第 2 章　网络访问控制技术

教学目标

以各实训任务的内容和需求为背景，以完成企业园区网的各种网络访问控制技术为实训目标，通过任务方式由浅入深地模拟网络访问控制技术的典型应用和实施过程，以帮助学生理解网络访问控制技术的典型应用，具备企业园区网网络访问控制的实施和灵活应用能力。

教学要求

任务要点	能力要求	关联知识
企业网基本访问控制	(1)掌握交换机基础配置 (2)掌握 VLAN 基础配置 (3)掌握单臂路由配置 (4)掌握基本访问控制列表配置 (5)掌握 FTP 服务器配置	(1)交换机基础及配置命令 (2)VLAN 的划分与配置命令 (3)单臂路由基础及配置命令 (4)访问控制列表技术基础 (5)基本访问控制列表基础及配置命令
企业网高级访问控制	(1)掌握高级访问控制列表技术 (2)掌握 WWW 站点搭建 (3)通过高级访问控制列表技术实现网络资源精细化控制	(1)高级访问控制列表基础及配置命令

重点难点

- 交换机基础配置。
- 交换机 VLAN 技术。
- 单臂路由配置。
- 基本访问控制列表配置。
- 高级访问控制列表配置。
- 访问控制列表配置注意事项与原则。

2.1　任务 1：企业网基本访问控制

2.1.1　基本 ACL 任务描述

某公司有两个部门：市场部和产品部。该公司构建了一台文件服务器，该文件服务器上存储了大量的市场相关信息，非常重要，只允许该公司的市场部员工访问，而产品部员工不能访问，并要求两个部门之间能相互通信，请你规划并实施网络。该公司的组织结构如图 2-1 所示。

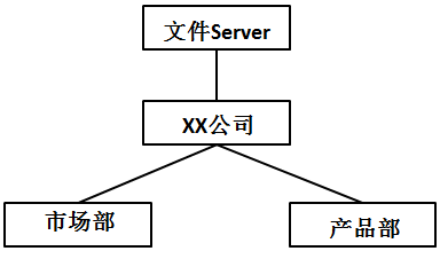

图 2-1　公司的组织结构

2.1.2　基本 ACL 任务目标与目的

1. 任务目标

针对该公司的网络需求，设置基本的网络访问控制，以实现对网络资源的访问控制。

2. 任务目的

通过本任务进行路由器的基本配置、基本访问控制列表(ACL)配置，以帮助读者深入了解路由器的配置方法、基本 ACL 配置方法，具备灵活运用基本 ACL 技术提高网络安全性的能力。

2.1.3　基本 ACL 任务需求与分析

1. 任务需求

该公司办公区共有两个部门：市场部和产品部。每个部门配置不同数量的计算机。网络须满足几个需求：采用当前主流技术构建网络，部门内部能实现相互通信，要求网络具有较高的可管理性、安全性；部门之间都能实现相互访问；并要求只有市场部员工能访问 FTP 服务器，而产品部员工不能访问 FTP 服务器。公司办公区具体的计算机分布如表 2-1 所示。

表 2-1　公司办公区具体的计算机分布表

部　门	计算机数量	部门	计算机数量
市场部	40	产品部	110
服务器	1		

2. 需求分析

需求 1：采用当前主流技术构建网络，部门内部能实现相互通信，具有较高的可管理性、安全性。

分析 1：采用交换式以太网技术构建网络，利用 VLAN 技术将相同部门划入相同的 VLAN，不同部门划分为不同的 VLAN。

需求 2：不同部门之间能相互通信。

分析 2：利用路由器单臂路由技术实现部门之间相互通信。

需求 3：市场部能够访问文件服务器，产品部不能访问文件服务器 FTP。

分析 3：利用基本访问控制技术拒绝产品部员工访问文件服务器 FTP。

根据任务需求和需求分析，组建公司办公区的网络结构，如图 2-2 所示，每个部门以一台计算机表示。

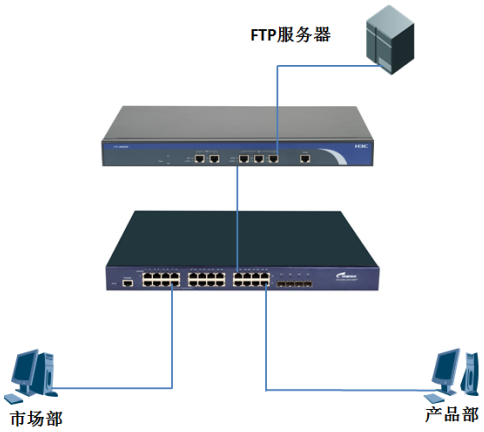

图 2-2　公司办公区的网络结构

2.1.4　基本 ACL 知识链接

1. 交换技术

局域网交换技术是在传统的以太网技术的基础上发展而来的。随着局域网范围的扩大和网络通信技术的发展，目前在企业网络中以太网交换技术是网络发展中非常活跃的部分，交换技术在局域网中处于非常重要的地位。

局域网交换技术是 OSI 参考模型中的第二层——数据链路层(Data Link Layer)上的技术，所谓“交换”，实际上就是指转发数据帧(frame)。实现交换技术的网络设备就是以太网交换机(Switch)。

2. 虚拟局域网

VLAN(Virtual Local Area Network)，即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术，这些网段内的机器有着共同的需求并与物理位置无关，如图 2-3 所示。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，每一个 VLAN 都有一个明确的标识符即 VLAN ID 号，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络，并能进一步结合 IP 技术实现三层交换功能。

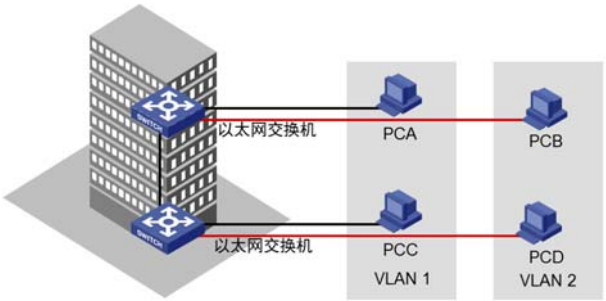

图 2-3　VLAN 结构示意

VLAN 其实只是局域网给用户提供的一种服务，对用户而言是透明的，并不是一种新型的局域网。

VLAN 可以根据具体的网络结构选择合适的 VLAN 类型来构造虚拟局域网，在划分方法和功能上这些类型也有所差别。

1)　基于端口的 VLAN

顾名思义，基于端口的 VLAN 就是明确指定各端口属于哪个 VLAN 的设定方法。基于端口的 VLAN 的划分简单、有效，但其缺点是当用户从一个端口移动到另一个端口时，网络管理员必须对 VLAN 成员进行重新配置。这是最常应用的一种 VLAN 划分方法，目前绝大多数 VLAN 协议的交换机都提供这种 VLAN 配置和划分方法，如图 2-4 所示。

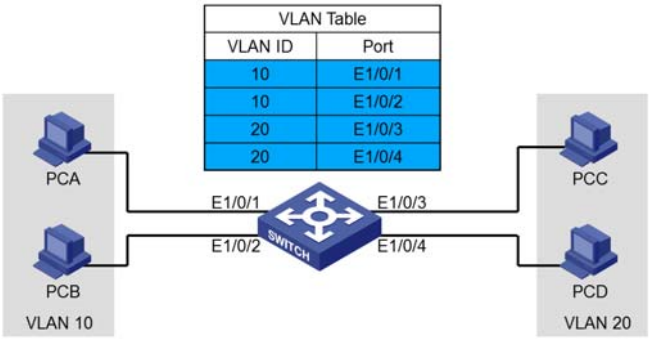

图 2-4　基于端口的 VLAN

2)　基于 MAC 的 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，将特定 MAC 地址划分相应 VLAN，它实现的机制就是每一块网卡都对应唯一的 MAC 地址，VLAN 交换机跟踪属于 VLAN MAC 的地址。这种方式的 VLAN 允许网络用户从一个物理位置移动到另一个物理位置时，自动保留其所属 VLAN 的成员身份，如图 2-5 所示。

3)　基于子网的 VLAN

根据主机所属的 IP 子网来划分 VLAN，即对每个 IP 子网的主机都配置属于哪个组，无论节点处于哪一个物理网段，都可以以它们的 IP 地址为基础或根据报文协议的不同来划分子网，如图 2-6 所示，这使网络管理和应用变得更加方便。

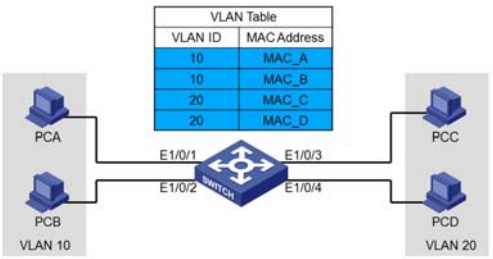

图 2-5　基于 MAC 的 VLAN

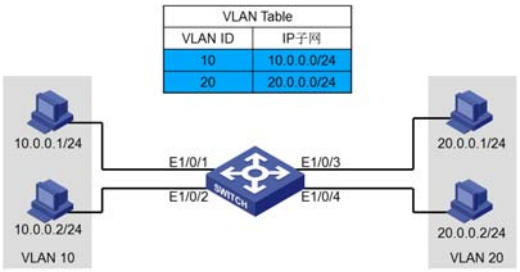

图 2-6　基于子网的 VLAN

4)　基于协议的 VLAN

VLAN 按网络层协议来划分，可以分为 IP、IPX、DECnet、AppleTalk、Banyan 等 VLAN 网络。这种按网络层协议来组成的 VLAN，可使广播域跨越多个 VLAN 交换机。这种方法的优点是若用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。还有，这种方法不需要附加帧标签来识别 VLAN，这样可以减少网络的通信量。这种方法的缺点是效率低，因为检查每一个数据包的网络层地址都需要消耗处理时间。

3. 单臂路由

单臂路由(router-on-a-stick)是指在路由器的一个接口上通过配置子接口(或“逻辑接口”，并不存在真正的物理接口)的方式，实现原来相互隔离的不同 VLAN(虚拟局域网)之间的互联互通。

VLAN 能有效分割局域网，实现各网络区域之间的访问控制。但现实中，往往需要配置某些 VLAN 之间的互联互通。例如，将公司划分为领导层、销售部、财务部、人力部、科技部、审计部，并为不同部门配置不同的 VLAN，部门之间不能相互访问，从而有效地保证了各部门的信息安全。但领导层经常需要跨越 VLAN 访问其他各个部门，这个功能就由单臂路由来实现。

单臂路由的优点是：实现不同 VLAN 之间的通信，有助于理解、学习 VLAN 原理和子接口概念。其缺点是：容易成为网络单点故障，配置稍显复杂，只适合小型企业网络。

4. 访问控制列表(ACL)技术

1)　访问控制列表的基本概念

访问控制是网络安全防范和保护的主要策略，其主要任务是保证网络资源不被非法使用和访问。它是保证网络安全重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

ACL 技术是一种基于包过滤的流控制技术，在路由器中被广泛采用。标准访问控制列表把源地址、目的地址及端口号作为检查数据包的基本元素，并可以规定符合条件的数据包是否允许通过。ACL 通常应用在企业的出口控制上，通过实施 ACL 可以有效地部署企业网络出口策略。随着局域网内部网络资源的增加，一些企业已经开始使用 ACL 来控制对局域网内部资源的访问能力，进而来保障这些资源的安全性。

ACL 是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以

收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来决定。访问控制列表从概念上来讲并不复杂，复杂的是对它的配置和使用。

使用 ACL 可以实现对数据报文的过滤、策略路由以及特殊流量的控制。一个 ACL 中可以包含一条或多条针对特定类型数据包的规则(ACE)，这些规则告诉路由器，对于与规则中规定的选择标准相匹配的数据包是允许还是拒绝通过。访问控制规则 ACE 是根据以太网报文的某些字段来标识以太网报文的，这些字段包括如下内容。

二层字段(Layer 2 fields)：48 位的源 MAC 地址、48 位的目的 MAC 地址。

三层字段(Layer 3 fields)：源 IP 地址字段(可以定义源 IP 地址或对应的子网)、目的 IP 地址字段(可以定义目的 IP 地址或对应的子网)。

四层字段(Layer 4 fields)：可以定义 TCP 的源端口、目的端口，以及 UDP 的源端口、目的端口。

2)　访问控制列表的分类

访问控制列表的类型主要有以下几种。

(1)　标准 IP 访问控制列表，也称基本访问控制列表。一个标准 IP 访问控制列表匹配 IP 包中的源地址或源地址中的一部分，可以对匹配的包采取拒绝或允许两个操作。编号范围从 1 到 99 的访问控制列表，是标准 IP 访问控制列表。

(2)　扩展 IP 访问控制列表，也称高级访问控制列表。扩展 IP 访问控制列表比标准 IP 访问控制列表具有更多的匹配项，包括协议类型、源地址、目的地址、源端口、目的端口、建立连接的类型和 IP 优先级等。编号范围从 100 到 199 的访问控制列表，是扩展 IP 访问控制列表。

(3)　命名的 IP 访问控制列表，也称用户自定义的访问控制列表，其以列表名代替列表编号来定义 IP 访问控制列表，同样包括标准和扩展两种列表，定义过滤的语句与编号方式相似。

H3C 网络设备对于访问控制列表的分类如图 2-7 所示。

访问控制列表的分类	数字序号的范围
基本访问控制列表	2000～2999
扩展访问控制列表	3000～3999
基于二层的访问控制列表	4000～4999
用户自定义的访问控制列表	5000～5999

图 2-7　H3C 网络设备对于访问控制列表的分类

3)　访问控制列表的原理

访问控制列表，由一系列规则构成，通过规则对进出的数据包逐个过滤。ACL 部署应用实例如图 2-8 所示。

通过 ACL 过滤的数据包，将交由路由器去处理：或丢弃，或允许通过。ACL 必须应用于接口上，可以在每个接口的出入双向过滤(Inbound、Outbound)，仅当数据包经过一个接口时，才能被此接口的此方向的 ACL 过滤。通过的数据包，交给路由转发进程进行转发。ACL 入站包过滤工作流程如图 2-9 所示。

