三级网络技术 2014 版考点汇总

1、（1）、HFC 的基本结构：

电视头端（接受各种信源的电视频道）、长距离干线（高质量的同轴电缆）、放大器、馈线与下引线（普通的 CATV 同轴电缆）组成。

传统有线电视网络重的放大器是单向地从头端传输到用户的模拟信号。经双向传输改造，双向传输服务成为可能。

光纤结点通过同轴电缆下引线可以为 500-2000 个用户服务。

HFC 改善了信号质量，提高了传输的可靠性，线路可以使用的带宽甚至高达 1GHz

电话拨号上网的速率一般是 36.6-56.6kbps；本地电话公司提供的 ISDN 的速率是 128Kbps；使用 ADSL 专线上网的速率是 1.8Mbps,传输距离不超过 5km，使用 Cable Modem，通过有线电视宽带接入 Internet 的，数据传输速率可达 10-36Mbps

有线电视网络主要的优点是频带宽、速度快，主要的缺点是存在回传信道干扰，多用户对有限带宽的争用影响接入速率、建设和双向改造的造价高。

（2）、电缆调制解调器 Cable Modem 的分类：

电缆调制解调器 Cable Modem 是一种专门利用有线电视网络进行数据传输设计的，它把计算机与有线电视同轴电缆连接起来，利用频分复用的方法将双向信道分为上行信道（带宽为 200Kbps-10M）和下行信道(带宽最高可达 36Mbps)。

分类：从传输方式上分为双向对称式和非对称式，对称式速率为 2-4Mbps，最高为 10Mbps,非对称式速率为下行 30Mbps，上行为 300kbps-2.56Mbps.

从数据传输方向上可以分为双向和单向。

从同步方式上可以分为同步和异步交换两类。同步类似于 Ethernet 网，异步交换类似于 ATM 技术。

从接入的角度可以分为个人 Cable Modem 和宽带多用户 Cable Modem（具有网桥功能，可以将一个计算机局域网接入）。

从接口的角度分为外置式（缺：通过网卡连接计算机）、内置式和交互式机顶盒三种。

2.

802.11 定义了使用红外、调频扩频、直接序列扩频技术，传输速率为 1 或 2Mbps 的无线局域网标准。

802.11b 定义了使用直序扩频技术，传输速率为 1Mbps、2Mbps、5.5Mbps、11Mbps 的无线局域网标准。

802.11a 将传输速率提高到了 54Mbps.

802.11 定义了物理层和媒体访问控制 MAC 协议的规范

802.11 定义了两种类型的设备：无线结点（由一台接入设备上加一块无线接口卡构成）和无线接入点（作用是提供无线和有线网络之间的桥接，由一个无线输出口和一个有线的网络接口（802.3 接口）构成，桥接软件符合 802.1d 协议）。

802.11 最初定义的三个物理层包含了两个扩频技术和一个红外传播规范，无线传输的频率定义在 2.4G 的 ISM 波段内，这个频段属于非注册使用频段。扩频技术保证了 802.11 的设备在这个频段上的可用性和高可靠性的吞吐量，可以保证同其他使用同一频段的设备相互不影响。

802.11 标准定义的传输速率为 1Mbps和 2Mbps，可以使用 FHSS(调频扩频和)DSSS（直

序扩频）技术，两者在运行机制上完全不同，使用这两种技术的设备没有互操作性。

802.11 无线局域网协议中，冲突检测存在“Near/Far”（检测冲突）现象，所以采用了新的协议 CSMA/CA 或者 DCF(分布式协调功能)，利用 ACK 信号来避免冲突。（只有当客户端受到网络上返回的 ACK 信号以后才能确认发送的数据已经正确的到达目的）。

另外一个 MAC 层的问题是“hidden node”问题，为此 802.11 引入了一个 Send/Clear to send(RTS/CTS)选项。

在 802.11 协议中，每一个在无线网络中传输的数据报都被附加上了校验位以保证他在传输中不会出现错误。802.11 还具有分片的功能。

802.11b 运作模式分为点对点模式（最多可连接 256 台主机）和基本模式（无线网络扩充和有线网络并存时，插上无线网卡的 PC 通过接入点与另一台 PC 相连，一个接入点最多可连接 1024 台 PC）。

802.11b 的典型解决方案：对等解决方案、单接入点解决方案（接入点相当于有线网络中的集线器，无线接入点可以连接周边的无线网络终端，形成星形网络结构，同时通过 10base-t 端口与有线网络相连，所有无线终端都能访问有线网络的资源，并可通过路由器访问 Internet）、多接入点解决方案(网络规模较大，超过了单个接入点的覆盖范围，就得采用多个接入点)、无线中继解决方案、无线冗余解决方案（两个接入点放在同一位置）、多蜂窝漫游工作方式。

3）. 宽带城域网保证服务质量要求的技术主要有：资源预留 RSVP、区分服务 DiffServ 与多协议标记交换 MPLS.

服务质量主要体现在延时、抖动、吞吐量和包丢失率。

管理和运营宽带城域网的关键技术主要有：带宽管理、网络管理、用户管理、服务质量 QOS、统计与计费、IP 地址的分配与地址转换、网络安全。

宽带城域网在组建方案中，一定要按照电信运营级的要求，考虑设备冗余、线路冗余、路由冗余、系统故障的快速诊断和自动修复。同时宽带城域网必须充分的考虑网络攻击的问题。

4） 弹性分组环 RPR 是直接在光纤上高效传输 IP 分组的传输技术。其标准是 802.17

环形结构是目前城域网的主要拓扑构型

弹性分组环 RPR 采用双环结构，这一点与 FDDI 结构相同。两个 RPR 结点之间裸光纤间的距离可达 100km，其中顺时针传输的光纤叫外环，逆时针传输的光纤叫内环。内环和外环都可以采用统计复用的方法传输 IP 分组，同时可以实现“自愈环”的功能。内环和外环都可以传输数据分组和控制分组。每一个结点都可以使用两个方向的光纤与相邻结点通信。

RPR 技术主要的特点：带宽利用率高、公平性好（每一个结点都执行 SRP 公平算法、加权公平法则和入口、出口速率限制）、快速保护和恢复能力强（50ms 可以隔离出故障的结点和光线段）、保证服务质量（优先级）。

5）路由器背板交换能力大于 40G 的称为高端路由器，低于 40G 的称为中低端路由器。

高端路由器一般用作核心层的主干路由器，企业级路由器一般用作汇聚层的路由器，低端路由器一般用作接入层的接入路由器。

路由器的关键技术指标：

吞吐量：指路由器的包转发能力。设计两个方面的内容:端口吞吐量和整机吞吐量。路由器的包转发能力与路由器端口数量、端口速率、包长度和包类型有关。

背板能力：高性能路由器一般采用是交换式结构。背板能力决定了路由器的吞吐量。

丢包率：通常是衡量路由器超负荷工作时的性能指标之一。

延时与延时抖动：与包长度和链路传输速率有关，高速路由器要求长度为 1518B 的 IP 包，延时小于 1ms.延时抖动是指延时的变化量。

突发处理能力：以最小帧间隔发送数据包而不引起丢失的最大发送速率来衡量。

路由表容量：Internet 要求执行 BGP 协议的路由表一般要储存数十万条路由表项。高速路由器必须满足存储 25 万个 BGP 对等实体地址和 50 万个 IGP 邻居的网络地址。

服务质量：主要体现在队列管理机制、端口硬件队列管理、支持 QoS 协议。

网管能力：

可靠性与可用性：路由器的冗余是为了保证设备的可靠性和可用性。主要体现在设备冗余、热拔插组件、内部时钟精度、无故障工作时间。路由器的冗余主要体现在接口冗余、电源冗余、时钟板冗余、系统板冗余、整机设备冗余。

典型的高端路由器的可靠性与可用性指标应该达到：

1. 无故障工作时间大于 10 万个小时。
2. 系统故障恢复时间要小于 30 分钟。
3. 系统具有自动保护和切换功能，主备用切换时间小于 50 毫秒。
4. SDH 和 ATM 接口自动保护功能，切换时间小于 50 毫秒。
5. 主处理器、主存储器、交换矩阵、电源、总线管理器与网络管理接口等主要设备需要有热拔插冗余备份，显卡要求有备份，并提供远程测试诊断能力。
6. 系统内部不存在单故障点。

6） $(24\times100+4\times1000)\times2=12800$

交换机的主要技术指标：

★ 1. 背板能力：

2. 全双工端口带宽:端口×数端口速率×2
3. 帧转发速率：每秒钟能够转发的帧的最大数量
4. 机箱式交换机的扩张能力
5. 支持 VLAN 能力：

7.服务器的性能主要表现在：

1. 运算处理能力：
2. 磁盘存储能力：表现在磁盘存储容量与 I/O 服务速度上，而决定这两个参数的因素又在于磁盘接口总线与硬盘两个方面。

★ 3. 系统高可用性：MTBF/(MTBF+MTBR)其中 MTBF 为平均无故障时间，MTBR 为平均修复时间

如果系统高可用性达到 99.9%，那么每年的停机时间≤8.8 小时；如果系统高可用性达到 99.99%，那么每年的停机时间≤53 分钟；如果系统的高可用性达到 99.999%，那么每年的停机时间≤5 分钟。

4. 可管理性：
5. 可扩展性：

8.略

★ 9.IP 地址短缺的修复方法是 NAT 网络地址转换，其设计的基本思路是为每一个公司分配一个或少量的 IP 地址，用于传输 Internet 流量。在公司内部的每一台主机分配一个不能够在 Internet 上使用的保留的专用的 IP 地址。专用 IP 地址用于内部网络的通信，如果需要访问外部 Internet 主机，必须由运行网络地址转换的主机或是路由器将内部的专用 IP 地址转换为全局的 IP 地址。

NAT 方法的局限性：

1. 违反了 IP 地址结构模型的设计原则
2. 使 IP 协议由面向无连接变成了面向连接

3. 违反了基本的网络分层结构模型的设计原则
4. 使得 P2P 应用实现出现困难
5. 同时存在对高层协议和安全性的影响问题

网络地址转换时，传输层客户进程的端口号也需要改变。NAT 可以分为“一对一”和“多对多”两类，其中一对一转换方式属于静态 NAT，多对多属于动态 NAT.

★ 10.

10.0.11.0/27	00001010 00000000 00001011	00000000
10.0.11.32/27	00001010 00000000 00001011	00100000
10.0.11.64/26	00001010 00000000 00001011	01000000
	00001010 00000000 00001011	0 ⟶ 10.0.11.0/25

最长前缀匹配法进行路由选择

11.

IPv6 的主要特征：新的协议格式、巨大的地址空间、有效的分级寻址和路由结构、地址自动配置、内置的安全机制、更好的支持 QoS 服务。

IPv6 地址长度为 128 位，可以提供 3.4×10^{38} 个 IP 地址。128 位中 64 位作为子网地址空间 64 位作为局域网 MAC 地址空间。

IPv6 可以分为单播地址、组播地址、多播地址、特殊地址。

为简化主机配置，IPv6 支持地址自动配置。

★ IPv6 地址表示方法为冒号十六进制表示法：128 位地址按每 16 位划分为一个位段，每个位段转换为一个 4 位的十六进制数，并用冒号隔开。

IPv6 中可能会出现多个二进制数 0，通过压缩某个位段中的前导 0 来简化 IPv6 地址的表示，但不可把每个位段内部的 0 也压缩掉。每个位段至少有一个数字。

如果连续几个位段的值都为 0，那么这些 0 可以简写为“::”，称为双冒号表示法。且在一个 IPv6 地址中双冒号表示法只能出现一次。确定::之间代表了压缩了多少位 0 可以数一下地址还有多少个位段，然后用 8 减去这个数，再将结果乘以 16.

IPv6 不支持子网掩码，只支持前缀长度表示法。

12. 外部网关协议 BGP 是不同自治系统的路由器之间交换路由信息的协议。

BGP-4 采用了路由向量路由协议，在配置 BGP 时，每个自治系统的管理员要选择至一个路由器作为自治系统的“BGP 发言人”，一系统的 BGP 发言人要与另一个系统的 BGP 发言人要交换路由就要先建立 TCP 连接，然后再此连接上交换 BGP 报文以此建立 BGP 会话。每个 BGP 发言人除了运行 BGP 协议外还必须运行该自治系统所使用的内部网关协议。

BGP 协议交换路由信息的结点数是以自治系统数为单位的。

在 BGP 刚刚运行时，BGP 边界路由器与相邻的 BGP 边界路由器交换整个 BGP 路由表，但只要发生变化时只更新变化的部分。

BGP 路由选择协议的四种分组：打开 open、更新 update、保活 keepalive、通知 notification。

撤销路由可以以此撤销很多条，而增加新路由时，每个更新报文只能增加一条。

13. 路由表的建立：当路由表刚启动时，对其（V,D）路由表进行初始化。初始化的路由器只包含与该路由器直接相连的网络的路由。初始（V,D）路由表中各路由的距离都为 0.

★ 路由表信息的更新：在路由表建立之后，各路由器周期性地向外广播其（V,D）路由表的内容。Router1 接受到 Router2 发送的（V,D）报文，按照如下的规则更新路由表：Router1 中没有这一项，Router 在路由器中增加这一项，由于要经过 Router2 转发，距离 D 要加 1。如果 Router1 中距离 1 比 Router2 中该项距离值加 1 还要大，则要修改该表项，其距离值应

该是 Router2 中距离值加 1.

路由信息协议要求路由器周期性地向外发送路由刷新报文。路由刷新报文主要内容是由若干个（V,D）构成。（V,D）表中 V 代表矢量（Vector）,标识该路由器可以达到的目的网络或目的主机；D 代表距离（distance），指出该路由器到达目的网络或目的主机的距离。距离 D 对应该路由器上的跳数（hop count）。其他路由器在接收到某个路由器的（V,D）报文后，按照最短路径原则对各自的路由表进行刷新。

★ 14. 与 RIP 相比较，OSPF 具有以下特点：

OSPF 使用的是分布式链路状态协议而 RIP 使用的是距离向量协议。

OSPF 协议要求路由器发送的信息是本路由器和哪些路由器相邻，以及链路状态的度量（费用、距离、延时、带宽）。

OSPF 要求当链路状态发生变化是使用**洪泛法**向所有路由器发送信息，而 RIP 协议相邻的几个路由器发送信息。

所有的路由器都最终能建立一个链路状态数据库，这个数据库实际上就是全网的拓扑结构图，且在全网范围内保持一致。RIP 虽然知道到所有网络的距离和下一跳路由器，但不知道全网的拓扑结构。

为了适应规模很大的网络，是其更新过程收敛速度更快，OSPF 协议将一个自治区域划分为若干个更小的范围，叫做区域。每个区域有一个 **32 位**的区域标识符（点分十进制），在一个区域内的路由器的个数不超过 200 个。划分区域的好处是将利用洪泛法将链路状态信息的范围局限在每一个区域内而不是整个自治系统。因此每一个区域内部的路由器只知道该区域内的完整拓扑结构而不知道其他区域的网络拓扑结构。

为了使每一个区域都和其他区域进行通信，OSPF 协议使用层次结构的区域划分。它将一个自治系统内部分成主干区域和若干区域。主干区域的路由器称为主干路由器，连接各个区域的路由器叫做区域边界路由器。在主干区域内还要有一个路由器专门和该自治系统之外的其他自治系统交换路由信息，这样的路由器叫做自治系统边界路由器。

OSPF 协议执行过程中路由器的初始化过程中 OSPF 让每一个路由器用数据库描述分组和相邻路由器交换本数据库中已有的链路状态摘要信息。在网络运行过程中由于一个路由器的链路状态只涉及相邻路由器的状态信息，因而与整个 Internet 的规模无关。

15. 交换机的分类：

交换机按多支持的局域网标准可以分为以太网交换机、FDDI 交换机、ATM 交换机、令牌环交换机。根据交换机所支持的传输速率和介质标准，以太网交换机可以分为快速以太网交换机（100Mbps）、千兆以太网交换机(1G bps)、万兆以太网交换机(10 Gbps)。

按交换机的架构可以分为单台交换机、堆叠交换机、箱体模块化交换机。

按交换机工作在 OSI 参考模型的层次分类：工作在数据链路层的二层交换机（没有路由功能）、工作在网络层的三层交换机，工作在传输层的四层交换机和多层交换机。

16. 综合布线系统常用的传输介质有双绞线和光缆。双绞线扭绞的目的是使对外的电磁辐射和遭受外界的电磁干扰减少到最小。UTP 是非屏蔽双绞线，STP 具有屏蔽作用。

连接硬件包括主件的连接器（适配器），成对连接器及接插软线，但不包括某些应用系统对综合布线系统用的连接硬件，也不包括有源或无源电子线路的中间转接器或其他器件。

综合布线采用的主要的连接部件分为建筑群配线架 CD、大楼主配线架 BD、楼层配线架 FD、转接点 TP、通信引出端 TO。FD 和 TP 之间的水平线缆的最大长度不要超过 90 米。

信息插座大致可以分为嵌入式安装插座（双绞线）、表面安装插座、多介质信息插座（铜缆和光纤）。

17. BPDU 数据包又两种类型，一种是包含配置信息的配置 BPDU（不超过 35 个字节），另一种是包含拓扑变化信息的拓扑变化通知 BPDU（不超过 4 个字节）。配置 BPDU 中包含

的 Bridge ID 是选取根网桥和根交换机的主要依据。Bridge ID 最小的为根网桥或根交换机。Bridge ID 与 Root ID 相同，他们都用 8 个字节表示，Bridge ID 有两个字节的优先级和六个字节的交换机 MAC 地址组成。优先级的取值范围为 0-61440，增量是 4096，值越小，优先级越高，一般交换机的默认设置为 32768。

BPDU 携带了实现生成树协议算法的有关信息，包括 Root ID、 Root Path Cost、 Bridge ID 、Port ID 、Hello time 、Max Age 等。

18. 在交换设备之间实现 Trunk 功能，必须遵守相同的 VLAN 协议。IEEE802.1Q 可以使不同厂商的交换设备互连在一起，并提供 Trunk 功能，使网络更具开放性。

虚拟网 VLAN 是以交换式网络为基础，把网络上终端设备划分为若干个逻辑工作组，每个逻辑工作组就是一个 VLAN。它是一个独立的逻辑网络，具有单一的广播域，不受实际交换机区段的限制，也不受用户实际物理位置和物理网段的限制。逻辑组的设定是在软件中完成的。虚拟网技术提供了动态组织工作环境的功能。

VLAN 的技术特征：

工作在数据链路层。

每个 VLAN 都是一个独立的逻辑网段，一个独立的广播域。VLAN 的广播信息只发送给同一个 VLAN 的成员，不发送给其他 VLAN 的成员。

每个 VLAN 都是一个独立的逻辑网络，他们都又唯一的子网号，VLAN 之间不能直接通信，是因为必须通过第三层的路由功能，而它只工作数据链路层。

VLAN 通常用 VLAN ID(VLAN 号：由 **12 位**组成，可以支持 4096 个 VLAN,1~1005 是标准范围，1025~4096 是扩展范围，可用于以太网的是 2~1000，FDDI 和 Token Ring 的是 1002~1005）和 VLAN name(VLAN 名：32 位标识符组成，可以是字母和数字)来标识,1 是缺省 VLAN,只能使用但不能删除它。

VLAN Trunk（虚拟局域网中继技术）是交换机和交换机之间或交换机和路由器之间存在一条物理链路，而在这一条物理链路上传输多个 VLAN 信息的技术。

VLAN Trunk 的标准机制是帧标签。帧标签为每个帧指定一个唯一的 VLAN ID 作为识别码，表明该帧是属于哪个 VLAN 的。它在传送数据帧到达网络主干时，会在每个帧的表头中放置一个唯一的识别码，交换机会解析与测试识别码。当数据帧从网络主干转发至目标终端之前，交换机先除掉这个识别码。

划分 VLAN 的方法：

基于端口划分 VLAN(静态 VLAN)

基于 MAC 地址划分 VLAN（动态 VLAN）：连接到每个交换设备的 MAC 地址。需要一个保存 VLAN 管理数据库的 VALN 配置服务器。

基于第三层协议类型或地址（动态 VLAN）

VTP 是 VLAN 中继协议，也称 VLAN 干道协议。VTP 具有三种工作模式：①VTP Server（维护 VTP 域中所有 VLAN 表信息，可以建立、删除或修改 VLAN）、 ②VTP Client(维护所有 VLAN 表信息，VLAN 配置信息是从 VTP Server 中学到的，可是他不能建立、删除和修改 VLAN)、③VTP Transparent（相当于是一个独立的交换机，不从 VTP Server 学习 VLAN 的配置信息，不参与 VTP 工作，只拥有本设备上维护的 VLAN 配置信息，可以建立、删除或修改本机上的 VLAN）。

配置 vtp 域名：1.进入全局配置模式 Switch-PHY-3548#config t

Switch-PHY-3548(config)#

2.配置 vtp 域名 Switch-PHY-3548#vtp domain pku (设置 vtp 域名为 pku)

配置 vtp 工作模式：Switch-PHY-3548(config)#vtp mode server

Switch-PHY-3548(config)#vtp mode client

Switch-PHY-3548(config)#vtp mode transparent

建立和删除 VLAN：1.建立 VLAN 进入 VLAN 配置模式 Switch-PHY-3548#vlan data

Switch-PHY-3548(vlan)#

建立 VLAN Switch-PHY-3548(vlan)#vlan 1000 name vlan1000

退出并返回特权用户模式 Switch-PHY-3548(vlan)#exit

2.删除 Switch-PHY-3548(vlan)#VLAN no vlan1000

3.修改 VLAN Switch-PHY-3548(vlan)#vlan 1000 name vlan1000

为交换机端口分配 VLAN: 进入交换机端口配置模式 Switch-PHY-3548#configure t

Switch-PHY-3548(config)#int fo/24

Switch-PHY-3548(config-if)#

为端口分配 VLAN Switch-PHY-3548(config-if)#switchport access vlan248

VLAN trunk 的配置：进入交换机接口配置模式 Switch-PHY-3548# configure t

Switch-PHY-3548(config-if)#int fo/24

配置 VLAN trunk 模式 Switch-PHY-3548(config-if)#switchport mode trunk【set trunk 5/1 on dot1q】

封装 VLAN 协议 Switch-PHY-3548(config-if)#switchport trunk encapsulation dot1q

Switch-PHY-3548(config-if)#switchport trunk encapsulation isl

Switch-PHY-3548(config-if)#switchport trunk encapsulation negotiate P(自动协商)

设置允许中继的 VLAN Switch-PHY-3548(config-if)#switchport trunk allowed vlan 10,14

Switch-PHY-3548(config-if)#switchport trunk allowed vlan10-24

Switch-PHY-3548(config-if)#switchport trunk allowed vlan except 100-1000

【set trunk 5/1 vlan 37-42 在端口 5/1 的允许 VLAN 列表中添加 37~42 号 VLAN】【clear trunk 5/24 3-36 从端口 5/24 的允许 VLAN 列表中清除 3~36VLAN】

19.略

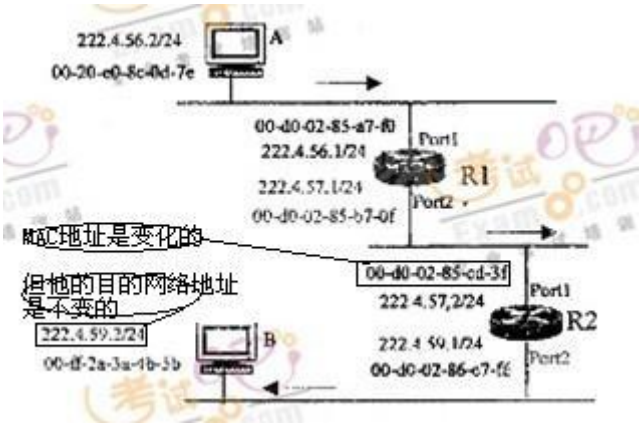
20.生成树协议 STP 是一个二层链路管理协议，他的主要功能是保证网络中没有回路的情况下，允许在二层链路中提供冗余路径，以保证网络可靠、稳定的运行。

目前最流行，应用最广泛的 STP 协议是 IEEE.1D 标准。

STP 的基本工作原理是：通过在交换机之间传递网桥协议数据单元 BPDU，并用生成树算法对其进行比较计算。

Bridge ID 有两个字节的优先级和六个字节的交换机 MAC 地址组成。优先级的取值范围为 0-61440，增量是 4096，值越小，优先级越高，一般交换机的默认设置为 32768。当优先级相同时，那么就要根据 MAC 地址决定根网桥，MAC 地址小的路由器就是根网桥。

21.



路由器的基本功能是路由选择和分组转发.

路由选择的核心是确定下一跳路由器的 IP 地址。

路由选择算法根据各自的判断准则为网络上的路由产生一个权值，权值越小路由越佳。

路由表的内容主要有目的网络地址、下一跳路由器地址和目的端口、缺省路由信息。

缺省路由又称缺省网关，它是配置在主机上的 TCP/IP 属性的一个参数。缺省网关是与主机在同一个子网的路由器的端口的 IP 地址。

在数据分组通过每一个路由器转发时，分组中的目的 MAC 地址是变化的，但它的目的网络地址是不变的。

22. 路由器的硬件构成：CPU(中央处理器)、Memory（内存）、Storage（存储器）和 Interface（接口）。

路由器的软件为互联网操作系统 IOS 组成。

CPU 负责实现路由协议、路径选择计算、交换路由信息、查找路由表、分发路由表、维护各种表格以及转发数据包。

路由器内存用于保存路由器配置、路由器操作系统、路由协议软件等。路由器内存主要有：只读内存 ROM(永久保存路由器的开机诊断程序、引导程序和操作系统软件，主要任务是完成路由器的初始化进程，具体包括路由器启动时的硬件诊断，装入路由器操作系统 IOS)、随机存储器 RAM（存储路由表、快速交换缓存、ARP 缓存、数据分组缓冲区和缓冲队列、运行配置文件，以及正在执行的代码和一些临时数据信息。）、闪存 Flash（存储当前使用的操作系统映像文件和一些微代码）、非易失随机存储器 NVRAM（存储启动配置文件和备份配置文件）

路由器接口主要有局域网接口、广域网接口和路由器配置接口。

23. IP 地址的动态分配使用动态主机配置协议 DHCP，但仍然不能解决 IP 地址的冲突问题。

DHCP 采用的是客户机/服务器（Client/Server）工作模式

DHCP 服务器主要完成两个功能：建立和管理 IP 地址池，接受并处理用户提出的 DHCP 请求。

DHCP 客户端的主要功能是提交 DHCP 请求。

DHCP 协议允许使用备份 DHCP 服务器的功能。

DHCP 客户从 DHCP 服务器申请 IP 地址的步骤是：客户机发送一个“DHCPDISCOVER”广播包给服务器，服务器用一个“DHCPOFFER”单播数据包给予应答，并提供客户机所需的 TCP/IP 的属性配置参数（IP 地址、子网掩码、缺省网关、域名和域名服务器的 IP 地址）。然后主机发送一个“DHCPREQUEST”广播包给服务器，确认与此服务器建立地址租借关系，并通告其他的 DHCP 服务器。正常情况下，服务器会恢复一个“DHCPACK”广播包给

客户机，这是一个确认相互关系的应答包。

DHCP 客户机广播“DHCP 发现”消息时使用的源 IP 地址是 0.0.0.0

路由器交换机上 DHCP IP 地址池的配置内容：IP 地址池的子网地址和子网掩码、缺省网关、域名和域名服务器的 IP 地址、IP 地址的租用时间和取消地址池冲突记录日志等参数。

在全局配置模式下，配置 IP 地址池的名称，并进入 DHCP Pool 配置模式。

Router(config)#ip dhcp pool ttt

Router(dhcp-config)#

Router(config)#ip dhcp pool 234

Router(dhcp-config)#

在 DHCP Pool 配置模式下配置子网地址和子网掩码的方法是：

network <网络地址> <子网掩码>

Router(dhcp-config)#network 201.23.98.0 255.255.255.0

Router(dhcp-config)#

Router(dhcp-config)#network 201.23.98.0/24

Router(dhcp-config)#

配置不用于动态分配的 IP 地址是 在全局配置模式下

Router(config)#ip dhcp excluded-address 201.23.96.2 201.23.96.10（排除从 201.23.96.2 到 201.23.96.10 的一段 IP 地址）

Router(config)#

Router(config)#ip dhcp excluded-address 201.23.96.211(排除单个 IP 地址)

Router(config)#

配置 IP 地址池的缺省网关：在 DHCP Pool 配置模式下

Router(dhcp-config)# default-router 201.23.98.1 命令中的网关地址最多允许配置 8 个。

Router(dhcp-config)#

配置 IP 地址池的域名：在 DHCP Pool 配置模式下

Router(dhcp-config)#domain-name pku.edu.cn

Router(dhcp-config)#

配置 IP 地址池的域名服务器的 IP 地址：在 DHCP Pool 配置模式下

Router(dhcp-config)#dns-server address 212.105.129.27 212.105.129.26 【第一个是主域名服务器的 IP 地址，后面的一个是辅助域名服务器域名的 IP 地址】

Router(dhcp-config)#

配置 IP 地址池的租用时间：设置租用时间为 5 个小时 在 DHCP Pool 配置模式下

Router(dhcp-config)#lease 0 5 【可以以日、时、分、秒为单位 也可以设置为无限时间 infinite】

Router(dhcp-config)#

取消地址冲突记录日志：在全局配置模式下 Router(config)#no ip dhcp conflict logging

24. 访问控制列表主要有两种类型，一种是标准访问控制列表，另一种是扩展访问控制列表。标准访问控制列表只能检查数据包的源地址。标准访问控制列表的表号范围是 1~99，后来扩展到 1300~1999.扩展访问控制列表可以检查数据包的源地址和目的地址，还可以检查制定的协议、端口号。扩展访问控制列表的表号为 100~199，后来扩展到 2000~2699。

在配置访问控制列表时，“access-list”只能使用表号标识列表，而“ip access-list”既可以使用表号，也可以使用名字标识一个访问控制列表。在配置了访问控制列表之后，还必须

配置其相应的接口才能控制数据流的流入或流出。

在配置过滤准则时，要特别注意 ACL 的语句顺序。

在配置访问控制列表的源地址和目的地址时，在允许和拒绝的 IP 地址后面，有一个参数是 wildcard-mask-通配符（或通配符掩码）的意思，为 32 位二进制表示，实际上是掩码的反码。通配符作用是指出访问控制列表过滤的 IP 地址范围。通配符为 0 表示检查相应的某位，通配符为 1 表示忽略，不检查相应的某位。

配置访问控制列表的具体步骤是：首先是定义一个标准的或是扩展的访问控制列表，然后为访问控制列表配置过滤准则，最后在配置访问控制列表的应用接口。

配置标准访问控制列表：在全局配置模式下：

Router(config)#access-list 10 permit 211.105.130.0 0.0.0.255

Router(config)#

配置应用接口：Router(config)#line vty 0 5

Router(config-line)#access-class 10 in

access-class 是控制路由器发起的 telnet 会话，不进行包过滤

access-group 是控制接口上进出的数据包流量

用 access-class 将访问控制列表施加于 VTY 线路，或 WEB 接口，access-group 则施加到接口

用在不同的接口啊，在控制台口与 VTY 口用 ACCESS-CLASS，别的一般用 IP ACCESS-GROUP

限制别人 telnet 你的时候用 access-class

line vty 0 4 是什么意思？（主要解释一下 0 4）

0-4 指的是虚拟终端的五条虚拟线路，通过 TELNET 可以连接

查看访问控制列表的配置信息：在特权用户模式下：Router#show configuration

查看访问控制列表：在特权用户模式下：Router#sh access-lists

只允许源地址为 182.105.130.111 和 222.112.7.56 的两台主机登录路由器

在全局配置模式下：Router(config)#access-list 20 permit 182.105.130.111

Router(config)#access-list 20 permit 222.112.7.56

Router(config)#access-list 20 deny any

配置应用接口：Router(config)#line vty 0 5

Router(config-line)#access-class 20 in

禁止地址为非法地址的数据包进入路由器或从路由器输出

在全局配置模式下：Router(config)#access-list 30 deny 10.0.0.0 0.255.255.255 log

Router(config)#access-list 30 deny 192.168.0.0 0.0.255.255

Router(config)#access-list 30 deny 127.0.0.0 0.255.255.255

Router(config)#access-list 30 deny 172.16.0.0 0.15.255.255

Router(config)#access-list 30 permit any

配置应用接口：Router(config)#interface g0/1

Router(config-if)#ip access-group 30 in

配置扩展访问控制列表：

拒绝转发所有 IP 地址进出的，端口号为 1434 的 UDP 协议数据包

在全局配置模式下：Router(config)#access-list 30 deny udp any any eq 1434

Router(config)#access-list 30 permit ip any any

Router(config)#

扩展访问控制列表实现	Router(config)#ip access-list extended 130 (进入扩展访问控制列表) Router(config-ext-nacl)#deny udp any any eq1434 Router(config-ext-nacl)#permit ip any any Router(config-ext-nacl)#

配置应用接口： Router(config)# interface g0/1
Router(config-if)#ip access-group 130 in
Router(config-if)#ip access-group 130 out
Router(config-if)#

封禁某一台主机

在全局配置模式下：Router(config)#access-list 110 deny ip host 202.112.60.230 any log
Router(config)#access-list110 deny ip any host 202.112.60.230 log
Router(config)#access-list 110 permit ip any any

配置应用接口：Router(config)#interface g0/1
Router(config-if)#ip access-group 110 in
Router(config-if)#ip access-group 110 out

封禁 ICMP 协议，只允许 162.105.141.0/24 和 202.38.97.0/24 子网的 ICMP 数据包通过路由器。 在全局配置模式下：

Router(config)#access-list 198 permit icmp 162.105.141.0 0.0.0.255 any
Router(config)# access-list 198 permit icmp 202.38.97.0 0.0.0.255 any
Router(config)#access-list 198 deny icmp any any
Router(config)#access-list 198 peimit ip any any 【是 peimit ip 还是 peimit icmp】
Router(config)#

配置应用接口： Router(config)#interface g0/1
Router(config-if)#ip access-group 198 in
Router(config-if)#ip access-group 198 out

用名字标识符访问控制列表的配置方法：

禁止源地址为非法地址的数据包进入路由器或从路由器输出

在全局配置模式下：

Router(config)#ip access-list standard test
Router(config-std-nacl)#deny 10.0.0.0 0.255.255.255 log
Router(config-std-nacl)#deny 192.168.0.0 0.0.255.255
Router(config-std-nacl)#deny 127.0.0.0 0.255.255.255
Router(config-std-nacl)#deny 172.16.0.0 0.15.255.255
Router(config-std-nacl)#permit any【是不是应该是 permit ip any any】

配置应用接口：Router(config)#interface g0/1
Router(config-if)#ip access-group test in
Router(config-if)#ip access-group test out

禁止端口号为 1434 的 UTP 数据包和端口号为 444 的 TCP 数据包

在全局配置模式下：

Router(config)#ip access-list extended block1434

```
Router(config-ext-nacl)#deny utp any any eq 1434
Router(config-ext-nacl)#deny tcp any any eq 444
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#
```

25. 在一个大楼中或是很大的平面里面部署布线无线网络时，可以布置多个接入点构成一套微蜂窝系统。微蜂窝系统允许用户在不同的接入点覆盖区域内任意漫游。随着位置的变化，信号会由一个接入点自动切换到另一个接入点。整个漫游过程对用户是透明的，虽然提供服务的接入点发生了变化，但对用户的服务是不会中断的。

26. 802.11b 运作模式分为点对点模式（最多可连接 256 台主机）和基本模式（无线网络扩充和有线网络并存时，插上无线网卡的 PC 通过接入点与另一台 PC 相连，一个接入点最多可连接 1024 台 PC）。

无线局域网主要包含如下的硬件设备：无线网卡、无线接入点 AP（一个 AP 可以连接 30 台左右的无线网络终端或者是其他的无线 AP）、天线、以及无线网桥、无线路由器和无线网关。

Cisco 公司的 Aironet 1100 系列接入点兼容 IEEE 802.11b 和 IEEE 802.11g，工作在 2.4GHz 频段，使用 Cisco 公司的 IOS 操作系统。

在安装和配置无线接入点之前，先向网络管理员询问一下信息，用于配置无线接入点：

系统名

无线网络中对大小写敏感的服务集标识符

如果没有连接到 DHCP 服务器，则需要为接入点指定一个 IP 地址

如果接入点与 PC 不在同一个子网内，则需要子网掩码和默认网关

简单网络管理协议集合名称以及 SNMP 团体属性（如果使用 SNMP）

将无线接入点连接至网络的两种方法：使用线内供电连接以太网和使用本地电源连接以太网。

第一次配置无线接入点，一般采用本地配置方式。默认的 IP 地址是 10.0.0.1，并成为小型的 DHCP 服务器。可以为下列设备分配多达 20 个的 10.0.0.x 范围的 IP 地址。

连接在接入以太网端口上的 PC 机

没有配置 SSID 或配置 SSID 为 tsunami,并且关闭所有安全配置的无线设备

按照下列步骤本地连接无线接入点：

1. 使用五类以太网电缆连接 PC 机和无线接入点，通过无线接入点的以太网端口进行配置，或将 PC 机置于无线接入点的电波覆盖范围内，安装无线客户端适配器，关闭所有安全设置，将 SSID 配置为 tsunmami 或不配置。

2. 给无线接入点加电

3.确认 PC 机获得了 10.0.0.x 网段的地址

4.打开互联网浏览器

5.在浏览器的地址栏输入无线接入点的 IP 地址 10.0.0.1，然后回车，出现输入网络密码对话框

6.按 Tab 键越过用户名到密码字段

7.输入大小写敏感的密码 Cisco,确定。出现接入点汇总状态的页面。点击“Express Setup”进入快捷配置页面。

8.输入各配置数据

9.保存

SSID 是客户端设备用来访问接入点的唯一标识。

27.略

28. DNS 服务器配置的主要参数：

正向查找区域：将域名映射到 IP 地址的数据库，用于将域名解析为 IP 地址。

反向查找区域：将 IP 地址映射到域名的数据库，用于将 IP 解析为域名。将主机资源记录手动添加到正向查找区域时，使用“更新相关的指针 PTR”选项，可以将指针记录自动添加到反向查找区域中。

资源记录：区域中的一组结构化的记录。常用的记录包括：主机地址（A）资源记录，它将 DNS 域名映射到 IP 地址；邮件交换器资源记录(MX)，为邮件交换器主机提供邮件路由；别名资源记录(CNAME)，将别名映射到标准 DNS 域名。

转发器：也是一个 DNS 服务器，是本地 DNS 服务器用于将外部 DNS 名称的 DNS 查询转发给该 DNS 服务器。

在缺省情况下，Windows 2003 服务器没有安装 DNS 服务器。

DNS 服务器的基本配置包括正向查找区域、反向查找区域、增加资源记录等。

在安装 DNS 服务时，13 个根 DNS 服务器被自动加入到系统中。

主机资源记录的生存默认值是 3600 秒

可以对 DNS 服务器进行简单查询测试和递归查询测试。

使用命令行程序测试 DNS 服务器：开始---运行---cmd---nslookup

29. 在使用 DHCP 时，网络上至少有一台 Windows 2003 服务器上安装并配置了 DHCP 服务，网络上要使用 DHCP 服务的主机必须设置成使用 DHCP 自动获得 IP 地址。

作用域是指接受 DHCP 服务的网络上的单个物理子网。

客户机的地址租约默认是 8 天，续订由客户端自动完成。

作用域激活后，DHCP 服务器才可以为客户机分配 IP 地址。

DHCP 服务器为一客户机分配固定 IP 地址时，需要执行的操作是新建保留。

释放地址租约：ipconfig/release

重新获取地址租约：ipconfig/renew

DHCP 服务器中常用的配置作用域选项有路由器选项和 DNS 服务器选项。

30. 浏览器与服务器之间传送信息的协议是 HTTP，即超文件传输协议，用于传输网页等内容，使用 TCP 协议，默认端口号是 80.

在 Windows2003 中只要添加操作系统的集成组建 IIS 就可以实现 WEB 服务。

一个网站对应服务器上的一个目录，建立 WEB 站点时必须为每个站点指定一个主目录，当然也可以是默认的子目录。

设置网站选项中可以设置网站的标识、站点的连接限制以及启用日志记录并配置站点的日志记录格式。

若 Web 站点未设置默认内容文档，访问站点时必须提供首页内容文件名

设置目录安全选项卡可以选择配置下列三种方法：身份认证和访问控制、IP 地址和域名限制、安全通信。

设置性能选项卡可以设置影响带宽使用的属性，以及客户端 WEB 连接的数量。

IIS 自动将带宽限制设置成最小值 1024byte/s.

设置筛选器选项：ISAPI 筛选器是在处理 HTTP 请求选项中响应事件的程序。可以列出每个筛选器的状态（可以启用或是禁用）、名称，以及加载到内存中的优先级。

设置 HTTP 头选项：可以在 HTML 页的标题中设置返回浏览器的值，还可以设置内容分级及定义 MIME 类型(MIME 类型就是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。)。

设置自定义错误选项：可以使用 IIS 提供的一般默认 HTTP1.1 错误或详细的自定义错误文件，或是创建自己的自定义错误文件。这些值可以对所有站点进行全局设置，也可以在每个站点中单独设置，IIS 对于这些设置使用继承模式。

IIS 6.0 可以使用虚拟服务器的方法在一台服务器上构建多个网站，各网站可以使用主机头名称、IP 地址、非标准 TCP 端口号来进行区分。另外还可以使用虚拟目录的方法来发布多个网站。

31. FTP 使用“客户机/服务器”的工作方式。

构建 FTP 服务器的软件有 IIS.6.0 中集成的 FTP 服务、Serv-U FTP Server。

FTP 服务器缺省的端口号是 21。

服务器域的存储位置对话框中，对于小的域选择.INI 文件存储，对于大的域（用户数大于 500）应选择注册表可以提供更高的性能。

FTP 服务器的选项包括服务器选项、域选项、组选项和用户选项。服务器选项包括最大上传速度和最大下载速度、最大用户数量、检查匿名用户密码、删除部分已上传的文件、禁用反超时调度、拦截“FTP-BOUNCE”攻击和 FXP(File Exchange Protocol 文件交换协议

FXP 是一个服务器之间传输文件的协议，这个协议控制着两个支持 FXP 协议的服务器，在无需人工干预的情况下，自动地完成传输文件的操作。在我们的客户机上，可以简单的发送一个传输的命令，即可控制服务器从另一个 FTP 服务器上下载一个文件，下载过程中，无须客户机干预，客户机甚至可以断网关机。这种协议通常只适用于管理员作管理的用途，在一般的公开 FTP 服务器上，是不会允许 FXP 的，因为这样会浪费服务器资源，而且有可能出现安全问题。).

域常规选项可以设置域内最大的同时在线用户数、最小密码长度、是否要求复杂密码等选项。

域虚拟路径选项窗口可以将物理目录映射为虚拟目录，虚拟目录建立完成以后，并不是该域下的每个用户都可以访问，需要对用户的路径进行设置。

域 IP 访问选项：可以通过设置 IP 访问来限制某些 IP 地址是否能够访问 FTP 服务器。也可以针对每个用户进行设置。

域消息选项：域消息要事先创建并编辑。

域记录选项：可以选择各种消息和记录是否显示在屏幕上、是否记录在域的日志文件中，还可以设置日志文件的命名方法及创建规则。

域上传/下载率选项：可以添加用户访问服务器时不计入到上传/下载率的文件。

用户账号选项：在此窗口中【禁用账号】会临时禁用一个账号，而不需要将其删除；选择【自动】会将一个仅需要使用一段时间、以后不再使用的一个账号，在指定日期删除。

用户常规选项：可以设置最大上传/下载率。

用户目录访问选项：访问权限分为文件（读取、写入、追加、删除、执行）、目录（列表、建立、移动）、子目录三类。

用户上传/下载率选项：要求 FTP 客户端在下载信息的同时也要上传文件。可以设置各种计算方法。

用户配额选项可以限制用户上传信息占用的存储空间。

★ 32. 电子邮件系统使用的协议主要有简单邮件传送协议 SMTP，默认的 TCP 端口号是 25，用于发送电子邮件。邮局协议 POP3,默认的 TCP 端口号是 110，访问并读取邮件服务器上的邮件信息。Internet 消息访问协议 IMAP4，默认的端口号是 143 是用于客户端管理邮件服务器上的邮件的协议。

邮件系统的工作过程：

1. 用户使用客户端软件创建新邮件。

2. 客户端软件使用 SMTP 协议将邮件发送到发放的邮件服务器上。
3. 发方的邮件服务器使用 SMTP 协议将邮件发送到接受方的邮件服务器，接受方的邮件服务器将接受的邮件发送到用户的邮箱里等待用户处理。
4. 接受方客户端软件使用 POP3/IMAP4 协议从邮件服务器读取邮件。

