختلف مسیرهای متفاوتی وجود دارد بر خلاف شـــبکه های پخش همگانی که فقط یک کانال و یا یک مســـیر وجود دارد. انتخاب مســـیر بین فرسـتنده و گیرنده توسـط مسـیریابی انجام می شـود. امروزه از هر دو نوع شـبکه در کاربردهای گوناگون استفاده می شود.



شکل ۱-۲: شبکه‌های نقطه به نقطه

۱-۱۱-Topology یا همبندی یا ریخت شناسی

شبکه، اتصال چندین دستگاه به یکدیگر از طریق رسانه انتقال است.

سئوال: به چه اشکال یا روش هایی می توان گره ها را به یکدیگر متصل کرد؟

چگونگی اتصال واقعی گره ها به یکدیگر توسط رسانه انتقال یا کانال را توپولوژی می گویند.

به عبارت دیگر توپولوژی، ساختار یک شبکه را بیان می کند.

۱-۱۱-۱-انواع توپولوژی

۱-باس (Bus): در این توپولوژی (شکل ۱-۳) همه کامپیوترها مستقیماً به یک کانال مشترک متصل هستند.

مزایا:

- برپاسازی ساده و هزینه آن ارزان می باشد.

معایب: