16级软件工程一班 田金东

2018年9月

**网络技术知识点总结**

**计算机三级网络技术**

# 第一章 网络系统结构与设计基本原则

## 一．核心交换层、边缘汇聚层与用户接入层的主要功能

* 核心交换层

核心交换层提供宽带城域网的用户访问Internet所需要的路由服务。

* 汇聚层

进行本地路由

## 二．服务质量QoS要求的技术主要有

1. 资源预留（**RSVP**）
2. 区分服务（**Diff-Serv**）
3. 多协议标记交换（**MPLS**）

## 三．管理宽带城域网的三种基本方案

1. 带内网络管理

利用传统电信网络进行网络管理称为“带内”。

1. 带外网络管理

利用IP网络及协议进行网络管理称为“带外”。可以利用SNMP实现带外网络管理。

1. 同时使用带内和带外网络管理

## 四．基于弹性分组环RPR技术的城域网

* 弹性分组环是一种用于直接在光纤上高效传输IP分组的传输技术，它的工作基础是**动态分组传送（DPT）**技术。

1. 弹性分组环技术采用**双环结构**。
2. 两个RPR节点之间的裸光纤最大长度可以达到100KM。
3. 顺时针传输的是外环，逆时针传输的是内环。
4. 内环和外环都采用**统计时分多路复用**的方法传输IP分组，同时可以实现“自愈环”的功能。
5. RPR内外环都可以传输数据分组与控制分组。

* **RPR技术特点**

1. 带宽利用率高

在传统FDDI环网中，源节点向目的节点成功发送数据帧后，这个数据帧要由源节点从环中收回。而在RPR环中就不会收回。

1. 公平性好

RPR环中每一个结点都执行**SRP公平算法。**

1. 快速保护和恢复能力强

能在**50ms**内隔离故障结点光纤段完成自愈。

## 六．三网融合

1. 计算机网络
2. 电信网络
3. 广播电视网

## 七．数字用户线xDSL接入技术

下行/上行 5KM 下行/上行 3.6KM

* ADSL（非对称） 1.5Mbps/64Kbps 6Mbps/640Kbps
* HDSL（对称） 1.544Mbps 1.544Mbps

## 八．光纤同轴电缆混合网（HFC）

1. 光纤结点：将光纤干线与同轴电缆分配线相连接。
2. 光纤结点通过同轴电缆下引线可以为500-2000个用户服务
3. 从用户角度看，光纤到同轴电缆混合网是经过双向改造的有线电视网络。

## 九．电缆调制解调器（Camble Model）

Camble Modem把用户计算机与有线电视同轴电缆连接起来。

Camble Modem 采用**频分复用**将信道分为上行与下行信道。

## 十．光纤接入技术

OC-3 51.84\*3 Mbps

OC-12 51.84\*12Mbps

## 十一. 宽带无线接入技术

**802.16标准的无线城域网**

* 1. 802.16标准主要制定2-66MHZ频段的规范。
  2. 802.16d（不动）主要针对固定的无线网络部署。
  3. 802.16e（移动）主要针对火车，汽车等移动物体。
  4. 802.16标准组对应的论坛组织为WiMAX。
  5. 802.16最高传输速率为**134Mbps**

**802.11标准无线局域网**

1. 802.11a 54Mbps
2. 802.11b 11Mbps
3. 802.11定义了使用红外、跳频与直接序列扩频技术。

## 十二. 宽带接入技术总结

# 第二章 中小型网络系统总体规划

## 一．网络需求详细分析

1. 网络总体需求分析
2. 综合布线需求分析
3. 网络可用性与可靠性分析
4. 网络安全性需求分析
5. 网络工程造价估算

## 二．网络总体设计方法

网络设计通常分为三层：核心层、汇聚层、接入层。

* 如果结点数为250-5000个，一般需要按三层结构来设计
* 如果结点数为100-500个可以不必设计接入层网络
* 如果节点数为5-250个可以不设计接入层与汇聚层网络

**核心层网络结构设计**

核心层网络一般要承担整个网络流量的40%-60%。目前应用于核心层网络的技术标准主要是GE/10GE，核心设备是高性能交换路由器，连接核心路由器的是具有冗余链路的光纤。

