网络规划设计师笔记

第 1 章 计算机网络原理

1.1 计算机网络概论（P1-10）

1、定义与应用

计算机网络是一个将分散的、具有独立功能的计算机系统，通过通信设备与线路连接起来，由功能完善的软件实现资源共享的系统。

计算机网络的几个应用方向：

对分散的信息进行集中、实时处理；共享资源；电子化办公与服务；通信；远程教育；娱乐等。

2、计算机网络组成

A：计算机网络物理组成

从物理构成上看，计算机网络包括硬件、软件、协议三大部分。

B：功能组成

从功能上，计算机网络由资源子网和通信子网两部分组成。

C：工作方式

从工作方式上看，也可以认为计算机网络由边缘部分和核心部分组成。

3、计算机网络分类

A：按分布范围分类

WAN、MAN、LAN、PAN（个域网）

B：按拓扑结构分类

总线型网络、星型网络、环形网络、树型网络、网格型网络等基本形式。也可以将这些基本型网络互联组织成更为复杂的网络。

C：按交换技术分类（注意区别各自的优缺点）

线路交换网络、报文交换网络、分组交换网络等类型。

D：按采用协议分类

应指明协议的区分方式。

E：按使用传输介质分类

有线（再按各介质细分）、无线

F：按用户与网络的关联程度分

骨干网、接入网、驻地网

4、网络体系结构

A：分层与协议

注意分层的三个基本原则

B：接口与服务

SAP

计算机网络提供的服务可分为三类：面向连接的服务与无连接的服务、有应答服务与无应答服务、可靠服务与不可靠服务

服务数据单元 SDU、协议控制信息 PCI、协议数据单元 PDU。三者的关系为：

N-SDU+N-PCI=N-PDU=（N-1）SDU

C：ISO/OSI 与 TCP/IP 体系结构模型

OSI 有 7 层，从低到高依次称为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。各层对应的数据交换单元分别为：比特流、帧、分组、TPDU、SPDU、PPDU、APDU

TCP/IP 从低到高各层依次为网络接口层、互联网层、传输层、应用层。网络接口层相当于 OSI 的物理层和数据链路层；互联网层相当于 OSI 的网络层；传输层相当于 OSI 的传输层；应用层相当于 OSI 的应用层；没有表示层和会话层。

第 1 章 计算机网络原理

1.2 数据通信基础（P11-46）

1、数据通信概念

A：数字传输与模拟传输

数字传输是指用数字信号来传送消息的通信方式。模拟传国是指以模拟信号来传输消息的通信方式。不论是数字数据还是模拟数据，都可以采用两种传输方式之一进行传输。

B：基带传输与频带传输

基带传输是指信号没有经过调制而直接送到信道中去传输的一种方式。频带传输是指信号经过调制后再送到信道中传输的一种方式，接收端要进行相应的解调才能恢复原来的信号。

2、数据通信系统

A：数据通信系统模型

数据通信系统的基本组成一般包括发送端、接收端、收发两端之间的信道三个部分。

参见 P16 图 1-11

B：同步方式

同步的实现包括位同步、字符同步、帧同步

C：检错与纠错（参阅 P43 1.2.7 节内容）

包括二维奇偶校验、循环冗余校验等检错方法。

检错重发方法有：停发等候重发、返回重发和选择重发。

3、数据调制与编码

A：数字数据的编码与调制

数字数据编码为数字信号：不归零码、曼彻斯特编码、差分曼彻斯特编码、双极性半空占码（AMI）、双极性 8 零替换码（B8ZS）、三阶高密度双极性码（HDB3）、nB/mB 码等。

数字数据调制为模拟信号：

基本调制方法：幅移键控（ASK）、频移键控（FSK）、相移键控（PSK）

正交振幅调制（QAM）

B：模拟数据的编码与调制

模拟数据编码为数字信号：PCM

模拟数据调制为模拟信号：AM、FM、PM

4、复用技术

A：时分复用

TDM，在进行通信时，复用器和分用器总是成对地使用。

时分复用(Time Division Multiplexer,TDM)是把一个传输通道进行时间分割以传送若干话路的信息，把 N 个话路设备接到一条公共的通道上，按一定的次序轮流的给各个设备分

配一段使用通道的时间。当轮到某个设备时，这个设备与通道接通，执行操作。与此同时，其它设备与通道的联系均被切断。待指定的使用时间间隔一到，则通过时分多路转换开关把通道联接到下一个要连接的设备上去。时分制通信也称时间分割通信，它是数字电话多路通信的主要方法，因而 PCM 通信常称为时分多路通信。 TDM 包括同步时分复用和统计时分复用。

B：频分复用

FDM，主要用于模拟信号。主要应用：无线电广播系统和有线电视系统。

频分复用(FDM，Frequency Division Multiplexing)就是将用于传输信道的总带宽划分成若干个子频带(或称子信道)，每一个子信道传输 1 路信号。频分复用要求总频率宽度大于各个子信道频率之和，同时为了保证各子信道中所传输的信号互不干扰，应在各子信道之间设立隔离带，这样就保证了各路信号互不干扰(条件之一)。频分复用技术的特点是所有子信道传输的信号以并行的方式工作，每一路信号传输时可不考虑传输时延，因而频分复用技术取得了非常广泛的应用。频分复用技术除传统意义上的频分复用(FDM)外，还有一种是正交频分复用(OFDM)。

C：波分复用

WDM 就是光的频分复用。波分复用系统主要由光发射机、光接收机、光放大器和光纤组成。

D：码分复用

教材暂无内容，需自己网上查找。

码分复用(CDM，Code Division Multiplexing)是靠不同的编码来区分各路原始信号的一种复用方式，主要和各种多址技术结合产生了各种接入技术，包括无线和有线接入。例如在多址蜂窝系统中是以信道来区分通信对象的，一个信道只容纳 1 个用户进行通话，许多同时通话的用户，互相以信道来区分，这就是多址。移动通信系统是一个多信道同时工作的系统，具有广播和大面积覆盖的特点。在移动通信环境的电波覆盖区内，建立用户之间的无线信道连接，是无线多址接入方式，属于多址接入技术。联通 CDMA(Code Division Multiple Access)就是码分复用的一种方式，称为码分多址，此外还有频分多址(FDMA)、时分多址(TDMA)和同步码分多址(SCDMA)。

E：统计时分复用

STDM 是一种改进的时分复用方法，它能明显地提高信道的利用率。集中器常使用这种方法。

5、数据交换方式

A：电路交换

主要用于电话系统。两大优点和两大缺点要记住：延迟小，无冲突，但建立时间长,资源浪费。

B：报文交换

采用的是存储—转发技术，动态分配线路，使得线路能够共享，提高了资源利用率。但它对数据块大小没有限制，所以不适合交互式通信。

C：分组交换

现代网络绝大多数采用分组交换技术。根据内部机制的不同，分组交换技术又分为数据报和虚电路两种方式。

数据报：每个分组的首部都带有完事的目的地址，交换机根据转发表转发分组。注意 6 特点。

虚电路：在发送数据之前，在源主机和目的主机之间建立一条虚连接。注意 6 特点。

D：信元交换

是异步传输模式 ATM 采用的交换方式，在很大程度上就是按照虚电路方式进行分组转发。在 ATM 网络中与众不同的一点是，分组长度是固定不变的，称为信元。信元长度为 53 字节，5 字节的首部，48 字节的有效载荷。

6、传输介质

A：双绞线

分为 STP 和 UTP

EIA/TIA-568-A 标准，规定了从 1 类线到 5 类线的 UTP 标准，其中 3 类线和 5 类线用于计算机网络

B：同轴电缆

具有很好的抗干扰特性，广泛用于传输较高速率的数据。

分为：50Ω同轴电缆（用于基带数字信号传送，10Mbps 可达 1KM）

75Ω同轴电缆（用于模拟传输系统，是 CATV 中的标准传输电缆）

C：光纤

就是能导光的玻璃纤维，有光脉冲表示比特 1，无光脉冲表示比特 0。注意 7 大特点。

光纤按传输方式可分为多模光纤和单模光纤。

多模光纤（MMF）：源为发光二极管，发出的可见光定向性较差，只适合于近距离传输。多模光纤电缆容许不同光束于一条电缆上传输，由于多模光缆的芯径较大，故可使用较为廉宜的偶合器及接线器，多模光缆的光纤直径为 50μm 至 100μm。

基本上有两种多模光缆，一种是梯度型（graded）另一种是引导型（stepped），对于梯度型（graded）光缆来说，芯的折光系数（refraction index)于芯的外围最小而逐渐向中心点不断增加，从而减少讯号的振模色散，而对引导型（Stepped Inder）光缆来说，折光系数基本上是平均不变，而只有在色层（cladding）表面上才会突然降低引导型（stepped）光缆一般较梯度型（graded）光缆的频宽为低。在网络应用上，最受欢迎的多模光缆为 62.5/125，62.5/125 意指光缆芯径为 62.5μm 而色层（cladding）直径为 125μm，其他较为普通的为 50/125 及 100/140。

相对于双绞线，多模光纤能够支持较长的传输距离，在 10mbps 及 100mbps 的以太网中，多模光纤最长可支持 2000 米的传输距离，而于 1GpS 千兆网中，多模光纤最高可支持 550 米的传输距离。

业界一般认为当传输距离超过 295 尺，电磁干扰非常严重，或频宽需要超过 350MHz，那便应考虑采用多模光纤代替双绞线作为传输载体。

多模光纤的芯线标称直径规格为 62.5μm/125μm.或 50μm/125μm.。规格（芯数）有 2、4、6、8、12、16、20、24、36、48、60、72、84、96 芯等。线缆外护层材料有普通型；普通阻燃性；低烟无卤型；低烟无卤阻燃型。

当用户对系统有保密要求，不允许信号往外发射时，或系统发射指标不能满足规定时，应采用屏蔽铜芯对绞电缆和屏蔽配线设备，或采用光缆系统。

单模光纤（SMF）：直径减小到只有一个光的波长大小，可使光线沿直线传播。光源采用定向性很好的激光二极管。因此，它的损耗较小，传输距离远。

几种单模光纤

G.652 单模光纤

满足 ITU-T.G.652 要求的单模光纤，常称为非色散位移光纤，其零色散位于 1．3um 窗口低损耗区，工作波长为 1310nm（损耗为 0．36dB／km）。我国已敷设的光纤光缆绝大多数是这类光纤。随着光纤光缆工业和半导体激光技术的成功推进，光纤线路的工作波长可转移到更低损耗（0.22dB／km）的 1550nm 光纤窗口。

G.653 单模光纤

满足 ITU-T.G.653 要求的单模光纤，常称色散位移光纤（DSF＝Dispersion Shifled Fiber），其零色散波长移位到损耗极低的 1550nm 处。这种光纤在有些国家，特别在日本被推广使用，我国京九干线上也有所采纳。美国 AT&T 早期发现 DSF 的严重不足，在 1550nm 附近低色散区存在有害的四波混频等光纤非线性效应，阻碍光纤放大器在 1550nm 窗口的应用。但在日本，将色散补偿技术*用于 G.653 单模光纤线路，仍可解决问题，而且未见有日本的 G.655 光纤，似属个谜。

G.655 单模光纤

满足 ITU-T.G.655 要求的单模光纤，常称非零色散位移光纤或 NZDSF（＝NonZero Dispersion Shifted Fiber)。属于色散位移光纤，不过在 1550nm 处色散不是零值（按 ITU-T.G.655 规定，在波长 1530-1565nm 范围对应的色散值为 0.1-6.0ps / nm.km)，用以平衡四波混频等非线性效应。商品光纤有如 AT&T 的 TrueWave 光纤，Corning 的 SMF-LS 光纤（其零色散波长典型值为 1567.5nm,零色散典型值为 0.07ps / nm2.km)以及 Corning 的 LEAF 光纤。我国的"大宝实"光纤等。

D：无线

包括陆地微波、卫星微波、无线电、红外线等

第 1 章 计算机网络原理　　1.3 网络体系结构（网络分层与功能）（P46-62）

1、应用层

A：应用层功能

应用管理、系统管理

B：应用层实现模型

P48 图 1-40 应用层实现模型，注意理解记忆

2、 传输层

A：传输层的功能

连接管理

优化网络层提供的服务质量

提供端到端的透明数据传输

多路复用的分流

B：传输层的实现模型

服务质量：主要是指差错率。因为无论何种网络，传输层都要向高层提供同样的服务，所以，如果通信子网的服务质量好，传输层所具有的功能就可以相应的少，反之，则多。

注意服务质量 A、B、C 三种类型

寻址：传输地址的构成有两种方法：层次地址和平面地址空间

建立和释放连接：

传输服务有两大类：面向连接的传输服务和无连接的传输服务。

面向连接的传输服务的两个用户进行相互通信，一般要经历三个过程：建立连接、数据传输和释放连接。（注意理解三个过程）

C：流量控制策略

流量控制是连接管理的基本内容之一，缓存是实行流量控制的必要措施。

3、 网络层

A：网络层功能

网络连接功能、路由选择功能、拥塞控制功能、数据传输功能、其它功能

B：数据报与虚电路

有两类构造通信子网的方法，即面向连接和无连接的方法。通常称连接为虚电路（VC），采用面向连接方法构造的通信子网称为虚电路通信子网。采用无连接方法构造的通信子网称为数据报通信子网。

4、 数据链路层

A：数据链路层功能

帧同步、链路管理、差错控制、流量控制

B：数据链路层差错控制方法

前向纠错（开销较大，不适合计算机通信）

检错重发（在计算机通信中常用检错重发方法）：目前，主要使用的检错码是奇偶校验码和循环冗余。

C：基本链路控制规程

数据链路层有两上基本链路控制规程:面向字符型链路控制规程和面向比特型链路控制规程（典型代表 HDLC）

D：数据链路层协议

最有代表性的是高级数据链路控制协议（HDLC）

HDLC 协议定义了三种站类型（主站、从站、复合站）、两种链路结构（不平衡型结构、平衡型结构）和三种数据响应模式（正常响应方式 NRM、异步响应方式 ARM、异步平衡方式 ABM）

5、物理层

注意：物理层并不是指物理设备或传输介质，而是有关物理设备通过特刊传输介质进行描述和规定

A：物理层功能

物理连接的建立、维持和释放

物理服务数据单元的传输

物理层管理

B：物理层协议

在物理层最常用的两种物理层标准是：EIA-232-E 接口标准和 RS-449 接口标准

本节还介绍了覆盖网与对等网（P2P），注意了解

第 1 章计算机网络原理 1.4 网络设备与网络软件（P62-72）

1、网卡

网络接口卡（NIC），又称网络适配器（NIA），简称网卡。用一雪窑冰天邮差 网计算机和网络电缆之间的物理连接。

网卡完成物理层和数据链路层的大部分功能。每块网卡都有一个唯一的地址（MAC）。

2、调制解调器（MODEM）

是计算机与电话线之间进行信号转换的装置。目前主要有两种：内置式和外置式。

它的一个重要性能参数是传输速率，有：28.8K、33.6K、56K。

3、交换机

也叫多端口网桥，工作在数据链路层，能够识别帧的内容。

A：交换机的功能

主要有三个功能：学习、转发/过滤、消除回路

B：交换机的工作原理

交换机根据收到 数据帧中的源 MAC 地址建立该地址同交换机端口的映射关系并将其写入 MAC 地址表中。当一台计算机发送过一次数据帧时，就被交换机记录下来；如果有其他的计算机向这台计算机发送数据时，数据只会从特定端口转发出去，而不会从其他端口转发。如果交换机收到的数据帧中的目的 MAC 地址不在 MAC 地址表中，则向所有端口转发。另个，广播帧和组播帧也向所有的端口转发。

交换机可以隔离冲突域，交换机的每个端口就是一个小的冲突域。

MAC 地址与端口的映射表（CAM），其中的记录时效为 300s，如果 300s 内没有得到更新，记录就会被删除。

C：交换机的类型（详细分类请参阅：交换机的类型）

（一）根据网络覆盖范围分：局域网交换机和广域网交换机。

（二）根据传输介质和传输速度划分： 以太网交换机、快速以太网交换机、千兆以太网交换机、10 千兆以太网交换机、ATM 交换机、FDDI 交换机和令牌环交换机。

（三）根据交换机应用网络层次划分：企业级交换机、校园网交换机、部门级交换机和工作组交换机、桌机型交换机。

（四）根据交换机端口结构划分：固定端口交换机和模块化交换机。

（五）根据工作协议层划分：第二层交换机、第三层交换机和第四层交换机。

（六）根据是否支持网管功能划分：网管型交换机和非网管理型交换机。

注意区别交换机堆叠与级联，掌握其各自的优缺点。

4、路由器

是属于网络层的互联设备，用于连接多个逻辑上分开的网络。

A：路由器的功能

网络互连、路由选择、分组转发、拆分和包装数据包、拥塞控制、网络管理、网络计费等功能

B：路由器的结构与工作原理

一般 来说，路由器的主要工作是对数据包进行存储转发，具体过程如下：

第一步，主要是对数据的完事性进行验证。

第二步，开始处理数据帧的 IP 层，是路由器功能的核心。

第三步，根据跟路由表所查到的下一跳 IP 地址，将 IP 数据包送往相应的输出链路层。

简单地说，路由器的主要工作就是为经过路由器的每个数据包寻找一条最佳传输路径，江将该数据包有效地传送到目的站点。

5、网关

又叫协议转换器。主要用于不同体系结构的网络或者局域网与主机系统的连接。它一般是软件产品。

6、无线局域网设备（AP、AC）

AP 即无线接入点，单纯性无线 AP 就是一个无线的交换机，仅仅是提供一个无线信号发射的功能。理论上最大可达 300M，实际使用范围：室内 30M、室外 100M（无障碍物）

AC 即无线控制器

7、防火墙

教材暂无内容，需自行到网上搜索

8、网络操作系统

教材暂无内容，需自行到网上搜索

9、常用的网络软件

主要包括：通信软件、网络协议软件、网络应用系统等

第 1 章计算机网络原理 1.5 局域网（P73-95）

1、局域网基础知识

A：局域网定义

局域网为计算机局部区域网络（LAN）的简称。

IEEE 标准中描述：局域网是一种为单一机构所拥有的专用计算机网络，其通信被限制在中等规模的地理范围，具有较高数据速率和较低的误码率，能有效实现多种设备之间互联、信息交换和资源共享。

B：局域网拓扑结构

主要有总线型（最早，已经被淘汰）、环型（基本上不再使用，但环形广域网还在广泛使用）、星型（是目前广泛使用的）

2、访问控制方式

A：访问控制方式的分类

访问控制方式 用于控制节点对介质的访问。按实现方式的不同，可以将访问控制方式分为以下三类：不加控制、集中控制、分布控制

B：令牌访问控制方式

原理、问题及对策。P75

C：CSMA/CD 访问控制方式

原理、延迟时间的确定。P76

3、局域网协议

A：IEEE802LAN 体系结构与协议

了解参阅 P77 页内容。

B：IEEE802.3 协议

现在帧格式是直接封装 IP 包的格式。FCS（帧校验和）按 CRC-32 生成 4 字节的 CRC 校验和。原始的802.3物理层采用曼彻斯特编码,但802.3u采用4B/5B编码,802.3z采用8B/10B编码，802.3ae 采用 64B/66B 编码。

4、高速局域网

A：100M 以太网(IEEE802.3u)

100Base-T 标准定义了介质无关接口（MII）。

有以下三种传输介质标准：

100Base-TX：2 对 5 类 UTP，最长 100M，4B/5B，全双工。

100Base-T4：4 对 3 类 UTP，最长 100M，8B/6T,半双工。

100Base-FX：两条光纤，最长 415M，4B/5B-NRZI，全双工。

B：1G 以太网(IEEE802.3z)

包括 4 种物理层标准：

1000Base-LX：光纤、星型、MMF 半双工最长 316M，全双工最长 550M、SMF 半双工最长 316M，全双工最长 5000M、8B/10B 编码。

1000Base-SX：光纤、星型、62.5umMMF 时半和全双工最长均 275M、50umMMF 半和全双工最长均为 550M、8B/10B 编码。

1000Base-CX：特殊的 STP、星型、半双工最长 25M、全双工最长 50M、8B/10B

1000Base-T：4 对 5 类 UTP、星型、最长 100M、RJ-45 接口、PAM5 编码方法（PAM5 采用 5 种不同的信号电平编码来代替简单的二进制编码，可以达到很好的带宽利用。基本 PAM5 的 10GBASE-T 对布线带宽的需求是 625MHz。）

C：10G 以太网

主要物理层协议：

10000Base-ER：1550nm 波长激光、10umSMF 最长 40KM、64B/66B 编码

10000Base-EW：1550nm 波长激光、10umSMF 最长 40KM、64B/66B 编码

10000Base-LR：1310nm 波长激光、10umSMF 最长 40KM、64B/66B 编码

10000Base-L4：1310nm 波长激光、62.5umMMF 最长 240M、50umMMF 最长 300M、10umSMF 最长 40KM、8B/10B 编码

