ISBN 978-7-121-32234-1

网络工程项目实践教程

新时代新工匠职业教育改革创新系列教材　全国技工教育规划教材

付笔贤　李家骏　主编

CONTENT

项目一
SOHO网络项目

用户需求

致远食品公司原是一家入住SOHO大厦的新公司，公司职员有十几人，部门分为财务部和市场部。由于资金等因素的限制，并且出于管理简单、方便的考虑，构建了工作组模式网络。公司接入了因特网，但不对外提供服务。该网络组建的主要目的是用于实现资源的共享和计算机之间的通信，硬件设备主要包括文件服务器、客户机、磁盘阵列、打印机、扫描仪、交换机、路由器等。每个用户自己决定其计算机上的哪些数据在网络上共享，并且决定不同用户对文件的不同访问权限。

致远公司原有IT架构规模较小，建立在Windows和Linux平台上，构建了工作组模式的网络，操作系统主要是Windows 2000 Professional和Windows XP Professional，以及Windows Server 2003和Linux。随着企业的规模扩大，公司的业务增多，公司的经营越来越依赖于企业内部网的办公自动化和企业外部网，如互联网。公司已经认识到优秀的网络架构能大大提高企业的办公效率和增强企业信息的安全性。

● 网络搭建部分具体需求如下：

1. 要求按照层次型网络结构进行网络设计和网络实施。
2. 公司根据部门业务进行划分。
3. 内部用户利用私网地址访问Internet，需要网络出口设备提供地址转换。
4. 公司内部采用动态路由协议来简化路由配置，要求配置简单，适用于小型网络。
5. 公司的服务需要对内网用户提供服务，不对外网服务。
6. 适当使用网络访问控制措施，保证内部网络的安全性。

● 内部应用系统需求如下：

1. 需要添加一台存放公司重要数据的专门服务器，能对不同职能部门的用户提供不同的访问权限。
2. 建立一台Web服务器，来展示企业形象和增加公司业务。
3. 由于公司申请了域名，希望通过域名来访问公司的主机和服务器。

VLAN

虚拟局域网（Virtual LAN，VLAN）是交换机端口的逻辑组合。VLAN工作在OSI模型的第2层，一个VLAN就是一个广播域，VLAN之间的通信是通过第3层的路由器来完成的。

VLAN有以下优点。

（1）控制网络的广播问题：每一个VLAN都是一个广播域，一个VLAN上的广播不会扩散到另一个VLAN中。

（2）简化网络管理：当VLAN中的用户位置移动时，网络管理员只需设置几条命令即可。

（3）提高网络的安全性：VLAN能控制广播，VLAN之间不能直接通信。

定义交换机的端口在VLAN上的常用方法有以下两种。

（1）基于端口的VLAN：管理员把交换机某一端口指定为某一VLAN的成员。

（2）基于MAC地址的VLAN：交换机根据结点的MAC地址，决定将其放置在哪个VLAN中。

RIP

动态路由协议包括距离矢量路由协议和链路状态路由协议。路由信息协议（Routing Information Protocol，RIP）是使用最广泛的距离矢量路由协议。RIP 是为小型网络环境设计的，因为这类协议的路由学习及路由更新将产生较大的流量，占用过多的带宽。

RIP是由Xerox在20世纪70年代开发的，最初定义在RFC 1058中。RIP用两种数据包传输更新和请求，每个有RIP功能的路由器默认情况下每隔30s利用UDP 520端口向与它直连的网络邻居广播（RIPv1）或组播（RIPv2）路由更新。因此，路由器不知道网络的全局情况，如果路由更新在网络上传播慢，将会导致网络收敛较慢，造成路由环路。为了避免路由环路，RIP采用了水平分割、毒性逆转、定义最大跳数、闪式更新、抑制计时5个机制。