**汇聚层网络与接入层网络就结构设计**

* 人们经常采用多个并行的GE/10GE交换机堆叠的方式来扩展端口密度。
* 上联带宽与下联带宽之比一般控制在1:20

## 三．路由器选型依据

路由器一般根据路由器背板交换能力来划分。背板交换能力大于40Gbps的称为高端路由器，背板能力低于40Gbps的称为中低端路由器。

**路由器关键技术指标**

1. **吞吐量**

吞吐量是指路由器的包转发能力。路由器的包转发能力与路由器端口数量、端口速率、包长度、包类型有关。

1. **背板能力**

传统的路由器采用的是共享背板的结构，高性能路由器一般采用交换式结构。背板能力决定路由器的吞吐量。

1. **丢包率**

丢包率是指在稳定持续负荷情况下，由于包转发能力的限制而造成的包丢失概率。丢包率是衡量路由器超负荷工作时的性能指标之一。

1. **延时与延时抖动**

延时：第一个比特进入路由器，到该帧最后一个比特离开路由器所经历的的时间间隔。（高速路由器一般要求长度为1518B的IP包，延时小于1ms）

延时抖动：延时抖动是指延时的变化量。语音、视频业务对延时抖动要求较高。

1. **突发处理能力（以速率为单位）**

突发处理能力是指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的。

1. **路由表容量**
2. **服务质量**
3. **网管能力**
4. **可靠性与可用性**

**典型的高端路由器的可靠性与可用性指标应达到：**

1. **无故**障连续工作时间（MTBF）大于十万个小时
2. 系统故障恢复时间小于30分钟
3. 系统具有自动保护切换功能，主备用切换时间小于50ms
4. SDH与ATM接口自动保护切换功能，切换时间小于50ms
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部件需要有热插拔冗余备份，线卡要求有备份，并提供远程测试诊断能力
6. 路由器内部不存在单点故障

## 四．交换机分类与主要技术指标

**全双工端口的带宽**

**全双工端口的计算方法：端口数\*端口速率\*2**

**交换机的交换模式可以分为三种**

1. 快速转发直通式，交换机收到帧的前14个字节，前七个字节为前缀，一个字节的帧起始和六个字节的目的地址时就立刻转发帧。
2. 碎片丢弃式：它不保存整个数据帧，只接收364个字节，就开始转发帧。如果帧长度小于64个字节，则被视为碎片，交换机将直接丢弃。
3. 存储转发式：转发前将整个帧读入到内存中。

## 五．网络服务器

1. 网络服务器从应用角度分类：文件服务器、数据库服务器、Internet通用服务器与应用 服务器等。
2. 网络服务器从硬件角度分类：基于CISC处理器的Intel结构的PC服务器

基于RISC结构处理器的服务器

小型机服务器

1. 各种大型、中型计算机和超级服务器都是RISC结构处理器，操作系统是UNIX。
2. 企业级服务器一般支持4-8个CPU，采用对称多处理（SMP）技术。对称多处理技术可以在多个CPU结构的服务器中均衡负荷。
3. **集群技术**：如果其中一台主机出现故障，它所运行的程序立即转移到其它主机，因此集群技术可以大大提高服务器的可靠性、可用性与容灾能力。
4. 评价高性能存储技术的指标主要是存取I/O速度和磁盘容量。由于服务器容量不断增大，硬盘的存取速度经常会成为服务器的瓶颈。要解决这个问题就必须采用小型机系统接口（SCSI）标准。同时采用**独立磁盘冗余阵列（RAID）**技术，将若干硬盘驱动器组成一个整体，由阵列管理器管理。提高硬盘的存取速度和吞吐量。通过磁盘的容错处理，提高系统的可靠性。
5. **热插拔技术**：热插拔技术允许用户在不切断电源的情况下，更换存在故障的硬盘、板卡等部件。