安装邮件服务器软件之前要安装 IIS。

在快速设置向导中，可以输入新建用户的信息，包括用户名、域名及用户密码。

Winmail 邮件管理工具包括系统设置（对邮件服务器的系统参数设置，包括 SMTP、邮件过滤、更改管理员密码）、域名设置（可以增加新的域，用于构建虚拟邮件服务器、删除已有的域、还可以对域的参数进行修改）、用户和组（增删用户、修改用户的配置、管理用户）、系统状态和系统日志。

Winmail 邮件服务器允许用户自行注册新邮箱

为了使其他邮件服务器将收件人的邮件转发到该邮件服务器，需要建立邮件路由，即在 DNS 邮件服务器中建立邮件服务器主机记录和邮件交换器记录。

33. 数据备份从备份模式来看，可以分为物理备份和逻辑备份：从备份策略来看可以分为完全备份、增量备份和差异备份；根据备份服务器在备份过程中是否可以接受用户响应和数据更新，又可以分为离线备份和热备份。

逻辑备份也可以称作基于文件的备份。它的缺点是对于文件的一个很小的改动也需要备份整个文件。

物理备份有称基于快的备份或是基于设备的备份，文件的恢复变得复杂和缓慢。它适合于指定一个特定的文件系统来实现，并且不易移植。它的另一个缺点是可能产生数据的不一致。

	完全备份	增量备份	差异备份
空间使用	最多	最少	少于完全备份
备份速度	最慢	最快	快于完全备份
恢复速度	最快	最慢	快于增量备份

完全备份工作量大、成本高、备份时间长。但直观、简单，也是最基本的备份方式。

增量备份只备份相对于上一次备份操作以来新创建或者更新过的数据。但是在发生数据丢失和误删除操作时，恢复工作会变得比较麻烦，可靠性差。完全备份+增量本分+增量备份+增量备份+……

差异备份备份上一次完全备份后产生和更新的所有新的数据。工作量小于完全备份，但大于增量备份。 完全备份+差异备份。

冷备份不接受用户与应用对数据的更新，很好的解决了并发操作带来是数据不一致问题。缺点是备份时间较长。

热备份会产生数据不一致的现象。

常用的备份设备有：磁盘阵列、光盘塔、光盘库、磁带机、磁带库、光盘网络镜像服务器。

Windows2003 备份程序支持的五种备份方法：

副本备份：复制所有选中的文件，但不将这些文件标记为已备份（即不清除存档属性）。

每日备份：已备份文件在备份后不做标记。

差异备份：备份后不标记为已备份文件。

增量备份：备份后标记文件。

正常备份：备份后标记文件。

34. 根据防火墙的实现技术，防火墙可以分为包过滤路由器、应用级网关、应用代理和状

态检测。

防火墙的系统结构可以分为报过滤路由器结构、双宿主主机结构（运行应用级网关软件的计算机必须非常可靠---堡垒主机）、屏蔽主机结构、屏蔽子网结构（两个过滤路由器、两个堡垒主机）。

当使用具有 3 个网络接口的防火墙时，就会产生 3 个网络：内部区域（内网）、外部区域（外网）、非军事化区（DMZ）。

Cisco PIX 525 防火墙提供四种管理访问模式：非特权模式（开机自检进入，提示符为 pixfirewall>）、特权模式(输入 enable 进入，提示符为 pixfirewall#)、配置模式(在特权模式下输入 configure terminal,提示符为 pixfirewall(config)#)、监视模式(防火墙在开机或重新启动过程中按 Esc 键或是发送一个“Break”字符，提示符为 monitor>，在监视模式下，可以进行操作系统映像更新、口令恢复等操作)。

配置防火墙接口的名字，并指定安全级别：

Pix525(config)#nameif ethernet0 outside security 0

Pix525(config)#nameif ethernet1 inside security 100

Pix525(config)#nameif ethernet dmz security 50

缺省情况下，ethernet0 并命名为外部接口（outside），安全级别是 0，ethernet1 是内部接口（inside），安全级别是 100。安全级别取值范围是 0~99，数字越大，安全级别就越高。

配置以太网接口：

Pix525(config)#interface ethernet0 auto 采用自动协商方式

Pix525(config)#interface ethernet1 100full 采用 100Mbps 全双工方式

配置网卡的 IP 地址：

Pix525(config)#ip address outside 202.113.79.1 255.255.255.240

防火墙在外网的 IP 地址是 202.113.79.1

Pix525(config)#ip address inside 192.168..0.1

防火墙在内网的 IP 地址是 192.168..0.1

指定要转换的内部地址：nat 作用是将内网的私有 IP 地址转化为外网的公有 IP 地址。

Pix525(config)#nat (inside) 1 192.168..0.1 255.255.255.0

192.168..0.1 这个网段内的主机可以访问外网

global 为指定外部 IP 地址范围（地址池）。

Pix525(config)#global (outside) 1 201.113.79.1-202.113.79.14

设置外部地址池为 201.113.79.1-202.113.79.14

设置指向内网和外网的静态路由 route

Pix525(config)#route outside 00 218.81.20.1 1

配置静态 nat ：如果从外网发起一个会话，会话的目的地址是内网的 IP 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。

Pix525(config)#static (inside,outside) 202.113.79.4 192.168.0.4

建立了内部 IP 地址 192.168.0.4 和外部 IP 地址 202.113.79.4 之间的静态映射。

conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口。

Pix525(config)#conduit permit tcp host 192.168.0.4 eq www any 允许任何外部主机对全局地址 192.168.0.4 的这台主机进行 http 访问。

fixup 是启用、禁止、改变一个服务或是协议通过 PIX 防火墙，由 fixup 命令指定的端口是 PIX 防火墙要侦听的服务。

Pix525(config)#fixup protocol http 80

Pix525(config)#no fixup protocol stmp 启用 http 协议，并指定 http 端口号是 80，禁用 stmp 协议。

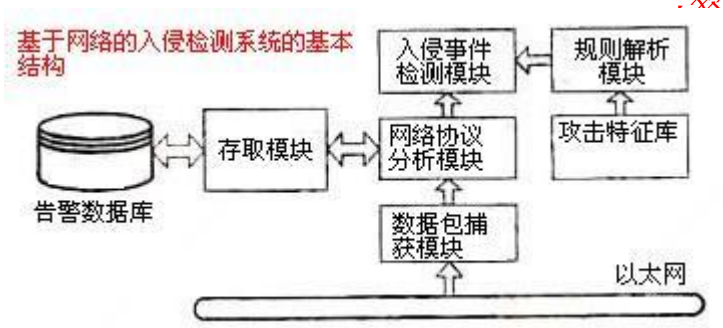
35. 入侵检测系统一般是由事件发生器、事件分析器、响应单元与事件数据库组成。

入侵检测技术可以分为异常检测（基于统计异常检测、基于神经网络入侵异常检测、基于数据采掘的异常检测）、误用检测（基于模式匹配的误用入侵检测、基于模型推理的毋庸入侵检测、基于专家系统的误用入侵检测、基于状态迁移分析的误用入侵检测）两种方式的结合。

按照检测的数据来源，入侵检测系统可以分为：基于主机的入侵检测系统（系统日志和应用程序日志为数据来源）和基于网络的入侵检测系统（网卡设置为混战模式，原始的数据帧是其数据来源）。

分布式入侵检测系统的三种类型为层次型（存在单点失效）、协作型（存在单点失效）和对等型（无单点失效）。

网络入侵检测系统一般有控制台和探测器组成。



网络入侵检测系统的探测器部署方法：

网络接口卡与交换设备的监控端口连接。

在网络中增加一台监控器改变网络的拓扑结构，通过集线器（共享式监听方式）获取数据包。

通过一个分路器 TAP 设备对交互式网络中的数据包进行分析和处理。当需要多个监听接口时：

对于多端口探测器，可以将 TAP 的引线分别直接接入探测器的监听接口。

对于不提供多端口的，可以将 TAP 的引线接到交换机或是集线器上。

入侵防护系统整合了防火墙技术和入侵检测技术，采用 In-Line 工作模式。

入侵防护系统主要有嗅探器、检测分析组件、策略执行组件、状态开关、日志系统和控制台。

嗅探器：负责接受数据包，对数据包协议类型进行解析，依据协议类型开辟缓冲区，保存接受到的数据包，并提交检测分析组件进行分析处理。

检测分析组件：接受来之嗅探器的数据包，从中检测攻击事件的发生，通过特征匹配、流量分析和协议分析、会话重构等技术，并结合日志中的历史记录来分析攻击的类型和特点。将经过分析得到的系统防护策略提交给策略执行组件，并将攻击数据包信息、攻击事件分析结果及相应策略提交至日志系统保存，并将告警信息提交控制台。

策略执行组件：负责执行分级保护策略，是对抗攻击的核心部分。所有接受到的数据都要通过策略执行组件进行转发。策略执行组件主要由简单的地址端口过滤、特征值匹配、会话阻断、流量控制以及一些针对蠕虫病毒和拒绝服务攻击的特殊模块组成。攻击发生时，策略执行组件将按照组件内的策略集和检测分析组件提供的防御策略进行防御。防御执行过

程将在日志系统中进行记录。

日志系统：负责对整个系统的工作过程进行数据采集、记录、统一分析和存储管理。日志数据的来源是检测分析组件和策略执行组件。控制台和检测分析组件是日志系统的使用者。他们根据需要通过数据库管理系统和海量数据统计分析系统提供数据。

状态开关：负责接受来之检测分析组件的状态转换指令，并驱动策略执行组件转换工作状态，对分布式拒绝服务攻击进行有效防御。

控制台：负责配置、管理、和控制 IPS 系统中其他组件。控制台收集来之各组件的工作状态信息和来之检测分析组件的报警信息，并且以适当方式呈现给管理员。

入侵防护系统的分类：基于主机的入侵防护系统（安装在受保护的主机系统中）、基于网络的入侵防护系统（布置于网络出口处，一般串联于防火墙和路由器之间）和应用入侵防护系统（部署于应用服务区前端）。

对于网络入侵防护系统来说，入侵检测的准确性和高性能是至关重要的。

36. 网络管理命令：

ipconfig 显示当前 TCP/IP 设置

hostname 显示当前主机名称

ARP 显示和修改 ARP 表项

NBTSTAT 显示本机与远程计算机的基于 TCP/IP 的 NetBIOS 的统计及连接信息

NET 管理网络环境、服务、用户、登记等本地信息

NETSTAT 显示活动的 TCP 连接、侦听的端口、以太网统计信息、IP 路由表和 IP 统计信息。

ping 通过发送 ICMP 报文并侦听回应报文，来检查与远程或本地计算机的连接。默认情况下发送 4 个报文，每个报文包含 64 个字节数据。

tracert 通过发送包含不同 TTL 报文并侦听回应报文，来探测到达目的计算机的路径

pathping 结合了 ping 和 tracert 命令的功能，将报文发送到所经过地所有路由器，并根据每跳返回的报文进行统计。

route 显示或修改本地 IP 路由表的网关条目。

37. 略

38. 常见的网络入侵与攻击的基本方法：

木马入侵：C/S 结构，主要的感染途径有：黑客入侵后植入；利用系统或软件的漏洞植入；受到夹带木马的电子邮件，运行后植入；通过即时聊天软件，发送含有木马的链接或是文件，接收者运行后被植入；在自己的网站上放置一些伪装后的木马程序，宣称是好玩的或有用的工具等名目，让不知道的人下载后运行后便可成功植入木马。

木马植入后所进行的操作：如同使用资源管理器一样对一些文件或是电子邮件进行复制或是删除等非法操作；转向入侵，利用被黑者的计算机来进入其他计算机或是服务器进行各种黑客行为，也就是找个替罪羊；监控被黑者的计算机屏幕画面的键盘操作来获取各种密码，例如进入各种会员网页的密码、拨号上网的密码、网络银行的密码、邮件密码等；远程遥控，操作对方的 Windows 系统、程序、键盘。

漏洞入侵：Unicode 漏洞入侵、跨站脚本注入、sql 注入入侵

协议欺骗攻击：针对网络协议的缺陷假冒用户身份截取信息获得特权的攻击方式。主要的协议欺骗攻击有 IP 欺骗攻击、ARP 欺骗攻击、DNS 欺骗攻击、源路由欺骗攻击。

口令入侵：

缓冲区溢出漏洞攻击：

拒绝服务攻击 DoS：Smurf 攻击：攻击者冒充受害者主机的 IP 地址，向一个大的网络发送 echo request 的定向广播包，此网络的许多主机都作出回应，受害主机会收到大量的 echo

reply 消息。

SYNFlooding（同步泛滥技术（SYNflooding））:利用 TCP 连接的三次握手过程进行攻击。使用无效的 IP 地址。

DDoS 分布式拒绝服务攻击：攻击者攻破了多个系统，并利用这些系统去集中攻击其他目标，成百上千的主机发送大量的请求，受害设备因为无法处理而拒绝服务。

Ping of Death：通过构造出重组缓冲区大小的异常的 ICMP 包进行攻击。

Teardrop：利用 OS 处理分片重叠报文的漏洞进行攻击。

Land 攻击：向某个设备发送数据包，并将数据包的源地址和目的地址都设置成攻击目标地址。

39. 常用的漏洞扫描工具有 ISS、Microsoft Baseline Security Analyzer、X-Scanner 等。

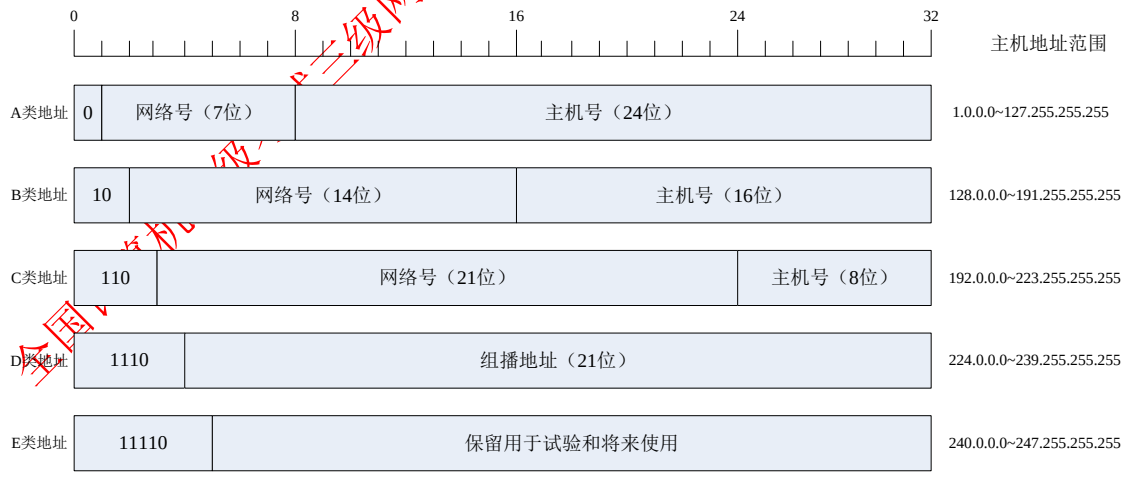
40. 计算机病毒的主要特征：非授权可执行性、隐蔽性、传染性、潜伏性、表现性或破坏性、可触发性。