10000Base-SR：850nm 波长激光、62.5umMMF 最长 35M、50umMMF 最长 300M、64B/66B 编码

10000Base-SW：850nm 波长激光、62.5umMMF 最长 35M、50umMMF 最长 300M、64B/66B 编码

5、无线局域网

A：Wi-Fi(802.11)无线局域网

无线传输介质按所采用的传输技术可以分为三类：红外线局域网、扩频局域网和 OFDM（正交频分多路复用）局域网。

红外线局域网的数据传输有三种基本技术：定向光束红外传输、全方位红外传输、漫反向红外传输。红外线波长 850～950nm，数据传输速率为 1Mbps 或 2Mbps。注意优缺点。

扩频无线局域网有两种数据传输技术：FHSS、DSSS

OFDM 无线局域网将无线信号分成多路正交的信号，合在一起传输。

由一个访问点 AP 和若干移动主机组成一个基本服务集 BSS、多个 BSS 组成一个扩展服务集 ESS。

WLAN 的两种访问控制方式：点协调功能（PCF）、分布式协调功能（DCF，即 CSMA/CA）。

B：蓝牙技术

蓝牙系统的基本单元是微微网。每个微微网都饮食一个主节点，最多 7 个活动的从节点，以及可以多达 255 个静观节点。

1.0 标准规定主从节点之间的距离不超过 10M、数据率为 720Kbps。

2.0 标准有望 100M、10Mbps

6、虚拟局域网

A：VLAN 的概念

是由一些 LAN 网段构成的与物理位置无关的逻辑组。主要标准是 IEEE802.1Q

B：VLAN 的实现

VLAN 是通过软件的方法，逻辑的而不是物理地将节点划分成一个个网段。

C：IEEE802.1Q/ISLVTP 协议

在一个 VTP 环境里，一台交换机可以是以下三种不同的角色之一。可以是一台 VTP 服务器、一台 VTP 客户机、或者工作在透明模式。

7、冗余网关技术（HSRP、VRRP、GLBP）

教材暂无内容

8、以太网环保护技术（RPR）

教材暂无内容

第 1 章计算机网络原理 1.6 广域网与接入（P95-124）

1、 广域网的概念

WAN 是指将跨地区的各种局域网、计算机、终端等互边在一起的计算机通信网络。

常见的 WAN 有公用电话网、公用分组交换网、公用数字数据网、宽带综合业务数字网、帧中继网和大量的专用网。

2、 拥塞控制

A：拥塞概念

当网络中存在过多的数据包时，网络的性能就会下降，这种现象称为拥塞。

B：拥塞控制原理

拥塞控制算法可以分为开环控制和闭环控制两大类。当流量特征可以准确规定、性能要求可以事先获得时，适于使用开环控制；当流量特征不能准确描述或者当系统不提供资源预留时，适于使用闭环控制。

Internet 中主要采用闭环控制方式，以动态适应网络的变化。

C：拥塞控制方法

主要有基于终端的拥塞控制和基于链路的拥塞控制。

3、 公用通信网

A：PSTN

即公共电话交换网

B：ISDN/BISDN 网络

ISDN 即综合数字网。有 N-ISDN 和 B-ISDN。

B-ISDN 即宽带 ISDN 最高可达 622Mbps 数量级。

C：SDH 网络

即光同步数字传输网。

主要特点：统一的光接口、自愈环、SDH 网同步。

D：WDM 网络

波分复用（WDM）实质是光域上的 FDM 技术。系统由光合波器和可以提取独立光波长的光分波器组成。

主要特点：传输容量大、对各类业务信号“透明”、网络扩容方便、组建动态可重构光网络时具有高度灵活性可靠性生存性。

E：MSTP 网络

即基于 SDH 的多业务传送平台，是指基于 SDH 平台同时实现 TDM、ATM、以太网等业务的接入、处理和传送，提供统一网管的多业务节点。

主要特点：业务的带宽灵活配置、可以根据业务的需要，工作在端口组方式和 VLAN 方式、可以工作在全双工、半双工和自适应模式下、QoS 设置、对每个客户独立运行生成树协议。

F：移动通信网络

第二代移动通信网络主要有 GSM、GPRS、CDMA 等。

第三代（3G）网络依据三大主流无线接入技术有：WCDMA、CDMA2000、TD-SCDMA 网络。

4、接入技术

A：PSTN 接入

即拨号接入。已面临着逐渐被淘汰的局面。

B：ISDN 接入

俗称“一线通”。特点：一线多能、连接速度快、成本低连接质量好。

但逐步会被 ADSL 接入所取代。

C：xDSL 接入

数字用户线路。可以分为两大类：非对称 DSL 和对称 DSL。目前共有 7 种 DSL。

注意了解：ADSL、VDSL

D：Cable Modem 接入

主要用于有线电视系统。

E：局域网接入

目前新建住宅小区和商务楼流行局域网方式接入。

F：无线接入

无线接入扶杖在致可分为三种：

低速无线本地环、宽带无线接入、卫星接入

宽带无线接入当前有以下几大技术注意了解：

LMDS（本地多点分配系统）、MMDS（多点多信道分配系统）、无线局域网、蓝牙及其他（如红外等）

G：光网络接入（PON）

光纤接入网是指局端与用户之间完全以光纤作为传输媒体。方案有：光纤到路边(FTTC)、光纤到小区（FTTZ）、光纤到办公楼（FTTB）、光纤到楼面（FTTF）、光纤到家庭（FTTH）。

光纤接入网可以粗分为有源和无源两类。

无源光网络（PON）由光线路终端（OLT）、光网络单元（ONU）和光分配网络（ODN)组成。

目前 PON 技术主要有 APON(基于 ATM 的 PON)、EPON(基于以太网的 PON)和 GPON(Gigabit PON）等几种。

广域网组网可划分为三及网络：第一级为骨干网、第二级为分布网、第三级为接入网。网络规模不大时可直接由骨干网和接入网组成。

第 1 章计算机网络原理 1.7 网络互连（P124-142）

1、 网络互连概念

网络互连（internetworking）是指利用各种网络互连设备将同一类型的网络或不同类型网络及其产品相互连接起来组成地理覆盖范围更大、功能更强的网络。

2、 网络互连方法

主要包括：

A：LAN-LAN

互连设备是：

中继器：物理层设备。两端连接是相同的媒体，同样的速率。最简单最廉价的方法，但所构成的网络为介质共享网络即共享式网络，所有设备都处于一个冲突域或碰撞域中。只有当网络负载很轻和网络时延要求不高的条件下才能使用这种网络。

集线器：被你为多口中继器，也工作在物理层。全部端口属于一个冲突域，又属于一个广播域。使用集线器扩展 LAN 扩大了局域网覆盖的地理范围，但同时碰撞域也增大了，总的吞吐量并未提高。当不同碰撞域使用不同数据率时，不能用集线器将它们互连起来。共享式 HUB 正逐渐退出局域网领域。

网桥：工作在数据链路层，它根据 MAC 帧的**目的地址**对收到的帧进行转发。

网桥的功能有：源地址跟踪、帧的转发和过滤、协议转换。

使用风格扩展局域网时，所有主机都处于一个广播域上。所以不能使用风格互连规模较大的网络，以免形成广播风暴。

交换机：工作在数据链路层，可以看做是高档集线器，也你为交换式集线器。

路由器：工作在网络层。通过路由器可以形成更多的广播域或逻辑网段，从而提高网络的性能。如果互连的局域网高层采用了不同的协议，就需要用多协议路由器。

B：LAN-WAN

LAN-WAN 的互连发生在网络层。互连设备是路由器。我国绝大多数路由器运行 TCP/IP 协议。

C：WAN-WAN

WAN-WAN 互连发生在传输层及其上层。互连设备是网关。

3、路由算法

A：静态路由算法

也就非自适应路由选择算法。特点是：算法简单、开销较小、但性能差、效率低。分为以下几类：固定路由算法、分散通信量法、洪泛法、随机走动法。

B：自适应路由算法

也叫动态路由选择算法。特点是：能较好地适应网络状态的变化，但实现起来比较复杂。

分为以下几类：

a、孤立自适应路由选择算法。热土豆算法、反向探知算法

b、分布式路由选择算法。距离向量路由选择算法、链路状态路由选择算法

C：广播路由算法

a、广播路由选择算法：独立发送法、扩散方法、多目的路径选择、生成树方法、逆向转发方法。

b、组播路由选择算法。

D：分层路由算法

也就分组路径选择算法，其基本思想就是先将网络分成区域，将区域分成簇，再将簇分成区，区分为组，直到最后每个单位内节点较少为止。

第 1 章计算机网络原理 1.8 Internet 协议（P142-203）

1、网络层协议

（1）IPv4 协议

IP 地址是由 32 位二进制数年，即 4 个字节组成的，它与硬件没有任何关系，所以也称为逻辑地址。

（2）IP 地址与子网概念

IP 地址由网络号和主机号两个字段组成。因特网的 IP 地址分为 5 类，即 A 类到 E 类。目前大量使用的 IP 地址是 A、B、C 三类。当某单位申请到一个 IP 地址时，实际上只是获得了一个网络号 NET-ID，具体的各个主机号由本单位自行分配。

A 类：0.0.0.0～127.255.255.255

B 类：128.0.0.0～191.255.255.255

C 类：192.0.0.0～223.255.255.255

D 类：224.0.0.0～239.255.255.255

E 类：240.0.0.0～255.255.255.255

特殊含义的地址：

网络号	主机号	含义
127	任意	回播地址
全 0 二进制	任意	当前子网中的主机
全 1 的二进制	全 1 的二进制	本地子网的广播（也称受限广播地址或有限广播地址）
任意	全 1 的二进制	特定子网的广播（直接广播地址）

内部私有地址

A 类 10.0.0.0--10.255.255.255

B 类 172.16.0.0--172.31.255.255

C 类 192.168.0.0--192.168.255.255

在一个局域网中，有两个 IP 地址比较特殊，一个是网络号，一个是广播地址。网络号是用于三层寻址的地址，它代表了整个网络本身，另一个是广播地址，它代表了网络全部的主机。网络号是网段中的第一个地址，广播地址是网段中的最后一个地址，这两个地址是不能配置在计算机主机上的。

在 IP 地址中增加一个 subnet-id 字段，使二级的 IP 地址变成为三级的 IP 地址。这种做法叫做划分子网，划分子网纯属一个单位内部的事情。

VLSM、CIDR 都可进一步提高 IP 地址资源的利用率

（3）IPv4 分组格式

P145 页图 1-84 注意即可。

（4）IP 封装与分片

IP 数据报处于网络层，它的长度一定不能超过数据链路层的最大传送单元 MTU。通常以太网的 MTU 为 1500B，PPP 的 MTU 为 296B，FDDI 的 MTU 为 4352B，令牌环的 MTU 为 4464B。封装与分版见 P145 图 1-85

（5）路由协议

路由协议的核心就是路由算法

（6）路由信息协议 RIP

是一种分布式的基于距离向量的路由选择协议。它允许一条路径最多只能包含 15 个路由器。距离的最大值为 16 时即为不可达。

RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离记录，并依此来形成自己的路由表。且按固定时间（一般 为 30s）和相邻路由器交换路由表。

RIP 属于应用层协议，它使用运输层的用户数据报 UDP 进行传送。

（7）开放最短路径优先协议 OSPF

是分布式的链路状态路由协议。每个路由器需要定期（10s）向邻居路由器发送 HELLO 分组。如果 40s 都没有收到邻居的 HELLO 信息，则认为该邻居是不连通的，应该立即修改链路状态数据库中所对应的记录，并要重新计算路由表。

除了 HELL 问候分组外，OSPF 协议还有 4 种分组：链路状态更新分组、链路状态确认分组、数据库描述分组、链路状态请求分组。

（8）边界网关协议 BGP

是不同自治系统的路由器之间交换路由信息的协议。BGP 只是尽力找一条能够到达目的网络且比较好的路由（不能兜圈子），而不像内部网关协议一样要寻找一条最佳路由。

当一个 BGP 发言人与其他自治系统中的 BGP 发言人交换路由信息时，首先要建立 TCP 连接，然后在此连接上交换 BGP 报文以建立 BGP 会话，利用 BGP 会话交换路由信息。

BGP-4 共有 4 种报文：打开报文、更新报文、保活报文、通知报文。

（9）组播协议 PIM 与 MOSPF

PIM 能在现砒 IP 网上传输组播数据。PIM 是一种独立于路由协议的组播协议，可以工作在 PIM-DM（密集模式，报文分组默认向所有端口转发）和 PIM-SM（疏松模式，只向有请求的端口发送组播数据）。

MOSPF 是为单播路由组播使用设计的，属于 PIM-DM 的组播路由协议。它依赖于 OSPF 作为单播路由协议，在一个 OSPF/MOSPF 网络中每个路由器都维持一个最新的全网络拜年结构图。

第 1 章计算机网络原理 1.8 Internet 协议（P142-203）

（10）地址解析协议 ARP 与反向地址解析协议 RARP

ARP：**将 IP 地址转换为相应物理地址**

RARP：正好相反

（11）Internet 控制报文协议 ICMP

ICMP 协议允许路由器报告差错情况和提供有关异常情况的报告。ICMP 报文有 ICMP 差错报文和 ICMP 询问报文两种。

注意 P153 表 1-8 几种 ICMP 报文及功能。

（12）IPv6 协议

IPv6 是"Internet Protocol Version 6"的缩写，也被称作下一代互联网协议，它是由 IETF 设计的用来替代现行的 IPv4 协议的一种新的 IP 协议。

IPv6 是为了解决 IPv4 所存在的一些问题和不足而提出的，同时它还在许多方面提出了改进，例如路由方面、自动配置方面。经过一个较长的 IPv4 和 IPv6 共存的时期，IPv6 最终会完全取代 IPv4 在互连网上占据统治地位。对比 IPv4，IPv6 有如下的特点，这些特点也可以称作是 IPv6 的优点：简化的报头和灵活的扩展 ；层次化的地址结构 ；即插即用的连网方式 ；网络层的认证与加密 ；服务质量的满足 ；对移动通讯更好的支持。

（13）IPv6 地址

从 IPv4 到 IPv6 最显著的变化就是网络地址的长度。RFC 2373 和 RFC 2374 定义的 IPv6 地址，就像下面章节所描述的，有 128 位长；IPv6 地址的表达形式一般采用 32 个十六进制数。

IPv6 中可能的地址有 2 ≈ 3.4×10 个。也可以想象为 16 个因为 32 位地址每位可以取 16 个不同的值。

在很多场合，IPv6 地址由两个逻辑部分组成：一个 64 位的网络前缀和一个 64 位的主机地址，主机地址通常根据物理地址自动生成，叫做 EUI-64（或者 64-位扩展唯一标识）。

（14）IPv6 分组格式

IPv6 包头长度固定为 40 字节，去掉了 IPv4 中一切可选项，只包括 8 个必要的字段，因此尽管 IPv6 地址长度为 IPv4 的四倍，IPv6 包头长度仅为 IPv4 包头长度的两倍。

（15）IPv6 地址自动配置

IPv6 的一个重要目标是支持节点即插即用。也就是说，应该能够将节点插入 IPv6 网络并且不需要任何人为干预即可自动配置它。

自动配置的类型

IPv6 支持以下类型的自动配置：

全状态自动配置。

无状态自动配置。

IPv6 移动性

移动设备的迅速普及带来了一项新的要求：设备必须能够在 IPv6 Internet 上随意更改位置但仍维持现有连接。为提供此功能，需要给移动节点分配一个本地地址，通过此地址总可以访问到它。在移动节点位于本地时，它连接到本地链路并使用其本地地址。在移动节点远离本地时，本地代理（通常是路由器）在该移动节点和正与其进行通信的节点之间传递消息。

（16）邻节点发现过程

邻居发现协议中定义了 5 种类型的信息：路由器宣告、路由器请求、路由重定向、邻居请求和邻居宣告。

（17）IPv4 向 IPv6 的过渡

对于 IPV4 向 IPV6 技术的演进策略，业界提出了许多解决方案。特别是 IETF 组织专门成立了一个研究此演变的研究小组 NGTRANS，已提交了各种演进策略草案，并力图使之成为标准。纵观各种演进策略，主流技术大致可分如下几类：

双栈策略

隧道技术

TB（Tunnel Broker，隧道代理）

双栈转换机制（DSTM）

协议转换技术

SOCKS64

传输层中继（Transport Relay）

应用层代理网关（ALG）

2、传输层协议 TCP 与 UDP

（1）TCP 协议

TCP 是面向连接的协议，提供可靠的、全双工的、面向字节流的、端到端的服务。

（2）TCP 定时管理机制

重传机制是保证 TCP 可靠性的重要措施。

（3）TCP 拥塞控制策略（含 RED）

TCP 拥塞控制主要有以下 4 种方法：慢开始、拥塞避免、快重传、快恢复、随机早期检测 RED。

（4）UDP 协议

UDP 只在 IP 的数据报服务之上增加了很少一点的功能，即端口的功能和差错检测的功能。

3、应用层协议

（1）域名系统 DNS

功能是把 Internet 中的主机域名解析为对应的 IP 地址。域名系统 DNS 是一个联机分布式数据库系统。工作方式采用客户服务器方式。

每一级地域名都由英文字母和数字组成（不超过 63 个字符，并且不区分大小写字母），完事的域名不超过 255 个字符。

目前顶级域名（TLD）有国家顶级域名、国际顶级域名、通用顶级域名三大类。

域名服务器分为根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器 4 种不同类型。

在域名的解析过程上，本地域名服务器可以采用递归查询和迭代查询两种查询方式。

（2）电子邮件协议

有发送协议 SMTP、接收协议 POP3/IMAP4。

邮件保密：PGP 协议、PEM 协议

（3）文件传输协议 FTP

主要功能是养活或消除在不同操作系统下处理文件的不兼容性。

FTP 的客户和服务器之间需要建立两个 TCP 连接：控制连接和数据连接。

FTP 的命令主要有 get、put、mput、mget、ls。

（4）远程登录协议 Telnet

一个 TELNET 连接就是一个用来传输带有 TELNET 控制信息数据的 TCP 的连接。

（5）Web 应用与 HTTP 协议

www 使用统一资源定位符 URL 来标识分布在整个 INTERNET 上的文档。

Web 文档有三类：静态 WEB 文档、动态 WEB 文档、活动 WEB 文档。

超文本传输协议（HTTP）

（6）动态主机配置协议 DHCP

动态主机設定協定（DHCP）是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。在 IP 网络中，每个连接 Internet 的设备都需要分配唯一的 IP 地址。DHCP 使网络管理员能从中心结点监控和分配 IP 地址。当某台计算机移到网络中的其它位置时，能自动收到新的 IP 地址。

DHCP 使用了租约的概念，或称为计算机 IP 地址的有效期。租用时间是不定的，主要取决于用户在某地联接 Internet 需要多久，这对于教育行业和其它用户频繁改变的环境是很实用的。通过较短的租期，DHCP 能够在一个计算机比可用 IP 地址多的环境中动态地重新配置网络。

DHCP 支持为计算机分配静态地址，如需要永久性 IP 地址的 Web 服务器。

DHCP 和另一个网络 IP 管理协议 BOOTP 类似。目前两种配置管理协议都得到了普遍使用，其中 DHCP 更为先进。某些操作系统，如 Windows NT/2000，都带有 DHCP 服务器。DHCP 或 BOOTP 客户端是装在计算机中的一个程序，这样就可以对其进行配置操作。

（7）P2P 应用协议

P2P 是 peer-to-peer 的缩写

点对点技术（peer-to-peer，简称 **P2P**）又称**对等互联网络技术**，是一种网络新技术，依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。但 P2P 并非纯粹的点对点技术，实为解作群对群(Peer-to-Peer)。在虚拟私人网

络 VPN (Virtual Private Network)中，也有 P2P 这个名称，它才是真正解作点对点(Point-to-Point)。

下面试图用三句话来揭示 P2P 的影响：

对等联网：是只读的网络的终结（Peer-to-peer is the end of the read-only Web）

对等联网：使你重新参与互联网（Peer-to-peer allows you to participate in the Internet again）

对等联网：使网络远离电视(Peer-to-peer steering the Internet away from TV)如上文所言，P2P 不是一个新思想，从某些角度看它甚至是整个最初创建互联网的最基本的思想。我们不妨花时间作一点回顾。

4、代理与 NAT

应用层代理工作在 TCP/IP 模型的应用层之上，它只能用于支持代理的应用层协议（如 HTTP、FTP）

网络地址转换（NAT）有三种类型：静态 NAT、动态地址 NAT、端口地址转换 PAT

5、无线网路协议

（1）移动 IP 协议

教材上暂时没有，请参阅以下文章

移动 IP 技术简介

（2）无线 TCP

教材上暂无内容。

（3）无线 Web 协议 WAP

WAP 协议栈的组成结构：WAE（应用层即无线应用环境）、WSP（无线会话层）、传输协议层（WTP）、安全协议层（WTLS）、数据报协议层(WDP)