**系统的高可用性**

系统的高可用性=

MTBF为平均无故障时间，MTBR为平均修复时间。

如果系统可用性达到99.9%，那么每年的停机时间<=8.8小时；

如果系统可用性达到99.99%，那么每年的停机时间<=53分钟；

如果系统可用性达到99.999%，那么每年的停机时间<=5分钟；

# 第三章 IP地址规划设计技术

## 一．IP地址分类

A类：1.0.0.0——127.255.255.255

B类：128.0.0.0——191.255.255.255

C类：192.0.0.0——223.255.255.255

## 二．地址的特殊形式

1. 直接广播地址

网络号不变，主机号全为1

1. **受限广播地址**

255.255.255.255

1. 主机地址

网络号全为0，主机号不变

1. 回送地址

## 三．子网划分

在子网划分中，子网号可以全零或全一，但主机号不能全0和全1.。

## 四．IPv6地址

1. IPv6地址表示方式：16位分为一段，一共有8段，每段用4个十六进制数表示，段与段之间用冒号隔开。
2. 前导零压缩法：双冒号在一个地址中只能出现一次，不能压缩有效的“零”。
3. IPv6不支持子网掩码，只支持前缀长度表示法。

# 第四章 路由设计基础

## 一．Internet路由选择协议



## 二．路由信息协议RIP

路由信息协议（RIP）它是一种分布式、基于**距离向量**的路由选择协议。适用于相对较小的自治系统，它们的直径“跳数”一般小于15。

路由信息协议（RIP）的思想：它要求路由器**周期性地**向外发送路由刷新报文。

路由信息协议的工作过程：

1. 没有的表项，学习目的网络，距离加一，路由指向被学习的路由器。
2. 已有的路由表项，若更新的路由距离加一比原先小，则距离加一后学习，并将路由指向被学习的路由器。如果距离比原先的大，则不学习。

## 三．最短路径优先协议OSPF

主要特点：

1. OSPF最主要特征就是使用**分布式链路状态协议**，而RIP使用的是距离向量协议。
2. OSPF协议要求路由器发送的信息是本路由器与哪些路由器相邻，以及链路状态的度量。链路状态的“度量”主要指费用、距离、延时、带宽等。
3. OSPF协议要求当链路状态发生变化时采用**洪泛法**向**所有路由器**发送此信息。
4. 在执行OSPF协议的路由器中都能建立一个链路状态信息库，这个数据库实际上就是**全网的拓扑结构图**
5. 为了适应规模很大的网络，并使更新过程收敛的很快，OSPF协议将一个自治域再划分成若干个更小的范围，叫做“区域”。每一个区域有一个32位的标识符，在一个区域内的路由器不超过200个。
6. 划分区域后，路由器只知道自己所在区域的网络拓扑，而不知道其他区域的网络拓扑情况。
7. 为了使每一个区域能够和别的区域进行通信，OSPF使用层次结构的区域划分。他将一个自治系统内部划分成若干区域与主干区域。主干区域连接多个区域，主干区域内部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。在主干区域中专门与自治域之外的其它自治域进行通信的路由器叫做自治域边界路由器。
8. 链路状态的度量包括：费用、距离、收敛时间、带宽等。

## 四．边界网关协议BGP

1. 外部网关协议是不同自治系统的路由器之间交换路由信息的协议。
2. BGP-4采用**路由向量**路由协议
3. 在配置BGP时，每个自治系统的管理员要选择至少一个路由器（一般是BGP边界路由器）作为该自治系统的“**BGP发言人**”。一个BGP发言人与其他自治系统中的BGP发言人要交换路由信息，就必须建立TCP连接。
4. 在BGP刚刚运行时，BGP边界路由器与相邻边界路由器交换整个的BGP路由表。但以后只需要在发生变化时更新有变化的部分。

BGP路由选择协议的四种分组（英文也要记）

1. 打开分组（open）

打开分组用来与相邻的另一个BGP发言人建立关系。

1. 更新分组（update）

更新分组用来发送某一路由信息，以及列出要撤销的多条路由。

1. 保活分组（keepalive）

保活分组用来确认打开报文，以及周期性的证实相邻边界路由器的存在。

1. 通知分组（notification）

通知分组用来发送检测到的差错

**两个BGP发言人彼此要周期性的（一般是每个30秒）交换保活分组**。“更新分组”是BGP协议的核心。

# 第五章 局域网技术

## 一．虚拟局域网组网定义方法

1. 用交换机端口号定义虚拟局域网

2. 用Mac地址定义虚拟局域网

3. 用网络层地址定义虚拟局域网

4. 基于IP广播组的虚拟局域网

## 二．以太网组网的具体方法

**传统以太网物理层标准的命名方法是：IEEE 802.3 x Type-y Name。**

x表示：数据传输速率，单位：Mbps

y表示：网段的最大长度，单位：100m

Type表示：传输方式是基带还是频带

Name表示：局域网的名称

**10BASE-T标准以太网组网**

1. 10BASE-T物理层标准要求采用非屏蔽双绞线
2. 目前组建以太网几乎都采用10BASE-T标准，使用集线器、非屏蔽双绞线和RJ-45接口。
3. 集线器是以太网的中心连接设备
4. 集线器依然工作在物理层
5. **同一个“冲突域”在任何一个时间段中，只能有一个节点可以发送数据帧，而其他结点只能处于接收状态。**