计算机病毒按几声方式可以分为引导型病毒（寄生在磁盘引导区或主引导区。主引导区病毒有大麻病毒、2708 病毒、火炬病毒。分引导区病毒有小球病毒、Girl 病毒）、文件型病毒（感染可执行文件或是数据文件，有 1575/1591 病毒、848 病毒感染.COM 和.EXE 等可执行文件、Macro/Concept、Macro/Atoms 等宏病毒感染、新世纪病毒、One-half 病毒）和复合型病毒（Flip 病毒、新世纪病毒、One-half 病毒）。

计算机病毒按照破坏性可以分为良性病毒（小球病毒、1575/1591 病毒、救护车病毒、扬基病毒）和恶性病毒（黑色星期五病毒、火炬病毒、米开朗.基罗病毒）。

恶意代码：蠕虫：是一个自我包含的程序，他能够传播自身的功能或拷贝自身的片段到其他的计算机系统中。不需要把自身的附加在一段程序上，而是一个独立的程序，能够主动运行。有两种类型的蠕虫病毒：宿主计算机蠕虫和网络蠕虫。

木马：寄生在用户的计算机系统中，盗用用户信息，并通过网络发送给黑客。没有自我复制功能。传播途径主要有电子邮件、软件下载和会话软件。



标准分类的IP地址

直接广播地址：主机号全为 1，它用来使路由器将一个分组以广播方式发送给特定网络上的所有主机。

受限广播地址：32 位全为 1 的 IP 地址（255.255.255.255），用来将一个分组发送给本网络上的所有主机。

“这个网络上的特定主机”地址：网络号为全 0，主机号为特定的值，这样的分组限

制在本网内部，由相应的主机接收。

回送地址：127.0.0.0，用于网路软件测试和本地进程通信。

专用地址：10.0.0.0~10.255.255.255；172.16~172.31；192.138.0~192.168.255

最初在描述划分子网的 RFC 文档中规定了不使用第一个和最后一个网络地址。

一个子网的定向广播地址是比下个子网号小 1 的地址。

★ 255.192.0.0 11111111 11000000 00000000 00000000

121.175.21.9 01111001 10101111 00010101 00001001

01111001 10000000 00000000 00000000 ⟶ 121.128.0.0/10（网络地址）

255.192.0.0 11111111 11000000 00000000 00000000

121.175.21.9 01111001 10101111 00010101 00001001

01111001 10111111 11111111 11111111 ⟶ 121.191.255.255（直接广播地址）

⟶ 121.191.255.254（最后一个可用的 IP 地址）

175=128+0+32+0+8+4+2+1 10101111

192=128+64+0+0+0+0+0+0 11000000

192	11	000000
175	10	101111

32+0+8+4+2+1=47 ⟶ 0.47.12.9（主机号）

2. 路由器是连接不同逻辑子网的网络互连设备。

路由表的内容主要包括目的网络地址及其对应的目的端口或下一跳路由器地址和缺省路由信息。

路由表项内容：

第一列是路由源码，他说明路由表项是通过什么方式，采用什么路由选择协议获得的。其中 C 表示为直连；S 表示为静态路由；I 使用 IGRP 内部网关协议获得路由信息；O 使用 OSPF 开放最短路径优先协议获得路由信息；R 使用 RIP 路由信息协议获得路由信息；i 使用 IS-IS 内部网关协议获得路由信息；B 使用 BGP 外部网关协议获得路由信息；E 使用 EGP 外部网关协议获得路由信息。

第二列是目的网络地址和掩码

第三列是目的端口或是下一跳路由器地址：如果是直连，则给出的是目的端口；如果有下一跳路由器，则这个字段给出的就是目的端口。

S* 0.0.0.0/0 【1/0】via 202.112.41.217 为缺省路由表项，该行信息说明这是一条静态路由，是由管理员手工配置的。其目的网络为 0.0.0.0 的下一跳路由器地址是 202.112.41.217，即他的缺省路由是 202.112.41.217。这里“0”地址表示路由信息没有直接显示在路由表里的所有网络。

第一列仍然是路由源码

第二列表示路由类型：E1 OSPF 外部路由类型 1；E2 OSPF 外部路由类型 2.

第三列仍然是目的网络及其掩码

第四列前面的值是管理距离，后面的值是权值或成本：管理距离用于衡量路由表中给定的路由信息源的“可信度”。管理距离的值越小，路由信息源的可信度越高。直接连接的可信度越高，其次是静态路由。

【O E1 222.29.2.0/24 [110/3] via 162.105.1.145, 00:13:43,Vlan1】

权值是路由器通过路径选择算法为网络上的路径产生一个数字。路由器根据这个值确定最佳路径。一般来说，权值愈小，路径愈佳。

路由器的工作模式：

用户模式：Router>

特权模式：在用户模式下，输入“enable”和超级用户密码，就可以进入特权模式。

Router#

设置模式：当通过 Console 端口进入一台刚出厂的没有任何配置的路由器时，控制台就会进入设置模式。

全局配置模式：在特权模式下，输入“configure terminal”就可以进入全局配置模式。Router（config）#

其他配置模式：

在全局配置模式下，进入接口配置模式：Router（config）# int f0/2

在全局配置模式下，进入虚拟终端配置模式：Router（config）# line vty 0 15

在全局配置模式下，进入 RIP 路由协议配置模式：Router（config）# router rip

RXBOOT 模式：为路由器的维护模式，在密码丢失时，可以进入 RXBOOT 模式以恢复密码。

路由器的配置方式：1.使用控制端口配置（Console）配置。2.使用 AUX 端口连接一台 Modem,通过拨号远程配置路由器。3.使用 telnet 远程登录到路由器上进行配置。4.使用 TFTP 服务，以拷贝配置文件、修改配置文件的方式，对路由器进行配置（在特权用户模式下，用 write 和 copy 命令拷贝配置文件到 TFTP Server;）。5.通过网络管理协议 SNMP 修改路由配置文件的形式，对路由器进行配置。

配置路由器的主机名：在全局配置模式下，Router(config)#hostname Router-phy

Router-phy(config)#

配置超级用户口令：Router(config)#enable secret phy123

Router(config)#enable password 7 phy123

Router(config)#

设置系统时钟：在特权用户模式下：Router#calendar set 10:24:00 22 march 2007

退出命令 exit：从端口配置模式返回全局配置模式，还是从全局配置模式返回到特权配置模式，都可以使用 exit 一级一级的退出，也可以使用 end 命令，直接返回特权用户模式。

Router(config-if)#exit

Router(config)#exit

Router#

Router(config)#end

Router#

保存配置 write：在特权用户模式下，Router#write momory (保存到路由器的 NVRAM 中)

Router#write network tftp(保存在 tftp 服务器下)

删除配置：在特权模式下，Router#write erase

telnet：一个路由器可以支持 5 个 telnet 连接。

在用户模式下，Router>telnet paris (或是 IP 地址)

ping：在用户模式或是特权模式下，ping 网络上的一台主机。

Router>ping 182.105.130.110

trace：用于查询网络上数据传输流向的理想工具，跟踪测试分组转发路径的每一步，可用于了解路径上每一级路由器的工作状况和延迟时间。如果路径中任何一台路由器不可到达，则出现三个星号***,用星号来取代路由器名。此时，trace 将尝试到达下一步，直到使用 Ctrl-Shift-6 退出。在用户模式和特权用户模式下：Router>trace 237.189.11.73

show：查看 flash ：Router>show flash

查看系统时钟：Router>sh clock

查看路由器软硬件版本号：Router>sh version

查看路由器配置：在特权用户模式下，Router#sh configuration

查看路由表：在特权用户模式下，Router#sh ip route

查看 IP 路由协议的详细信息：在特权用户模式下，Router#sh ip protocols

配置接口的描述信息：进入接口配置模式，使用 description 命令。

Router (config)#int g6/0

Router (config-if)#description To-Beijing Foreign Studies University

配置接口带宽：进入接口配置模式，使用 bandwith 设置接口带宽，带宽单位是 kbps。

Router (config)#interface POS/3

Router (config-if)#bandwith2 500 000 (设置接口带宽为 2.5G)

配置接口的 IP 地址：进入接口配置模式，使用 ip address 命令配置接口的 IP 地址。

Router (config)#interface f2/3

Router (config-if)#ip address 202.112.7.249 255.255.255.252

接口的开启与关闭：进入接口配置模式，使用 shutdown、no shutdown 命令关闭和开启接口。 Router (config)#interface f2/3

Router (config-if)#shutdown (关闭接口)

Router (config-if)#

Router (config-if)#no shutdown （开启接口）

配置标准以太网接口：标准以太网接口的类型为 Ethernet,可简写为 e

Router (config)#interface Ethernet0

配置快速以太网接口：快速以太网接口类型为 FastEthernet，可简写为 f

Router (config)#interface f0/2

Router (config-if)#duplex full 全双工

Router (config-if)#no ip direct-broadcast 禁止对某一特定网段的直接广播

Router(config-if)#no ip proxy-arp 不做 arp 代理

配置千兆以太网接口：千兆以太网的接口类型是 GigabitEthernet,可简写为 g

Router (config)#interface g0/1

配置异步串行接口：异步串行接口类型是 Async,可简写为 a。Async 主要用于连接 Modem 设备，为网络用户提供拨号上网服务。

Router (config)#interface a1

Router (config-if)#ip unnumbered ethernet0 指定 a1 口的 IP 地址为 e0 口的 IP 地址

Router (config-if)#encapsulation ppp 封装协议为 ppp

Router (config-if)#async default ip address 202.112.7.129 异步串行接口缺省 ip 为~

Router (config-if)#async dynamic routing 异步串行接口采用动态路由

Router (config-if)#async mode interactive 设置异步串行口的工作方式为交互式

配置高速同步串行接口：高速同步串行接口类型是 Serial，可简写为 s。它主要用于 DDN 专线、帧中继、卫星、微波等广域网连接。需要配置的参数主要有接口带宽、接口协议和接口的 IP 地址。

Router (config)#interface s1/1

配置 POS 接口：POS 支持光纤介质，它所使用的链路层协议主要有 hdlc 和 ppp.

Router (config)#interface POS3/0

Router (config-if)#crc 32 可选的 CRC 校验位是 32 位（可选 16 位和 32 位）

Router (config-if)#pos framing sdh 可选的帧格式是 sdh（可选 sdh 和 sonet）

Router (config-if)#pos flag s1 s0 2 (s1so=00 表示是 SONET 帧格式

s1s0=10(十进制 2)表示是 SDH 帧格式)

loopback 接口没有一个实际的物理接口与之相对应，也没有与其他网络节点相连接的物理链路。它是一个虚拟的接口，loopback 接口号的有效值为 0~2147483647。主要作用是他作为一台路由器的管理地址，使网络管理员可以随时登录到路由器上，对路由器进行配置管理。它还可以作为动态路由协议 ospf 和 bgp 的 router id ，使路由器功能更加稳定可靠。每台路由器上都配置一个环回接口，它永远处于激活状态。网络管理员为 loopback 接口分配一个 IP 地址作为管理地址，其掩码应为 255.255.255.255。在全局模式下，对其进行配置：

Router (config)#int loopback 0

Router (config-if)#no ip route-cache 关闭快速交换（对包的处理方式）

Router (config-if)#no ip mroute-cache 关闭路由缓存

静态路由的配置方法与步骤：在全局配置模式下，使用“ip route”命令配置静态路由，使用“no ip route”命令删除静态路由配置。

ip route <目的网络地址><子网掩码><下一跳路由的 IP 地址>

Router (config)#ip route 59.65.96.0 255.255.240.0 222.112.37.1

RIP 路由协议只根据路由器的跳数来决定最佳路径，不考虑带宽、延时和其他因素。总是把具有最小跳数值的路径作为最佳路径。限制最大跳数是 15，如果跳数是 16，则意味着不可到达。RIP 路由更新报文中不能携带子网掩码信息，也就是不支持可变长掩码，30s 更新一次路由。

在 RIP 的基本配置中，在配置网路地址时不需要给定掩码。在全局配置模式下：

Router(config)#router ip

Router(config-router)# network 159.105.0.0

Router(config-router)#network 212.112.7.0 (参与 IP 路由的网络地址)

配置被动接口：所谓的被动接口，就是指在指定的接口上抑制路由更新，也就是阻止路由更新报文通过该路由器接口。在 RIP 路由配置模式下，使用“passive-interface”命令指定一个路由器接口为被动接口。在全局配置模式下：

Router(config)#router rip

Router(config-router)#passive-interface ethernet 0

Router(config-router)#exit

Router(config)#exit

Router#

配置路由过滤：路由过滤的功能是在指定的路由器接口上，既可以过滤掉进入的路由更新信息，也可以过滤输出的路由更新信息。在 RIP 配置模式下，使用“distribute-list”命令配置路由过滤。在全局配置模式下：

Router(config)#access-list 12 deny any

Router(config)#router rip

Router(config-router)#distribute-list 12 in ethernet0

Router(config-router)#end

Router#

配置管理距离：管理距离 AD 是测量路由可信度的值，AD 的值越小，路由的可信度就越高，缺省的 AD 值是 120。在 RIP 配置模式下，使用“distance”命令指定一个管理距离值，有效的管理距离值是 1~255。在全局配置模式下：

Router(config)#router rip
Router(config-router)#distance 50
Router(config-router)#exit
Router(config)#exit
Router#

定义临近路由器：在 RIP 配置模式下，使用“neighbor”命令指定临近路由器，以单播的方式发送路由更新信息。在全局配置模式下：

Router(config)#router rip
Router(config-router)#neighbor 202.112.7.2
Router(config-router)#exit
Router(config)#exit
Router#

开放式最短路径优先协议 OSPF 采用链路状态算法，收敛速度快、路由汇聚使路由表变小、支持可变长掩码、路由更新信息量小、路由更新不采用广播报文而是使用组播报文。

OSPF 可以划分区域，路由更新信息只在本区域内传递，不同区域间不交换路由信息，以减少路由器存储和维护的信息量。区域用数字标识，称之为区域 ID,区域 ID 是一个 32 位的无符号数值。数值范围是 0~4294967295。区域 ID 的标识形式有两种：一种是十进制整数表示形式，一种是点分十进制表示形式。当区域 ID 是 0 或是 0.0.0.0 时，则表示是骨干区域。

在全局配置模式下，使用 router ospf <Process ID>命令，启动 OSPF 进程。其中 PID 是 OSPF 的进程号，可以在指定的范围内（1~65535）随意设置。

在路由器的 OSPF 配置模式下，使用“network ip <子网号><wildcard-mask>area<区域号>”其中 <wildcard-mask>是子网掩码的反码。定义参与 OSPF 的子网地址。或使用“area<区域号>range<子网地址><子网掩码>”命令定义某一特定范围子网的聚合。

使用 network 命令定义参与 ospf 的子网地址。

在全局配置模式下：单个 IP 地址参与 OSPF

Router(config)#router ospf63
Router(config-router)#network 131.107.25.1 0.0.0.0 area 0
Router(config-router)#exit
Router(config)#exit
Router#

在全局配置模式下：网络地址参与 OSPF

Router(config)#router ospf 63
Router(config-router)#network 133.181.0.0 0.0.255.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#

使用 area range 命令定义参与 OSPF 的子网地址：

Router(config)#router ospf 63
Router(config)#area 0 range 212.37.123.0 255.255.255.0
Router(config-router)#exit
Router(config)#exit

```
Router#
```

在全局配置模式下，使用“passive-interface”命令配置路由器的被动接口：

```
Router(config)#router ospf 63
Router(config-router)#passive-interface ethernet 0
Router(config-router)#end
Router#
```

配置路由过滤：

```
Router(config)#access-list 12 deny any
Router(config)#router ospf 63
Router(config-router)#disterbute-list 12 in serial 0
Router(config-router)#end
Router#
```

配置管理距离：OSPF 默认的管理距离是 110。在全局配置模式下：

```
Router(config)#router ospf 63
Router(config-router)#distance 10
Router(config-router)#end
Router#
```

配置 OSPF 引入外部路由的花费值 metric(0~16777214)：在全局配置模式下：

```
Router(config)#router ospf 63
Router(config-router)#redistribute metric 100
Router(config-router)#end
Router#
```

配置引入外部路由时缺省的标记值（0~4294967295）：在全局配置模式下：

```
Router(config)#router ospf 63
Router(config-router)#redisterbute tag 10
Router(config-router)#end
Router#
```

配置引入外部路由时缺省的类型：

```
Router(config)#router ospf 63
Router(config-router)#redistribute connected metric-type 1 subnets
Router(config-touter)#end
Router#
```

IP 访问控制列表主要有两种类型，一种是标准访问控制列表，一种是扩展访问控制列表。

当要配置对虚拟终端的访问控制权限，也就是配置允许远程登录到路由器上的权限时，可以使用标准访问控制列表。设定凡来之网络管理员的 IP 地址可以允许通过 vty line 远程登录到路由器。

为了防止冲击波蠕虫病毒的传播，可以使用扩展访问控制列表设定拒绝 TCP 协议的 444 端口的所有数据包通过路由器。

3.