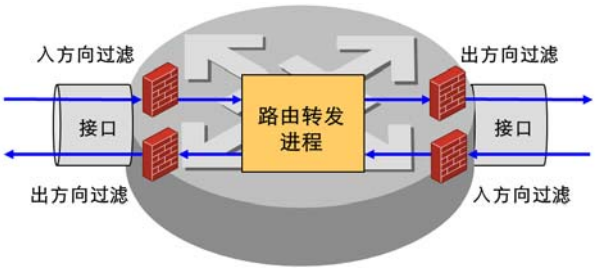

图 2-8　ACL 部署应用实例

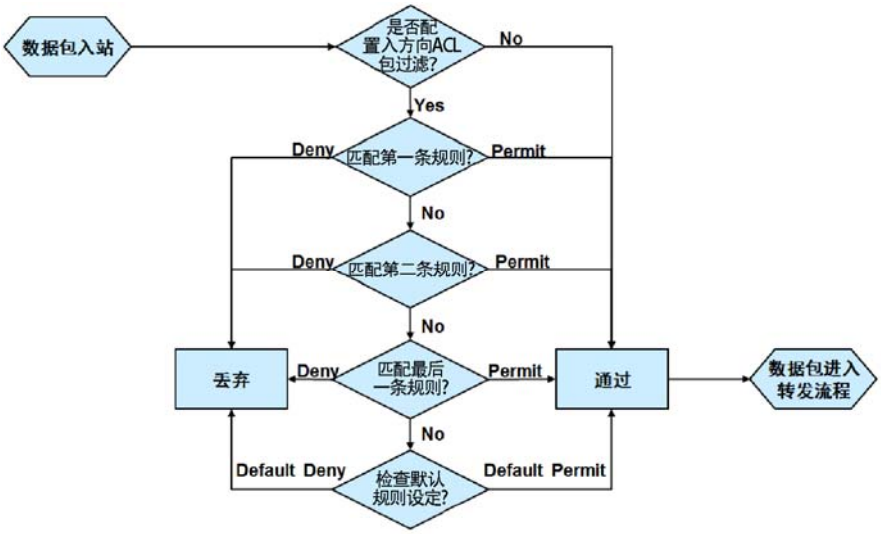

图 2-9　ACL 入站包过滤工作流程

ACL 出站包过滤工作流程如图 2-10 所示。

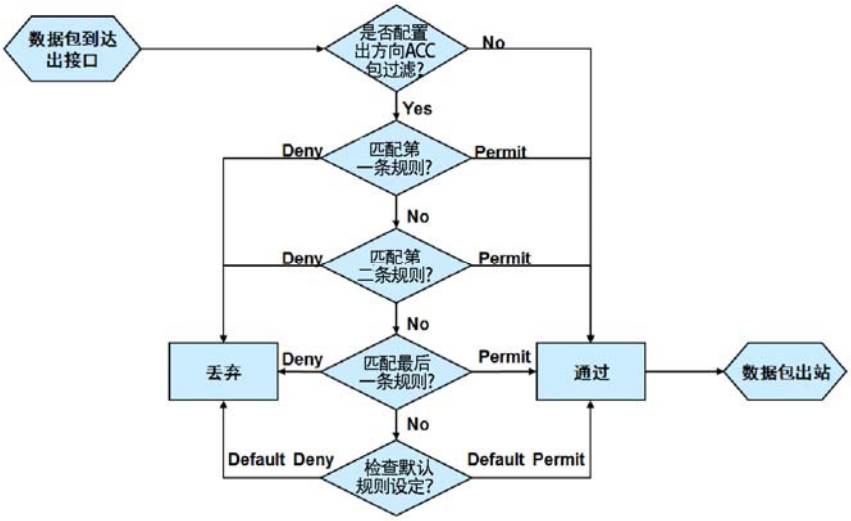

图 2-10　ACL 出站包过滤工作流程

4)　基本访问控制列表的原理

基本 ACL 只能根据 IP 数据包里的源 IP 地址对数据实施过滤。基本 ACL 的工作原理如图 2-11 所示。

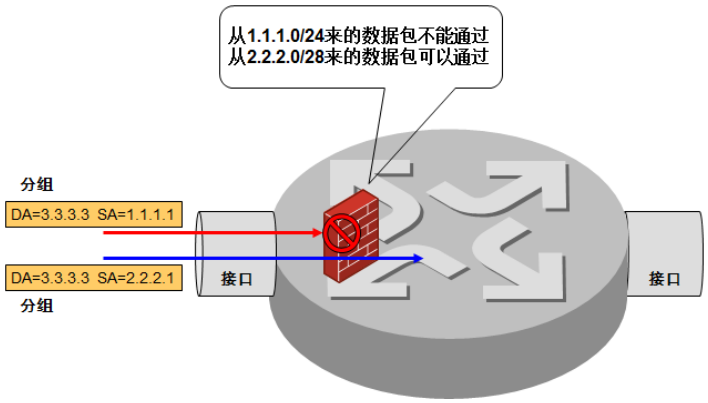

图 2-11　基本 ACL 的工作原理

5)　ACL 部署原则

(1)　每个接口、每个协议、每个方向只允许配置一个访问列表。这意味着如果创建了 IP 访问列表，每个接口只能有一个入口访问列表和一个出口访问列表。

(2)　任何时候在访问列表中添加新条目时，路由器都把新添加的条目放置在列表的最末尾。强烈推荐用文本编辑器先编辑好访问列表，然后将访问列表复制到命令行。

(3)　不能删除访问列表中的部分内容。如果尝试这样做，将删除整个列表。使用命名访问列表时例外。

(4)　除非在访问列表末尾有 permit any 命令，否则所有和列表测试条件不符合的数据包将被丢弃。

(5)　先创建访问列表，然后将列表应用到某个接口。

(6)　将标准的访问列表尽可能地放置在靠近目的地址的位置。

(7)　将扩展的访问列表尽可能地放置在靠近源地址的位置。

(8)　访问列表设计是为了过滤通过路由器的流量，但不过滤路由器自身产生的流量。

5. 配置命令

路由器的基本管理方式和配置模式与交换机类似，请参照第 3 章交换机的配置模式和配置命令。在 H3C 系列和 Cisco 系列路由器上配置单臂路由和基本 ACL 协议的相关命令，如表 2-2 所示。

表 2-2　单臂路由和基本 ACL 配置命令

功　能	H3C 系列设备		Cisco 系列设备	
	配置视图	基本命令	配置模式	基本命令
划分子接口	系统视图	[H3C]interface GigabitEthernet 0/0.1	全局配置模式	Cisco(config)#interface fastEthernet 0/1.1
封装 802.1q 协议，并与特定 vlan 关联	具体视图	[H3C-GigabitEthernet0/0.1] vlan-typ dot1q vid　10	具体配置模式	Cisco(config-subif)#encapsulation dot1Q 10

续表

功　能	H3C 系列设备		Cisco 系列设备	
	配置视图	基本命令	配置模式	基本命令
子接口 IP 参数配置	具体视图	[H3C-GigabitEthernet0/0.1] ip address　192.168.10.254 255.255.255.0	具体配置模式	Cisco(config-subif)#ip address　192.168.10.254 255.255.255.0
关闭子接口	具体视图	[H3C-GigabitEthernet0/0.1] shutdown	具体配置模式	Cisco(config-subif)#shutdown
重启子接口	具体视图	[H3C-GigabitEthernet0/0.1] undo shutdown	具体配置模式	Cisco(config-subif)#no shutdown
使能防火墙功能	系统视图	[H3C]firewall　enable		
创建基本 ACL	系统视图	[H3C]acl number 2000		
创建规则	具体视图	[H3C-acl-basic-2000]rule 0 deny source 192.168.20.0 0.0.0.255	全局配置模式	Cisco(config)#access-list 1 deny 192.168.10.0 0.0.0.255
进入接口视图	系统视图	[H3C]interface　Ethernet　0/1	全局配置模式	Cisco(config)#interface fastEthernet 0/1
将 ACL 应用到接口出方向	具体视图	[H3C-Ethernet0/1]firewall packet-filter　2000 outbound	具体配置模式	Cisco(config-if)#ip access-group 1 out