第 1 章计算机网络原理 1.9 网络管理（P203-246）

1、网络管理基本概念

网络管理是指对网络的运行状态进行检测和控制，并能提供有效、可靠、安全、经济的服务。简单地说，网络管理就是对网络的监测和控制。

在网络管理中，一般采用管理站-代理的管理模型。

2、管理信息的组织与表示

（1）抽象语法表示 ASN.1

ASN.1 是由 CCITT 和 ISO 共同开发的正规语言，它与应用层一起使用，可在系统间进行数据的传输。

它定义的通用数据类型有 20 种，可分为四大类：简单类型、构造类型、标签类型、其他类型。

（2）管理信息结构 SMI

经 SNMP 协议传输的所有管理信息都被收集到一个或多个管理信息库（MIB）中，被管对象类型按照 SMI 和标识定义。管理信息结构主要包括以下三个方面：对象的标识、对象的语法、对象的编码。

（3）管理信息库 MIB

1988 年 8 月，在 RFC1066 中第一组被管对象，被认为是 MIB-1，它包括了 8 个对象组，约 100 个对象。

1990 年 5 月，在 RFC1158 中公布了 MIB-2，扩展了 MIB-1 已有的对象组。

在 RFC1213 中，MIB-2 被彻底修订并采纳 RFC212 中的简洁 MIB 定义，这一文档使 RFC1158 失效。

3、 简单网络管理协议

（1）SNMPv1、SNMPv2、 SNMPv3

A：SNMPv1 规定了 5 种协议数据单元（PDU），用来管理进程和代理之间的交换。

GetRequest 操作、GetNextRequest 操作、SetRequest 操作、GetResponse 操作、Trap 操作。前面三种操作是由管理进程向代理进程发出的，后面的两个操作是代理进程发给管理进程的。

SNMP 报文共有三个部分组成,即公共 SNMP 首部、Get/Set 首部、Trap 首部、变量绑定。

B：SNMPv2 改进了 SNMPv1

SNMPv2 消息中可以传送 7 类 PDU。除 SNMPv1 中的 5 种 PDU 具有完全相同的格式，并且也可以看作是 error-status 和 error-index 两个字段被置 0 的 ResPonse PDU 的格式。

C：1999 年 4 月发布的 SNMPv3 新标准，包含了全面的安全性技术。SNMPv3 只是一个安全规范，没有定义其他新的 SNMP 功能，只为 SNMPv1 和 SNMPv2 提供安全方面的功能。

（2）RMON

远程网络监视（RMON）是对 SNMP 标准的重要补充，是简单网络管理向互联网管理过渡的重要步骤。RMON 扩充了 SNMP 的管理信息库 MIB-2。

4、网络管理工具

（1）基于 Web 的管理

WBM。具有以下优点：地理上和系统上的可移动性、具有统一的网络管理程序界面、网络管理平台具有独立性、网络管理系统之间可无缝连接。

WBM 的实现方式有两种：一种是基于代理的解决方案、一种是嵌入式解决方案。

（2）典型网络管理工具

CiscoWorks for Windows

HP OpenView

IBM Tivoli NetView

Sun Net Manager

第 1 章计算机网络原理 1.10 服务质量控制技术（P246-271）

1、IntServ

A、定义：最初试图在因特网中将网络提供的服务划分为不同类别的是 IEEE 提出的综合服务 IntServ。IntServ 可对单个的应用会话提供服务质量的保证。

B、特点：（1）资源预留

（2）呼叫建立

C、分类

IntServ 定义了三种服务：（1）有保证的服务：为端到端的分组排队的延时提供稳定的（数学上可证明的边界，使得提供保证延时和带宽的服务成为可能。（2）受控负载的服务：提供近于尽力而为型服务。

（3）尽力服务：不提供任何类型的服务保证。

D、组成部分

IntServ 的四个组成部分：

（1）资源预留协议 RSVP，也就是信令协议

（2）接纳控制（admission control）程序

（3）分类程序（classifier）

（4）调度程序（scheduler）

2、DiffServ

区分服务体系结构（DiffServ）定义了一种可以在互联网上实施可扩展的服务分类的体系结构。它的设计目标是提供一种简单的、容易实现并且是低成本的工具来支持一系列的网络服务，这些服务在性能的基础上有所区分。

DiffServ 基实现途径：简化网络内部节点的服务机制、简化网络内部节点的服务对象。

特点：层次化结构、总体集中控制策略、增强了灵活性与通用性、不影响路由。

体系结构：DS 域与 DS 区、区分服务标记域与区分服务码点 DSCP、边界节点的传输分类与调节机制、逐跳行为（PHB）。

服务类型：优质服务、确保服务、其他服务类型。

3、MPLS（Multi-Protocol Label Switching）

多协议标签交换（MPLS）是一种用于快速数据包交换和路由的体系，它为网络数据流量提供了目标、路由、转发和交换等能力。更特殊的是，它具有管理各种不同形式通信流的机制。MPLS 独立于第二和第三层协议，诸如 ATM 和 IP。它提供了一种方式，将 IP 地址映

射为简单的具有固定长度的标签，用于不同的包转发和包交换技术。它是现有路由和交换协议的接口，如 IP、ATM、帧中继、资源预留协议（RSVP）、开放最短路径优先（OSPF）等等。

在 MPLS 中，数据传输发生在标签交换路径（LSP）上。LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。现今使用着一些标签分发协议，如标签分发协议（LDP）、RSVP 或者建于路由协议之上的一些协议，如边界网关协议（BGP）及 OSPF。因为固定长度标签被插入每一个包或信元的开始处，并且可被硬件用来在两个链接间快速交换包，所以使数据的快速交换成为可能。

MPLS 主要设计来解决网路问题，如网路速度、可扩展性、服务质量（QoS）管理以及流量工程，同时也为下一代 IP 中枢网络解决宽带管理及服务请求等问题。

转发等价类

MPLS 作为一种分类转发技术，将具有相同转发处理方式的分组归为一类，称为转发等价类 FEC（Forwarding Equivalence Class）。相同转发等价类的分组在 MPLS 网络中将获得完全相同的处理。

转发等价类的划分方式非常灵活，可以是源地址、目的地址、源端口、目的端口、协议类型、VPN 等的任意组合。例如，在传统的采用最长匹配算法的 IP 转发中，到同一个目的地址的所有报文就是一个转发等价类。

MPLS 的基本工作过程：

1. LDP 和传统路由协议（如 OSPF、ISIS 等）一起，在各个 LSR 中为有业务需求的 FEC 建立路由表和标签映射表；

2. 入节点 Ingress 接收分组，完成第三层功能，判定分组所属的 FEC，并给分组加上标签，形成 MPLS 标签分组，转发到中间节点 Transit；

3. Transit 根据分组上的标签以及标签转发表进行转发，不对标签分组进行任何第三层处理；

4. 在出节点 Egress 去掉分组中的标签，继续进行后面的转发。

由此可以看出，MPLS 并不是一种业务或者应用，它实际上是一种隧道技术，也是一种将标签交换转发和网络层路由技术集于一身的路由与交换技术平台。这个平台不仅支持多种高层协议与业务，而且，在一定程度上可以保证信息传输的安全性。

第 2 章计算机网络规划与设计 2.1 设计基础（P272-291）

1、网络基本元素

计算机网络由多种基本元素组合而成，常见的网络基本元素包括计算机平台、应用软件、物理设备和拓扑结构、网络软件和实用软件、互联设备和广域网连接等。

2、网络互联设备

注意参阅 P274 表 2-1。

网络互联设备主要包括中继器、集线器、网桥、交换机、路由器、网关等。

熟记 P275 图 2-1

3、网络性能

在进行网络设计时，对网络性能参数的考虑是设计工作的重点内容之一，需要考虑的网络性能参数包括响应时间、吞吐量、延迟、带宽、容量等。

4、网络设计文档

分为两类：一类是网络设计过程中填写的各种图表，可称为工作表格；另一类是应编制的技术资料或技术管理资料，可称为文档或文件。

文档的质量：针对性、精确性、清晰性、完整性、灵活性。

文档的管理和维护：注意 6 个方面的事。

第 2 章计算机网络规划与设计 2.2 网络分析与设计过程（P292-303）

1、网络生命周期

一个网络系统从构思开始，到最后被淘汰的过程被称为网络的生命周期。一般来说网络的生命周期至少包括网络系统的构思计划、分析设计、实时运行和维护的过程。

它首先是一个循环迭代的过程，每次循环迭代的动力都来自于网络应用需求的变更；其次每次循环过程事，都存在需求分析、规划设计、实施调试和运营维护等阶段。

目前没有哪个迭代周期可以完美描述所有项目的开发构成，但是常见的主要有三种：

四阶段周期：构思与规划阶段、分析与设计阶段、实施与构建阶段和运行与维护阶段。

长处：工作成本较低、灵活性高。

适用于网络规模较小、需求较为明确、网络结构简单的网络工程。

五阶段周期：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

优势：所有的计划在较早的阶段完成，所有负责人对系统的具体情况以及工作进度都非常清楚，更容易协调工作。

缺点：比较死板，不灵活。

适用于网络规模较大，需求较为明确，在一次迭代过程中需求变更较小的网络工程

六阶段周期：需求分析、逻辑设计、物理设计、设计优化、实施及测试、监测及性能优化。

偏重于网络 的测试和优化，侧重于网络需求的不断变更。

适合于大型网络的建设工作。

2、网络开发过程

网络开发过程主要是指一次迭代过程。

由于网络工程中，中等规模的网络较多，主要讲了五阶段迭代周期方式。

5 个阶段是：需求分析、通信规范分析、逻辑网络设计、物理网络设计、安装和维护。在这 5 个阶段中，每个阶段都必须依据上一阶段的成果，完成本阶段工作，并形成本阶段的工作成果，作为下一阶段的工作依据；这些阶段成果分别为“需求规范”、“通信规范”、“逻辑网络设计”、“物理网络设计”。

3、网络设计文档要素

教材暂无相关内容。

第 2 章计算机网络规划与设计 2.3 网络需求分析（P303-330）

1、 需求分析内容

业务需求：

包括以下内容：确定主要相关人员、确定关键时间点、确定网络的投资规模、确定业务活动、预测增长率（确定网络的伸缩性需求）、确定网络的可靠性和可用性、确定 Web 站点和 Internet 的连接性、确定网络的安全性、确定远程访问。

输出——业务需求清单（具体内容参见 P307-308 内容）

用户需求：

为了设计出符合用户需求的网络，收集用户需求过程应从当前的网络用户开始，必须找出用户需要的重要服务或功能。

收集用户需求的过程中，需要注意与用户的交流，网络设计者应将技术性语言转化为普通的交流性语言，并且将用户描述的非技术性需求转换为特定的网络属性要求。

输出——用户服务表（具体内容参见 P311 表 2-4）

应用需求：

应用需求收集工作应考虑如下因素：应用的类型和地点、使用方法、需求增长、可行性和可用性需求、网络响应。

这些需求因素的收集工作，通常可以从两个角度来完成，一是从应用类型自身的特性角度，另一个是从应用对资源的访问角度。

应用的种类较多，基中觉的分类方式主要有 4 种：按功能分类、按共享分类、按响应分类、按网络模型分类。

输出——应用需求表（具体参见 P314 表 2-5）

计算机平台需求：

收集计算机平台需求是网络分析与设计过程中一个不可缺少的步骤，需要调查的计算机平台主要分为 5 类：个人计算机、工作站、小型机、中型机、大型机。

输出——计算机平台需求表（具体参见 P318 表 2-6）

网络需求：

包括以下内容：局域网功能、网络拓扑结构、性能、网络管理、网络安全、城域网/广域网的选择。

输出——局域网功能、网络拓扑结构、网络管理、网络安全、城域网/广域网选择等分项需求表。

2、业务流量分析要素与方法

教材中暂无具体内容

3、通信量分析要素与方法

教材中暂无具体内容

4、网络设计的约束条件（P301-303）

政策约束、预算约束、时间约束、应用目标检查。

这些约束条件的冲突问题可以依据两种解决，一是由用户的信息主管部门协调解决，一是针对冲突的约束条件排定优先级，优先满足最高级别的约束条件。

5、需求说明书编制

a、数据准备：

第一步是要将原始数据制所表，从各个表看其内在的联系及模式。

第二步是要把大量的手写调查问卷或表格信息转换成电子表格或数据库。

另外，对于需求收集阶段产生的各种资料，都应该编辑目录并归档，便于后期查阅。

b、需求说明书的组成

说明书应该做到尽量简明且信息充分，以节省管理人员的时间。

两点要求：首先，无论需求说明书的组织开工如何，网络需求说明书应包含业务、用户、应用、计算机平台、网络 5 个方面的需求内容；其次，为了规范需求说明书的编制，一般情况下，需求说明书应该包括以下 5 个部分：

综述。

需求分析阶段概述。

需求数据总结。

按优先级排队的需求清单。

申请批准部分。

注意对照 P329-330 页内容，熟悉上述 5 个部分的具体内容。

第 2 章计算机网络规划与设计 2.4 通信规范（P330-357）

1、通信规范分析

包括：通信模式分析、通信边界分析、通信流分布分析、通信量分析、网络基准分析、编写通信规范

2、通信模式

通信模式基本与应用软件的网络处理模型相同，也分为 4 种：

对等通信模式：

参与的网络节点是平等角色，即是服务的提供者，也是服务的享受者。

流量通常是双向对称的。

最大用用途在于局域网段中，另外还有 P2P。

典型的对等通信模式包括以下内容：（1）利用 P2P 协议的 BT、超级旋风等软件（2）处于远程站点的商业人员之间使用视频会议系统召开会议是对等通信应用的一个例子。

在进行通信规范分析时，可以认为对于每个节点来说，都抽象成一个双向的输入输出流，该流的输入和输出流量一致。

客户机—服务器通信模式：

由服务器负责进行应用计算、客户机进行用户交互的通信模式，也是目前应用最为广泛的一种通信方式。它有其方向性，通信流取决于各个客户机使用的应用程序类型。

信息流量以双向非对称的方式流动，可以分解成客户机至服务器和服务器至客户机两个住处流向，在不同的应用中，这两个流向的通信流量是不同的，要分开进行计算。（1）服务器至客户机流量大：主要是多媒体类型服务，基于 HTTP 协议的 WWW 服务、OLAP 等服务，也属于这种情况。可以忽略客户端至服务器端的流量。（2）客户机至服务器流量大：应用比较少，是基于 SNMP 协议的网管服务。主要是监控、日志等类型的服务，在进行通信规范设计时，可以对服务器至客户机的流量进行忽略。（3）双向流量大：大多数应用双向的流量都比较大。在进行通信规范设计时，这类服务的双向流量都不能被忽略，应根据应用的情况评估流量的大小。

浏览器—服务器通信模式：

是三层模式与四层模式的典型代表。这咱模式较为特殊，可以将应用服务器与客户机之间的通信看成是一个典型的 C/S 通信模式，而将应用服务器与数据库服务器之间的通信看成是一个只有一台客户机的 C/S 通信模式。应用服务器与客户机之间的通信，一般 情况下属于“服务器至客户机流量大”的类型；而应用服务器与数据库之间的通信，一般属于“双向流量大”的类型。

分布式计算通信模式：

它的常务委员流量特征比较复杂，一般 情况下系统中存在少量任务管理节点和大量计算节点。通信流量难以预测。

大多数时候，网络节点会同时工作在多种模式下。

3、通信边界

通信边界主要以三种形式存在：

局域网通信边界：

主要是网络中的冲突域和广播域。主要是通过划分冲突域和广播域来限制通信量。

在网络中划分广播域可以采用两种方法，一种方法是采用交换机上提供的虚拟局域网技术（VLAN），另外一种方法是采用路由器连接多个交换机形成的广播域

一般情况下路由器的一个端口就是一个独立的物理广播域。VLAN 划分出来的广播域是逻辑边界。

广域网络中的通信边界：

广域网的通信边界，主要由路由的自治系统、路由协议中的域和各局域网构成。

虚拟专用网络的通信边界：

实现 VPN 的协议分成三种：第一种是工作于第二层数据链路层的 L2TP 等隧道协议，第二种是工作于第三层网络层的 IPSec、GRE 等隧道协议，第三种是依据标签封装机制而形成的 MPLS VPN 技术。

4、通信流量分布的简单规则

80/20 规则：对一个网段内部的通信流量，不进行严格的分布分析，仅仅是根据对用户和应用需求的统计，产生网段内的通信问题大小，主为总量的 80%是在网段内部的流量，而 20%是对网段外部的流量。

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

20/80 规则：根据对用户和应用需求的统计，产生网段内的通信总量大小，认为总量的20%是在网段内部的流量，而80%是对网段外部的流量。

虽然80/20规则和20/80规则是一些简单的规则，但是这些规则是建立在大量的工程经验基础上的。

5、通信流量分析的步骤

（1）把网络分成易管理的网段。

（2）确定个人用户和网段应用的通信流量。

（3）确定本地和远程网段上的通信流量。

（4）对每个网段重复步骤（1）～（3）。

（5）分析基于各网段信息的广域网和网络骨干的通信流量。

6、网络基准

基准法是更为精确的基于通信流量的计算法。对于升级的网络工程，基准法可替代通信流量计算法作为设计依据，也可以配合合用；对于新建网络工程，可以使用基准法中的仿真机制，作为设计工作的验证机制。

采用基准法测量需要专门的监视器设备和应用软件，一般很昂贵，所以通常只依靠估算法确定和记录网络的性能。但是只要条件允许，最好能同进使用估算法和基准法。

7、编写通信规范说明书

通信规范说明书是通信分析阶段的主要产物，它描述的是当前网络正在做什么。

通信说明书由下面主要内容组成：

执行情况概述、分析阶段概述、分析数据总结、设计目标建议、申请批准部分、修改说明书。

第2章计算机网络规划与设计 2.5 逻辑网络设计 A（P357-408）

1、逻辑设计过程概述

逻辑设计过程主要由以下4个步骤组成：

确定逻辑设计目标

网络服务评价

技术选项评价

进行技术决策

（1）逻辑网络设计目标

目标主要来自于需求分析说明书中的内容，网络需求部分。一般情况下，逻辑网络设计的目标包括以下一些内容：

合适的应用运行环境。

成熟而稳定的技术选型。

合理的网络结构。

合适的运营成本。

逻辑网络的可扩充性能。

逻辑网络的易用性。

逻辑网络的可管理性。

逻辑网络的安全性。

（2）需要关注的问题

设计要素：用户需求、设计限制、现有网络、设计目标。

设计面临的冲突：最低的安装成本、最低的运行成本、最高的运行性能、最大的适应性、最短的故障时间、最大的可靠性、最大的安全性。不可能存在一个网络设计方案，能够使得所有的子目标都达到最优。可采用优先级和建立权重的方法权衡各目标的关心度。