RIP分为版本1和版本2。不论是版本1还是版本2，都具备下面的特征。

（1）都是距离矢量路由协议。（2）使用跳数作为度量值。（3）默认路由更新周期为30s。（4）管理距离为120。

（5）支持触发更新。（6）最大跳数为15跳。（7）支持等价路径，默认4条，最大6条。（8）使用UDP 520端口进行路由更新。

RIPv1和RIPv2的区别如图所示。

RIPv1	RIPv2
在路由更新的过程中不携带子网信息	在路由更新的过程中携带子网信息
不提供认证	提供明文和MD5认证
不支持VLSM和CIDR	支持VLSM和CIDR
采用广播更新	采用组播（224.0.0.9）更新
有类别路由协议	无类别路由协议

NAT

网络地址转换（Network Address Translation，NAT）是一个IETF 标准，允许一个机构以一个地址出现在Internet上。NAT技术使得一个私有网络可以通过Internet 注册IP地址并连接到外部世界，位于Inside网络和Outside网络中的NAT路由器在发送数据包之前，负责把内部IP地址翻译成外部合法IP地址。NAT将每个局域网结点的IP地址转换成一个合法IP地址，反之亦然。它也可以应用到防火墙技术中，把个别IP地址隐藏起来不被外界发现，对内部网络设备起到了保护的作用，同时，它还帮助网络超越了地址的限制，合理地安排网络中的公有IP地址和私有IP地址的使用。

NAT有3种类型：静态NAT、动态NAT和端口地址转换（Port Address Translation，PAT）。

（1）静态NAT

静态NAT中，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail 服务器或FTP 服务器等可以为外部用户提供的服务，这些服务器的IP地址必须采用静态地址转换，以便外部用户使用这些服务。

（2）动态NAT

动态NAT首先要定义合法地址池，然后采用动态分配的方法映射到内部网络中。动态NAT是动态一对一的映射。

（3）PAT

PAT把内部地址映射到外部网络中的一个单独的IP地址上。

ACL

访问控制列表（Access Control List，ACL）使用包过滤技术，在路由器上读取第3层及第4层包头中的信息，如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL有很多种，不同场合应用不同种类的ACL。

（1）标准ACL

标准ACL最简单，它通过使用IP 包中的源IP地址进行过滤，表号为1～99或1300～1999。

（2）扩展ACL

扩展ACL比标准ACL具有更多的匹配项，功能更加强大和细化，可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP连接建立等进行过滤，表号为100～199或2000～2699。

（3）命名ACL

命名ACL以列表名称代替列表编号来定义ACL，同样包括标准和扩展两种列表。

在访问控制列表的学习中，要特别注意以下两个术语。

① 通配符掩码：一个32位的数字字符串，规定了当一个IP地址与其他的IP地址进行比较时，该IP地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略IP地址中对应的位，而“0”表示该位必须匹配。两种特殊的通配符掩码是“255.255.255.255”和“0.0.0.0”，前者等价于关键字“any”，而后者等价于关键字“host”。

② Inbound和Outbound：当在接口上应用访问控制列表时，用户要指明访问控制列表是应用于流入数据还是流出数据。

总之，ACL的应用非常广泛，它可以实现如下功能。

① 拒绝或允许流入（或流出）的数据流通过特定的接口。

② 为DDR应用定义感兴趣的数据流。

③ 过滤路由更新的内容。

④ 控制对虚拟终端的访问。

⑤ 提供流量控制。

项目二
小区网络工程项目

用户需求

为建设一个以电信为基点娱乐影音为一体的数字化小区，并以现代网络技术为依托建立扩展性强、覆盖楼宇的家庭主干网络，拟将小区服务等公共设施与有关广域网相连，方便各种消息的发布与资源的获取；并在此基础上建立能满足影音娱乐和小区管理工作需要的软、硬件环境，部署完善各类信息库与应用系统，为小区各类人员提供充分的网络信息服务。系统总体设计本着总体规划、分步实施的原则，充分体现系统技术的先进性、安全可靠性、开放性、可扩展性及建设经济性。