**快速以太网组网**

快速以太网即100Mbps以太网，1995年正式批准快速以太网协议标准，IEE 802.3u

**快速以太网物理层标准**

1. 100BASE-TX：使用2对5类非屏蔽双绞线，最大长度100m，**一对**双绞线用于发送，**另一对**双绞线用于接收；数据传输采用4B/5B编码方式；采用**全双工方式**工作。
2. 100BASE-T4：使用4对3类非屏蔽双绞线，最大长度100m，三对双绞线用于数据传输，一对双绞线用于冲突检测；数据采用8B/6T编码方法；采用**半双工方式**工作。
3. 100BASE-FX：使用**两条光纤**（F表示光纤），最大长度为415m，一条光纤用于发送，另一条光纤用于接收；数据传输采用4B/5B-NRZI编码方法，采用**全双工方式**工作。

## 三．局域网互联设备类型

* **中继器**

中继器只能起到对传输介质上信号波形的接收、放大、整形与转发的作用，这是物理层的功能。中继器工作在物理层，只能用于连接物理协议相同的局域网。

* **集线器**

1. 在网络链路中串接一个集线器可以监听该链路中的数据包。
2. 集线器工作在物理层
3. 连接到一个集线器的**所有节点共享一个冲突域**，这些结点不能同时发送数据，但可以同时接收数据。
4. 当一个结点需要发送数据时，它将执行CSMA/CD介质访问控制方法。

* **网桥**

1. **网桥基本概念**
2. 网桥工作在数据链路层。
3. 网桥在数据链路层完成数据帧的接收、转发与地址过滤功能，它将用来**实现多个局域网之间的数据交换**。
4. **网桥可以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。**
5. **网桥最重要的维护工作是构建和维护MAC地址表。MAC地址表记录不同结点与网桥转发端口的关系。**
6. **网桥分类**
7. 根据网桥的帧转发策略类分类，可以分为透明网桥与源路由网桥。
8. 根据网桥端口数来分类，可以分为双端口网桥与多端口网桥
9. 根据网桥的连接线路来分类，可以分为普通网桥、无线网桥、远程网桥。
10. **透明网桥的特点**
11. 透明网桥的标准是IEEE 802.1d
12. **透明网桥一般用于两个MAC层协议相同的网段之间的互联**
13. 透明网桥最大的优点是容易安装，他是一种即插即用的设备。
14. **生成树算法与协议**

生成树算法是为了避免网桥互联的网络中不出现环状结构。

根据生成树算法制定的协议称为生成树协议（STP） 。生成树协议可以从网络拓扑中清除数据链路层的环路。它能够逻辑的阻断网络中存在的冗余链路，消除路径中的环路，并可以在活动路径出现故障时，重新激活冗余链路来恢复网络连通，保证网络的正常工作。

* **交换机**

局域网交换机可以在它的多个端口之间建立多个并发连接。典型的交换式局域网是交换式以太网，它的核心部件是以太网交换机。

局域网交换机的三个功能：

1.建立和维护MAC地址表和交换机端口的对应关系；

2.在发送节点与接收节点建立虚连接；

3.完成数据帧的转发和过滤。

连接在二层交换机上的不同vlan成员不能直接通讯（VLAN用于隔离广播域的）

## 四．综合布线子系统设计

1. 信息插座大致可分为嵌入式安装插座（暗座）、表面安装插座和多介质信息插座（光纤和铜缆）。其中嵌入式安装插座是用来连接双绞线的，**多介质信息插座是用来连接铜缆和光纤**。
2. UTP是非屏蔽双绞线，STP、FTP、SFTP双绞电缆都是有屏蔽层的屏蔽线缆。UTP价格便宜，但抗干扰性不如有屏蔽线缆。
3. 在设备连接器采用不同信息插座的连接器时，可选用专用电缆或适配器。
4. **当在单一信息插座上进行两项服务时，宜采用“Y”型适配器或一线两用器**。
5. 在配线（水平）子系统中选用的电缆类别不同于设备所需的电缆类别时，宜采用适配器。
6. 在连接使用不同信号的数模转换或速率转换装置时，宜采用适配器。
7. **水平布线子系统电缆长度应该在90m以内**
8. 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。

**建筑群子系统设计**

1. 架空布线：成本低，但影响美观，保密性、安全性、灵活性差。
2. 巷道布线：利用原有管道进行布线。如下水道
3. 直埋布线：直埋布线应该埋在距离地面60cm以下的地方。
4. 管道内布线法：这种方法对电缆提供了最好的机械保护。