编号	源 IP 地址	目的 IP 地址	报文摘要
1	192.168.1.1	192.168.1.36	DHCP:Request,Type:DHCP release
2	0.0.0.0	255.255.255.255	DHCP:Request,Type:DHCP discover
3	192.168.1.36	255.255.255.255	DHCP:Reply, Type:DHCP offer
4	0.0.0.0	255.255.255.255	DHCP:Request, Type:DHCP requ
5	**192.168.1.36**	**255.255.255.255**	**DHCP:Reply, Type:DHCP ack**
6	192.168.1.1	192.168.1.47	WINS: C ID=33026 op=register name=xp

DHCP服务器地址

DHCP: ----- DHCP Header -----

DHCP: Boot record type = 2 (Reply)

.....

DHCP: Client self-assigned address = [0.0.0.0]

DHCP: Client address = [192.168.1.11]

客户机获得的IP地址

DHCP: Next Server to use in bootstrap = [0.0.0.0]

DHCP: Relay Agent = [0.0.0.0]

DHCP: Client hardware address = 000F1F52EFF6

MAC地址

.....

DHCP: Vendor Information tag = 63825363

DHCP: Message Type = 5 (DHCP Ack)

DHCP: Address renewel Interval = 345600 (seconds)

DHCP: Address rebinding interval = 604800 (seconds)

DHCP: Request IP Address lease time = 691200 (seconds)

DHCP: Subnet mask = 255.255.255.240

路由器地址

DHCP: Gateway address = [192.168.1.100]

DHCP: Domain Name Server address = [202.106.46.151]

DNS服务器地址

4. 网卡一般具有四种接受模式：广播、组播、单播和混杂模式。

嗅探器通过将本地网卡设置为混杂模式，来监听并捕捉其所连接的网段的所有数据。并通过软件将捕捉到的数据进行实时分析，进而分析网络的运行状态。

实现网络监听的关键是经嗅探器部署于侦听网络上。有以下两种部署方法：在共享性网络中，只要将嗅探器部署到网络中的任意一个接口上或是插入到任何一个节点的通信链路中，即可捕捉到所有的数据包。 在交换式网络中，交换机将数据包转发到相应的端口。因此需要采用通过对交换机端口进行镜像的方式来获取网络中流量。

镜像的方法：配置被镜像端口：Switch(config)#monitor session 1 source interface Gi2/16

配置镜像端口：Switch(config)#monitor session 1 destination interface Gi/12

检查配置：show session 1

常见的网络数据监听工具有：Sniffer Pro、Ethereal、TCPdump。其中 Sniffer Pro 是一个功能强大的可视化网络数据监听工具。主要功能有：1.捕捉网络流量，进行数据包解码分析。2.实时检测网络活动。3.内置分析器诊断网络故障。4.存储各种历史信息，并可进行基线的分析。5.当探测到网络故障时可以发出警报。6.可以模拟生成数据包对网络进行探测。

网络监听模块提供的主要功能有：

Dashboard：实时显示网络的数据传输率、带宽利用率和出错率，并可以提供各种统计数据的图形化显示。

Host Table：以表格和图形方式显示网络中各节点的数据传输情况。

Matrix：实时显示网络中各结点的连接信息，并提供统计功能。

Protocol Distribution ：统计网络流量中各协议和应用的分布情况。统计信息可以通过表格或图形方式显示。

Application Respone Time ：实时检测客户端与服务器的应用连接相应时间。当发现相应超时，就会发出警报。

History Sample ：收集一段时间内的各种网络流量信息。通过这些信息可以建立网络运行状态的基线，设置网络异常的报警阈值。也可以根据这些信息推测网络流量的发展趋势，为网络的升级提供依据。

Global Statistics：统计多种类型的统计信息。

数据包的捕捉：当只想捕捉特定的数据包时，可以在捕捉前进行设定：第一步是通过“define a capture fliter”定义数据包过滤器来限定数据包的特征。第二步是使用“select a capture filter”来启动滤波器。

★ 数据包分析：Sniffer Pro 的专家模块 Expert 提供了强大的解码功能。

Summary 部分：显示状态、收发双方的地址、协议、长度、捕获时间等。

Detail：显示在 Summary 中选定数据包的协议解码信息。

Hex 部分：以十六进制和 ASCII 码显示被解码的数据包载荷。

数据包生成：向网络发送定制的数据包来测试网络。使用数据包生成器也可以回放捕获的数据包。

★ 四、 使用 59.17.148.64/26 划分 3 个子网，其中第一个子网能容纳 13 台主机，第二个子网能容纳 12 台主机，第三个子网容纳 30 台主机。请写出子网掩码、各子网网络地址及可用的 IP 地址段。(9 分) (注:请按子网序号顺序分配网络地址)

59.17.148.64 00111011 .00010001 . 00010100 . 01000000

11111111. 11111111. 11111111 . 11000000 → 128+64=192

00111011 .00010001 . 00010100 . 01000000

11111111. 11111111. 11111111 . 11100000 → 255.255.255.224（掩码 3）

00111011 .00010001 . 00010100 . 01000000 → 59.17.148.64

00111011 .00010001 . 00010100 . 01011111 → 59.17.148.95 →

59.17.148.65 ~ 59.17.148.94 （子网 3 可用 IP）

11111111. 11111111. 11111111 . 11100000(子网 3) 255.255.255.

11111111. 11111111. 11111111 . 11100000（子网 1、2）

↓

11111111. 11111111. 11111111 . 11100000（子网 1）

11111111. 11111111. 11111111 . 11110000 → 255.255.255.240 (子网 1、2 掩码)

00111011 .00010001 . 00010100 . 01100000 → 59.17.148.96

00111011 .00010001 . 00010100 . 01101111 → 59.17.148.111 →

59.17.148.97~59.17.148.110 （子网 1 可用的 IP 地址）

11111111. 11111111. 11111111 . 11110000（子网 2）

00111011 .00010001 . 00010100 . 01110000 → 59.17.148.112

00111011 .00010001 . 00010100 . 01111111 ⟶ 59.17.148.127 ⟶

59.17.148.113~59.17.148.126（子网 2 可用 IP 地址）

（3）Router(config)#interface Gil/3

Router(config)#ip access-group 105 in

Router(config)#ip access-group 105 out

(4).路由器交换机上 DHCP IP 地址池的配置内容：IP 地址池的子网地址和子网掩码、缺省网关、域名和域名服务器的 IP 地址、IP 地址的租用时间和取消地址池冲突记录日志等参数。

补充：

1. 工作区子系统设计：指从设备出线到信息插座的整个区域。工作区子系统的设计主要有两个部分：

1.确定信息插座的数量和类型。信息插座大致可以分为嵌入式安装插座（双绞线）、表面安装插座和多介质信息插座（铜线和光缆）。A.根据已经掌握的用户需要，确定信息插座的类别。B.根据楼层平面图计算实际可用空间（0.75 建筑面积）。C.根据以上两点估计工作区和信息插座的数量，可分为基本型（9~10 m^2 安装一个双孔信息插座，即每个工作区提供一部电话和一部计算机终端）和增强型（9~10 m^2 安装两个两个双孔插座，即每个工作区提供两部电话和一部计算机终端）两种。D.根据建筑物的不同，可采用不同的安装方式（嵌入式用于新建筑，表面安装用于现有建筑）。

2.适配器的使用：A.在设备采用不同的信息插座的连接器时，看选用专用电缆和适配器。B.当在单一信息插座上进行两项服务时，宜采用“Y”型适配器或是一线两用器。C.在配线（水平）子系统中选用的电缆类型不同于设备所需的电缆类别（介质）时，宜采用适配器。

水平子系统设计：由建筑物各层的配线间至各工作区所配置的线缆构成。采用 5 类或是 6 类 4 对非屏蔽双绞线。对计用户有高速率终端要求的场合，可采用光纤直接到桌面的方案。水平子系统布线线缆长度应该在 90m 以内，信息插座应该在内部做固定线使用。设计系统主要包含一下步骤：1.确定导线的类型：A.对于 10Mbps 以下低速率数据和语音的传输，采用 4 类或 5 类双绞线。B.对于 100Mbps 以下，10Mbps 以上的高速数据的传输采用 5 类或是 6 类双绞线。C.对于 100Mbps 以上、宽带的数据和复合数据的传输采用光纤或是 6 类双绞线。2.确定导线的长度：A.确定布线方法和布线走向。B.确定管理间或接线间所管理的区域。C.确定离接线间最远的信息插座的距离（L_{max}）。D.确定离接线间最近的信息插座的距离（L_{min}）。E.计算平均电缆的长度：$L_{avr}=(L_{max}+L_{min})/2$ F.计算总电缆长度：$L_{sum}=L_{avr}+$备用部分$+$端接误差，其中备用部分约为平均电缆长度的 10%。3.确定布线方式：走廊金属布线、内部走线法。

管理子系统设计：指干线间或是卫星接线间内的交叉连接设备。管理区子系统设置在每层配线间内，由交接间的配线设备（双绞线跳线架、光纤跳线架）以及输入输出设备组成。管理子系统主要有三种应用：水平/干线连接、主干线系统相互连接、入楼设备的连接。用户可以在管理子系统中更改、增加、交换、扩展线缆用于改变线缆路由。

干线子系统设计：即建筑物主馈电缆，既包括设备间的主干电缆，也包括干线接线间

至卫星接线间、设备间至网络端口、主设备间与计算机中心、设备间至建筑群子系统设备间的连接线缆。

干线子系统设计的原则是：在确定干线子系统所需要的电缆对数之前，必须确定电缆中语音和数据信号的共享原则；应选择干线电缆最短、最安全、最经济的路由，选择带盖的封闭通道铺设干线电缆；干线电缆可以采用点对点连接、也可以采用分支递减端接或是电缆直接连接的方法；如果设备间与计算机机房处于不同地点，而且需要把语音电缆连接至设备间，把数据电缆连接到计算机机房，则宜在设计中选取干线电缆的不同部分来满足语音和数据的需要。需要时，也可以采用光缆系统。

干线线缆敷设经常采用两种结合方式，即点对点结合和分支结合。

设备间子系统设计：设置在建筑物的中部或是一二层，并为以后的扩展留有余地，不设置在地下室或是楼层的顶部，而且建筑物的线缆进入建筑物时应有过流、过压保护措施。设备间的温度应该保持在 10^0C ~27^0C 之间。相对湿度应该保持在 30%~80%，照明应该满足一定的照度标准，并有良好的防尘措施。

建筑群子系统：可以是架空布线、巷道布线、直埋布线和地下管道布线或是四种敷设方式的任意组合。

2.交换机的配置方式：

使用控制端口（Console）配置交换机：Console 是一个用来连接配置终端的异步串行口，接口标准为 RJ-45.是交换机刚出厂时，第一次对其进行配置所用的方法。 使用 Console 端口配置交换机时，需要准备一台已经安装了超级终端软件的计算机作为配置终端，同时还需要一条由厂家提供的 RJ-45 到 9 针或 25 针异步串行接口的信号电缆。使用超级终端软件对异步串行口进行参数配置：传输速率 9600，数据位 8 位，停止位 1 位。

使用 telnet 配置交换机：必备条件：作为模拟终端的计算机与交换机都必须与网络联通，它们之间能够通过网络进行通信；计算机必须有访问交换机的权限；交换机必须预先配置好设备管理地址，包括 IP 地址、子网掩码和缺省路由；交换机必须预先配置好远程登录的密码。

使用浏览器配置交换机：必备条件：在用于配置的计算机和用于被管理的交换机上都已经配置好了 IP 地址，它们之间能够通过网络进行通信；呗管理计算机必须支持 HTTP 服务，并且已经启用该服务；在用于管理的计算机中，需安装有支持 JAVA 的 Web 浏览器；在用于管理的计算机上，需要下载并安装 Java-plugin;在被管理的计算机上，需要拥有管理权限的用户账号和密码。启用交换机的 HTTP Server 服务：

进入全局配置模式：Switch-3548>enable
Password:**********
Switch-3548#config t
Switch-3548(config)#

启用 HTTP Server: Switch-3548(config)#ip http server

```
Switch-6509>enable
Enter password:
Switch-6509>（enable）set ip http server enable
Switch-6509>(enable)
```

配置 HTTP 用户认证方式：在全局配置模式下，用“ip http authentication”命令选择用户认证方式如下：enable 用超级用户口令（缺省配置，不建立新用户，只提供系统用户名 enable，系统用户口令 enable Password）

local 本地用户名和口令

tacacs 用 tacacs 完成用户认证

CSM 网络管理界面可以完成端口配置、VLAN 配置以及查看交换机运行状态等一系列网络管理工作。

查看交换机前面板的端口状态：View-Front Panel-绿色的是正在工作的端口。

显示网络拓扑图：View-Topology

端口配置：Port-Port Setting 可以配置端口速率、通信方式。

3. 交换机端口配置：在交换机端口配置模式下，可以对交换机端口的描述信息、通信方式、传输速率、VLAN 分配、Q0S 质量保证策略、资源预留协议（RSVP）、安全属性、广播信息流量限制、数据的流量控制以及 IEEE802.1X 和 IEEE802.1Q 等协议进行配置。

配置交换机的端口描述信息：

一、进入端口配置模式：Switch-PHY-3548(config)#interface f0/24
Switch-PHY-3548(config-if)#

二、配置端口描述信息：Switch-PHY-3548(config-if)#description To-lib
Switch-PHY-3548(config-if)#

端口描述的内容最多不超过 240 个字符。

配置交换机端口的关闭与开启：

一、进入端口配置模式 Switch-PHY-3548(config)#interface f0/24
Switch-PHY-3548(config-if)#

三、关闭或开启端口： Switch-PHY-3548(config-if)#shutdown (关闭端口)
Switch-PHY-3548(config-if)#no shutdown (开启端口)