- 网络搭建部分具体需求如下：

（1）规模：游乐小区现有住户100户，两栋大楼，2个保安室，1个社区居委会。

（2）主干网带宽：采用百兆带宽。

（3）安全性：具有良好的和全面的安全性，能抵御来自外部的攻击。

（4）互联网服务及出口：具有百兆以太网电信Internet出口。

- 内部应用系统需求如下：

（1）核心应用：建立文件服务器，为社区提供影音游戏文件下载。

（2）特别应用：建立社区论坛，为社区提供一个交流互助的平台。

OSPF

在一个大型OSPF网络中，SPF算法的反复计算，庞大的路由表和拓扑表的维护以及LSA的泛洪等都会占用路由器的资源，因而会降低路由器的运行效率。OSPF 协议可以利用区域的概念来减小这些不利的影响。因为一个区域内的路由器将不需要了解它们所在区域外的拓扑细节。OSPF多区域的拓扑结构具有如下优势。

① 降低SPF计算频率。
② 减小路由表。
③ 降低了通告LSA的开销。
④ 将不稳定限制在特定的区域。

（1）OSPF路由器类型

当一个AS划分成几个OSPF区域时，根据一个路由器在相应的区域之内的作用，可以对OSPF路由器做如下分类。

① 内部路由器：OSPF路由器上所有直连的链路都处于同一个区域。
② 主干路由器：具有连接区域0接口的路由器。
③ 区域边界路由器：路由器与多个区域相连。
④ 自治系统边界路由器：与AS 外部的路由器相连并互相交换路由信息。

（2）LSA类型

一台路由器中所有有效的LSA通告都被存放在它的链路状态数据库中，正确的LSA通告可以描述一个OSPF区域的网络拓扑结构。常见的LSA有以下6类。

① 路由器LSA：所有的OSPF路由器都会产生这种数据包，用于描述路由器上连接到某一个区域的链路或某一接口的状态信息。该LSA只会在某一个特定的区域内扩散，而不会扩散至其他的区域。
② 网络LSA：由DR产生，只会在DR所处的广播网络的区域中扩散，不会扩散至其他的OSPF区域。
③ 网络汇总LSA：由ABR产生，描述ABR和某个本地区域的内部路由器之间的链路信息。

这些条目通过主干区域被扩散到其他的ABR中。

④ ASBR汇总LSA：由ABR产生，描述到ASBR的可达性，由主干区域发送到其他ABR中。
⑤ 外部LSA：由ASBR产生，含有关于自治系统外的链路信息。
⑥ NSSA外部LSA：由ASBR产生的关于NSSA的信息，可以在NSSA区域内扩散，ABR可以将类型6的LSA转换为类型5的LSA。

（3）区域类型

一个区域所设置的特性控制着它所能接收到的链路状态信息的类型。区分不同OSPF区域类型的关键在于它们对外部路由的处理方式。OSPF区域类型如下。

① 标准区域：可以接收链路更新信息和路由汇总。
② 主干区域：连接各个区域的中心实体，其他的区域都要连接到这个区域上交换路由信息。
③ 末节区域（Stub Area）：不接收外部自治系统的路由信息。
④ 完全末节区域（Totally Stubby Area）：不接收外部自治系统的路由以及自治系统内其他区域的路由汇总，完全末节区域是Cisco专有的特性。
⑤ 次末节区域（Not-So-Stubby Area，NSSA）：允许接收以7类LSA发送的外部路由信息，并且ABR要负责把类型6的LSA转换成类型5的LSA。

LAMP

LAMP指的是Linux（操作系统）、Apache-HTTP服务器，MySQL和PHP的第一个字母，一般用来建立Web服务器。

虽然这些开放源代码程序本身并不是专门设计成同另几个程序一起工作的，但由于它们的免费和开源，这个组合开始流行（大多数Linux发行版本捆绑了这些软件）。当一起使用的时候，它们表现得像一个具有活力的解决方案包一样。其他的方案包有苹果的WebObjects、Java/J2EE和微软的.NET架构。