# 第六章 交换机配置

## 一．生成树协议STP

生成树协议STP是一个二层链路管理协议。它主要保证网络中没有回路产生。

STP的基本工作原理：通过在交换机之间传送“网桥协议数据单元”（BPDU），并用生成树算法（STA）对其进行计算。**IEEE802.1d标准规定了STP协议**。

BPDU数据包有两种类型：

1. 一种是包含配置信息的**配置BPDU（不超过35字节）**
2. 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）**

## 二．优先级

优先级的取值范围 **0-61440**

**数值越小，优先级越大**

增量值是 **4096**

## 三．VLAN技术

1. VLAN工作在OSI参考模型的第二层（数据链路层）
2. VLAN ID用12bit表示，可以支持4096个。1-1005是标准范围，1025-4096是扩展范围。其中**可用于以太网的是1-1000。**
3. VLAN Name 用32个字符表示。缺省的VLAN name用VLAN ID生成。（VLAN00XXX “XXX”是VLAN ID）

# 第七章 路由器配置

一．路由器分组转发工程中，数据包中包含的是**目的主机**IP地址和**下一跳路由器**物理地址。

二．如果配置**默认路由**时IP地址要填写下一跳IP地址。

# 第八章 无线局域网设备安装与调试

## 一．蓝牙技术与标准

1. 工作频段：2.402GHz-2.480GHz。（2.4GHz）
2. 双工方式：TDD
3. 标称数据率：1Mbps
4. 异步信道速率：**非对称连接723.2kbps/57.6kbps**

**对称连接433.9kbps（全双工模式）**

1. 同步信道速率：**64kbps（3个全双工信道）**
2. 发射功率及覆盖：0dBm（1mW），覆盖1-10m；

20dBm（100mW），覆盖扩展至100m

1. 调频速率：1600次/s
2. 秘钥：以8bit单位增减，最长128bit。

## 二．HiperLAN技术标准

1. HiperLAN/1标准采用5G射频频率，上行20Mbps的速率。
2. HiperLAN/2上行速率可以达到54Mbps。HiperLAN/2系统同时兼容3G标准。
3. HiperLAN/2在典型的网络拓扑结构中，一个AP（接入点）所覆盖的区域称为一个小区，一个小区覆盖范围在**室内一般为30m，在室外一般为150m**。
4. HiperLAN/2技术特点：采用先进的**OFDM调制技术**；HiperLAN/2网络中数据传输是**面向连接**的。

## 三．IEEE 802.11标准

1. **IEEE 802.11标准基本概念**
2. 802.11定义了两种类型的设备：**无线结点**和**无线接入点**。无线接入点的作用是提供无线和有线网络之间的桥接。
3. 802.11最初定义的3个物理层包括两个扩频技术（FHSS、DSSS）和一个红外传播规范，无线传输的频道定义在2.4GHz的**ISM波段**内。
4. 802.11无线标准定义的传输速率是1Mbps和2Mbps
5. CSMA/CA利用ACK信号来避免冲突的发生。
6. 802.11在MAC层引入了一个新的（PTS/CTS）选项。

|  |  |  |  |
| --- | --- | --- | --- |
| 属性 | 802.11b | 802.11a | 802.11g |
| 最大数据传输速率 | 11Mbps | 54Mbps | 54Mbps |
| 最大容量 | 33Mbps | 432Mbps | 162Mbps |
| 实际吞吐量 | 5-7Mbps | 28-31Mbps | 28-31Mbps（全部在802.11g环境下）  10-12Mbps（与802.11b客户端混合的环境） |
| 与802.11b的后向兼容性 | **是**  在**2.4GHz ISM频段**上运行 | **否**  在**5GHz UNII频段**上运行 | 是  在**2.4GHz ISM频段**上运行 |
| 室内距离 | 100m | 与802.11b和802.11g相比，在30m内有更快的速度 | 与802.11b相比在30m内有更快的速度 |

1. **.IEEE 802.11b的基本运作模式**
2. 点对点模式（Ad hoc）：指无线网卡和无线网卡之间的通讯方式。**点对点模式最多可连接256台PC**。
3. 基本模式：指无线和有线网络并存时的通讯方式。**基本模式一个接入点最多连接1024台PC**，接入点可作为无线网和有线网的桥梁。

## 四．常用无线局域网设备

**无线网桥、无线路由器和无线网关**

**无线网桥主要连接几个不同的网段。**无线路由器和无线网关是具有路由功能的AP，一般情况下它具有NAT功能。

## 五．无线接入点的安装和调试

**无线接入点的功能是集合有线或无线终端**

思科公司的Aironet 1100系列接入点是一款无线局域网收发器，**兼容IEEE 802.11b和IEEE 802.11g**，**工作在2.4GHz频段**。Aironet 1100系列无线接入点使用**Cisco的IOS操作系统**。