成本与性能：设计方案时，所有不超过成本限制、满足用户要求的方案，都称为可行方案。

款项支付：网络建设的成本分为一次性投资作周期性投资。合理的支付能保证工程的进度和质量。

（3）主要网络服务

网络管理服务：网络故障诊断、网络的配置及重配置、网络监视。

网络安全：明确需要安全保护的系统、确定潜在的网络弱点和漏洞、尽量简化安全、安全制度。

（4）技术评价

通信带宽、技术成熟性、连接服务类型、可扩充性、高投资产出

（5）具体工作内容

逻辑网络设计工作主要包括如下的内容：

网络结构的设计

物理层技术选择

局域网技术选择与应用

广域网技术选择与应用

地址设计和命名模型

路由选择协议

网络管理

逻辑网络设计文档

2、网络结构设计

网络结构与网络拓扑结构的最大区别：网络拓扑结构中，只有点和线，不会出再任何的设备和计算机节点；网络结构主要是描述连接设备和计算机节点的连接关系。

（1）局域网结构：

核心局域网结构

双核心局域网结构

环形局域网结构

层次局域网结构

（2）广域网结构

单核心广域网结构

双核心广域网结构

环形广域网结构

半冗余广域网结构

对等子域广域网结构

层次子域广域网结构

（3）层次化网络设计模型

A、层次化网络设计模型

一个典型的层次化网络结构包括以下特征：

由经过可用性和性能优化的高端路由器和交换机组成的核心层。

由用于实现策略的路由器和交换机会聚层。

由用于连接用户的低端交换机等构成的接入层。

B、三层层次化模型：

主要将网络划分为

核心层：提供不同区域或者下层的调整连接和最优传送路径。

会聚层：将网络业务连接到接入层。

接入层：为局域网接入广域网或者终端用户访问网络提供接入。

核心层设计要点：

a、采用冗余组件设计，使其具备高可靠性，能快速适应变化。

b、应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

c、核心层应具有有限的和一致的范围。

d、核心层应包括一条或多条连接到外部网络的连接，这样可以实现外部连接的可管理性和高效性。

会聚层设计要点：

a、应尽量将出于安全性原因对资源访问的控制、出于性能原因对通过核心层流量 的控制等，都 在会聚层实施。

b、应该向核心层隐藏接入层的详细信息。

c、也会对接入层屏蔽网络其他部分的信息。

d、各种协议的转换都应在会聚层完成。

接入层设计要点：

a、要解决相信用户之间的互访需要，并且为这些访问提供足够的带宽。

b、还应当适当负责一些用户管理功能。

c、还负责一些用户信息收集工作。

C、层次化设计的原则

a、在设计时，设计者应该尽量控制层次化的程序，一般情况下，由核心层、会聚层、接入层三个层次就足够了。

b、在卑怯应当保持对网络结构的严格控制。

c、为了保证网络的层次性，不能在设计中随意加入额外连接。

d、在进行设计时，应当首先设计接入层，再集资完成各上层的设计。

e、除去接入层的其他层次，应尽量采用模块化方式，每个层次由多个模块或者设备集合构成，每个模块间的边界应非常清晰。

(4)网络冗余设计

网络冗余设计中，对于通信线路常见的设计目标主要有两个：一个是备用路径，另外一个是负载分担。

3、物理层技术选择

（1）技术选择原则

可扩展性与可伸缩性

可靠性、可用性和可恢复性

安全性

节约与成本

（2）物理介质和网卡的考虑

注意 P377 表 2-14 中物理介质特性和表 2-15 中网上特性表

4、局域网技术选择与应用

（1）生成树协议（IEEE802.1D）

STP 是实现交换机设备间透明桥接的关键技术。交换机之间通过发送桥接协议数据单元（BPDU）来建立和维护生成树，协议在交换机启动时就参与了 STP 的收敛过程，当设备的端口、连接发生变化时，也会发送维护数据单元。

a、STP 收敛过程：4 个步骤。

确定最优 BPDU 的顺序标准如下：

最小根网桥 ID

到根网桥的最低路径开销

发送者最小桥 ID

最小端口 ID

交换机的所有端口在启动后将经历 4 个阶段：

阻塞、监听、学习、传输

b、选择根网桥

如果默认，最小的 MAC 地址交换机就成了根网桥。

设计人员必须针对 STP，对交换机的优先权部分进行手工设置，通过确保特定的交换机拥有较小的优先权，来避免低速、非核心交换机成为根网桥。

c、根保护

根保护功能需要在所有不应该成为根网桥的交换机的所有端口上开启，避免这些产端口成为根端口。

d、STP 更新时间

一般情况下 STP 协议更新的时间为 30s，特殊情况会长达 50s；默认传送时延为 15s，默认最大计时为 20s。

一旦网络中出现较大的连接关系变化，则意味着局域网络可能中断 30s 或者 50s。

（2）扩展生成树协议（IEEE802.1W、IEEE802.1S）

A、快速生成树协议（RSTP，IEEE802.1W）

B、基于 VLAN 的扩展协议：IEEE802.1S、Espan、BPDU 倾斜检测

（3）虚拟局域网

A、VLAN 划分方法

5 种方法：基于设备端口、基于 MAC 地址、基于网络地址、基于 IP 组播、基于策略。

注意各种方法的优缺点。基中基于端口划分的方法最常用。

B、VLAN 划分方案

管理 VLAN、服务器 VLAN、用户的部门 VLAN

C、VLAN 的跨设备互连

一般来说，在基于端口方式 下，网络端口可以处于以下几种状态：

静态访问端口、动态访问端口、VLAN 互连端口（TRUNK）

对于 Trunk 端口一般要考虑以下配置信息：

Trunk 端口允许互连的 VLAN、封装协议、Trunk 端口的默认 VLAN。

D、VLAN 间路由

借助于独立路由器、借助于三层交换机。

目前借助于三层交换机实现 VLAN 间通信是局域网设计的主流方法。

（4）无线局域网

设计无线局域网络需要考虑以下四个部分的内容：

A、定位 AP 实现最大覆盖率

B、无线局域网中的虚拟局域网设计

C、冗余无线接入点

D、网络 SSID

（5）线路冗余和负载分担

备份方式：网络必须丰在交换机或者链路处于闲置的状态，导致资源的浪费。

负载分担方式：可以避免冗余设备和冗余链中在网络中的闲置。

（6）交换机设备应用

A、链路聚合：是将两个或更多数据信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现，采用链路聚合后，逻辑链路的带宽增加了大约（n-1）倍，n 为聚合的路数。

B、冗余网关：大多数核心交换机都会提供冗余网关协议，使得网络中至少两台交换机成为各个 VLAN 的网关，避免网关的单点故障效应。常见的冗余网关协议包括通用的虚拟路由器冗余协议（VRRP）和 Cisco 公司提供的热备份路由器协议（HSRP）与网减负载均衡协议（GLBP）。

C、以太网供电（POE）

是通过以太网线路为 IP 电话、WLAN 接入点、网络摄像机等小型网络设备直接提供电源的技术。

D、多业务模块

目前常见的业务模块包括防火、入侵者检测、入侵者防御、流量控制等。

（7）服务器冗余和负载均衡

A、使用负载服务均衡器

B、使用网络地址转换

C、使用 DNS 服务器

D、高可用性技术

5、广域网技术选择与应用

（1）城域网远程接入技术

PSTN、ISDN、CATV、DSL

（2）广域网互连技术

DDN、SDH、MSTP、传统的 VPN 技术、MPLS VPN 技术

（3）广域网性能优化

可以从以下方面进行考虑：

广域网网络瓶颈、利用路由器实现广域网预留带宽、拨号线路的应用、压缩、链路聚合、数据优先排序、协议带宽预留、对话公平

第 2 章计算机网络规划与设计 2.5 逻辑网络设计 B（P408-447）

6、地址设计与命名模型

（1）分配网络层地址的原则

使用结构化网络层编址模型、通过中心授权机构管理地址、编址的分布授权、为终端系统使用动态编址、私有地址的使用

（2）使用层次化模型分配地址

A、层次化编址的优势

B、层次化路由选择：需要配合层次化地址编码

C、无类路由选择协议

D、路由汇聚

E、可变长度子网掩码

（3）设计命名模型

在网络命名系统中，将名字映射到地址的方法主要包括现两种类型，一种是使用命名协议的动态方法，一种是借助于文件等方式的静态方法。

7、路由选择协议

（1）路由协议选择原则

A、路由协议类型选择：

选择距离向量路由选择协议的条件

选择链路状态路由选择协议的条件

B、路由选择协议度量：

主要考虑两个方面：一是对度量值 的限制设定。二是多个路由协议共存时的度量值转换。

C、路由选择协议顺序：

设计人员可以在网络中运行多个路由选择协议，并约定这些协议之间的顺序，这些顺序可以用路由协议权值 来表示，可能会最小的协议顺序越靠前；一旦多个路由协议都选举出了最优路径，则具有最小权值的路由协议的路径生效。

D、层次化与非居次化路由选择协议：

对于采用层次化设计的网络来说，最好采用层次化路由选择协议。

E、内部与外部路由选择协议

F、分类与无类路由选择协议

G、静态路由选择协议：即默认路由。

（2）内部网关协议——OSPF

在实际中可根据需要调整下列规则：

A、OSPF Router ID

B、OSPF 时间参数

C、OSPF COST

D、OSPF DR 与 BDR

（3）外部网关协议——BGP

在实际中可根据需要调整下列规则：

A、BGP 对等体

B、BGP 时间参数

C、BGP 本地优先级

D、BGP MED

E、BGP 联盟

F、BGP 同步

G、BGP 路由发布

H、BGP 路由过滤

I、静态路由

8、网络管理

（1）行政管理手段

注意各岗位职责及管理制度

（2）传输管理系统（TMS）

（3）网络管理系统（NMS）

注意书中所列 11 条功能需求

（4）资源管理系统（RMS）

在网络层次中，网络资源管理系统处于整个网络运营管理支撑系统的基础和核心，其主要功能包括网络规、网络设计、网络资料管理、网络资源高度、工程施工、网络维护、网络质量管理。

（5）应用管理系统（AMS）

应用管理系统的主要监控对象是两部分内容：一部分是向网络用户提供的各种 Internet、Intranet 上的服务；一部分是网络平台上运行的各类专业应用系统。

9、网络安全

（1）机房及物理线路安全

主要是指存放、支撑网络设备运行的物理环境设施及物理线路情况。

A、机房安全：安全措施应符合 GB/T9361-1988、GB/T2887-1989

B、物理线路安全：

包括计算机通信线路安全和骨干线路冗余防护

（2）网络安全

A、安全域划分

B、边界安全策略：允许高安全级别的安全域访问低级别的安全域，限制低级别的安全域访问高安全级别的安全域，不同安全域内部分区进行安全防护，做到安全可控。

C、路由交换设备安全配置

D、防火墙安全配置

E、网闸安全配置

F、入侵检测安全配置

G、抗 DdoS 攻击安全配置

H、虚拟专用网（VPN）功能要求

I、流量管理部署与功能要求

J、网络监控与审计部署与功能要求

K、访问控制网络监控与审计部署与功能要求

（3）系统安全

A、身份认证

B、账户管理

C、主机系统配置管理

D 漏洞与补丁发现系统

E、内核加固

F、病毒防护

G、桌面安全管理

H、系统备份与恢复

I、系统监控与审计

J、访问控制

（4）应用安全

A、数据库安全

B、邮件服务安全

C、Web 服务安全

D、应用系统的安全要求

（5）数据容灾与恢复

A、总体要求

B、容灾系统建设

C、数据备份与恢复

（6）安全运维服务体系

A、信息安全风险评估工作

B、应急服务

C、安全监控与管理服务

D、其他安全服务

（7）安全管理体系

A、安全管理体系框架

B、建立安全组织机构

C、人员安全管理

D、外部技术支持

E、安全管理规章制度

F、变更管理和控制

G、安全系统建设管理

10、编写逻辑设计文档

编写逻辑设计文档必须使用非技术性描述的语言，并与客户就业务需求详细讨论网络设计方案，从而设计出符合用户需要的网络方案。

（1）主管人员评价

对项目进行概述

（2）逻辑网络设计讨论

应将重点放在要解决的问题上，而不是解决问题所用的工具上

（3）新的逻辑设计图表

包括新设备、链路或实话安全级别等

（4）总成本估测

要想得到新技术总的成本估价，可以将各个独立方案的成本组合在一起。注意，要考虑一次性成本和需要重复支出的成本。此外，还要考虑包含新的培训成本、咨询服务费用以及雇用新员工等在内的成本。

（5）审批部分

为使文档生效，需要各个管理者在逻辑设计文档说明书上签名，网络设计组代表也要签名。

（6）修改逻辑网络设计方案

第 2 章计算机网络规划与设计 2.6 物理网络设计（P447-469）

1、 结构化布线设计

（1）基本概念

几个特点：实用性、灵活性、开放性、模块化、扩展性、经济性

（2）系统构成

工作区子系统、水平布线子系统、干线子系统、设备间子系统、管理子系统、建筑群子系统

（3）设计要点

工作区子系统设计要点。

水平布线子系统设计要点。

干线子系统设计要点。

设备间子系统设计要点。

管理子系统设计要点。

建筑群子系统设计要点。

（4）布线距离

P451 表 2-17

（5）线缆铺设准则

注意 P452 页所列的 13 条

2、机房设计

机房的设计应参照 GB 50174-1993《电子计算机机房设计规范》。注意下列项目的细节。

（1）机房位置及设备布置

（2）环境条件

（3）空气调节

（4）电气技术

（5）给水排水

（6）消防与安全

（7）机房区域划分

（8）机械使用规范

（9）标签牌使用规范

（10）设计图纸

3、设备选型

应考虑到以下方面的内容：

（1）产品技术指标

（2）成本因素

（3）原有设备的兼容性

（4）产品的延续性

（5）设备可管理性

（6）厂商的技术支持

（7）产品的备品备件库

（8）综合满意度分析

4、物理网络设计文档规范

物理网络设计文档要清楚、简明，还必须正确和完整，包括以下要素：

（1）主管人员评价

（2）物理网络设计图表

（3）注释和说明

（4）软硬件清单

（5）最终费用估计

（6）审批部分

（7）物理网络设计的修改

第 2 章计算机网络规划与设计 2.7 网络测试运行和维护（P469-480）

1、网络测试概述

（1）网络测试方法

根据测试中是否向被测网络注入测试流量，可以将网络测试方法分为主动测试和被动测试。

主动测试：具备良好的灵活性、能够按照测试者的意图进行，容易进行场景仿真。但安全性存在隐患。

被动测试：安全性好。但不够灵活，局限性较大。

（2）网络测试工具

主要有线缆测试仪、网络协议分析仪、网络测试仪（大多用于大型网络的测试）。

2、线路与设备测试

（1）线路测试

线路测试是基础测试。统计数据表明，50%以上的网络故障与布线有关。

注意 P471 表 2-19 双绞线与光纤测试指标。

（2）网络设备测试

主要设备测试标准：

交换机：YD/T 1096-2001、YD/T 1097-2001。

路由器：GB/T 18019-1999、GB/T 18020-1999、YD/T 1132-2001。

防火墙：GB/T 18019-1999、GB/T 18020-1999、YD/T 1132-2001

3、网络系统测试

主要是网络是应用系统提供了稳定、高效的网络平台。对于常规的以太网进行系统测试，主要包括系统连通性、链路传输速率、吞率、传输专题片及链路层健康状况测试等基本功能测试。

注意表 2-20、2-21、2-22、2-23 所示的指标要求。

4、网络应用测试

（1）应用服务标准

DHCP 服务器响应时间应不大于 0.5s。

DNS 服务器响应时间应不大于 0.5s。

WEB 访问服务性能指标：内部网站点访问时间应不大于 1s。内部网站访问速率应不小于 10000bps。

E-mail 服务性能指标：1K 字节邮件写入服务器时间应不大于 1s。从服务器读取 1K 字节邮件的时间应不大于 1s。

文件服务性能指标见表 2-24

（2）应用服务性能测试方法

5、测试报告

测试报告应对测试中的测试对象、测试工具、测试环境、测试内容和测试结果等进行详细论述。形式并不固定，可以是一个简短的总结，也可以是很长的书面文档，通常测试报告包含以下信息：

测试目的、结论、测试结果总结、测试内容和方法、测试配置。

测试报告包括对各测试项目的测试结果，应以数字、图形和列表等方式记录下来，结论则以书面文档方式叙述。

第 2 章计算机网络规划与设计 2.8 网络故障分析与处理（P480-493）

1、网络故障排除思路

（1）准确定义故障。

（2）收集有且罪恶地确定故障症结的各种信息。

（3）依据所收集到的各种信息考虑可能引发故障的症结。

（4）根据剩余的潜在症结制订故障的排查计划。从最有可能的症结入手，每次只做一处改动。

（5）实话制订好的故障排除计划，认真执行每一步骤，同时进行测试，查看相应的现象是否消失。

（6）当做出一处发动时，要注意收集相应操作的反馈信息。

（7）分析相应操作的结果，并确定故障是否已被排除。

（8）如果故障依然存在，就得针对剩余的潜在症结中最可能的一个制订相应的故障排除计划。回到步骤（4），依每次只做一处发动，重复此过程，直到故障被排除为止。

在网络故障的排除过程中，最为关键的是确保当前掌握的信息及资料是最新的。

2、网络故障排除工具

总的来说可以分为三类：

A、设备或系统诊断命令

Show 命令、debug 命令、ping 命令、trace 命令

B、网络管理工具

书中介绍有 Cisco Works、HP OpenView 等。

C、专用故障排除工具

（1）欧姆表、数字万用表及电缆测试哭喊可以用于检测电缆设备的物理连通性。

（2）TDR 与 OTDR 可以用于测定电缆断裂、阻抗不匹配以及电缆设备其他物理故障的具体位置。

（3）断接盒、智能测试盘和位/数据块错误测试器可以用于外围接口的故障排除。

（4）网络监测器通过持续跟踪穿越网络的数据包，能每隔一段时间提供网络活动的准确图像。

（5）网络分析仪可以对 OSI 所有 7 层上出现的问题进行解码，自支实时地发现问题。

3、网络故障分层诊断

A、物理层及其诊断

主要表现为设备的物理连接方式 是否恰当；连接电缆是否正确。

B、数据链路层及其诊断

通过查看路由器的配置检查其封装，或者使用 show 命令查看相应接口的封装情况。

C、网络层及其诊断

排队网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由。然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障，包括 RIP 或者 IGRP 路由协议出现的故障。

D、应用层及其诊断

基本方法是：首先可在服务器上检查配置，测试服务器是否正常运行，如果服务器没有问题再检查应用客户端是否正确配置。

4、网络故障排队案例分析

注意书中所列 4 个案例。

第 3 章网络资源设备 3.1 网络服务器（P494-504）

1、RISC 架构服务器

RISC，即精简指令集。目前中高档服务器特别是高档服务器中普遍采用 RISC 指令系统的 CPU。

RISC 架构服务器采用的是封装的发展策略。

2、IA 架构服务器

IA 架构的服务器（通常将采用英特尔处理器的服务器称为 IA(Intel Architec-ture)架构服务器）采用了开放体系结构，有大量的硬件和软件的支持者。

A、CISC 架构

CISC，即复杂指令系统计算。

CISC 架构的服务器主要以 IA-32 架构为主，而且多数被 中低档服务器所采用。

B、VLIW 架构

VLIW，即超长指令集架构。采用了先进的 EPIC（清晰并行指令）设计，也叫“IA-64 架构”。

目前基于这种指令架构的微处理器主要有 Intel 的 IA-64 和 AMD 的 x86-64 两种。

3、性能要求及配置要点

A、性能要求

性能要稳定、以够用为准则、应考虑扩展性、要全球操作管理、满足特殊要求、配件搭配合理、理性看待价格、售后服务要好。

B、配置要点

（1）数据库服务器

对于硬件需求的优先级为：内存、磁盘、处理器。

（2）文件服务器

对于硬件需求的优先级为：网络系统、磁盘系统、内存。

（3）WEB 服务器

静态站点对硬件需求的优先级为：网络系统、内存、磁盘系统、CPU。

动态站点对硬件需求的优先级为：内存、CPU、磁盘子系统和网络系统。

（4）邮件服务器

对于硬件需求的优先级为：内存、磁盘、网络系统、处理器。

（5）终端服务器

对于硬件需求的优先级为：处理器、内存、磁盘和网络系统。

4、服务器相关技术

（1）64 位计算

目前主流 CPU 使用的 64 位技术主要有 AMD 公司的 AMD64 位技术、Intel 公司的 EM64T 技术、和 Intel 公司的 IA-64 技术。其中 IA-64 是 Intel 独立开发，不兼容现在的传统的 32 位计算机，仅用于 Itanium（安腾）以及后续产品 Itanium 2，一般用户不会涉及到。

（2）双核和多核处理器

双核就是 2 个核心，核心（Die）又称为内核，是 CPU 最重要的组成部分。CPU 中心那块隆起的芯片就是核心，是由单晶硅以一定的生产工艺制造出来的，CPU 所有的计算、接受/存储命令、处理数据都由核心执行。各种 CPU 核心都具有固定的逻辑结构，一级缓存、二级缓存、执行单元、指令级单元和总线接口等逻辑单元都会有科学的布局。

多核心 cpu 主要分原生多核和封装多核。

原生多核指的是真正意义上的多核，最早由 AMD 提出，每个核心之间都是完全独立的，都拥有自己的前端总线，不会造成冲突，即使在高负载状况下，每个核心都能保证自己的性能不受太大的影响，通俗的说，原生多核的抗压能力强，但是需要先进的工艺，每扩展一个核心都需要很多的研发时间。

封装多核是只把多个核心直接封装在一起，比如 Intel 早期的 PD 双核系列，就是把两个单核直接封装在一起，但两核心只能共同拥有一条前端总线，在两个核心满载时，两个核心会争抢前端总线，导致性能大幅度下降，所以早期的 PD 被扣上了“高频低能”的帽子，要提高封装多核的性能，在多任务的高压下尽量减少性能损失，只能不断的扩大前端总线的总体大小，来弥补多核心争抢资源带来的性能损失，但这样做只能在一定程度上弥补性能的不足，和原生的比起来还是差了很多，而且后者成本比较高，优点在于多核心的发展要比原生快的多。

（3）PCI-E 技术

继 PCI （个人计算机扩展总线接口规范）之后的规范。PCI 属于并行传输方式，即使用多条信号线同时并行传输多位数据，但 PCI Express 采用的是每次 1 位的串行传输方式，其最高数据传输速度为 8Gbit / s ，最大电缆长度 3m 。开发阶段的代号是 3GIO 。

（4）ECC 内存技术

ECC 是“Error Checking and Correcting”的简写，中文名称是“错误检查和纠正”。ECC 是一种能够实现“错误检查和纠正”的技术，ECC 内存就是应用了这种技术的内存，一般多应用在服务器及图形工作站上，这将使整个电脑系统在工作时更趋于安全稳定。