LAMP包的脚本组件中包括了CGIweb接口，它在20世纪90年代初期变得流行。这个技术允许网页浏览器的用户在服务器上执行一个程序，并且和接收静态的内容一样接收动态的内容。程序员使用脚本语言来创建这些程序，因为它们能很容易地获得有效的操作文本流，甚至当这些文本流并非源自程序自身时也是。正是由于这个原因，系统设计者经常称这些脚本语言为胶水语言。

Linux：Linux是免费开源软件，这意味着它是源代码可用的操作系统。

Apache：Apache是使用中最受欢迎的一个开放源码的Web服务器软件。

MySQL：MySQL是多线程、多用户的SQL数据库管理系统。

MySQL由Oracle公司自2010年1月27日通过Sun购买。Sun最初于2008年2月26日收购了MySQL。

PHP：PHP是一种编程语言，最初用于设计生产动态网站。PHP 是主要用于服务器端的应用程序软件。

项目三
园区网络项目

用户需求

某街道有A和B两个生活社区；A、B两个社区之间通过路由器VPN专线实现互连；A社区作为互联网出口，A、B两个社区均通过该接口访问互联网；主要服务器放在A社区中；在B社区中使用两台三层交换机作为双核心，交换机设置链路汇聚；B社区各大楼划分VLAN管理。

优化网络配置，使得整个园区网络高效、稳定、安全。

社区需要搭建多种网络服务，提供主页发布、文件共享、邮件收发等常用的功能。

● 网络搭建部分具体需求如下：

1. 社区A使用一台路由器作为网络唯一出口接入互联网，PC11模拟互联网上的机器；PC12也接入该路由器作为社区网内服务器。
2. PC12作为服务器主机，所有服务运行在虚拟机中。
3. 社区B使用一台路由器与社区A通过VPN(IPSec)技术互连；社区B的路由器分别下连两台三层交换机作为汇聚交换机，分别通过三层互连；两台三层汇聚交换机之间至少通过两条线路进行链路汇聚通信。
4. PC21和PC22分别接入三层交换机A和三层交换机B；PC21划归VLAN 10，PC22划归VLAN 20。

● 内部应用系统需求如下：

1. 建立虚拟机作为服务器。
2. 设置DNS服务，为社区服务器提供域名解析。
3. 设定FTP服务，为园区提供文件下载和远程管理Web站点内容服务。
4. 设定Web服务，发布园区主题网。
5. 邮箱服务，为园区人员提供邮箱服务。

HDLC

路由器经常用于构建广域网，广域网链路的封装和以太网上的封装有着非常大的差别。

常见的广域网封装有HDLC、PPP、Frame-Relay等，这里主要介绍HDLC和PPP。相对而言，PPP有较多的功能。

HDLC是点到点串行线路上（同步电路）的帧封装格式，其帧格式和以太网帧格式有很大的差别，HDLC帧没有源MAC地址和目的MAC地址。Cisco公司对HDLC进行了专有化，Cisco的HDLC封装和标准的HDLC不兼容。如果链路的两端都是Cisco设备，使用HDLC封装没有问题，但当Cisco设备与非Cisco设备进行连接时，应使用PPP。HDLC不能提供验证，缺少了对链路的安全保护。默认时，Cisco路由器的串口是采用Cisco HDLC封装的。如果串口的封装不是HDLC，则要把封装改为HDLC时可使用命令“encapsulation hdlc”。

PPP

和HDLC一样，PPP也是串行线路上（同步电路或者异步电路）的一种帧封装格式，但是PPP可以提供对多种网络层协议的支持。PPP支持认证、多链路捆绑、回拨、压缩等功能。PPP经过4个过程在一个点到点的链路上建立通信连接。