将接入点接入网络，需要先向管理员询问一下信息，用于配置无线接入点：

1. 系统名
2. 无线网络中对大小写敏感的服务集标识符（SSID）
3. 如果没有连接到DHCP服务器，则需要为接入点指定一个唯一的IP地址
4. 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
5. 使用SNMP时的SNMP集合名称以及SNMP属性。

配置接入点

1. 第一次配置无线接入点时，因为没有连接DHCP服务器所以无法获得IP地址，它的默认IP地址为10.0.0.1
2. 接入点可以配置多达**20个**10.0.0.X范围的IP地址。
3. 使用**五类双绞线**连接PC和无线接入点
4. 确认PC获得10.0.0.x网段的地址
5. 输入大小写敏感的密码Cisco然后按回车，或者点击确定。这时会出现接入点汇总的页面。**点击“Express Setup”进入快速配置页面**。
6. 根据管理员提供的信息，输入各项配置信息，各个配置数据的含义如下：

Radio Service Set ID：SSID是客户端设备用于访问接入点的唯一标识。区分大小写。

Broadcast SSID in Beacon：设定允许设备不指定SSID而访问接入点。其中**YES是默认值**，允许设备不指定SSID访问接入点

# 第九章 网络信息服务系统的安装与配置

## 一．DNS服务器

1. 正向查找区域（用于将域名解析为IP4地址）
2. 反向查找区域（将IP地址映射到域名的数据库）
3. 资源记录
4. 转发器

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。

1. DNS服务器的根DNS服务器**不需要**手动配置。
2. 使用**nslookup命令**可以测试正向和反向查找。

## 二．DHCP服务器

保留：保留地址可以使用作用域地址范围中的任何IP地址，即使该IP地址同时还位于某个排除范围内。

## 三．WWW服务器

浏览器与服务器之间传输信息的协议是HTTP，使用TCP协议，默认端口80

## 四．FTP服务器

用户登录时不需要输入密码，这种FTP服务称为匿名FTP服务。

21端口用于建立数据连接

20端口用于数据传输（TCP连接）

域：一个域是由IP地址和端口号唯一识别的。

## 五．安装DNS服务器

1. 执行ip config /flushdns可以清除DNS缓存。
2. 安装DNS服务器时，根服务器被自动加入到系统中。
3. 正向查找区域自动增加主机的指针记录，而反向查找域可以手动增加主机的指针记录。
4. DNS服务器的地址必须为静态IP，不能为动态IP。
5. 动态更新类型：
6. 只允许安全的动态更新
7. 允许非安全和安全动态更新
8. 不允许动态更新
9. 在nslookup命令提示符“>”下输入域名[ftp.abc.com完成域名到Ip](ftp://ftp.abc.com完成域名到Ip)地址的转换；也可以输入IP地址到域名的转换。（既可以正向查找，也可以反向查找）

## 六，安装DHCP服务器

1. DHCP服务器负责多个网段IP地址分配时，需要配置多个作用域。
2. 在添加排除对话框中，添加排除的IP范围（排除一个IP则不用写范围，并且排除地址不需要写MAC地址）
3. 在添加保留对话框中，输入保留名称IP地址、MAC地址（与排除不同的是，保留必须填写MAC地址）
4. 保留地址可以使用作用域地址范围中的任何IP地址（包括排除地址）

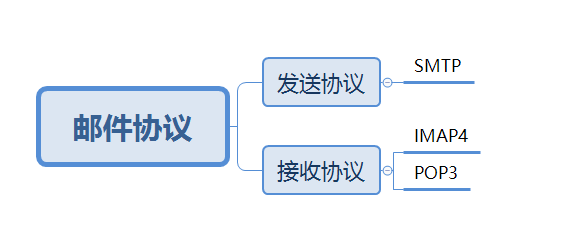
## 七．安装WWW服务器

1. Web站点可以配置动态IP，也可以配置静态IP。
2. Web站点必须为每个站点指定一个主目录，当然也可以是虚拟目录
3. 设置目录安全选项：
4. 身份验证和访问控制
5. IP地址和域名限制
6. 安全通信
7. 设置性能选项
8. 带宽限制
9. 网络连接（客户端Web连接数量）
10. 同一服务器上的多个网站可以使用如下标识符
11. 主机头名称
12. IP地址
13. 非标准TCP端口号