（5）刀片服务器

是一种 HAHD（高可用高密度）的低成本服务器平台，是专门为特殊应用行业和高密度计算机环境设计的。

每一块"刀片"实际上就是一块系统主板。它们可以通过"板载"硬盘启动自己的操作系统，如 Windows NT/2000、Linux 等，类似于一个个独立的服务器，在这种模式下，每一块母板运行自己的系统，服务于指定的不同用户群，相互之间没有关联。不过，管理员可以使用系统软件将这些母板集合成一个服务器集群。在集群模式下，所有的母板可以连接起来提供高速的网络环境，并同时共享资源，为相同的用户群服务。在集群中插入新的

"刀片"，就可以提高整体性能。而由于每块"刀片"都是热插拔的，所以，系统可以轻松地进行替换，并且将维护时间减少到最小。

（6）SMP 技术

对称多处理"（Symmetrical Multi-Processing）又叫 SMP，是指在一个计算机上汇集了一组处理器(多 CPU),各 CPU 之间共享内存子系统以及总线结构。它是相对非对称多处理技术而言的、应用十分广泛的并行技术。在这种架构中，一台电脑不再由单个 CPU 组成，而同时由多个处理器运行操作系统的单一复本，并共享内存和一台计算机的其他资源。虽然同时使用多个 CPU，但是从管理的角度来看，它们的表现就像一台单机一样。系统将任务队列对称地分布于多个 CPU 之上，从而极大地提高了整个系统的数据处理能力。所有的处理器都可以平等地访问内存、I/O 和外部中断。在对称多处理系统中，系统资源被系统中所有 CPU 共享，工作负载能够均匀地分配到所有可用处理器之上。

（7）集群技术

详见 Cluster 集群

（8）模块化结构

主要包括计算模块、I/O 模块和少量存储器模块。

（9）硬件分区

是将一台服务器的硬件分割成多个分区的体系结构。

（10）ISC

ISC：（Intel Server Controller）服务器控制.是 Intel 的服务器管理软件。只适用于使用 Intel 架构的带有集成管理功能主板的服务器。采用这种技术后，用户在一台普通的客户机上，就可以监测网络上所有使用 Intel 主板的服务器，监控和判断服务器的工作状态是否正常。一旦服务器内部硬件传感器进行实时监控或第三方硬件中的任何一项出现错误，就会报警提示管理人员。并且，监测端和服务器端之间的网络可以是局域网也可以是广域网，可直接通过网络对服务器进行启动、关闭或重新置位，极大地方便了管理和维护工作。

（11）EMP

EMP（Emergency Management Port）:应急管理端口技术,也是一种远程管理技术,利用 EMP 技术可以在客户端通过电话线或电缆直接连接到服务器，来对服务器实施异地操作，如关闭操作系统、启动电源、关闭电源、捕捉服务器屏幕、配置服务器 BIOS 等操作，是一种很好的实现快速服务和节省维护费用的技术手段。

应用 ISC 和 EMP 两种技术可以实现对服务器进行远程监控管理。

（12）I2O

I2O:（Intelligent I/O）用于智能 I/O 系统的标准接口是智能型输入/输出总线模式，它的传输速率更高。可达到 160MB/S。能够在不同的操作系统和软件版本下工作，旨在满足更高的 I/O 吞吐量需求。因目前 CPU 主频速度提升很快，I/O 速度遂成为系统的瓶颈。为了解决该瓶颈，厂商将 I/O 子系统中加入 CPU，负责中断处理、缓冲和数据传输等任务，提高了系统的吞吐能力，解放了服务器的主处理器，使其能腾出空间和时间来处理更为重要的任务，这就是智能输入输出技术。这样，使用了 I2O 技术的 PC 服务器，即使硬件规模不变的情况下，也能处理更多的任务。

（13）热插拔

即带电插拔，热插拔功能就是允许用户在不关闭系统，不切断电源的情况下取出和更换损坏的硬盘、电源或板卡等部件，从而提高了系统对灾难的及时恢复能力、扩展性和灵活性等，例如一些面向高端应用的磁盘镜像系统都可以提供磁盘的热插拔功能。

具体用学术的说法就是：热替换（Hot replacement）、热添加（hot expansion）和热升级（hot upgrade），而热插拔最早出现在服务器领域，是为了提高服务器用性而提出的，在我们平时用的电脑中一般都有 USB 接口，这种接口就能够实现热插拔。如果没有热插拔功能，即使磁盘损坏不会造成数据的丢失，用户仍然需要暂时关闭系统，以便能够对硬盘进行更换，而使用热插拔技术只要简单的打开连接开关或者转动手柄就可以直接取出硬盘，而系统仍然可以不间断地正常运行。

第 3 章网络资源设备 3.2 网络存储系统（P504-529）

1、SCSI 接口卡与控制卡

（1）接口分类

存储系统中目前普遍应用的硬盘接口主要包括 SATA、SCSI、SAS、FC 等

（2）SCSI

即小型计算机系统接口，是一种专门为小型计算机系统设计的存储单元接口模式，通常用于服务器承担关键业务的较大的存储负载，价格也较贵。

（3）SCSI 控制卡

是一种提供一个或一个以上的 SCSI 接口内置板卡，它可插在服务器主板上的普通 PCI 插槽上，实现多个 SCSI 接口的提供。

2、独立磁盘冗余阵列（RAID）

（1）磁盘阵列的特点

一是速度；二是安全。

（2）RAID 技术分类

全软阵列：就是指 RAID 的所有功能都是由 OS 和 CPU 来完成。

半软半硬阵列：该阵列主要缺乏自己的 I/O 处理芯片，所以这方面的工作仍要由 CPU 和驱动程序来完成。

全硬阵列：全面具备了自己的 RAID 控制/处理芯片和 I/O 处理芯片，甚至还有阵列缓存。全硬阵列有两种方式：一是 RAID 适配卡；二是主板集成 RAID 控制/处理芯片。

（3）RAID 的基本工作模式

现在有 RAID0 到 6 这 7 种基本的 RAID 级别。以及一些基本 RAID 级别的组合形式。如 RAID10（RAID0 与 RAID1 的组合），RAID50（0 和 5 的组合）

几种常用的 RAID 形式：

A：RAID0

又称为 Stripe（条带化）或 Striping，它代表了所有 RAID 级别中最高的存储性能。

缺点：不提供数据冗余。

特别适用于对性能要求较高，而对数据安全要求低的领域。如图形工作站。对于个人用户，RAID0 也是提高硬盘存储性能的绝佳选择。

B：RAID1

又称为 Mirror 或 Mirroring（镜像），它的宗旨是最大限度地保证用户数据的可用性和可修复性。在所有 RAID 级别中，RAID1 提供最高的数据安全保障。

适用于存放重要数据，如服务器和数据库存储等领域。

C：RAID3

是把数据分成多个“块”，按照一定的容错算法存放在 N+1 个硬盘上。适合大文件类型且安全性要求较高的应用，如视频编辑、硬盘播出机和大型数据库等。

D：RAID5

是一种存储性能、数据安全和存储成本兼顾的存储解决方案。

可以理解为是 RAID0 和 RAID1 的折衷方案。

E：RAID0+1

是 RAID0 和 RAID1 的组合形式，也称为 RAID10。

特点是它提供与 RAID1 一样的数据安全保障的同时，也提供了与 RAID0 近似的存储性能。

特别适用于既有大量数据需要存取，同时又对数据安全性要求严格的领域，如银行、金融、商业超市、仓储库房和各种档案管理等。

（4）RAID 级别的选择

有三个主要因素：可用性（数据冗余）、性能和成本。

如果不要求可用性，选择 RAID0 以获得最佳性能。

如果可用性和性能是重要的面成本不是一个主要因素，则根据硬盘数据选择 RAID1。

如果可用性、成本和性能都同样重要，则根据一般的数据传输和硬盘的数量选择 RAID3 或 RAID5。

3、磁带库

（1）备份设备类型

备份设备主要分为磁带机、自动加载机和磁带库，而磁带库又分为入门级、企业级和超大容量等几个级别。

（2）磁带驱动技术

目前主流的磁带驱动技术包括 Quantum 公司的 DLT 和 SuperDLT，IBM、HP 和 Seagate 共同制定的 LTO，STK 的 9840，IBM 的 3590,Exabyte 的 Mammoth-2，Sony 的 AIT-2、AIT-3、DTF、DTF-2 等。

磁带驱动技术最主要的指标是数据传输率和单盘容量，另外可行性也是一个指标。

（3）带机、带库厂商及产品

带机厂商包括 Quantum、Exabyte 和 Sony 等。

Quantum 带机在中档产品中占据了市场大部分份额，产品有 SuperLoader 等。

Exabyte 的驱动技术包括 8mm Mammoth 和 VXA 技术。

Sony 的基于 AIT 技术的带机产品：AIT-1、AIT-2 和 AIT-3。

磁带库厂商相对品牌较多，目前主流的有 STK、Quantum、Exabyte 和 IBM 等。

市场份额最大的是 STK，其最主要的产品线是 L 系列，包括 L20、L40、L80、L180、L700、L5500 等。

（4）产品选购指南

A：要选择符合应用特点的驱动技术。

B：根据需要备份的数据量、信息系统对备份窗口的要求以及采用何种备份策略等因素，确定所需带库的容量和备份速度。

C：性价比。

D：一定请厂家或代理商核查兼容性列表。

E：注意扩展需求。

（5）虚拟磁带库

VTL，是使用磁盘阵列效仿标准磁带库的一种新概念产品。它通过光纤连接到备份服务器，为数据存储备份提供了调整、高效及安全的解决方案，极大地缩短了数据备份所需时间。更重要的是，VTL 通过冗余和热插拔设计保证了系统的不停顿及备份工作连续运行。

4、光盘塔

简单说就是把很多光驱连接在一起的一种设备，可以同时在多个光盘上读写数据。就像硬盘的磁盘阵列一样。

目前在网络上可实现 CD-ROM 光盘共享的设备有三种：硬盘阵列、光盘塔和光盘库。这三种设备分别是在光盘和硬盘产品的发展过程中，在不同历史阶段出现的典型产品。

硬盘阵列是一种可供大容量数据实现实时共享的设备。它的访问速度非常快，可使用的数据资源非常大。用户直接访问硬盘，实现网络资源的共享。

CD-ROM 光盘塔（CD-ROM Tower）是由多个 SCSI 接口的 CD-ROM 驱动器串联而成的，光盘预先放置在 CD-ROM 驱动器中。受 SCSI 总线 ID 号的限制，光盘塔中的 CD-ROM 驱动器一般以 7 的倍数出现。用户访问光盘塔时，可以直接访问 CD-ROM 驱动器中的光盘，因此光盘塔的访问速度较快。

CD-ROM 光盘库（CD-ROM Jukebox）是一种带有自动换盘机构（机械手）的光盘网络共享设备。光盘库一般配置有 1~6 台 CD-ROM 驱动器，可容纳 100~600 片 CD-ROM 光盘。用户访问光盘库时，自动换盘机构首先将 CD-ROM 驱动器中光盘取出并放置到盘架上的指定位置，然后再从盘架中取出所需的 CD-ROM 光盘并送入 CD-ROM 驱动器中。由于自动换盘机构的换盘时间通常在秒量级，因此光盘库的访问速度较低。

上述三种类型的产品由于各自的特点决定了它们各自不同的用途。硬盘阵列由于它的访问速度非常快，所以它主要用于数据的实时共享，还可以用于小型的 VOD 点播系统。CD-ROM 光盘塔的光驱访问速度相比于硬盘来说，速度慢了一些，而且光驱数量有限，数据源很少，

所以供同时使用的用户数量也很少，但是由于光驱的价格很低，作为低端产品，它还是能够适用于一些用户的要求。CD-ROM 光盘库的数据访问速度与 CD-ROM 光盘塔速度差不多，但是它所能提供的数据量非常大。

虽然硬盘阵列的访问速度非常快，但是由于硬盘的可以改写，导致硬盘阵列在一些安全性要求比较高的环境下，不能使用。而且，硬盘的保存时间也很短。CD-ROM 光盘塔在安全性方面，比硬盘阵列要强一些，但是它的数据量有限，所以在要求数据源很大时，光盘塔不能满足用户的要求。而 CD-ROM 光盘库能够同时满足高安全性、高可靠性、大数据源的要求，所以在要求比较高的环境里，CD-ROM 光盘库有着不可替代的作用。CD-ROM 光盘库主要应用于数据的备份。在访问量不是非常大，但是数据要长期保存的情况下，光盘库的作用很突出。随着科学技术的发展，光盘库产品已经系列化。

5、DAS 技术

DAS 即直连方式存储，英文全称是 Direct Attached Storage。

中文翻译成“直接附加存储”。顾名思义，在这种方式中，

存储设备是通过电缆（通常是 SCSI 接口电缆）直接到服务器的。I

/O（输入/输出）请求直接发送到存储设备。

DAS，也可称为 SAS（Server-Attached Storage，服务器附加存储）。它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统。

DAS 的适用环境

1） 服务器在地理分布上很分散，通过 SAN（存储区域网络）或 NAS（网络直接存储）在它们之间进行互连非常困难时(商店或银行的分支便是一个典型的例子)；

2） 存储系统必须被直接连接到应用服务器（如 Microsoft Cluster Server 或某些数据库使用的“原始分区”）上时；

3） 包括许多数据库应用和应用服务器在内的应用，它们需要直接连接到存储器上，群件应用和一些邮件服务也包括在内。

对于多个服务器或多台 PC 的环境，使用 DAS 方式设备的初始费用可能比较低，可是这种连接方式下，每台 PC 或服务器单独拥有自己的存储磁盘，容量的再分配困难；对于整个环境下的存储系统管理，工作烦琐而重复，没有集中管理解决方案。所以整体的拥有成本（TCO）较高。目前 DAS 基本被 NAS 所代替。下面是 DAS 与 NAS 的比较。

6、NAS 技术

NAS（Network Attached Storage：网络附属存储）是一种将分布、独立的数据整合为大型、集中化管理的数据中心，以便于对不同主机和应用服务器进行访问的技术。按字面简单说就是连接在网络上，具备资料存储功能的装置，因此也称为“网络存储器”。它是一种专用数据存储服务器。它以数据为中心，将存储设备与服务器彻底分离，集中管理数据，从而释放带宽、提高性能、降低总拥有成本、保护投资。其成本远远低于使用服务器存储，而效率却远远高于后者。

（1）NAS 提供了一个高效、低成本的资源应用系统。由于 NAS 本身就是一套独立的网络服务器，可以灵活地布置在校园网络的任意网段上，提高了资源信息服务的效率和安全性，同时具有良好的可扩展性，且成本低廉。

（2）提供灵活的个人磁盘空间服务。NAS 可以为每个学生用户创建个人的磁盘使用空间，方便师生查找和修改自己创建的数据资料。

（3）提供数据在线备份的环境。NAS 支持外接的磁带机，它能有效地将数据从服务器中传送到外挂的磁带机上，保证数据安全、快捷备份。

（4）有效保护资源数据。NAS 具有自动日志功能，可自动记录所有用户的访问信息。嵌入式的操作管理系统能够保证系统永不崩溃，以保证连续的资源服务，并有效保护资源数据的安全。

7、SAN 技术

存储域网络 (Storage Area Network）的支撑技术是 Fibre Channel(FC)技术，这是 ANSI 为网络和通道 I／O 接口建立的一个标准集成。支持 HIPPI，IPI，SCSI，IP，ATM 等多种高级协议，它的最大特性是将网络和设备的通讯协议与传输物理介质隔离开．这样多种协议可在同一个物理连接上同时传送，高性能存储体和宽带网络使用单 I/O 接口使得系统的成本和复杂程度大大降低。如通过 Switch 扩充至交换仲裁复用结构则可将用户扩至很多。FC 使用全双工串行通讯原理传输数据，传输速率高达 1062.5Mbps，Fibre Channel 的数据传输速度为 100MB／S，双环可达 200MB／S，使用同轴线传输距离为 30 米，使用单模光纤传输距离可达 10 公里以上。光纤通道支持多种拓扑结构，主要有：点到点（Links）、仲裁环（FC-AL）、交换式网络结构（FC-XS）。点对点方式的例子是一台主机与一台磁盘阵列透过光纤通道连接；其次为光纤通道仲裁环(FC-AL)，在 FC-AL 的装置可为主机或存储装置。第三种 FC-XS

交换式架构在主机和存储装置之间透过智能型的光纤通道交换器连接，使用交换架构需使用存储网络的管理软件。

FC 技术具有以下优越性：

（1）既具有单通道的特点，又具有网络的特点，它是把设备连接到网络结构上的一种高速通道。而这种网络结构描述了连接两套设备的单条电缆以及连接许多设备的交换机产生网状结构。

（2）光纤通道最大优点是速度快，它可以给计算机设备提供接近于设备处理速度的吞吐量。

（3）协议无关性，它有很好的通用性，是一种通用传输机制。适用范围广，可提供多性价比的系统，从小系统到超大型系统，支持存在的多种指令集，如 IP、SCSI、IPI。

光纤通道规范定义的速率最高可到 4Gbps，目前 T11 工程组对 10Gbps 传输速度的 FC 规范也在紧锣密鼓的制定之中。

FC 是一种分层结构，每个层次定义为一个功能级，但是所分的层不能直接映射到 OSI 模型的层上。FC 通道的五层定义为：物理媒介和传输速率、编码方式、帧协议和流控制、公共服务以及上级协议（ULP）接口。

8、备份系统及备份软件

（1）数据备份结构

常见的数据备份系统主要有 Host-Base、LAN-Base 和基于 SAN 结构的 LAN-Free、Server-Free 等多种结构。

（2）备份软件

（3）备份介质

磁带、磁盘、数据迁移技术。

（4）厂商及产品介绍

A：备份软件厂商中头把交椅当属 Vreitas 公司。

B：Legate 公司是备份领域内仅次于 Veritas 公司的主要厂商。

C：IBM Tivoli 也是重要角色之一。

D：CA 公司是软件领域的世无霸企业，虽然主要精力没有放在存储技术方面，但有 ARCServe 依然在低端市场具有相当广泛的影响力。新一代备份产品 BrightStor，定位直指中高端市场。

第 3 章网络资源设备 3.3 其它资源设备（P529-539）

1、网络传真机

（1）网络传真机类别

软件网络传真机、硬件网络传真机

（2）传真机选择标准

稳定性、适用性、兼容性、可扩展性、易用性、可集成性

（3）典型实例

系统实现 P530 下的 5 项功能。

2、网络打印机

（1）接入与控制

两种接入的方式：一种是打印机自带打印服务器（也称内置打印服务器）；另一种是打印机使用外置的打印服务器。

（2）性能指标

打印质量、打印速度、介质处理能力、网络打印方式、设备接口、兼容性、管理软件、辅助功能

3、视频会议系统

（1）系统工作原理

按技术不现可分为两类：一是基于单播网络和 H.323 协议族的视频会议；二是基于组播网络和开放软件的视频会议。

（2）解决方案

现阶段视频会议系统解决方案主要有硬件和软件两类。

（3）网络视频会议系统选型

A、制定具体需求

B、设备选型原则

（4）系统部署实例

参见 P536 实例。

4、网络电话系统

是一种利用 VoIP 技术，透过因特网实时传输音频信息及实现双边对话的网络应用系统。一般包括语音网关、网守、网络电话机等设备。

（1）方案及设备选型

A、VoIP 网关+网守+PBX+IP 电话/模拟电话

B、IP PBX+PBX+IP 电话/模拟电话

C、PC PBX+PBX+IP 电话/模拟电话

（2）系统部署实例

参见 P539 实例

第 4 章网络安全 4.1 恶意代码（P540-562）

1、恶意代码的定义与分类

（1）恶意代码的定义

未经用户授权便干扰或破坏计算机系统/网络的程序或代码被称为恶意软件(malware)或恶意代码。

（2）恶意代码分类

种类很多，主要类型有计算机病毒、网络蠕虫、特洛伊木马、后门、DDoS 程序、僵尸

程序、Rootit、黑客攻击工具、间谍软件、广告软件、垃圾邮件和弹出窗体程序等。

2、常见的恶意代码命名规则

恶意代码的一般命名格式为：

<恶意代码前缀>.<恶意代码名称>.<恶意代码后缀>

前缀表示了该病毒发作的操作平台或者病毒的类型，常见的前缀有：Trojan（木马程序）、Worm（网络蠕虫）、Macro、PE、Win32、Win95、VBS、BackDoor 等。如果没有前缀，一般表示 DOS 操作系统下的病毒。