① 链路的建立和配置协调：通信的发起方发送LCP 帧来配置和检测数据链路。

② 链路质量检测：在链路已经建立、协调之后进行，这一阶段是可选的。

③ 网络层协议配置协调：通信的发起方发送NCP 帧以选择并配置网络层协议。

④ 关闭链路：通信链路将一直保持到LCP 或NCP 帧关闭链路或发生一些外部事件时为止。

（1）密码验证协议

密码验证协议（Password Authentication Protocol，PAP）利用2次握手的简单方法进行认证。在PPP链路建立完毕后，源结点不停地在链路上反复发送用户名和密码，直到验证通过。PAP的验证中，密码在链路上是以明文传输的，而且由于源结点控制验证重试频率和次数，因此PAP不能防范再生攻击和重复的尝试攻击。

（2）询问握手验证协议

询问握手验证协议（Challenge Handshake Authentication Protocol，CHAP）利用3次握手周期地验证源端结点的身份。CHAP验证过程在链路建立之后进行，而且在以后的任何时候都可以再次进行，这使得链路更为安全。CHAP不允许连接发起方在没有收到询问消息的情况下进行验证尝试。

CHAP每次使用不同的询问消息，每个消息都是不可预测的唯一的值，CHAP不直接传送密码，只传送一个不可预测的询问消息，以及该询问消息与密码经过MD5加密运算后的加密值。所以，CHAP可以防止再生攻击，CHAP的安全性比PAP高。

DHCP

在动态IP地址的方案中，每台计算机并不设定固定的IP地址，而在计算机开机时才被分配一个IP地址，这台计算机被称为DHCP客户端。而负责给DHCP客户端分配IP地址的计算机称为DHCP服务器。也就是说，DHCP采用了客户机/服务器（Client/Server）模式，有明确的客户端和服务器角色的划分。DHCP的工作过程如下。

① DHCP客户机启动时，客户机在当前的子网中广播DHCPDISCOVER报文并向DHCP服务器申请一个IP地址。

② DHCP服务器收到DHCPDISCOVER报文后，它将从那台主机的地址区间中为它提供一个尚未被分配出去的IP地址，并把提供的IP地址暂时标记为不可用。服务器以DHCPOFFER报文送回给主机。如果网络中包含不止一个DHCP服务器，则客户机可能收到好几个DHCPOFFER报文，客户机通常只承认第一个DHCPOFFER。

③ 客户端收到DHCPOFFER后，向服务器发送一个含有有关DHCP服务器提供的IP地址的DHCPREQUEST报文。如果客户端没有收到DHCPOFFER报文并且记得以前的网络配置，则使用以前的网络配置（如果该配置仍然在有效期限内）。

④ DHCP服务器向客户机发回一个含有原先被发出的IP地址及其分配方案的一个应答报文（DHCPACK）。

⑤ 客户端接收到包含了配置参数的DHCPACK报文，利用ARP检查网络上是否有相同的IP地址。如果检查通过，则客户机接收这个IP地址及其参数，如果发现有问题，则客户机向服务器发送DHCPDECLINE信息，并重新开始新的配置过程。服务器收到DHCPDECLINE信息，将该地址标为不可用。

⑥ DHCP服务器只能将那个IP地址分配给DHCP 客户一段时间，DHCP 客户必须在该租用过期前对它进行更新。客户机在50%租借时间过去以后，每隔一段时间就开始请求DHCP服务器更新当前租借，如果DHCP 服务器应答则租用延期。如果DHCP服务器始终没有应答，则在有效租借期的87.5%，客户应该与任何一个其他的DHCP服务器通信，并请求更新它的配置信息。如果客户机不能和所有的DHCP服务器取得联系，租借时间到后，它必须放弃当前的IP地址并重新发送一个DHCPDISCOVER 报文开始上述的IP地址获得过程。