配置交换机端口的通信方式：

一、进入端口配置模式：Switch-PHY-3548(config)#interface f0/24
Switch-PHY-3548(config-if)#

二、配置端口通信方式： Switch-PHY-3548(config-if)#duplex auto (缺省为自适应)
Switch-PHY-3548(config-if)#duplex half (设置为半双工)
Switch-PHY-3548(config-if)#duplex full (设置为全双工)

配置交换机端口的传输速率：

一、进入端口配置模式：Switch-PHY-3548(config)#interface f0/24
Switch-PHY-3548(config-if)#

二、配置端口的传输速率：Switch-PHY-3548(config)#speed 10 (设置为 10Mbps)
Switch-PHY-3548(config-if)#speed 100 (设置为 100Mbps)
Switch-PHY-3548(config-if)#auto (设置为自动速率配置)

配置交换机的系统信息：

配置交换机的主机名：

一、进入全局模式：Switch-3548>enable
Password:**********
Switch-3548#config t
Switch-3548(config)#

二、配置主机名： Switch-3548(config)#hostname Switch-PHY-3548
Switch-3548(config)#

一、进入超级用户模式 Switch-6509>enable
Enter password:
Switch-6509>(enable)

二、设置系统名或设置系统提示

设置系统名：Switch-6509>(enable)set system name Switch-PHY-6500

设置系统提示：Switch-6509>(enable)set prompt Switch-PHY-6500>

Switch-6509>(enable)

配置超级用户口令：

Switch-3548(config)#enable secret 5 zzz(加密口令)

Switch-3548(config)#

Switch-3548(config)#enable password zzz(明码口令)

Switch-3548(config)#

Switch-3548(config)#enable password 7 zzz(加密口令)

Switch-PHY-6500>(enable)set enablepass

配置远程登录口令：

Switch-3548(config)#line vty 0 4

Switch-3548(config-line)#password 7 zzz(加密口令)

Switch-3548(config-line)#password 0 zzz(明码口令)

Switch-3548(config-line)#

Switch-PHY-6500>(enable)set password

改变系统时间设置：

Switch-PHY-3548#clock set 23:00:00 23 february 2007

Switch-PHY-3548#

Switch-PHY-6500>(enable)set time fri 2/23/2007 23:00:00

Switch-PHY-6500>(enable)

配置设备管理地址（IP 地址）：

配置 IP 地址：

Switch-PHY-3548（config）#interface VLAN

Switch-PHY-3548 (config-if)#ip address 203.105.0.62 255.255.255.0

Switch-PHY-3548(config-if)#

Switch-PHY-6500>(enable)set interface sco 203.105.1.63 255.255.255.0 203.105.1.255

配置缺省路由：

Switch-PHY-3548（config）#ip default-gateway 203.105.1.1

Switch-PHY-3548（config）#

Switch-PHY-6500>(enable)set ip route 0.0.0.0 203.105.1.1

防毒软件安装与配置

网络版防病毒软件通常是由系统中心、服务器端、客户端、管理控制台等子系统组成。

管理控制台既可以安装到服务器上也可以安装在客户机上，视网络管理员的需要，可以自由安装。

网络版防病毒软件的基本安装对象包括系统中心的安装、服务器端的安装、客户端的安装和管理控制台的安装。安装时建议先在服务器上安装系统中心然后再进行其他模块的安装，

安装系统中心时，安装程序将在服务器上同时安装一套服务器端系统和一套管理控制台系统。

安装系统中心的计算机应该具备一下条件：全天候开机、可以方便的连接 Internet。

对于大多数的网络版的防病毒系统，服务器端和客户端通常可以采用本地安装、远程安装、Web 安装、脚本安装等方式进行安装。

控制台的安装通常有两种方式：通过光盘安装控制台、远程安装控制台，系统管理员可以将管理控制台远程安装到其他计算机上。

系统升级设置：从网站升级、从上级中心升级、从网站上下载手动数据包。

扫描设置：通常包括文件类型、扫描病毒类型、优化选项、发现病毒后的处理方式、清除病毒后的处理方式、杀毒结束后的处理方式和病毒隔离系统的设置。

黑白名单设置：若白名单为空，则程序根据黑名单来判断是否允许注册；若白名单存在，先查看对象是否在白名单中，如果不在白名单中则拒绝注册，如果在白名单中，同时不在黑名单中，则接受注册，如果在白名单中又在黑名单中，则拒绝注册。

端口设置：为了使网络版防病毒软件的通信数据能顺利的通过防火墙，通常系统都会提供用于数据通信端口设置的界面。

5. Windows2003 网络管理命令

ipconfig 显示当前 TCP/IP 网络配置

hostname 显示当前主机的名称

ARP 显示和修改 ARP 选项

-s 添加一个 ARP 选项，将其 IP 地址（inet-addr）与 MAC 地址（eth-addr）关联

-d 删除 inet-addr 指定的 ARP 选项

-a 显示当前的 ARP 选项

NBTSTAT 显示本机与远程计算机的基于 TCP/IP 的 NetBIOS 的统计及连接信息。

-a 使用远程计算机名称列出名称列表。

-A 使用远程计算机的 IP 列出名称列表

-c 列出 NetBIOS 名称缓冲及其对应的 IP 地址

-n 列出本地 NetBIOS 名称

-r 列出通过广播和 WINS 解析的名称

-S 列出会话及目的 IP 地址

NET 管理网络环境、服务、用户、登录等本地信息

NET VIVE 显示域列表、计算机列表或指定计算机上共享资源列表

NET USER 显示、创建或是修改计算机上的用户帐户

NET USE 显示、建立或是取消计算机与共享资源的连接

NET START 显示或启动正在运行的服务

NET PAUSE 挂起一个 Windows 服务或资源

NET CONTINUE 重新激活一个被 NET PAUSE 挂起的 Windows 服务

NET STOP 终止 Windows 服务

NET STATISTICS 显示本地工作站或服务器服务的统计日志

NET SHARE 显示、建立或取消共享资源

NET SESSION 显示或中断本地服务器与其他计算机之间的会话

NET CONFIC 显示工作站或服务器服务的配置信息

NETSTAT 显示活动的 TCP 连接、侦听的端口、以太网统计信息、IP 路由表和 IP 统计信息 -a 显示所有连接和侦听端口

-e 显示以太网统计信息

-p 显示指定协议的连接

-r 显示路由表内容

-s 显示协议统计信息

ping 通过发送 ICMP 报文并侦听回应报文，来检查与远程计算机的连接。默认情况下发送 4 个报文，每个报文含有 64 个字节数据。

-t 检查与指定计算机的连接，直至用户中断本次操作

-a 将 IP 地址解析为主机名

-n count 按照 count 指定的数量发送报文

-l size 按照 size 指定的数量发送报文

-f 在报文中发送“不分段”标志，以保证数据包不被路由器分段

-w timeout 根据 timeout 给出的毫秒数设定等待应答的时间

tracert 通过发送包含不同 TTL 的 ICMP 报文并监听回应报文，来探测到达目的计算机的路径 -d 不将 IP 地址解析为主机名查于计算机的连接

-h maximum-hops 指定最大跳数

-j host-list 按照 host-list 给出的主机列表指出的稀疏源路由来探测。

-w timeout 按照 timeout 给出的毫秒数设定等待应答的时间

pathping 结合了 ping 和 tracert 命令的功能，将报文发送到所经过地所有路由器，并根据每跳返回的报文进行统计。

-p period 指定两次 ping 之间的时间间隔

-q num-queries 指定对每跳的查询次数

-R 查看每跳是否支持 RSVP 协议

route 显示或修改本地 IP 路由表的条目

-f 清除路由表中所有的网关条目

-p 与 add 命令一起使用时，将使增加的路由表项永久有效，即使重新启动系统

command 指定下列一个命令

print 打印理由

add 增加路由表项

delete 删除路由表项

change 修改路由表项

gateway 指定网关的 IP 地址

METRIC 指定路由所需跳数

7. SNMP 主要有管理站、代理和 MIB 组成，其管理模式是一个 Manager/Agent 模型。SNMP 的定义非常简单，并不是每层都定义有管理实体，只在 TCP/IP 协议层上定义了管理实体。

SNMP 采用一种分布式结构，一个管理站可以管理控制多个代理，反之，一个代理也可以被多个管理站控制。为此，SNMP 采用了“实体”这个概念来实现一些简单的控制。

每个团体都被指定拥有了一个团体名。一个团体包含一个代理和若干个管理控制该代理的管理站。他们之间发送、接受报文时都必须使用团体名进行认证，只有团体名正确、认证通过，报文才能被接受。一个团体可以规定具有一种访问模式（主要有 read-only 和 read-write 两种），甚至还可以规定一个管理数据库视阈（仅允许访问管理数据库中部分对象），这个团体内的各管理站只能按照规定的模式访问视阈规定范围内的对象。

一个代理可以设置几个团体，分别和各自团体内的管理站联系。而这些不同可以拥有不同的访问模式和不同的视阈。

如果一个管理站管理控制着多个代理，那么他和这些代理中的每一个都各构成一个团体，通信时使用各自的团体名。即使团体名相同，这些代理之间也没有任何关系，因为他们分别属于不同的团体。

MIB-2 具有树形结构并且被纳入 CMIP 所规定的树结构内。

MIB-2 库中的管理对象可以分为两大类：标量对象（只有一个值）和表对象（一二维表

格），每个表对象下面只有一个子节点，即该表的表项入口，这个子节点下面才是各个列对象。

MIB-2 中对象值的数据类型有简单类型（包括 32 位整数、八个一组的字符串和对象标识符）、应用类型（IP 地址、计数器（counter）、计量器（cauge）、时钟（timeticks））,其中时钟类型用来记录从某个事件的发生开始到目前为止所经过的时间，单位为 0.01 秒。计数器类型是一个非负的整数，从 0 开始逐步增加但不能减少，一直增加到 4294967295（即 $2^{32}-1$），然后回到 0，再从头开始。（SNMPv2 版本中增加了一种 64 位的计数器，其最大值为 $2^{64}-1$）。计量器类型的值可以增加也可以减少，而且增加到最大值以后不归 0，而是不再增加（封顶），但是可以降下来。

SNMP 支持的操作主要有获取（get）、设置(set)、通知(notification)等，每种操作都有相应的 PDU 格式。

get 操作用于管理站向代理查询被管理设备上的 MIB 库数据。又分为 Get 和 GetNext 两个操作，分别查询指定对象的值和查询指定对象的下一个相邻对象的值。当管理站需要查询时，就向某个代理（按其 IP 地址）发出一个包含有“团体名”和“GetRequestPDU”(或是 GetRequestPDU)的报文。这种请求 PDU 的内容就是“请求标识”（一个顺序号）和所谓的“变量绑定表”，也就是指定的一个个对象的标识符及其相应的值。

set 操作用于管理站命令代理对被管设备上 MIB 库中的对象值进行设置（团体名和 setRequestPDU）。只有团体的访问模式是 read-write 的条件下才能实现 Set 操作。

Notifications 操作用于代理主动向管理站报告被管理对象的某些变化。通知又可以分为自陷（Trap）（团体名和 TrapPDU）和通知（Inform,要向发送者回送一条确认信息）两类。

SNMP 与 CMIP 不同点：

1.SNMP 具有广泛的适用性，且在用于小规模设备时成本低、效率高，在实际中一般用于计算机网络管理，而 CMIP 则更适合大型系统，在实际中一般用于电信网络管理。

2.SNMP 主要基于轮询方式获得信息，而 CMIP 主要采用报告方式。

3.对传输服务的要求方面：SNMP 基于无连接的 UDP，而 CMIP 使用面向连接的传输。

4.CMIP 采用面向对象的信息建模方式，而 SNMP 则是用简单的变量表示管理对象。

创建或修改对 SNMP 团体的访问控制，在全局配置模式下：

（config）#snmp-server community<团体名>[view<视阈名>][ro|rw][<访问控制表号>]

其中：团体名是管理人员指定的一个字符串，用于同一团体内的管理站和代理之间进行通信认证。

视阈名是在此之前已经建立的一个视阈的名字，这个视阈规定了本团体内的访问管理信息库的范围。

ro 或 rw 代表访问权限为只读或可读写。

访问控制表号是一个 99 的整数，代表着一个“标准的 ACL”。该 ACL 规定了一个许可访问本路由器代理的 IP 地址范围，即规定哪些 IP 地址的主机是属于这个“团体”的管理站。

建立一个团体，团体名是 public,访问权限为只读，管理站的 IP 地址范围由 4 号 ACL 规定：（config）#snmp-server community public ro 4

建立一个团体，团体名是 admin,访问权限是可读写，访问 MIB 库的范围由视阈 part 规定：（config）#snmp-server community admin view part rw

创建或修改一个 SNMP 视阈：在全局配置模式下：

（config）#snmp-server view<视阈名><对象标识符或子树>{included|excluded}

对象标识符或子树就是在这个视阈中包含（included）或排除(excluded)的 MIB 库对象的标识符。

建立一个视阈，名为 part，它包含 mib-2 整个子树的所有对象。

（config）#snmp-server view part mib-2 included

建立一个视阈，名为 ext,它包括 mib-2 库中系统组的所有对象和 Cisco 私有库的所有对象。 （config）#snmp-server view ext system included

(config)#snmp-server view Cisco included

设置路由器上的 snmp 代理具有发出通知的功能：在全局配置模式下：

（config）#snmp-server enable traps[<通知类型>][<通知选项>]

在某个接口的配置模式下，指定当该接口断开或连接时要向管理站发出通知，命令格式为：（if-config）#snmp trap link-status

设置接受通知的管理站：在全局配置模式下：

（config）#snmp-server host<主机名或 IP 地址>[traps|informs][version{1|2c}]<团体名>[udp-port<端口号>][<通知类型>]

traps 或 informs 用于指定向这台主机发送自陷还是发送通知（缺省为发送自陷）

version1 或 2c 用于指定是哪个版本的 SNMP 发送

udp-port 用于指定这台主机上使用哪个 UDP 端口号接受（缺省为 162）

使该路由器可以向主机 monitor.tj.edu.cn 按照团体名 public 发送消息

（config）#snmp-server enable traps

(config)#snmp-server host monitor.tj.edu.cn public

Windows serbice 2003 提供五种权限：无、通知、只读、读写、读创建。

8.