名称是指一个恶意代码的家族特征，是用来区别和标识恶意代码家族的。如：CIH、Sasser（振荡波蠕虫）。

后缀是指一个恶意代码的变种特征，一般 都采用英文中的 26 个字母来表示，也可以采用数字与字母混合表示变种标识。

注意 P544 所列出的 10 种病毒前缀。

3、典型的恶意代码

（1）计算机病毒

A、特点：传染性、程序性、破坏性、非授权性、隐蔽性、潜伏性、可触发性、不可预见性。其中是否具有传播（染）性是判别一个程序是否为计算机病毒的最重要条件之一。

B、生命周期：潜伏阶段（并不是所有的病毒都经历此阶段）、传播阶段、触发阶段、发作阶段。

C、传播途径：软盘和光盘、移动存储设备、网络。

网络传播主要有以下几种方式：

通过局域网传播

通过穷举局域网其他计算机的管理员弱口令

电子邮件

各类即时通信软件

利用各类浏览器漏洞的网页挂马

P2P 下载渠道

各类软件下载站点

各类应用软件漏洞

各类系统漏洞

ARP 欺骗

无线设备传播

D、多种状态：静态病毒、动态病毒。内存中的动态病毒又分为：能激活态和激活态，另外还有一种特殊的状态：失活态，一般不会出现。

E、Windows 环境下的几类常见计算机病毒

Windows PE 病毒、脚本病毒、宏病毒

（2）网络蠕虫

不需要用户干预来触发，其传播速度要远远大于网络病毒。

A、计算机病毒与蠕虫的区别：

注意 P553 表 4-2

B、基本功能模块：

目标搜索或生成模块、攻击模块、传输模块

C、扩展功能模块：

主机驻留模块、隐藏模块、破坏模块、通信模块、控制模块

（3）特洛伊木马

详情请参阅：特洛伊木马

（4）后门

是留在计算机系统中，供特殊使用者通过某种特殊方式控制计算机系统的途径。

（5）网页木马

表面上伪装成普通的网页文件或是将而已的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

（6）Rootkit 程序

详情请参阅：rootkit 程序

（7）Exploit 与 ShellCode

Exploit 即漏洞被黑客利用。有漏洞不一定就有 Exploit（利用）。有 Exploit 就肯定有漏洞。

ShellCode 是用来执行 shell 的字节码。

（8）黑客攻击程序

（9）流氓软件

详情请参阅：流氓软件

4、典型反病毒技术和常用反病毒软件

（1）典型反病毒技术介绍

A、特征值查毒法

B、校验和技术

C、启发式扫描技术

D、虚拟机技术

E、行为监控技术

F、主动防御技术

（2）典型反病毒产品介绍

注意了解 P562 中的表。

第 4 章网络安全 4.2 黑客攻击及其预防（P562-581）

1、黑客和黑客攻击

黑客（Hacker）在当前的网络世界中有褒贬两重含义。从褒的方面讲，黑客特指一些特别优秀的程序员或技术专家。从贬义方面讲，黑客是一些蓄意破坏计算机和电话系统的人。真正的黑客把这些人叫做“骇客（cracker）”，并不屑与之为伍。

（1）信息的收集

网络监测、社会工程、公共资源和垃圾、后门工具

（2）黑客攻击方式

拒绝服务攻击、缓冲区溢出攻击、漏洞攻击、欺骗攻击

2、拒绝服务攻击与防御

DoS 是由人为或非人为发起的行动，使主机硬件、软件或两者同时失去工作能力，使系统不可访问并因此拒绝合法的用户服务要求。

对服务器实话 DoS 有两种思路：A 服务器的缓冲区满，不接收新的请求。B 使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。这也是 DoS 攻击实话的基本思想。

（1）传统拒绝服务攻击的分类

网络的内外部用户都可以发动这种攻击。

外部用户针对网络连接发动 DoS 攻击主要有以下几种模式：

消耗资源、破坏或更改配置信息、物理破坏或改变网络部件、利用服务程序中的处理错

误使服务失效。

（2）分布式拒绝服务攻击

详情请参阅：分布式拒绝服务攻击

（3）拒绝服务攻击的防御方法

A、加强对数据包的特征识别

B、设置防火墙监视本地主机端口的使用情况

C、对通信数据量进行统计也可获得有关攻击系统的位置和数量信息。

D、尽可能地修正已经发现的问题和系统漏洞。

3、缓冲区溢出攻击与防御

详情请参阅：缓冲区溢出攻击

针对缓冲区溢出，可以采取多种防范策略：

（1）系统管理上的防范策略

A、关闭不需要的特权程序

B、及时给程序漏洞打补丁

（2）软件开发过程中的防范策略

A、编写正确的代码

B、缓冲区不可执行

C、改进 C 语言函数库

D、使堆栈向高地址方向增长

E、程序指针完整性检查

F、利用编译器将静态数据段中的函数地址指针存放地址和其他数据的存放地址分离。

4、程序漏洞攻击与防御

（1）WEB 程序漏洞攻击与防御

A、CGI 漏洞攻击

CGI 的漏洞：配置错误、边界条件错误、访问验证错误、来源验证错误、输入验证错误、异常情况处理失败、策略错误

防范的方法：注意 P570 的 8 条。

B、SQL 注入攻击

SQL 注入攻击的过程主要包含以下几步：发现 SQL 注入位置、判断后台数据库类型、确定 XP_CMDSHELL 可执行情况、发现 WEB 虚拟目录、上传 ASP 木马、得到管理员权限。

防御方法：注意 P571 的 4 条

（2）TCP/IP 漏洞

A、Ping of Death 攻击

攻击类型：Ping Of Death 攻击是一种拒绝服务攻击。

攻击特征：该攻击数据包大于 65535 个字节。由于部分操作系统接收到长度大于 65535 字节的数据包时，就会造成内存溢出、系统崩溃、重启、内核失败等后果，从而达到攻击的目的。

检测方法：判断数据包的大小是否大于 65535 个字节。

反攻击方法：使用新的补丁程序，当收到大于 65535 个字节的数据包时，丢弃该数据包，并进行系统审计。

B、Teardrop 攻击

攻击类型：Teardrop 攻击是一种拒绝服务攻击。

攻击特征：Teardrop 是基于 UDP 的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。（利用 UDP 包重组时重叠偏移（假设数据包中第二片 IP 包的偏移量小于第一片结束的位移，而且算上第二片 IP 包的 Data，也未超过第一片的尾部，这就是重叠现象。）的漏洞对系统主机发动拒绝服务攻击，最终导致主机蹇掉；对于 Windows 系统会导致蓝屏死机，并显示 STOP 0x0000000A 错误。）

检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量（Offset）是否有误。

反攻击方法：添加系统补丁程序，丢弃收到的病态分片数据包并对这种攻击进行审计。

C、Winnuke 攻击

攻击类型：WinNuke 攻击是一种拒绝服务攻击。

攻击特征：WinNuke 攻击又称带外传输攻击，它的特征是攻击目标端口，被攻击的目标端口通常是 139、138、137、113、53，而且 URG 位设为“1”，即紧急模式。

检测方法：判断数据包目标端口是否为 139、138、137 等，并判断 URG 位是否为“1”。

反攻击方法：适当配置防火墙设备或过滤路由器就可以防止这种攻击手段（丢弃该数据包），并对这种攻击进行审计（记录事件发生的时间，源主机和目标主机的 MAC 地址和 IP 地址 MAC）。

D、Land 攻击

land 攻击是一种使用相同的源和目的主机和端口发送数据包到某台机器的攻击。结果通常使存在漏洞的机器崩溃。

在 Land 攻击中，一个特别打造的 SYN 包中的原地址和目标地址都被设置成某一个服务器地址，这时将导致接受服务器向它自己的地址发送 SYN 一 ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。对 Land 攻击反应不同，许多 UNIX 实现将崩溃，而 Windows NT 会变的极其缓慢（大约持续五分钟）。

5、欺骗攻击与防御

（1）ARP 欺骗

详情请参阅：ARP 欺骗

（2）DNS 欺骗

详情请参阅：DNS 欺骗

（3）IP 欺骗

详情请参阅：**ip 地址欺骗**

6、端口扫描

详情请参阅：端口扫描

7、强化 TCP/IP 堆栈以抵御拒绝服务攻击

（1）同步包风暴（SYN Flooding）

Synflood:该攻击以多个随机的源主机地址向目的路由器发送 SYN 包，而在收到目的路由器的 SYN ACK 后并不回应，这样，目的路由器就为这些源主机建立了大量的连接队列，而且由于没有收到 ACK 一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务，甚至导致路由器崩溃.服务器要等待超时(Time Out)才能断开已分配的资源。

防范措施：

A、设置 HALF-TCP 连接的最大个数。超过这个 MAX 后随机关闭已建立的 HALF-TCP 连接或者丢弃新来的 SYN 信息.

B、关闭 TCP 服务。攻击者使用无效的 ip 地址，利用 tcp 连接的三次握手过程，使得受害主机处于开放会话的请求之中，直至连接超时。在此期间，受害主机还会连续接受这种会话请求，最终因耗尽资源而停止响应。

（2）ICMP 攻击

防御基于 ICMP 的网络攻击的方法

A、**选择合适的防火墙**

有效防止 ICMP 攻击，防火墙应该具有状态检测、细致的数据包完整性检查和很好的过滤规则控制功能。

状态检测防火墙通过跟踪它的连接状态，动态允许外出数据包的响应信息进入防火墙所保护的网络。例如，状态检测防火墙可以记录一个出去的 PING（ICMP Echo Request），在接下

来的一个确定的时间段内，允许目标主机响应的 ICMP Echo Reply 直接发送给前面发出了 PING 命令的 IP，除此之外的其他 ICMP Echo Reply 消息都会被防火墙阻止。与此形成对比的是，包过滤类型的防火墙允许所有的 ICMP Echo Reply 消息进入防火墙所保护的网络了。许多路由器和基于 Linux 内核 2.2 或以前版本的防火墙系统，都属于包过滤型，用户应该避免选择这些系统。

新的攻击不断出现，防火墙仅仅能够防止已知攻击是远远不够的。通过对所有数据包进行细致分析，删除非法的数据包，防火墙可以防止已知和未知的 DoS 攻击。这就要求防火墙能够进行数据包一致性检查。安全策略需要针对 ICMP 进行细致的控制。因此防火墙应该允许对 ICMP 类型、代码和包大小进行过滤，并且能够控制连接时间和 ICMP 包的生成速率。

B、**配置防火墙以预防攻击**

一旦选择了合适的防火墙，用户应该配置一个合理的安全策略。以下是被普遍认可的防火墙安全配置惯例，可供管理员在系统安全性和易用性之间作出权衡。

防火墙应该强制执行一个缺省的拒绝策略。除了出站的 ICMP Echo Request、出站的 ICMP Source Quench、进站的 TTL Exceeded 和进站的 ICMP Destination Unreachable 之外，所有的 ICMP 消息类型都应该被阻止。下面是针对每个 ICMP 消息类型的过滤规则的详细分析。

Echo Request 和 Reply（类型 8 和 0）：允许 Echo Request 消息出站以便于内部用户能够 PING 一个远程主机。阻止入站 Echo Request 和出站 Echo Reply 可以防止外部网络的主机对内部网络进行扫描。如果您使用了位于外部网络的监视器来监视内部网络，就应该只允许来自于特定外部 IP 的 Echo Request 进入您的网络。限制 ICMP Echo 包的大小可以防止“Ping Floods”攻击，并且可以阻止那些利用 Echo Request 和 Reply 来“偷运”数据通过防火墙的木马程序。

Destination unreachable （类型 3）：允许其入站以便于内部网用户可以使用 traceroute。需要注意的是，有些攻击者可以使用它来进行针对会话的 DoS 攻击，如果您曾经历过类似的

攻击，也可以阻止它。阻止出站的 ICMP Destination unreachable 消息，因为它可能会泄漏内部网络的结构。不过有一个例外，对于那些允许外部网络通过 TCP 访问的内部主机（如位于 DMZ 区的 Web 服务器）发出的 Destination unreachable，则应该允许它通过。为了能够支持“Path MTU Discovery”，您应该允许出站的“Packet Too Big”消息（类型 3，代码 4）到达那些主机。

Source quench（类型 4）：阻止其入站，因为它可以作为一种 DoS 攻击，能够降低发送者的发送速度。允许其出站以便于内部主机能够控制发送端发送数据的速度。有些防火墙会忽略所有直接发送到防火墙端口的 Source Quench 消息，以防止针对于防火墙的 DoS 攻击。

Redirect、Router announcement、 Router selection（类型 5，9，10）：这些消息都存在潜在危险，因为它们可以用来把数据重定向到攻击者的机器。这些消息都应该被阻止。

TTL exceeded（类型 11）：允许其进站以便于内部用户可以使用 traceroute。“firewalking”使用很低的 TTL 值来对网络进行扫描，甚至可以通过防火墙对内网进行扫描，所以应该禁止其出站。一些防火墙可以阻止 TTL 值小于设定值的数据包进入防火墙。

Parameter problem（类型 12）：禁止其入站和出站。通过使用一个能够进行数据包一致性检查的防火墙，错误和恶意的数据包都会被阻塞。

（3）SNMP 攻击

8、系统漏洞扫描

（1）基于网络的漏洞扫描

（2）基于主机的漏洞扫描

第 4 章网络安全 4.3 防火墙应用配置（P581-620）

1、防火墙技术概述

（1）防火墙的定义

防火墙是设置在两个或多个网络之间的安全阻隔，用于保证本地网络资源的安全，通常是饮

食软件部分和硬件部分的一个系统或多个系统的组合。

（2）防火墙的分类及技术

A、按防火墙的软硬件形式分类：基于硬件的防火墙、基于软件的防火墙、嵌入式防火墙

B、按防火墙采用的技术分类：包过滤型防火墙、应用层网关防火墙、代理服务型防火墙

2、防火墙体系结构

堡垒主机：是指可能直接面对外部用户攻击的主机系统，在防火墙体系结构中特指那些处于内部网络的边缘，并且暴露于外部网络用户面前的主机系统。一般来说，堡垒主机上提供的服务越少越好。

双重宿主主机：是指通过不同网络接口连入我个网络的主机系统，又称为多穴主机系统。网桥是在数据链路层实现互连的双重宿主主机，路由器是在网络层实现互连的双重宿主主机，应用层网关是在应用层实现互连。

周边网络：是指在内部网络、外部网络之间增加的一个网络，也被称为非武装区域（DMZ）。

（1）双生宿主主机体系结构

是指以一台双重宿主主机作为防火墙系统的主体执行分离外部网络与内部网络的任务。

优点：网络结构简单、安全。

缺点：用户访问外部资源较为复杂、外部用户入侵了双重宿主主机，则内部网络处于不安全状态。

（2）被屏蔽主机体系结构

是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内部、外部网络的隔离和对内网的保护。

此结构中，有两道屏障，一是屏蔽路由器，二是堡垒主机。

优点：具有更高的安全性、访问外部网络较为方便和灵活、堡垒主机可以以更高的效率提供数据包过滤或代理服务。

缺点:外部用户在被允许的情况下可以访问内部网络、用户入侵堡垒主机则内部网络不安全、配置较为复杂较容易形成错误和漏洞。

（3）被屏蔽子网体系结构

主要由 4 个部件组成，分别为周边网络、外部路由器、内部路由器、堡垒主机。

优越性：双层防护、提高了内部安全性、避免了路由器失效产生的安全隐患、用户只能访问堡垒主机提供的服务、即使入侵堡垒机也无法进入内部网络。

缺点：成本高、配置复杂。

（4）其他体系结构

3、分布式防火墙技术

（1）分布式防火墙技术产生的背景

（2）分布式防火墙的结构

网络防火墙、主机防火墙、中心管理系统

（3）分布式防火墙的主要特点

主机驻留、嵌入 OS、安全策略的统一管理与部署

（4）分布式防火墙的主要优势

增强了系统安全性、提高了系统性能、系统的扩展性无限制、实话主机策略、应用更为广泛，支持 VPN 通信。

4、防火墙应用规则

防火墙具体部署方法要根据实际的应用需求而定，不是统一的。

（1）企业网络体系结构

A、企业网络体系结构中的三个区域：边界网络、外围网络、内部网络。

B、企业组织中的防火墙及其功能：分为外围防火墙和内部防火墙。外围防火墙主要提供对不受信任的外部用户的限制,而内部防火墙主要防止外部用户访问内部网络并且限制内部用户可以执行的操作。

C、选择防火墙时要考虑的因素：预算方面、现有设备、可用性、冗余部件、备用设备、可扩展性、所需功能。

（2）控制因特网用户对内部网络的访问

A、网络结构中划分不同的安全级别

内部网络：是防火墙重点保护的对象，是可信区域。

外部网络：是防火墙要防备的对象，是非可信网络区域。

DMZ 区域：受保护的的级别较低。

B、设置安全策略

（3）控制内部网络不同部门之间的访问

是指在一个企业内部网络之间，对一些安全造敏感的部门或者特殊主机进行的隔离保护。一种方法是通过配置 VLAN 实现逻辑隔离，另一种是采用防火墙进行隔离。

（4）控制对服务器中心的网络访问

两种实施方案：

A、为每个企业用户的服务器或服务器群单独配置一个独立的防火墙

B、采用虚拟防火墙方式。

5、内部防火墙系统应用设计

（1）网络上的用户分类

网络上的用户可以分为：信任用户、部分信任用户、不信任用户。

（2）防火墙的类别选择及考虑事项

从功能、设备属性、管理功能要求、吞吐量、可用性要求等方面考虑。

（3）内部防火墙规则

遵循 P599-600 的 19 条规则。

（4）内部防火墙的可用性需求

在内部防火墙方案中，根据具体实际需求，可以采用不同的防火墙系统配置方案，主要有：

A、没有冗余组件的单一防火墙

优点：成本低、管理简单、单个记录源

缺点：单一故障点、可能的通信瓶颈。

B、具有冗余组件的单一防火墙

优点：可用性有了一定程序的提高。

缺点：与无冗余组件的单一防火墙方案基本一样。

C、容错防火墙集——防火墙冗余对

优点：容错、集中通信日志、可能的状态共享。

缺点：复杂程度增加、配置更复杂、成本增加。

（5）内部容错防火墙集配置

A、主动/被动内部容错防火墙集

一个设备（活动节点）将处理所有通信，而另一个设备（被动节点）即不转发通信也不执行筛选，只是保持活动，监视主动节点的状态。类似于服务器双机容错方案中的“冷备份”。

优点：配置简单、可预测故障转移负载

缺点：低利用率。

B、主动/主动内部容错防火墙集

两个或多个节点主动侦听发送到每个节点共享的虚拟 Ipfbfhr 所有请示，与服务器双机容错方案中的“热备份”类似。

优点：效率高、吞吐量大

缺点：可能超负荷、复杂程度增加

（6）内部防火墙系统设计的其他因素要求

安全性、可伸缩性、整合、标准的支持。

6、外围防火墙系统应用设计

（1）外围防火墙规则

遵循 P607-608 的 11 条规则。

（2）外围防火墙系统的可用性要求

A、单个无冗余组件外围防火墙。

B、单个带冗余组件外围防火墙。

C、外围容错防火墙集。

7、防火墙与 DoS/DdoS 攻击

（1）防火墙抵御 DoS/DdoS 攻击原理

A、基于状态的资源控制，保护防火墙资源

B、智能 TCP 代理有效防范 SYN Flood

C、利用 Netflow 对 DoS 攻击和病毒进行监测

（2）防火墙抵御 DoS/DdoS 攻击配置示例

注意了解和记忆 P612-613 的各命令。

（3）使用防火墙防御 SYN Flood 攻击

A、两种主要类型防火墙的防御原理

应用代理型防火墙、包过滤型防火墙

B、防御 SYN Flood 攻击的防火墙设置

SYN 网关、被动式 SYN 网关、SYN 中继

8、防火墙应用实例

注意掌握 6 个基本命令：

nameif、interface、ip address、nat、global、route

第 4 章网络安全 4.4 ISA Server 应用配置（P620-643）

1、ISA Server 的安装

（1）安装准备

A、应保证网络正常工作

B、必须为连接到 ISA Server 服务器的每个网络单独准备一个网络适配器，至少需要一个网络适配器。

C、DNS 服务器。

（2）安装 ISA Server

详情请参阅图 4-33 至图 4-42

2、配置允许所有内部用户访问 Internet 的所有服务的访问规则

（1）网络规则

网络连接方式：路由、网络地址转换、本地主机访问、VPN 客户端到内部网络、Internet 访问。

（2）访问规则

A、防火墙系统策略

B、建立访问策略

（3）配置拨号连接

3、使用边缘防火墙模板建立访问策略

具体内容参阅 P635-638 内容。

4、配置启用 HTTP 缓存

具体参阅 P638-643

第 4 章网络安全 4.5 IDS 和 IPS（P643-658）

1、入侵检测系统概述

（1）IDS 的定义

是一种主动保护自己，使网络和系统免遭非法攻击的网络安全技术，它依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或攻击结果，以保证网络系统资源的机密性、完整性和可用性。