2.1.5　基本 ACL 任务实施

1. 实施规划

1)　实训拓扑结构

根据任务的需求与分析，实训的拓扑结构及网络参数如图 2-12 所示，以 PC1、PC2、Server 分别模拟公司的市场部、产品部和 FTP 服务器。

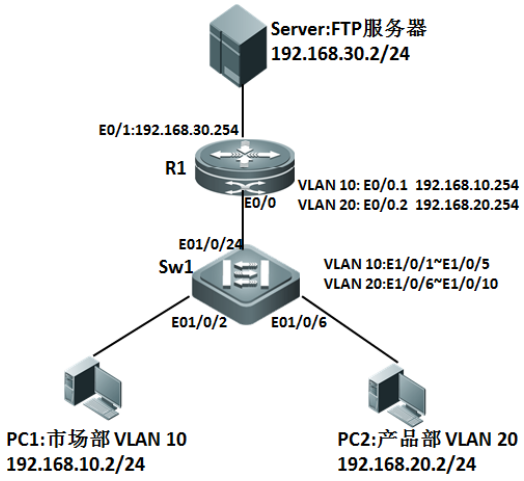

图 2-12　实训任务拓扑

2)　实训设备

根据任务的需求和实训拓扑，每个实训小组的实训设备配置清单如表 2-3 所示。

表 2-3　实训设备配置清单

设备类型	设备型号	数　量
路由器	H3C MSR20-40	1
交换机	H3C E126A	1
计算机	Windows 2003/Windows 7	3
双绞线	RJ-45	若干

3)　IP 地址规划

根据需求分析本任务的 IP 地址规划，如表 2-4 所示。

表 2-4　IP 地址规划

设　备	接　口	IP 地址	网　关
PC1		192.168.10.2/24	192.168.10.254
PC2		192.168.20.2/24	192.168.20.254
Server		192.168.30.2/24	192.168.30.254
R1	Ethernet 0/0.10	192.168.10.254/24	
	Ethernet 0/0.20	192.168.20.254/24	
	Ethernet 0/1	192.168.30.254/24	

4)　VLAN 规划

根据需求分析本任务的 VLAN 规划，如表 2-5 所示。

表 2-5　VLAN 规划

部门名称	主　机	Vlan	端　口
市场部	PC1	10	E 1/0/1 to E 1/0/5
产品部	PC2	20	E 1/0/6 to E 1/0/10

2. 实施步骤

任务的实施步骤如下。

(1)　根据实训拓扑图进行交换机、计算机的线缆连接，配置 PC1、PC2、PC3 的 IP 地址、子网掩码、默认网关等相关 IP 参数。

(2)　使用计算机 Windows 操作系统的“超级终端”组件程序通过串口连接到交换机的配置界面，其中，超级终端串口的属性设置还原为默认值(每秒位数 9600、数据位 8、奇偶校验无、数据流控制无)。

(3)　超级终端登录到路由器，进行任务的相关配置。

(4)　Sw1 主要配置清单如下。

```
一、vlan 配置:
<H3C>system-view
[H3C]sysname sw1
```

```
[sw1]vlan 10
[sw1-vlan10]port  Ethernet  1/0/1 to  Ethernet  1/0/5
[sw1-vlan10]vlan 20
[sw1-vlan20]port  Ethernet 1/0/6 to  Ethernet  1/0/10
二、上联端口为 trunk
[sw1-vlan20]quit
[sw1]interface  Ethernet  1/0/24
[sw1-Ethernet1/0/24]port link-type  trunk
[sw1-Ethernet1/0/24]port trunk  permit  vlan  all
```

(5) R 1 主要配置清单如下。

```
一、配置单臂路由
<H3C>system-view
[H3C]sysname r1
[r1]interface  Ethernet  0/0.10
[r1-Ethernet0/0.10]ip address  192.168.10.254 24
[r1-Ethernet0/0.10]vlan-type  dot1q  vid  10
[r1-Ethernet0/0.10]quit
[r1]interface  Ethernet  0/0.20
[r1-Ethernet0/0.20]ip address  192.168.20.254 24
[r1-Ethernet0/0.20]vlan-type  dot1q  vid  20
[r1-Ethernet0/0.20]quit
[r1]interface  Ethernet  0/1
[r1-Ethernet0/1]ip address  192.168.30.254 24
二、基本访问控制列表配置
1. 使能防火墙功能
[r1]firewall  enable
2. 创建 ACL
[r1]acl number 2000
3. 创建规则
[r1-acl-basic-2000]rule  0 deny source 192.168.20.0 0.0.0.255      /*拒绝来自 192.168.20.0/24 网段的数据通过
4. 将 ACL 应用到具体的接口
[r1-acl-basic-2000]quit
[r1]interface  Ethernet  0/1
[r1-Ethernet0/1]firewall  packet-filter  2000 outbound /*将访问控制列表 2000 应用到 e0/1 接口出方向
```

(6) FTP 服务器搭建。

FTP 服务器搭建，参考其他相关资料，此处略。

2.1.6 基本 ACL 任务验收

1. 设备验收

根据实训拓扑图检查验收路由器、计算机的线缆连接，检查 PC1、PC2、文件 Server 的 IP 地址。

2. 配置验收

查看访问控制列表：

```
r[r1]display  acl  all
Basic ACL  2000, named -none-, 1 rule,
ACL's step is 5
 rule 0 deny source 192.168.20.0 0.0.0.255 (19 times matched)
```