⑦ 客户端可以主动向服务器发出DHCPRELEASE 报文，将当前的IP地址释放。

QoS

网络带宽的发展永远跟不上需求，因此当网络出现堵塞时如何保证网络的正常工作呢？QoS（服务质量）是一个解决方法，QoS的基本思想就是把数据分类，放在不同的队列中。根据不同类数据的要求保证它的优先传输或者为它保证一定的带宽。QoS是在网络发生堵塞时才起作用的措施，因此QoS并不能代替带宽的升级。这里将介绍简单的QoS配置，实际上Cisco路由器现在推荐模块化的QoS配置。

QoS有3种模型：尽最大努力服务、综合服务、区分服务。尽最大努力服务实际上就是没有服务，先到的数据先转发。综合服务的典型就是预留资源，在通信之前所有的路由器先协商好，为该数据流预先保留带宽。区分服务是比较现实的模型，该服务包含了一系列分类工具和排队机制，为某些数据流提供比其他数据流优先级更高的服务。下面来介绍典型的区分服务。

（1）优先级队列

优先级队列（Priority Queue，PQ）中，有高、中、普通、低优先级4个队列。数据包根据事先的定义放在不同的队列中，路由器按照高、中、普通、低顺序服务，只有高优先级的队列为空后才为中优先级的队列服务，以此类推。这样能保证高优先级数据包一定被优先服务，然而，如果高优先级队列长期不空，则低优先级的队列永远不会被服务。所以，可以为每个队列设置一个长度，队列满后，数据包将被丢弃。

（2）自定义队列

自定义队列（Custom Queue，CQ）和PQ不一样，在CQ中有16个队列。数据包根据事先的定义放在不同的队列中，路由器为第一个队列服务一定包数量或者字节数的数据包后，为第二个队列服务。可以定义不同队列中的深度，这样可以保证某个队列被服务的数据包数量较多，但不会使某个队列永远不被服务。CQ中的队列0比较特殊，只有队列0为空时，才能为其他队列服务。

（3）加权公平队列

加权公平队列（Weight Fair Queue，WFQ）是低速链路（2.048Mb/s以下）上的默认设置。

WFQ将数据包区分为不同的流，如在IP中利用IP地址和端口号可以区分不同的TCP流或者UDP流。WFQ为不同的流根据权重分配不同的带宽，权因子是IP 数据包中的优先级字段。例如，有3个流，两个流的优先级为0，第三个为5，总权为（1＋1＋6）=8，则前两个流每个流得到带宽的1/8，第三个流得到带宽的6/8。

项目四
企业网络项目

用户需求

团总部公司有数百台PC；公司有多个部门，不同部门的相互访问要有限制，公司有自己的内部网站；公司有自己的OA系统；公司中的台式机能连接互联网；集团网内部覆盖多栋建筑物，分别是集团总部和公司的办公、生产经营场所；每层设有机房、少量的信息点，供需求使用；每层楼有一个设备间；每栋建筑和集团总部之间通过两条12芯的室外单模光纤连接；要求将全部信息点接入网络。

● 网络搭建部分具体需求如下：

1. 要求按照项目背景设计模拟实验拓扑图。
2. 网络设备要设置统一规范的名称，并按一定顺序摆放，统一系统时间。
3. 网络设备要设置登录密码。
4. 交换机要设置相应的VLAN，交换机端口要设置相应的安全措施。
5. 为了优化性能，交换机和路由器要设置QoS来优化网络性能。
6. 全网使用动态OSPF协议。
7. 适当使用网络访问控制措施，保证内部网络的安全性。

● 内部应用系统需求如下：

1. 集团需要添加一台存放公司开发数据的专门服务器，能对开发部门的用户提供文件共享服务。
2. 建立一台电子邮件服务器，为公司内部员工提供邮件服务。
3. 由于公司申请了域名，因此希望通过域名来访问公司的主机和服务器。