（2）IDS 的作用

A、通过检测和记录网络中的安全违规行为，惩罚网络犯罪，防止网络入侵事件的发生。

B、检测其他安全措施未能阻止的攻击或安全违规行为

C、检测黑客在攻击前的探测行为，预先给管理员发出警报。

D、报告计算机系统或网络中存在的安全威胁。

E、提供有关攻击的信息，帮助管理员诊断网络中存在的安全弱点，利于其进行修补。

F、在大型、复杂的计算机网络中布置入侵检测系统，可以显著提高网络安全管理的质量。

（3）IDS 的组成

一个 IDS 通常由探测器、分析器、响应单元、事件数据库组成。

（4）IDS 的类型及技术

基于主机的入侵检测、基于网络的入侵检测、混合入侵检测系统（结合前两种技术）

（5）分布式入侵检测系统

DIDS 采用了分布式智能代理的结构方式，由几个中央智能代理和大量分布的本地代理组成，其中本地代理负责处理本地事件，而中央代理负责整体的分析工作。

2、入侵检测系统实例

（1）RIDS-100

由瑞星公司自主开发研制的新一代网络安全产品，它集入侵检测、网络管理、网络监视功能于一身。是一套基于网络的 DIDS，它主要由入侵检测引擎和管理控制台两部分组成。

典型应用方案：

A、监听、检测发生在内网之间的连接和攻击

B、监听、检测外网对内网的攻击

（2）Cisco 入侵检测系统 4200

Cisco IDS 4210 可以监控 45Mbps 的流量，适用于 T1/E1 和 T3 环境。

Cisco IDS 4235 可以监控 200Mbps 的流量，可以在交换环境中、多个 T3 子网上以及在 10/100/1000 接口的支持下提供保护。另外，它还可以部署在部分使用的千兆位链路上。

Cisco IDS 4250 不但能以 500Mbps 的速度支持无与伦比的性能，还能保护千兆位子网以及正在穿越交换机的流量。

3、入侵防御系统

（1）入侵防御系统概述

IPS 提供主动、实时的防护，其设计旨在对网络流量中的恶意数据包进行检测，对攻击性的

流量进行自动拦截，使它们无法造成损失。IPS 如果检测到攻击企图，就会睡去地将攻击包丢掉或采取措施阻断攻击源，而不把攻击流量放进内部网络。

注意区别：IPS 与防火墙、IPS 与 IDS

IPS 系统根据部署方式可以分为在类：HIPS、NIPS、AIP

IPS 必须具备如下技术特征：嵌入式运行、深入分析的控制、入侵特征库、高效处理能力。

（2）入侵防御系统的原理

在 ISO/OSI 网路层次模型(见 OSI 模型) 中，防火墙主要在第二到第四层起作用，它的作用在第四到第七层一般很微弱。而除病毒软体主要在第五到第七层起作用。为了弥补防火墙和除病毒软体二者在第四到第五层之间留下的空档，几年前，工业界已经有入侵侦查系统(IDS: Intrusion Detection System）投入使用。入侵侦查系统在发现异常情况后及时向网路安全管理人员或防火墙系统发出警报。可惜这时灾害往往已经形成。虽然，亡羊补牢，尤未为晚，但是，防卫机制最好应该是在危害形成之前先期起作用。随后应运而生的入侵反应系统(IRS: Intrusion Response Systems) 作为对入侵侦查系统的补充能够在发现入侵时，迅速作出反应，并自动采取阻止措施。而入侵预防系统则作为二者的进一步发展，汲取了二者的长处。

入侵预防系统也像入侵侦查系统一样，专门深入网路数据内部，查找它所认识的攻击代码特征，过滤有害数据流，丢弃有害数据包，并进行记载，以便事后分析。除此之外，更重要的是，大多数入侵预防系统同时结合考虑应用程序或网路传输重的异常情况，来辅助识别入侵和攻击。比如，用户或用户程序违反安全条例、数据包在不应该出现的时段出现、作业系统或应用程序弱点的空子正在被利用等等现象。入侵预防系统虽然也考虑已知病毒特征，但是它并不仅仅依赖于已知病毒特征。

应用入侵预防系统的目的在于及时识别攻击程序或有害代码及其克隆和变种，采取预防措施，先期阻止入侵，防患于未然。或者至少使其危害性充分降低。入侵预防系统一般作为防火墙
和防病毒软体的补充来投入使用。在必要时，它还可以为追究攻击者的刑事责任而提供法律上有效的证据（forensic)。

（3）IPS 的检测技术

A、基于特征的匹配技术

B、协议分析技术

C、抗 DDoS/Dos 技术

D、智能化检测技术

E、蜜罐技术

（4）IPS 存在的问题

单点故障、性能瓶颈、误报率和漏报率。

第 4 章网络安全 4.6 访问控制技术（P658-670）

1、访问控制技术概述

（1）访问控制的基本模型

访问控制包括三个要素：主体、客体、控制策略。

访问控制包括认证、控制策略实现和审计三方面的内容。

（2）访问控制的实现技术

A、访问控制矩阵（ACM）

是通过矩阵形式表示访问控制规则和授权用户权限的方法

访问矩阵是以主体为行索引，以客体为列索引的矩阵，矩阵中的每一个元素表示一组访问方式，是若干访问方式的集合。

B、访问控制表（ACLs）

实际上是按列保存访问矩阵。访问控制表提供了针对客体的方便的查询方法。但是用它来查询一个主体对所有客体的所有访问权限是很困难的。

C、能力表

对应于访问控制表，这种实现技术实际上是按行保存访问矩阵。能力表实现的访问控制系统可以很方便地查询某一个主体的所有访问权限，但查询对某一个客体具有访问权限的主体信息是很困难的。

D、授权关系表

是即不对应于行也不对应于列的实现技术，只对应访问矩阵中每一个非空元素的实现技术。

如果授权关系表按主体排序，查询时就可以得到能力表的效率；如果按客体排序，查询时就可得到访问控制表的效率。

（3）访问控制表介绍

A、ACL 的作用

可以限制网络流量、提高网络性能；

提供对通信流量的控制手段；

是提供网络安全访问的基本手段；

可以在路由器端口处决定哪种类型的通信流量被转发或被阻塞。

B、ACL 的执行过程

一个端口执行哪条 ACL，这需要按照列表中的条件语句执行顺序来判断。如果一个数据包的报头跟表中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

数据包只有在跟第一个判断条件不匹配时，它才被交给 ACL 中的下一条件判断语句进行比较。

如果匹配，则不管是第一条还是最后一条语句，数据都会立即发送到目的接口。

如果甩有的 ACL 判断语句都检测完毕，仍没有匹配的语句出口，则该数据包将视为被拒绝而被丢弃。

注意，ACL 不能对本路由器产生的数据包进行控制。

C、ACL 的分类

分为标准 ACL 和扩展 ACL。

主要区别：标准 ACL 只检查数据包的源地址；扩展 ACL 既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。

D、ACL 的配置

在全局配置模式下，使用下列命令创建 ACL：

Router(config)# access-list *access-list-number* {permit|deny} {test-conditions}

在接口配置模式下，使用 access-group 命令 ACL 应用到某一接口上：

Router(config-if)# {protocol} access-group access-list-number {in|out}

E、标准 ACL 举例

注意 P662 到 663 页内容即可。

（4）访问控制的模型发展

2、传统访问控制技术

（1）自主型访问控制（DAC）

Discretionary Access Control

自主访问控制是一种最为普遍的访问控制手段，用户可以按自己的意愿对系统的参数做适当修改以决定哪些用户可以访问他们的文件，亦即一个用户可以有选择地与其它用户共享他的文件。用户有自主的决定权。

自主访问控制一个安全的操作系统需要具备访问控制机制。它基于对主体及主体所属的主体组的识别，来限制对客体的访问，还要校验主体对客体的访问请求是否符合存取控制规定来决定对客体访问的执行与否。这里所谓的自主访问控制是指主体可以自主地（也可能是单位方式）将访问权，或访问权的某个子集授予其它主体。

将数字信号转换为模拟信号

（2）强制型访问控制（MAC）

Mandatory Access Control .

强制访问控制允许加载新的访问控制模块，并借此实施新的安全策略，其中一部分为一个很小的系统子集提供保护并加强特定的服务，其他的则对所有的主体和客体提供全面的标签式安全保护。定义中有关强制的部分源于如下事实，控制的实现由管理员和系统作出，

而不像自主访问控制 (DAC, FreeBSD 中的标准文件以及 System V IPC 权限) 那样是按照用户意愿进行的。

强制访问控制是系统独立于用户行为强制执行访问控制，它也提供了客体（数据对象）在主体（数据库用户）之间共享的控制，但强制访问控制机制是通过对主体和客体的安全级别进行比较来确定授予还是拒绝用户对资源的访问，从而防止对信息的非法和越权访问，保证信息的保密性。与自主访问控制不同的是，强制访问控制由安全管理员管理，由安全管理员根据一定的规则来设置，普通数据库用户不能改变他们的安全级别或对象的安全属性；自主访问控制尽管也作为系统安全策略的一部分，但主要由客体的拥有者管理

3、基于角色的访问控制技术（RBAC）

基于角色的访问控制（Role-Based Access Control）引入了 Role 的概念，目的是为了隔离 User(即动作主体，Subject)与 Privilege(权限，表示对 Resource 的一个操作，即 Operation+Resource)。

Role 作为一个用户(User)与权限(Privilege)的代理层，解耦了权限和用户的关系，所有的授权应该给予 Role 而不是直接给 User 或 Group。Privilege 是权限颗粒，由 Operation 和 Resource 组成，表示对 Resource 的一个 Operation。例如，对于新闻的删除操作。Role-Privilege 是 many-to-many 的关系，这就是权限的核心。

基于角色的访问控制方法（RBAC）的显著的两大特征是：1.由于角色/权限之间的变化比角色/用户关系之间的变化相对要慢得多，减小了授权管理的复杂性，降低管理开销。2.灵活地支持企业的安全策略，并对企业的变化有很大的伸缩性。

RBAC 基本概念：

RBAC 认为权限授权实际上是 Who、What、How 的问题。在 RBAC 模型中，who、what、how 构成了访问权限三元组，也就是“Who 对 What(Which)进行 How 的操作”。

Who：权限的拥用者或主体（如 Principal、User、Group、Role、Actor 等等）

What：权限针对的对象或资源（Resource、Class）。

How：具体的权限（Privilege,正向授权与负向授权）。

Operator：操作。表明对 What 的 How 操作。也就是 Privilege+Resource

Role：角色，一定数量的权限的集合。权限分配的单位与载体,目的是隔离 User 与 Privilege 的逻辑关系.

Group：用户组，权限分配的单位与载体。权限不考虑分配给特定的用户而给组。组可以包括组(以实现权限的继承)，也可以包含用户，组内用户继承组的权限。User 与 Group 是多对多的关系。Group 可以层次化，以满足不同层级权限控制的要求。

RBAC 的关注点在于 Role 和 User, Permission 的关系。称为 User assignment(UA)和 Permission assignment(PA).关系的左右两边都是 Many-to-Many 关系。就是 user 可以有多个 role，role 可以包括多个 user。

凡是用过 RDBMS 都知道，n:m 的关系需要一个中间表来保存两个表的关系。这 UA 和 PA 就相当于中间表。事实上，整个 RBAC 都是基于关系模型。

Session 在 RBAC 中是比较隐晦的一个元素。标准上说：每个 Session 是一个映射，一个用户到多个 role 的映射。当一个用户激活他所有角色的一个子集的时候，建立一个 session。每个 Session 和单个的 user 关联，并且每个 User 可以关联到一或多个 Session.

在 RBAC 系统中，User 实际上是在扮演角色(Role)，可以用 Actor 来取代 User，这个想法来自于 Business Modeling With UML 一书 Actor-Role 模式。考虑到多人可以有相同权限, RBAC 引入了 Group 的概念。Group 同样也看作是 Actor。而 User 的概念就具象到一个人。

这里的 Group 和 GBAC（Group-Based Access Control）中的 Group（组）不同。GBAC 多用于操作系统中。其中的 Group 直接和权限相关联，实际上 RBAC 也借鉴了一些 GBAC 的概念。

Group 和 User 都和组织机构有关，但不是组织机构。二者在概念上是不同的。组织机构是物理存在的公司结构的抽象模型，包括部门，人，职位等等，而权限模型是对抽象概念描述。组织结构一般用 Martin fowler 的 Party 或责任模式来建模。

Party 模式中的 Person 和 User 的关系，是每个 Person 可以对应到一个 User，但可能不是所有的 User 都有对应的 Person。Party 中的部门 Department 或组织 Organization，都可以对应到 Group。反之 Group 未必对应一个实际的机构。例如，可以有副经理这个 Group，这是多人有相同职责。

引入 Group 这个概念，除了用来解决多人相同角色问题外，还用以解决组织机构的另一种授权问题：例如，A 部门的新闻我希望所有的 A 部门的人都能看。有了这样一个 A 部门对应的 Group，就可直接授权给这个 Group。

4、基于任务的访问控制模型（TBAC）

是从应用和企业层角度来解决安全问题，以面向任务的任务的角度来建立安全模型和实现安全机制，在任务处理的过程 提供动态实时的安全管理。

TBAC 模型由工作流、授权结构体、受托人和许可集 4 部分组成。

5、基于对象的访问控制模型（OBAC）

控制策略和控制规则 是 OBAC 访问控制系统的核心所在。

<>第 4 章网络安全 4.7 VPN 技术（P670-684）

1、IPSec

IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证协议 Authentication Header（AH）、封装安全载荷协议 Encapsulating Security Payload（ESP）、密钥管理协议 Internet Key Exchange （IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

（1）IPSec 的安全特性主要有：

A、不可否认性

"不可否认性"可以证实消息发送方是唯一可能的发送者，发送者不能否认发送过消息。"不可否认性"是采用公钥技术的一个特征，当使用公钥技术时，发送方用私钥产生一个数字签名随消息一起发送，接收方用发送者的公钥来验证数字签名。由于在理论上只有发送者才唯一拥有私钥，也只有发送者才可能产生该数字签名，所以只要数字签名通过验证，发送者就不能否认曾发送过该消息。但"不可否认性"不是基于认证的共享密钥技术的特征，因为在基于认证的共享密钥技术中，发送方和接收方掌握相同的密钥。

B、反重播性

"反重播"确保每个 IP 包的唯一性，保证信息万一被截取复制后，不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息后，再用相同的信息包冒取非法访问权（即使这种冒取行为发生在数月之后）。

C、数据完整性

防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSec 利用 Hash 函数为每个数据包产生一个加密检查和，接收方在打开包前先计算检查和，若包遭篡改导致检查和不相符，数据包即被丢弃。

D、数据可靠性（加密）

在传输前，对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读。该特性在 IPSec 中为可选项，与 IPSec 策略的具体设置相关。

E、认证

数据源发送信任状，由接收方验证信任状的合法性，只有通过认证的系统才可以建立通信连接。

（2）基于电子证书的公钥认证

一个架构良好的公钥体系，在信任状的传递中不造成任何信息外泄，能解决很多安全问题。IPSec 与特定的公钥体系相结合，可以提供基于电子证书的认证。公钥证书认证在 Windows 2000 中，适用于对非 Windows 2000 主机、独立主机，非信任域成员的客户机、或者不运行 Kerberos v5 认证协议的主机进行身份认证。

（3）预置共享密钥认证

IPSec 也可以使用预置共享密钥进行认证。预共享意味着通信双方必须在 IPSec 策略设置中就共享的密钥达成一致。之后在安全协商过程中，信息在传输前使用共享密钥加密，接收端使用同样的密钥解密，如果接收方能够解密，即被认为可以通过认证。但在 Windows 2000 IPSec 策略中，这种认证方式被认为不够安全而一般不推荐使用。

（4）公钥加密

IPSec 的公钥加密用于身份认证和密钥交换。公钥加密，也被称为"不对称加密法"，即加解密过程需要两把不同的密钥，一把用来产生数字签名和加密数据，另一把用来验证数字签名和对数据进行解密。

使用公钥加密法，每个用户拥有一个密钥对，其中私钥仅为其个人所知，公钥则可分发给任意需要与之进行加密通信的人。例如：A 想要发送加密信息给 B，则 A 需要用 B 的公钥加密信息，之后只有 B 才能用他的私钥对该加密信息进行解密。虽然密钥对中两把钥匙彼此相关，但要想从其中一把来推导出另一把，以目前计算机的运算能力来看，这种做法几乎完全不现实。因此，在这种加密法中，公钥可以广为分发，而私钥则需要仔细地妥善保管。

（5）Hash 函数和数据完整性

Hash 信息验证码 HMAC（Hash message authentication codes）验证接收消息和发送消息的完全一致性（完整性）。这在数据交换中非常关键，尤其当传输媒介如公共网络中不提供安全保证时更显其重要性。

HMAC 结合 hash 算法和共享密钥提供完整性。Hash 散列通常也被当成是数字签名，但这种说法不够准确，两者的区别在于：Hash 散列使用共享密钥，而数字签名基于公钥技术。hash 算法也称为消息摘要或单向转换。称它为单向转换是因为：

1）双方必须在通信的两个端头处各自执行 Hash 函数计算；

2）使用 Hash 函数很容易从消息计算出消息摘要，但其逆向反演过程以目前计算机的运算能力几乎不可实现。

Hash 散列本身就是所谓加密检查和或消息完整性编码 MIC（Message Integrity Code），通信双方必须各自执行函数计算来验证消息。举例来说，发送方首先使用 HMAC 算法和共享密钥计算消息检查和，然后将计算结果 A 封装进数据包中一起发送；接收方再对所接收的消息执行 HMAC 计算得出结果 B，并将 B 与 A 进行比较。如果消息在传输中遭篡改致使 B 与 A 不一致，接收方丢弃该数据包。

有两种最常用的 hash 函数：

• HMAC-MD5 MD5（消息摘要 5）基于 RFC1321。MD5 对 MD4 做了改进，计算速度比 MD4 稍慢，但安全性能得到了进一步改善。MD5 在计算中使用了 64 个 32 位常数，最终生成一个 128 位的完整性检查和。

• HMAC-SHA 安全 Hash 算法定义在 NIST FIPS 180-1，其算法以 MD5 为原型。 SHA 在计算中使用了 79 个 32 位常数，最终产生一个 160 位完整性检查和。SHA 检查和长度比 MD5 更长，因此安全性也更高。

（6）加密和数据可靠性

IPSec 使用的数据加密算法是 DES--Data Encryption Standard（数据加密标准）。DES 密钥长度为 56 位，在形式上是一个 64 位数。DES 以 64 位（8 字节）为分组对数据加密，每 64 位明文，经过 16 轮置换生成 64 位密文，其中每字节有 1 位用于奇偶校验，所以实际有效密钥长度是 56 位。 IPSec 还支持 3DES 算法，3DES 可提供更高的安全性，但相应地，计算速度更慢。

（7）密钥管理

• 动态密钥更新

IPSec 策略使用"动态密钥更新"法来决定在一次通信中，新密钥产生的频率。动态密钥指在通信过程中，数据流被划分成一个个"数据块"，每一个"数据块"都使用不同的密钥加密，这可以保证万一攻击者中途截取了部分通信数据流和相应的密钥后，也不会危及到所有其余的通信信息的安全。动态密钥更新服务由 Internet 密钥交换 IKE（Internet Key Exchange）提供，详见 IKE 介绍部分。

IPSec 策略允许专家级用户自定义密钥生命周期。如果该值没有设置，则按缺省时间间隔自动生成新密钥。

• 密钥长度

密钥长度每增加一位，可能的密钥数就会增加一倍，相应地，破解密钥的难度也会随之成指数级加大。IPSec 策略提供多种加密算法，可生成多种长度不等的密钥，用户可根据不同的安全需求加以选择。

• Diffie-Hellman 算法

要启动安全通讯，通信两端必须首先得到相同的共享密钥（主密钥），但共享密钥不能通过网络相互发送，因为这种做法极易泄密。

Diffie-Hellman 算法是用于密钥交换的最早最安全的算法之一。DH 算法的基本工作原理是：通信双方公开或半公开交换一些准备用来生成密钥的"材料数据"，在彼此交换过密钥生成"材料"后，两端可以各自生成出完全一样的共享密钥。在任何时候，双方都绝不交换真正的密钥。

通信双方交换的密钥生成"材料"，长度不等，"材料"长度越长，所生成的密钥强度也就越高，密钥破译就越困难。
除进行密钥交换外，IPSec 还使用 DH 算法生成所有其他加密密钥。

AH 报头字段包括：

• Next Header（下一个报头）：
识别下一个使用 IP 协议号的报头，例如，Next Header 值等于"6"，表示紧接其后的是 TCP 报头。

• Length（长度）： AH 报头长度。

• Security Parameters Index (SPI，安全参数索引)：
这是一个为数据报识别安全关联的 32 位伪随机值。SPI 值 0 被保留来表明"没有安全关联存在"。

• Sequence Number（序列号）：从 1 开始的 32 位单增序列号，不允许重复，唯一地标识了每一个发送数据包，为安全关联提供反重播保护。接收端校验序列号为该字段值的数据包是否已经被接收过，若是，则拒收该数据包。

• Authentication Data（AD，认证数据）：
包含完整性检查和。接收端接收数据包后，首先执行 hash 计算，再与发送端所计算的该字段值比较，若两者相等，表示数据完整，若在传输过程中数据遭修改，两个计算结果不一致，则丢弃该数据包。