3. 功能验收

功能验收的步骤如下。

(1)　在 PC1 上通过浏览器输入 ftp://192.168.30.2，可以正常访问，如图 2-13 所示。

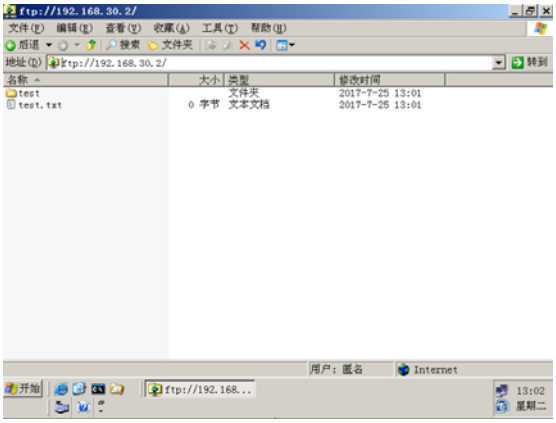

图 2-13　市场部能正常访问 FTP 服务器

(2)　在 PC2 上通过浏览器输入 ftp://192.168.30.2，则不能正常访问，如图 2-14 所示。

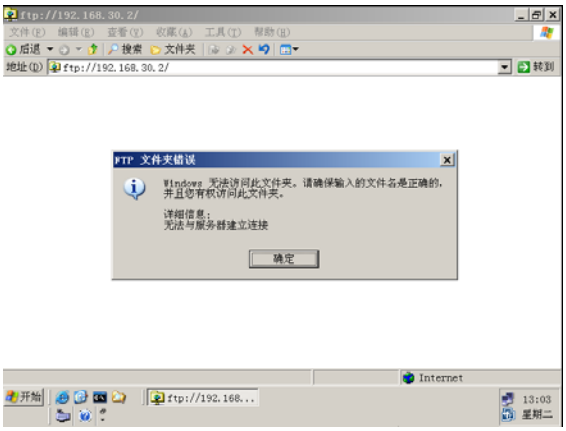

图 2-14　产品部无法正常访问 FTP 服务器

2.1.7　基本 ACL 任务总结

针对某公司办公区网络改造任务的内容和目标，根据需求分析进行了实训的规划和实施，通过本任务进行了路由器基本访问控制列表 ACL 的配置实训。

2.2 任务 2：企业网高级访问控制

2.2.1 高级 ACL 任务描述

某公司有两个部门：市场部和产品部。该公司购买了一台服务器，在网络中部署两个应用服务：WWW 服务和 FTP 服务。从安全和可管理角度考虑，要求市场部能够访问 FTP 服务器，不能够访问 WWW 服务器；产品部能够访问 WWW 服务器，不能访问 FTP 服务器；并要求两个部门之间能相互通信。请你规划并实施网络。该公司的组织结构如图 2-15 所示。

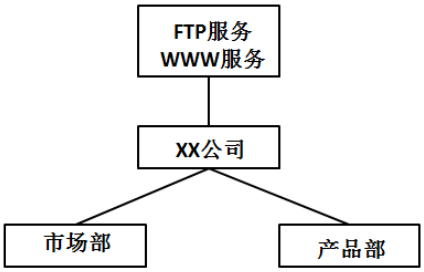

图 2-15 公司的组织结构

2.2.2 高级 ACL 任务目标与目的

1. 任务目标

针对该公司的网络需求，设置高级的网络访问控制，实现对网络资源更精细的访问控制。

2. 任务目的

通过本任务进行路由器的基本配置、高级访问控制列表(ACL)配置，以帮助读者深入了解路由器的配置方法、高级 ACL 配置方法，具备灵活运用高级 ACL 技术对网络进行更精细化的控制以保证网络安全的能力。

2.2.3 高级 ACL 任务需求与分析

1. 任务需求

该公司办公区共有两个部门：市场部和产品部。每个部门配置不同数量的计算机。网络须满足几个需求：采用当前主流技术构建网络，部门内部能实现相互通信，要求网络具有较高的可管理性、安全性；部门之间都能实现相互访问；网络中部署 WWW、FTP 两种网络应用服务；要求市场部能够访问 FTP 服务器，不能够访问 WWW 服务器；产品部能够

访问 WWW 服务器，不能访问 FTP 服务器。公司办公区具体计算机分布如表 2-6 所示。

表 2-6　公司办公区具体计算机分布表

部　门	计算机数量	服务器数量
市场部	40	1
产品部	110	0

2. 需求分析

需求 1：采用当前主流技术构建网络，部门内部能实现相互通信，具有较高的可管理性、安全性。

分析 1：采用交换式以太网技术构建网络，利用 VLAN 技术将相同部门划入相同的 VLAN，不同部门划分为不同的 VLAN。

需求 2：不同部门之间能相互通信。

分析 2：利用路由器单臂路由技术实现部门之间相互通信。

需求 3：市场部能够访问 FTP 服务器，不能够访问 WWW 服务器；产品部能够访问 WWW 服务器，不能访问 FTP 服务器。

分析 3：利用高级访问控制列表技术对网络资源实现精细化的访问控制。

根据任务需求和需求分析，组建公司办公区的网络结构，如图 2-16 所示，每个部门用一台计算机表示。

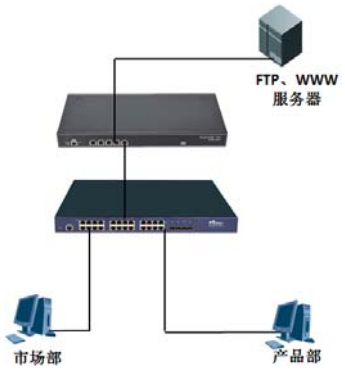

图 2-16　公司办公区的网络结构

2.2.4　高级 ACL 知识链接

1. 高级访问控制列表(ACL)技术

1)　访问控制列表的基本概念

访问控制列表，由一系列有顺序的规则组成。这些规则根据数据包的源地址、目的地址、端口号等来定义匹配条件，执行 permit 或 deny 操作。ACL 实质上是报文识别技术，广泛用于需要识别报文，对报文进行分类的场合。访问控制列表技术一般应用场合如下。