IP 地址	124.196.27.59
子网掩码	255.224.0.0
地址类别	【1】
网络地址	【2】
直接广播地址	【3】
主机号	【4】
子网内的最后一个可用 IP 地址	【5】

124.196.27.59 01111100 11000100 000110011 00111011

255.224.0.0 11111111 11100000 00000000 00000000 ⟶ 124.192.0.0

【网络地址】

124.196.27.59 01111100 11000100 000110011 00111011

⟶ 01111100 11011111 11111111 11111111 ⟶ 124.223.255.255

【直接广播地址】

⟶ 00000000 00000100 000110011 00111011 ⟶ 0.4.27.59

【主机号】

124.196.27.59 01111100 11000100 000110011 00111011

255.224.0.0 11111111 11100000 00000000 00000000 ⟶

01111100 11011111 11111111 11111111 ⟶ 124.233.255.255

⟶ 124.233.255.254

【子网内最后一个可用 IP 地址】

9. 使用 192.168.1.192/26 划分 3 个子网，其中第一个子网能容纳 25 台主机，另外两个

子网分别能容纳 10 台主机，请写出子网掩码、各子网网络地址及可用的 IP 地址段(9 分)。（注：请按子网序号顺序分配网络地址）

192.168.1.192　　11000000 10101000 00000001 11000000

11111111 11111111　11111111 11000000

11111111 11111111　11111111 11100000　→ 255.255.255.224

【子网 1 掩码】

11111111 11111111　11111111 11110000　→ 255.255.255.240

【子网 2、3 掩码】

11000000 10101000 00000001 11000000

11111111 11111111　11111111 11000000

11111111 11111111　11111111 11011111

11000000 10101000 00000001 11000000 → 192.168.1.192 【子网 1】

11000000 10101000 00000001 11011111 → 192.168.1.223

→ 192.168.1.193 ~ 192.168.1.222 【子网 1 可用 IP】

11000000 10101000 00000001 11000000

11111111 11111111　11111111 11100000【子网 2】

11000000 10101000 00000001 11100000 → 192.168.1.224 【子网 2】

11000000 10101000 00000001 11101111 → 192.168.1.239

→ 192.168.1.225 ~ 192.168.1.238 【子网 2 可用 IP】

11111111 11111111　11111111 11110000【子网 3】

11000000 10101000 00000001 11110000 → 192.168.1.240 【子网 3】

11000000 10101000 00000001 11111111 → 192.168.1.255

→ 192.168.1.241 ~ 192.168.1.254 【子网 3 可用 IP】

10.　网络管理工具

Windows2003 可以实现用户管理、性能管理、网络监视和远程访问管理等。

用户管理：Windows2003 中有两种用户：本地用户和域用户。本地用户信息存储在本地计算机的帐户管理数据库中，用户登录后，只能根据权限访问本地计算机。域用户信息存储在域控制器的活动目录中，用户登录后可以根据权限访问整个域中的资源。

域用户管理是通过工具“Active Directory 用户和计算机”实现的。“Active Directory 用户和计算机”是在配置为域控制器的计算机上安装的目录管理工具，允许在单位的目录中添加、修改、删除和组织 Windows2003 域用户帐户、计算机帐户、安全和通信组以及公布的资源。启用和禁用帐户、移动帐户、用户帐户的重命名、修改用户账号密码、查找用户帐户、修改用户账号属性，以及删除用户帐户。

性能管理：包括系统监视器和性能日志和警报。系统监视器提供有关操作系统特定组件和用于搜集性能数据的服务器程序所使用资源的详细数据，并图形化显示性能监视数据。性能日志和警报提供数据记录能力，当计数器值高于或低于定义的阈值时，警报将通过信使服务告知用户。

远程访问管理。安装 Windows2003 后，系统将本地主机作为路由和远程访问服务器。

补充二：

1. 设计一个宽带城域网将涉及“三个平台一个接口”：即网络平台、业务平台、管理平台与城市宽带出口。

宽带城域网的网络平台的层次结构又可以进一步分为：核心交换层、路由汇聚层、接入层。

核心层主要承担高速数据交换的功能。汇聚层主要承担路由与流量汇聚的功能。接入层主要承担用户接入与本地流量控制的功能。

核心交换层的基本功能：

1）：核心交换层将多个汇聚层连接起来，为汇聚层的网络提供高速分组转发、为整个城域网提供一个高速、安全、与具有 QOS 保障能力的数据传输环境。

2）：核心交换层实现与主干网络的互连，提供城市的宽带 IP 数据出口。

3）：提供宽带城域网的用户访问 Internet 所需要的路由服务。

核心交换层结构设计的重点是它的可靠性、可扩展性和它的开放性。

汇聚层的主要功能：

1）：汇接接入层的用户流量，进行数据分组传输的汇聚、转发与交换。

2）：根据接入层的用户流量，进行本地路由、过流、流量均衡、QOS 优先级管理，以及安全控制、IP 地址转换、流量整形等处理。

3）：根据处理结果把用户流量转发到核心交换层或在本地进行路由处理。

接入层的主要功能：

最后一公里问题，通过各种技术，连接最终用户，为它所覆盖的范围内的用户提供 Internet 以及其他的信息服务。

2.

	下/上行速率(距离 5.5km)	下/上行速率（距离 5.5km）	线对数
ADSL	1.5Mbps/64Kbps	6Mbps/640Kbps	1

ADSL 提供的非对称带宽特性，上行速率在 64~640kbps，下行速率在 500kbps ~ 7Mbps.

3. 无线接入技术主要有：802.11 标准的无线局域网接入、802.16 标准的无线城域网（WMAN）接入，以及正在发展的 Ad hoc 接入技术。

在无线宽带接入网的结构中，远距离采用 802.16 标准的 WiMAX 技术，可以在 50KM 范围内提供最高 70Mbps 的传输速率；近距离采用 802.11 标准的无线局域网 WLAN，可以满足一定地理范围内的用户无线接入需求。802.11 标准重点在于解决局域网范围移动结点通信问题，而 802.16 标准的重点是在于解决建筑物之间的数据通信问题。802.16 标准规定无线网络使用 10~66G 波段的频率。802.11d 主要针对固定的无线网络部署，802.16e 则针对火车、汽车等移动物体的无线通信标准问题。与 IEEE802.16 标准工作组对应的论坛组织为 WiMAX.

无线网格网 WMN 技术技术有两个发展方向，一是军事和特定行业发展和应用，在此基础上产生了无线传感器网络 WSN，一是民用方向，出现了无线网格网 WMN。

推动无线网格网发展的主要动力是 Internet 接入的应用需求。

4. 网络结点地理位置分布情况：用户数量及分布的位置、建筑物内部结构情况调查、建筑物群情况调查。

网络应用主要包括：Internet/Intranet 服务、数据库服务、网络基础服务（包括网络管理和服务软件、网络安全管理软件）。

网络需求详细分析主要包括：网络总体需求分析、综合布线需求分析、网络可用性与可靠性分析、网络安全性需求、以及分析网络工程造价估算。

网络系统方案设计阶段要完成以下任务：网络建设总体目标、网络系统方案设计原则、

网络系统总体设计、网络拓扑结构、网络设备选型、网络系统安全设计。

核心层网络一般要承载整个网络流量的 40%~60%

层次之间，上联带宽与下一级带宽之比一般控制在 1：20

5. 网桥：网桥在数据链路层完成数据帧接受、转发与地址过滤功能，它用来实现多个局域网之间的数据交换，使用网桥实现数据链路层的互连时，允许互连网络的数据链路层与物理层协议不同。网桥具有几个基本特征：能够互联两个采用不同数据链路层协议、不同传输介质与不同传输速率的网络；网桥以接收、转发与地址过滤的方式实现互联网络之间的通信。

网桥仍需要解决同种标准中不同传输速率的局域网在 MAC 层互联问题。

根据网桥的帧转发策略可以分为透明网桥和源路由网桥。

依据网桥的端口数来分类，可以分为双端口与多端口网桥。

依据网桥的连接线路来分，可以分为普通局域网网桥、无线网桥和远程网桥。

网桥最重要的维护工作是构建和维护 MAC 表

透明网桥主要有一下几个特点：透明网桥由每个网桥自己来进行路由选择，局域网上的各结点不负责路由选择，网桥对于互联网的各结点是“透明”的；透明网桥一般用于两个 MAC 层协议相同网段之间的互联；它最大的优点是容易安装，是一种即插即用设备。

透明网桥的 MAC 表要记录三类信息：站地址、端口和时间。

为了防止网桥互联的网络出现“环状结构”，透明网桥使用了生成树算法。

根网桥是从网络中选择的一个作为属性拓扑的树根，最短路径开销是一个网桥到达根网桥的最短路径；指定网桥负责转发到根网桥的数据；对于每一个非根网桥，都需要从它的端口中选择一个距离跟网桥距离最短的端口做为指定端口，负责将本网桥的数据发送到根网桥，这个端口就叫做指定端口，一个网段中只有一个指定端口；生成树协议为每一个网段选择一个指定端口，那么其他端口均处于阻塞状态，因此叫做阻塞端口。

网桥存在的两个主要问题是帧转发速率低与广播风暴，评价网桥性能的参数主要有真过滤速率与帧转发速率。

6. 交换机 STP 配置

打开或关闭 STP:Switch-PHY-3548(config)#spanning-tree vlan3

Switch-PHY-3548(config)#no spanning-tree vlan3

Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree enable 3

VLAN3 bridge spanning tree enabled

Switch-PHY-6500>(enable)set spantree disable 3

VLAN3 bridge spanning tree disabled

Switch-PHY-6500>(enable)

配置根网桥和备份根网桥：

设置主 root(primary root)

Switch-PHY-3548(config)#spanning-tree vlan 3 root primary

Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree root 1,200-204

设置备份 root

Switch-PHY-3548(config)#spanning-tree vlan 3 root secondary

Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree root secondary 1,200-204

配置生成树优先级：生成树优先级的取值范围是 0~61440，增量是 4096。优先级的值越小优先级越高，如果优先级为 0 是最高优先级，61440 优先级最低。

Switch-PHY-3548(config)#spanning-tree vlan 3 priority 8192
Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree priority 8192
Switch-PHY-6500>(enable)

配置 BackboneFast 生成树可选功能：

按生成树的一般规则，交换机的阻塞端口在转换成转发工作状态之前，需要等待一个生成树最大存活时间（spantree maxage）,而 BackboneFast 的功能就是阻塞端口不再等待这段时间，而是直接将端口由侦听和学习状态转为转发状态，这个转换任务大约需要 30s，从而提高了在间接链路失效情况下的收敛速度。

Switch-PHY-3548(config)#spanning-tree backbonefast
Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree backbonefast enable
Switch-PHY-6500>(enable)

配置 UplinkFast 生成树可选功能：

UplinkFast 的功能是当生成树拓扑结构发生变化和在使用上连链路组（uplink group）的冗余链路之间完成负载平衡时，提供快速收敛。

当出现直接链路失效时，UplinkFast 就将交换机上处于阻塞状态的端口跳过侦听和学习两种状态，直接转换到转发状态，这个转换过程大约只需要 1~5min。

Switch-PHY-3548(config)#spanning-tree uplinkfast max-update-rate 32000
Switch-PHY-3548(config)#spanning-tree uplinkfast
Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree uplinkfast enable
Switch-PHY-6500>(enable)set spantree uplinkfast enable rate 40

配置 PortFast 生成树可选功能：

PortFast 用于在接入层交换机端口上跳过正常的生成树操作，加快终端工作站接入到网路中的速度。它的功能是使交换机的端口跳过侦听和学习状态，直接由阻塞状态跳到转发状态。该端口一般只能用于连接单个主机或是服务器，不能连接集线器、集中器、交换机、网桥等设备。如果在配置了 PortFast 的交换机端口上连接这些设备，将可能造成暂时的生成树循环。因此，一般在所有连接计算机的端口上启用 PortFast，在所有连接交换机或未使用的端口上禁用 PortFast.　Switch-PHY-3548(config)#spanning-tree portfast default
Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree portfast 3/2 enable
Switch-PHY-6500>(enable)set spantree portfast 4/1-24 enable

配置 BPDU Fliter 生成树可选功能：

BPDU Fliter 会使交换机在指定的端口上停止发送 BPDUs，对于进入这个端口的 BPDUs 也不做任何处理，同时立刻将端口状态转化为转发状态。

Switch-PHY-3548(config)#spanning-tree portfast bpdufliter default
Switch-PHY-3548(config)#

Switch-PHY-6500>(enable)set spantree portfast bpdu-fliter enable
Switch-PHY-6500>(enable)set spantree portfast bpdu-fliter 3/1-24 enable

6. 加密技术：

密码技术包括密码编码学与密码分析学。

加密的基本思想是伪装其明文一隐藏其真是的内容。伪装明文的操作称作加密，加密

时所使用的变换规则成为加密算法。由密文恢复出原明文的过程成为解密，解密时所采用的信息变换规则成为解密算法。

现代密码学的一个基本规则是一切秘密寓于密钥之中。加密算法是可以公布的，而真正需要保密的是密钥。

对称加密算法中 N 个用户之间进行加密通信时，则需要 N×(N-1)个密钥。

数据加密标准（DES）是对称加密算法。其中 8 位用于奇偶校验，用户可以使用其中的 56 位，总共 64 位。目前，比 DES 算法更安全的对称加密算法如 IDEA 算法、RC2 算法、RC4 算法与 Skipjack 算法。

非对称加密技术可以防止用户对所发出的信息和接受信息在事后抵赖，并且保证了数据的完整性。可以实现多个用户发送的密文，只能由特定的接受方自己解读。如果以用户的私鈅作为加密密钥，而以公钥作为解密密钥，则可以实现由一个用户加密的消息能够被多个用户解读，这样非对称密钥密码就可以用于数字签名。

非对称加密技术中 N 个用户之间进行通信加密，仅需要 n 对密钥就可以了。常用的加密算法有 RSA 算法、DSA 算法、PKCS 算法与 PGP 算法。

RSA 算法体制的理论基础是寻找大素数是容易的，而分解两个大素数在计算上是不可行的。（大素数分解）

8.

IP 地址	126.150.28.57
子网掩码	255.240.0.0
地址类别	【 1 】
网络地址	【 2 】
直接广播地址	【 3 】
受限广播地址	【 4 】
子网内的第一个可用 IP 地址	【 5 】

126.150.28.57 10000000 10010110 00011100 00111001

255.240.0.0 11111111 11110000 00000000 00000000 ⟶ 126.144.0.0 【网络地址】

⟶ 126.144.0.1【第一个可用 ip】

10000000 10010110 00011100 00111001

10000000 10011111 11111111 11111111 ⟶ 126.158.255.255【直接广播地址】

9. 使用 IP 地址 202.113.10.128/25 划分 4 个相同大小的子网,每个子网中能够容纳 30 台主机,请写出子网掩码、各个子网网络地址及可用的 IP 地址段。（10 分）

202.113.10.128 11001010 01110001 00001010 10000000

11111111 11111111 11111111 10000000

11111111 11111111 11111111 11100000 ⟶ 255.255.255.224【掩码】

11001010 01110001 00001010 10000000 ⟶ 202.113.10.128【子网 1 网络地址】

11001010 01110001 00001010 10011111 ⟶ 202.113.10.159

⟶ 202.113.10.129 ~ 202.113.10.158

11001010 01110001 00001010 10100000 ⟶ 202.113.10.160【子网 2 网络地址】

11001010 01110001 00001010 10111111 ⟶ 202.113.10.191

⟶ 202.103.10.161 ~ 202.103.10.190

11001010 01110001 00001010 11000000 ⟶ 202.103.10.192【子网 3 网络地址】

11001010 01110001 00001010 11011111 ⟶ 202.103.10.223

⟶ 202.103.10.193 ~ 202.103.10.222

11001010 01110001 00001010 11100000 ⟶ 202.103.10.224【子网 4 网络地址】
11001010 01110001 00001010 11111111 ⟶ 202.103.10.255
⟶ 202.103.10.225 ~ 202.103.10.254