数据包结构：

如图二所示，AH 报头插在 IP 报头之后，TCP，UDP，或者 ICMP 等上层协议报头之前。一般 AH 为整个数据包提供完整性检查，但如果 IP 报头中包含"生存期（Time To Live）"或"服务类型（Type of Service）"等值可变字段，则在进行完整性检查时应将这些值可变字段去除。

2、GRE

（GRE: Generic Routing Encapsulation）

通用路由封装（GRE）定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议。

在大多数常规情况下，系统拥有一个有效载荷（或负载）包，需要将它封装并发送至某个目的地。首先将有效载荷封装在一个 GRE 包中，然后将此 GRE 包封装在其它某协议中并进行转发。此外发协议即为发送协议。当 IPv4 被作为 GRE 有效载荷传输时，协议类型字段必须被设置为 0x800。当一个隧道终点拆封此含有 IPv4 包作为有效载荷的 GRE 包时，IPv4 包头中的目的地址必须用来转发包，并且需要减少有效载荷包的 TTL。值得注意的是，在转发这样一个包时，如果有效载荷包的目的地址就是包的封装器（也就是隧道另一端），就会出现回路现象。在此情形下，必须丢弃该包。当 GRE 包被封装在 IPv4 中时，需要使用 IPv4 协议 47。

GRE 下的网络安全与常规的 IPv4 网络安全是较为相似的，GRE 下的路由采用 IPv4 原本使用的路由，但路由过滤保持不变
。包过滤要求防火墙检查 GRE 包，或者在 GRE 隧道终点完成过滤过程。在那些这被看作是安全问题的环境下，可以在防火墙上终止隧道。

3、MPLS VPN

（1）MPLS VPN 概述

随着网络经济的发展，企业对于自身网络的建设提出了越来越高的要求，主要表现在网络的灵活性、经济性、扩展性等方面。在这样的背景下，VPN 以其独有的优势赢得了越来越多企业的青睐。利用公共网络来构建的私有专用网络称为虚拟私有网络（VPN，Virtual Private Network）。在公共网络上组建的 VPN 象企业现有的私有网络一样提供安全性、和可管理性等。在所有的 VPN 技术中，MPLS VPN 具有良好的可扩展性和灵活性，是目前发展最为迅速的 VPN 技术之一。

A、 MPLS

MPLS(Multiprotocol Label Switching, 多协议标记交换)使用标签(Label)进行转发，一个标签是一个短的、长度固定的数值，由报文的头部携带，不含拓扑信息，只有局部意义。MPLS 包头的结构如下图所示，包含 20 比特的标签，3 比特的 EXP(通常用作 Cos)，1 比特的 S，用于标识此标签是否为最底层标签，8 比特的 TTL。

MPLS 可以看做是一种面向连接的技术。通过 MPLS 信令(如 LDP，Label Distribute Protocol，标签分配协议)建立好 MPLS 标记交换通道(Label Switched Path，简称 LSP），数据转发时，在网络入口对报文进行分类，根据分类结果选择相应的 LSP，打上相应的标签，中间路由器在收到 MPLS 报文以后直接根据 MPLS 报头的标签进行转发，而不用再通过 IP 报文头的 IP 地址查找。在 LSP 出口（或倒数第二跳），弹出 MPLS 标签，还原为 IP 包。

B、MPLS/BGP VPN

MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，根据 PE（Provider Edge）设备是否参与 VPN 路由处理又细分为二层 VPN 和三层 VPN，一般而言，MPLS/BGP VPN 指的是三层 VPN。

在 MPLS/BGP VPN 的模型中，网络由运营商的骨干网与用户的各个 Site 组成，所谓 VPN 就是对 site 集合的划分，一个 VPN 就对应一个由若干 site 组成的集合。

MPLS/BGP VPN 所包含的基本组件：

PE：Provider Edge Router，骨干网边缘路由器，是 MPLS L3VPN 的主要实现者。

CE：Custom Edge Router，用户网边缘路由器。

P router： Provider Router，骨干网核心路由器，负责 MPLS 转发。

VPN 用户站点（site）：VPN 中的一个孤立的 IP 网络，一般来说，不通过骨干网不具有连通性，公司总部、分支机构都是 site 的具体例子。

在 MPLS/BGP VPN 中，属于同一的 VPN 的两个 site 之间转发报文使用两层标签，在入口 PE 上为报文打上两层标签，外层标签在骨干网内部进行交换，代表了从 PE 到对端 PE 的一条隧道，VPN 报文打上这层标签，就可以沿着 LSP 到达对端 PE，然后再使用内层标签决定报文应该转发到哪个 site 上。

C、 L2 MPLS VPN

简单来说，MPLS L2VPN 就是在 MPLS 网络上透明传递用户的二层数据。从用户的角度来看，这个 MPLS 网络就是一个二层的交换网络。以 ATM 为例，每一个用户边缘设备（CE）配置一个 ATM 虚电路，通过 MPLS 网络与远端的另一个 CE 设备相连，与通过 ATM 网络实现互联是完全一样的。

在 MPLS L2VPN 中，CE、PE、P 的概念与 BGP/MPLS VPN 一样，原理也很相似：利用标记栈来实现用户报文在 MPLS 网络中的透明传送：外层标记（称为 tunnel 标记）用于将报文从一个 PE 传递到另一个 PE，内层标记（在 MPLS L2VPN 中，称为 VC 标记）用于区分不同 VPN 中的不同连接，接收方的 PE 根据 VC 标记决定将报文传递给哪个 CE。

当前 MPLS L2VPN 还没有形成正式的标准。存在两种主要的实现方式：Martini 方式和 Kompella 方式。前者使用扩展的 LDP 协议作为信令来传递 VC 标记，因此又被称为 LDP 方式的 L2VPN。Kompella 方式采用 BGP 扩展为信令来散发二层可达信息和 VC 标记，因此又被称为 BGP 方式的 L2VPN。

（2）MPLS VPN 的应用

采用 MPLS VPN 技术可以把现有 IP 网络分解成逻辑上隔离的网络，这种逻辑上隔离的网络的应用可以是千变万化的：可以是用在解决企业互连、政府相同/不同部门的互连、也可以用来提供新的业务，如为 IP 电话业务专门开通一个 VPN。

例如：

用 MPLS VPN 构建运营支撑网

利用 MPLS VPN 技术可以在一个统一的物理网络上实现多个逻辑上相互独立的 VPN 专网，该特性非常适合于构建运营支撑网，例如，目前国内很多省市的 DCN 网就采用华为的设备，在一个统一的物理网络上构建网管，OA，计费等多个业务专网。

MPLS VPN 在与运营商城域网的应用:

作为运营商的基础网络，宽带城域网需同时服务多种不同的用户，承载多种不同的业务，存在多种接入方式，这一特点决定城域网需同时支持 MPLS L3VPN，MPLS L2VPN 及其它 VPN 服务，根据网络实际情况及用户需求开通相应的 VPN 业务，例如，为用户提供 MPLS L2VPN 服务以满足用户节约专线租用费用的要求。

MPLS VPN 在企业网络的应用:

MPLS VPN 在企业网中同样有广泛应用。例如，在电子政务网中，不同的政府部门有着不同的业务系统，各系统之间的数据多数是要求相互隔离的，同时各业务系统之间又存在着互访的需求，因此大量采用 MPLS VPN 技术实现这种隔离及互访需求。

4、VPDN

VPDN 是基于拨号接入(PSTN、ISDN)的虚拟专用拨号网业务，可用于跨地域集团企业内部网、专业信息服务提供商专用网、
金融大众业务网、银行存取业务网等业务。

VPDN 采用专用的网络安全和通信协议，可以使企业在公共网络上建立相对安全的虚拟专网。VPN 用户可以经过公共网络，通过虚拟的安全通道和用户内部的用户网络进行连接，而公共网络上的用户则无法穿过虚拟通道访问用户网络内部的资源。

VPDN 技术适用于以下范围：

地点分散，在各地有分支机构，移动人员特别多的用户，例如企业用户、远程教育用户。

人员分散，需通过长途电信甚至国际长途手段联系的用户。

对线路的保密和可用性有一定要求的用户。

此外，通过 VPDN 技术，可实现对特定站点的封闭，可向小 ISP 和大集团用户提供一次、多次端口批发业务。

VPDN 网络结构由局端（或称为中心端）和客户系统组成。VPDN 客户系统包括两部分：企业端与远端。通常企业端是企业的内部局域网，以专线方式接入 UNINET；远端是拨号客户，以拨号方式访问企业内部局域网。

VPDN——（Virtual Private Dail-up Network 虚拟拨号专用网），业务名称为“网中网”，是指在中国公众多媒体通信网，在接入手段上的延伸，它以拨号方式实现，同时又允许专线接入，与其无缝结合，组成一个提供多种接入手段的虚拟专用网。

VPN 可划分为:VLL(Virtual Leased Lines)、VPDN(Virtual Private Dial Networks)、VPRN(Virtual Private Routed Networks...VPDN 网上办税认证平台”,每位纳税人可采用宽带上网或拨号上网方式,通过专用账户和密码,经 VPDN 专用隧道登录国税网站即可

第 4 章网络安全 4.8 企业网络安全隔离（P684-695）

1、网络隔离技术概述

面对新型网络攻击手段的出现和高安全度网络对安全的特殊需求，全新安全防护防范理念的网络安全技术——“网络隔离技术”应运而生。网络隔离技术的目标是确保隔离有害的攻击，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。网络隔离技术是在原有安全技术的基础上发展起来的，它弥补了原有安全技术的不足，突出了自己的优势。

网络隔离，英文名为 Network Isolation，主要是指把两个或两个以上可路由的网络（如：TCP/IP）通过不可路由的协议（如：IPX/SPX、NetBEUI 等）进行数据交换而达到隔离目的。由于其原理主要是采用了不同的协议所以通常也叫协议隔离（Protocol Isolation）.1997 年，信息安全专家 Mark Joseph Edwards 在他编写的＜Understanding Network Security＞一书中，就对协议隔离进行了归类。在书中他明确地指出了协议隔离和防火墙不属于同类产品。

网络隔离技术是把两个或两个以上可路由的网络通过不可路由的协议进行数据交换而达到隔离目的.

2、划分子网隔离

3、VLAN 隔离

（1）VLAN 隔离的概念

VLAN 是英文 Virtual Local Area Network 的缩写，即虚拟局域网。VLAN 是对连接到的第二层交换机端口的网络用户的逻辑分段，不受网络用户的物理位置限制而根据用户需求进行网络分段。一个 VLAN 可以在一个交换机或者跨交换机实现。VLAN 可以根据网络用户的位置、作用、部门或者根据网络用户所使用的应用程序和协议来进行分组。基于交换机的虚拟局域网能够为局域网解决冲突域、广播域、带宽问题。一方面，VLAN 建立在局域网交换机的基础之上；另一方面，VLAN 是局域交换网的灵魂。这是因为通过 VLAN 用户能方便地在网络中移动和快捷地组建宽带网络，而无需改变任何硬件和通信线路。这样，网络管理员就能从逻辑上对用户和网络资源进行分配，而无需考虑物理连接方式。 VLAN 充分体现了现代网络技

术的重要特征：高速、灵活、管理简便和扩展容易。是否具有 VLAN 功能是衡量局域网交换机的一项重要指标。网络的虚拟化是未来网络发展的潮流。VLAN 与普通局域网从原理上讲没有什么不同，但从用户使用和网络管理的角度来看，VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，甚至位于不同的国家。

传统的共享介质的以太网和交换式的以太网中，所有的用户在同一个广播域中，会引起网络性能的下降，浪费可贵的带宽；而且对广播风暴的控制和网络安全只能在第三层的路由器上实现。

VLAN 相当于 OSI 参考模型的第二层的广播域，能够将广播风暴控制在一个 VLAN 内部，划分 VLAN 后，由于广播域的缩小，网络中广播包消耗带宽所占的比例大大降低，网络的性能得到显著的提高。不同的 VLAN 之间的数据传输是通过第三层（网络层）的路由来实现的，因此使用 VLAN 技术，结合数据链路层和网络层的交换设备可搭建安全可靠的网络。网络管理员通过控制交换机的每一个端口来控制网络用户对网络资源的访问，同时 VLAN 和第三层第四层的交换结合使用能够为网络提供较好的安全措施。

另外，VLAN 具有灵活性和可扩张性等特点，方便于网络维护和管理，这两个特点正是现代局域网设计必须实现的两个基本目标，在局域网中有效利用虚拟局域网技术能够提高网络运行效率.

（2）VLAN 的优点

--增加了网络的连接灵活性：

--控制网络上的安全

--增加网络的安全性

（3）**VLAN 的分类**

基于端口的 VLAN:

基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员

只需要管理和配置交换端口，而不管交换端口连接什么设备。

基于 MAC 地址的 VLAN:

由于只有网卡才分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划属于某个 VLAN。

事实上，该 VLAN 是一些 MAC 地址的集合。当设备移动时，

VLAN 能够自动识别。网络管理需要管理和配置设备的 MAC 地址，显然当网络规模很大，设备很多时，会给管理带来难度。

基于第 3 层的 VLAN:

基于第 3 层的 VLAN 是采用在路由器中常用的方法：IP 子网和 IPX 网络号等。其中，局域网交换机允许一个子网

扩展到多个局域网交换端口，甚至允许一个端口对应于多个子网。

基于策略的 VLAN:

基于策略的 VLAN 是一种比较灵活有效的 VLAN 划分方法。该方法的核心是采用什么样的策略？目前，常用的策略

有（与厂商设备的支持有关）：按 MAC 地址，按 IP 地址，按以太网协议类型，按网络的应用等

（4）VLAN 的应用

4、逻辑隔离

逻辑隔离主要通过逻辑隔离器实现，逻辑隔离器是一种不同网络间的隔离部件，被隔离的两端仍然存在物理上数据通道连线，但通过技术手段保证被隔离的两端没有数据通道，即逻辑上隔离。一般使用协议转换、数据格式剥离和数据流控制的方法，在两个逻辑隔离区域中传输数据。并且传输的方向是可控状态下的单向，不能在两个网络之间直接进行数据交换。

5、物理隔离

物理隔离包含四个方面内容：VIGAP 隔离网闸技术

、水线

、物理隔离

、

物理隔离卡

。

1、ViGap 隔离网闸，它创建一个这样的环境，内、外网物理断开，但逻辑地相连。对于有连接的 PC，黑客可以使用各种方法，通过网络连接来对它进行控制，然而物理隔断却能杜绝这种情况发生。ViGap 就是在这两个网络之间创建了一个物理隔断，这意味着网络数据包不能从一个网络流向另外一个网络，并且可信网络上的计算机和不可信网络上的计算机从不会有实际的连接。

2、所谓“物理隔离”是指内部网不得直接或间接地连接公共网。物理安全的目的是保护路由器、工作站、各种网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击。

3、在每台电脑中通过主板插槽安装物理隔离卡，把一台普通计算机分成两台虚拟计算机，实现真正的物理隔离。

4、在单相电源系统中，水线的功能为传导回馈的电流，与插座端与接地分配在同一个区域。而在台湾地区，只有水线与火线之分。

也就是说，只有使内部网和公共网物理隔离，才能真正保证内部信息网络不受来自互联网的黑客攻击。此外，物理隔离也为内部网划定了明确的安全边界，使得网络的可控性增强，便于内部管理。

第 4 章网络安全 4.9 公钥基础结构（P696-715）

1、公钥密码

（1）公钥密码的思想

公钥算法是基于数学函数而不是基于替换和置换。公钥密码学是非对称的，它依赖于一个公开密钥和一个在数学 上相关但不相同的私钥，且仅根据密码算法和公开密钥来确定私钥在计算上是不可行的。公开钥用于加密和签名认证，私钥则对应地用于解密和签名。

（2）公钥加密算法

被广泛接受的公钥密码系统主要是大整数因子分解 IFP 困难性的 RSA 系统和基于椭圆曲线离散对数 ECDLP 的计算困难性的 ECC 系统。

（3）数字签名算法

数字签名是利用一套规则和一个参数集对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性，这里的数据计算通常是密码变换。

普通数字签名算法有：RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。

特殊数字签名有：盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名和具有消息恢复功能签名等，它与具体应用环境密切相关。

2、PKI 组成

PKI（Public Key Infrastructure ）

即"公钥基础设施"，是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。

PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

PKI 的基本组成:

完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口（API）等基本构成部分，构建 PKI 也将围绕着这五大系统来着手构建。

3、证书认证机构

CA(Certificate Authority)是数字证书认证中心的简称，是指发放、管理、废除数字证书的机构。CA 的作用是检查证书持有者身份的合法性，并签发证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。

数字证书实际上是存于计算机上的一个记录，是由 CA 签发的一个声明，证明证书主体（"证书申请者"拥有了证书后即成为"证书主体"）与证书中所包含的公钥的惟一对应关系。证书包括证书申请者的名称及相关信息、申请者的公钥、签发证书的 CA 的数字签名及证书的有效期等内容。数字证书的作用是使网上交易的双方互相验证身份，保证电子商务的安全进行。

解

释：受委托发放数字证书的第三方组织或公司。数字证书是用来建立数字签名和公-私(public-private)密钥对的。CA 在这个过程中所起的作用就是保证获得这一独特证书的人就是被授权者本人。在数据安全和电子商务中，CA 是一个非常重要的组成部分，因为它们确保信息交换各方的身份。

CA 的层级结构：

CA 建立自上而下的信任链，下级 CA 信任上级 CA，下级 CA 由上级 CA 颁发证书并认证。

CA 提供的服务：

颁发证书、废除证书、更新证书、验证证书、管理密钥。

CA 大概分以下几种：

1、行业性 CA

金融 CA 体系、电信 CA 体系、邮政 CA 体系、外经贸部 CA、

中国海关 CA、中国银行 CA、中国工商银行 CA、中国建设

银行 CA、招商银行 CA、国家计委电子政务 CA、南海自然

人 CA（NPCA）

2、区域性 CA

协卡认证体系（上海 CA、北京 CA、天津 CA）

网证通体系（广东 CA、海南 CA、湖北 CA、重庆 CA）

3、独立的 CA 认证中心

- 山西 CA、吉林 CA、宁夏西部 CA、陕西 CA、福建 CA、黑龙

江邮政 CA、黑龙江政府 CA、山东 CA、深圳 CA 、吉林省政

府 CA、福建泉州市商业银行网上银行 CA、天威诚信 CA

4、PKI 和数字证书的应用

（1）应用实例

虚拟专用网络、安全电子邮件、Web 安全

（2）PKI 的应用编程接口

目前比较常用的安全 API 接口有 CryptoAPI 和 CDSA。

5、PKI 标准

在 PKI 技术框架中，许多方面都经过严格的定义，如用户的注册流程、数字证书的格式、CRL 的格式、证书的申请格式以及数字签名格式等。

国际电信联盟 ITU X.509 协议，是 PKI 技术体系中应用最为广泛、也是最为基础的一个国际标准。它的主要目的在于定义一个规范的数字证书的格式，以便为基于 X.500 协议的目录服务提供一种强认证手段。但该标准并非要定义一个完整的、可互操作的 PKI 认证体系。

PKCS 是由美国 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。到 1999 年底，PKCS 已经公布了以下标准：

- PKCS#1：定义 RSA 公开密钥算法加密和签名机制，主要用于组织 PKCS#7 中所描述的数字签名和数字信封。
- PKCS#3：定义 Diffie-Hellman 密钥交换协议。

- PKCS#5：描述一种利用从口令派生出来的安全密钥加密字符串的方法。使用 MD2 或 MD5 从口令中派生密钥，并采用 DES-CBC 模式加密。主要用于加密从一个计算机传送到另一个计算机的私人密钥，不能用于加密消息。
- PKCS#6：描述了公钥证书的标准语法，主要描述 X.509 证书的扩展格式。
- PKCS#7：定义一种通用的消息语法，包括数字签名和加密等用于增强的加密机制，PKCS#7 与 PEM 兼容，所以不需其他密码操作，就可以将加密的消息转换成 PEM 消息。
- PKCS#8：描述私有密钥信息格式，该信息包括公开密钥算法的私有密钥以及可选的属性集等。
- PKCS#9：定义一些用于 PKCS#6 证书扩展、PKCS#7 数字签名和 PKCS#8 私钥加密信息的属性类型。
- PKCS#10：描述证书请求语法。
- PKCS#11：称为 Cyptoki，定义了一套独立于技术的程序设计接口，用于智能卡和 PCMCIA 卡之类的加密设备。
- PKCS#12：描述个人信息交换语法标准。描述了将用户公钥、私钥、证书和其他相关信息打包的语法。
- PKCS#13：椭圆曲线密码体制标准。
- PKCS#14：伪随机数生成标准。
- PKCS#15：密码令牌信息格式标准。

另外，PKCS#2 和 PKCS#4 已经合并到 PKCS#1 之中。PKIX 是由 IETF 组织中的 PKI 工作小组制定的系列国际标准。此类标准主要定义基于 X.509 和 PKCS 的 PKI 模型框架。PKIX 中定义的四个主要模型为用户、认证中心 CA、注册中心 RA 和证书存取库。