(1)　包过滤防火墙功能：用以实现对访问的限制。

(2)　NAT 技术：用于制定规则，确定哪些数据包需要转换，哪些不需要。

(3)　QoS 技术：用于实现对数据分类，不同类型的数据提供不同的优先级服务。

(4)　路由策略和过滤：利用 ACL 规则匹配路由信息中的相关参数，以实现路由过滤。

(5)　按需拨号：利用 ACL 对数据进行分类，实现只有相应种类的数据能触发路由器进行 PSTN/ISDN 的拨号连接。

2)　高级访问控制列表的原理

高级访问控制列表根据报文的源 IP 地址、目的 IP 地址、IP 承载的协议类型、协议特性等三、四层信息制定规则。高级访问控制列表的实现原理如图 2-17 所示。

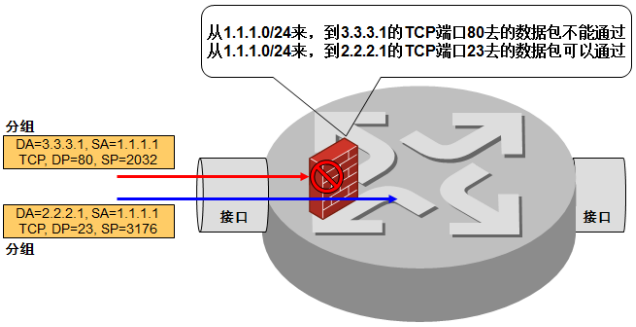

图 2-17　高级访问控制列表的实现原理

2. 配置命令

路由器的基本管理方式和配置模式与交换机类似，请参照第 3 章交换机的配置模式和配置命令。H3C 系列和 Cisco 系列路由器上高级 ACL 协议的相关命令如表 2-7 所示。

表 2-7　高级 ACL 配置命令

功　能	H3C 系列设备		Cisco 系列设备	
	配置视图	基本命令	配置模式	基本命令
使能防火墙功能	系统视图	[H3C]firewall　enable		
创建高级(扩展)ACL	系统视图	[H3C]acl　advanced 3000		
创建规则	具体视图	[H3C-acl-adv-3000]rule 0 deny　tcp　destination 192.168.30.2 0.0.0.0 destination-port eq www source 192.168.10.0 0.0.0.255		Cisco(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 192.168.30.2 0.0.0.0 eq www
进入接口视图	系统视图	[H3C]interface Ethernet 0/1	全局配置模式	Cisco(config)#interface fastEthernet 0/1
将 ACL 应用到接口上的入方向	具体视图	[H3C-Ethernet0/0.2]firewall packet-filter　3000 inbound	具体配置模式	Cisco(config-if)#ip access-group 1 in

2.2.5　高级 ACL 任务实施

1. 实施规划

1)　实训拓扑结构

根据任务的需求与分析，实训的拓扑结构及网络参数如图 2-18 所示，用 PC1、PC2、Server 分别模拟公司的市场部、产品部、FTP 和 WWW 服务器。

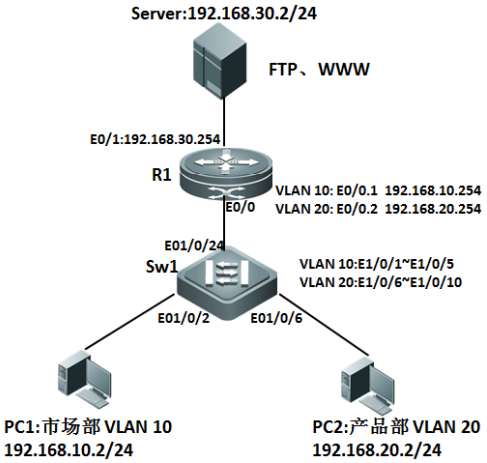

图 2-18　实训的拓扑结构及网络参数

2)　实训设备

根据任务的需求和实训拓扑，每个实训小组的实训设备配置清单如表 2-8 所示。

表 2-8　实训设备配置清单

设备类型	设备型号	数　量
路由器	H3C MSR20-40	1
交换机	H3C E126A	1
计算机	Windows 2003/Windows 7	3
双绞线	RJ-45	若干

3)　IP 地址规划

根据需求分析本任务的 IP 地址规划，如表 2-9 所示。

表 2-9　IP 地址规划

设　备	接　口	IP 地址	网　关
PC1		192.168.10.2/24	192.168.10.254
PC2		192.168.20.2/24	192.168.20.254
Server		192.168.30.2/24	192.168.30.254
Router1	Ethernet 0/0.10	192.168.10.254/24	
	Ethernet 0/0.20	192.168.20.254/24	
	Ethernet 0/1	192.168.30.254/24	

4)　VLAN 规划

根据需求分析本任务的 VLAN 规划，如表 2-10 所示。

表 2-10　VLAN 规划

部门名称	主　机	VLAN	端　口
市场部	PC1	10	E 1/0/1 to E 1/0/5
产品部	PC2	20	E 1/0/6 to E 1/0/10

2. 实施步骤

(1) 根据实训拓扑图进行交换机、计算机的线缆连接，配置 PC1、PC2、PC3 的 IP 地址、子网掩码、默认网关等相关 IP 参数。

(2) 使用计算机 Windows 操作系统的“超级终端”组件程序通过串口连接到交换机的配置界面，其中超级终端串口的属性设置还原为默认值(每秒位数 9600、数据位 8、奇偶校验无、数据流控制无)。