## 八．安装FTP服务器

1. 初始状态下，FTP服务器无管理员密码。
2. Serv-U FTP服务器中的每个虚拟服务器由IP地址和端口号唯一识别。
3. 创建域
4. 配置域的存储位置时，小的域应选择.INI文件存储，而大的文件应选择注册表存储。
5. IP地址为空时，意为服务器所有的IP地址，当服务器有多个IP地址或使用动态IP地址时，IP地址为空比较方便。
6. 新用户的添加必须由管理员来操作。
7. FTP服务器的端口号缺省是21
8. 添加匿名用户：在用户名称文本对话框中输入anonymous（手动添加）
9. 最大上传速度和最大下载速度是整个FTP服务器的带宽。
10. 用户配额选项可以限制用户上传信息占用的存储空间。

## 九．安装Email服务器



1. Winmail邮件服务器支持基于Web方式的访问和管理，**因此在安装邮件服务器之前，要安装IIS**。
2. Winmail邮件管理工具包括：系统设置、域名设置、用户和组、系统状态、系统日志。
3. 在快速设置向导中创建新用户：

输入新建用户信息，包括用户名、域名及用户密码，

1. 域名设置：

在域名管理界面中，可以增加新的域、删除已有的域，还可以对域的参数进行修改，例如：是否允许在本域中自行注册新用户等。

1. 邮件交换机的配置：

为了能够使其他邮件服务器将收件人为“用户名@mail.abc.com”的邮件转发到该邮件服务器，需要建立邮件路由，即在DNS服务器中建立邮件服务器**主机记录**和**邮件交换机记录**。

# 第十章 网络安全技术

## 一．备份策略

1. 完全备份：

完全备份是指对整个系统或用户指定的所有文件数据进行一次完全的备份。

1. 增量备份：

在偶尔进行完全备份后频繁的进行增量备份。

1. 差异备份：

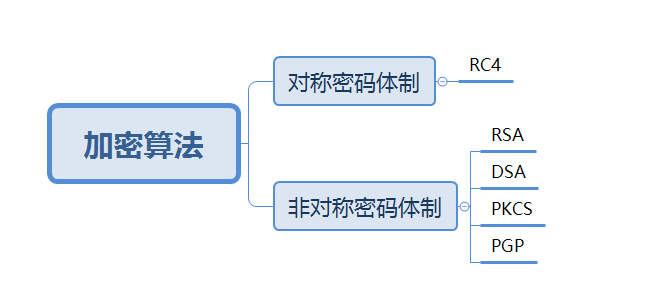
备份上一次完全备份后产生和更新的所有数据。

1. 备份策略的比较

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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 |

**记住：完全备份和增量备份不是最快就是最慢，差异备份永远是居中选择。**

## 二．加密算法



**我们只需要记住RC4是对称密码体制就行，其他的一般都是非对称密码体制**

1. 对称密码体制：当网络中有N个用户相互进行加密通讯时，则需要N\*(N-1)个密钥。
2. 非对称密码体制：非对称密码体制，可以大大简化密钥的管理，当n个用户之间进行通讯加密，仅仅需要2n个密钥即可。

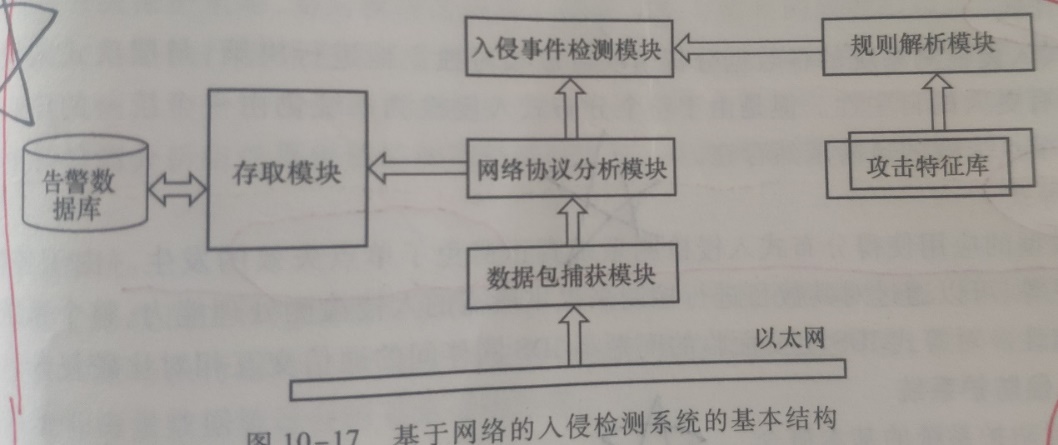
## 三．入侵检测技术

1. **入侵检测系统探测器获取网络流量有三种方法：**
2. 利用交换机设备的镜像功能
3. 在网络链路中串接一个集线器
4. 在网络中串接一个分路器
5. **基于网络的入侵检测系统**

基于网络的入侵检测系统一般是通过将网卡设置成“混杂模式”来收集在网络上出现的数据帧，使用原始的数据帧作为数据源，采用以下的基本识别技术：

1. 模式匹配
2. 频率或阈值
3. 时间的相关性
4. 统计意义上的非正常现象检测

**基于网络的入侵检测系统的基本结构：**

****

1. **分布式入侵检测系统**

分布式入侵检测系统可以分为以下三种类型：

1. 层次式
2. 协作式
3. 对等式：**对等模型的应用使得分布式入侵检测系统真正避免了单点故障的发生。**

## 四．入侵防护系统

1. 入侵防护系统（IPS）整合了防火墙技术和入侵检测技术，采用了In-Line的工作模式。
2. 入侵防护系统的分类
3. 基于主机的入侵防护系统（HIPS）

它与操作系统内核紧密捆绑在一起，检测系统调用，阻挡攻击，并记录日志。

1. 基于网络的入侵防护系统（NIPS）

布置于网络出口处，一般串联与防火墙与路由器之间。

1. 应用入侵防护系统（AIPS）

一般部署于应用服务器前端。

应用入侵防护系统能够防止诸多 入侵，其中包括Cookie篡改、SQL代码注入等（**HIPS和NIPS无法阻断**）

## 五．数据备份与软件安装和配置

1. 磁盘阵列有多种部署方式，也称不同的RAID级别，目前主要有RAID 0、RAID 1、RAID 3、RAID 5等几种，也可以是几种独立方式的组合，如：**RAID 10就是RAID 0和RAID 1 的组合**。
2. 有些服务器中主板中就自带有这个RAID控制器。

## 六．防火墙的安装与配置

防火墙通常具有三个接口，但许多早期的防火墙只有两个接口。当使用具有三个接口的防火墙时，就产生了三个网络：内部区域（内网）、外部区域（外网）、非军事化区（DMZ）。只有两个接口的防火墙是否没有DMZ区的。

基本配置：

1. 输入“enable”进入特权模式。
2. 在监视模式下，可以进行系统映像更新、口令恢复等操作。
3. 在特权模式下可以更改当前配置。
4. 在特权模式下输入 configure terminal进入配置模式，绝大部分系统配置都是在配置模式下进行的。

基本配置命令：

1. nameif: 配置防火墙额名字并指定安全级别。（安全级别取值范围为1-99，数字越大安全及被越高。缺省状态下，安全级别为0的，设置为外部接口；安全级别为100的设置为内部接口；安全级别为50的，设置为MDZ）
2. global: **指定外部IP地址范围（地址池）**。内网主机通过防火墙要访问外网时，防火墙将使用这段IP地址池为要访问外网的主机分配一个全局IP地址。
3. conduit:**该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界别的接口。**

# 第十一章 网络管理技术

1. 查找和排除故障的基本方法
2. 如果网关设置有误，就无法访问其他子网。
3. 拒绝服务攻击（DOS攻击）
4. Land攻击

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

1. SYNFlooding攻击

利用TCP三次握手过程进行攻击。

1. Ping of Death

通过构建出重组缓冲区大小的异常的ICMP包进行攻击。

1. Smurf攻击

攻击者冒充受害主机的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，受害主机会受到大量的echo reply消息。

1. 漏洞查找办法

被动扫描对网络上流量进行分析，不产生额外的流量，不会导致系统崩溃，其工作方式类似于IDS。

主动扫描则更多地带有入侵意为，可能会影响网络系统的正常工作。

1. ISS扫描器
2. Internet扫描器

包括对网络通信服务、操作系统、路由器、电子邮件、Web服务器、防火墙和应用程序检测，从而能识别被入侵者利用来非法进入网络的漏洞。

1. 系统扫描器

系统扫描器是在系统层面上通过依附于主机上的扫描器代理侦测主机内部的漏洞。

1. X-Scanner

X-Scanner采用多线程方式对指定IP地址段（或单机）进行安全漏洞扫描。