(3) 超级终端登录到路由器，进行任务的相关配置。

(4) Sw1 主要配置清单如下。

```
一、vlan 配置
<H3C>system-view
[H3C]sysname sw1
[sw1]vlan 10
[sw1-vlan10]port  Ethernet  1/0/1 to  Ethernet  1/0/5
[sw1-vlan10]vlan 20
[sw1-vlan20]port  Ethernet 1/0/6 to  Ethernet  1/0/10
二、上联端口为 trunk
[sw1-vlan20]quit
[sw1]interface  Ethernet  1/0/24
[sw1-Ethernet1/0/24]port link-type  trunk
[sw1-Ethernet1/0/24]port trunk  permit  vlan  all
```

(5) Router 1 主要配置清单如下。

```
一、配置单臂路由
<H3C>system-view
[H3C]sysname r1
[r1]interface  Ethernet  0/0.10
[r1-Ethernet0/0.10]ip address  192.168.10.254 24
[r1-Ethernet0/0.10]vlan-type  dot1q  vid  10
[r1-Ethernet0/0.10]quit
[r1]interface  Ethernet  0/0.20
[r1-Ethernet0/0.20]ip address  192.168.20.254 24
[r1-Ethernet0/0.20]vlan-type  dot1q  vid  20
二、配置接口 IP 参数
[r1]interface  Ethernet  0/1
[r1-Ethernet0/1]ip address  192.168.30.254 24
三、高级访问控制列表配置
[r1]firewall enable
[r1]acl  number  3000
[r1-acl-adv-3000]rule  0 deny  tcp  destination 192.168.30.2 0.0.0.0 destination-port eq www
source 192.168.10.0 0.0.0.255    /*拒绝来自于 190.168.10.0/24 网段的主机，去访问 IP 地址为
192.168.30.2 的服务器的 www 服务
[r1-acl-adv-3000]rule  1 deny  tcp  destination 192.168.30.2 0.0.0.0 destination-port eq  ftp
source 192.168.20.0 0.0.0.255    /*拒绝来自于 190.168.30.0/24 网段的主机去访问 IP 地址为
192.168.30.2 的服务器的 ftp 服务
```

```
四、将 ACL 应用到具体的接口
[r1-acl-adv-3000]quit
[r1]interface  Ethernet  0/0.10
[r1-Ethernet0/0.10]firewall  packet-filter  3000 inbound
[r1-Ethernet0/0.10]quit
[r1]interface  Ethernet  0/0.20
[r1-Ethernet0/0.20]firewall  packet-filter  3000 inbound
```

(6)　WWW、FTP 服务器搭建。

WWW、FTP 服务器搭建参考其他相关资料，此处略。

2.2.6　高级 ACL 任务验收

1. 设备验收

根据实训拓扑图检查验收路由器、计算机的线缆连接，检查 PC1、PC2、服务器的 IP 地址。

2. 配置验收

查看访问控制列表：

```
[r1]display  acl  3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 deny tcp source 192.168.10.0 0.0.0.255 destination 192.168.30.2 0
destination-port eq www (4 times matched)
 rule 1 deny tcp source 192.168.20.0 0.0.0.255 destination 192.168.30.2 0
destination-port eq ftp (21 times matched)
```

3. 功能验收

功能验收如下。

(1)　在 PC1(市场部)上通过浏览器输入 ftp://192.168.30.2，可以正常访问，如图 2-19 所示；输入 http://192.168.30.2 则不能访问，如图 2-20 所示。

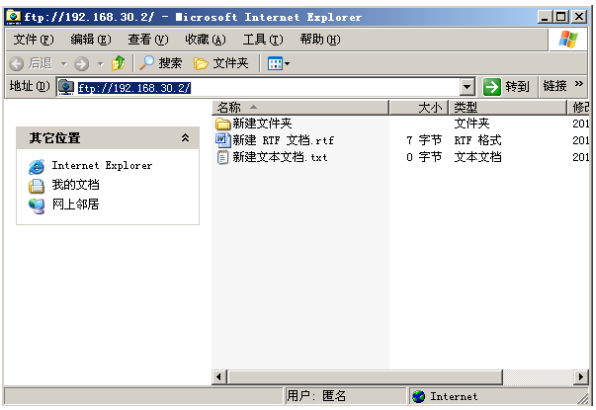

图 2-19　PC1 可以访问 FTP 服务

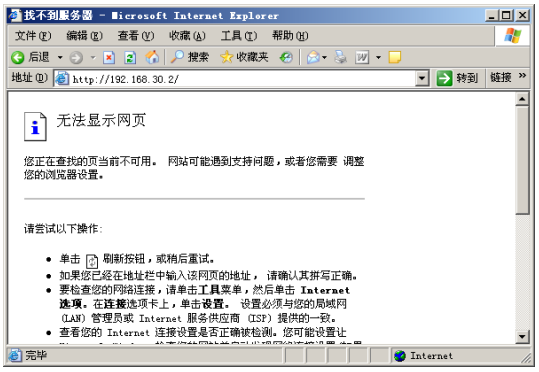

图 2-20　PC1 不能访问 WWW 服务

(2)　在 PC2(产品部)上通过浏览器输入 http://192.168.30.2，可以正常访问，如图 2-21 所示；输入 ftp://192.168.30.2，则不能正常访问，如图 2-22 所示。

图 2-21　PC2 可以访问 WWW 服务

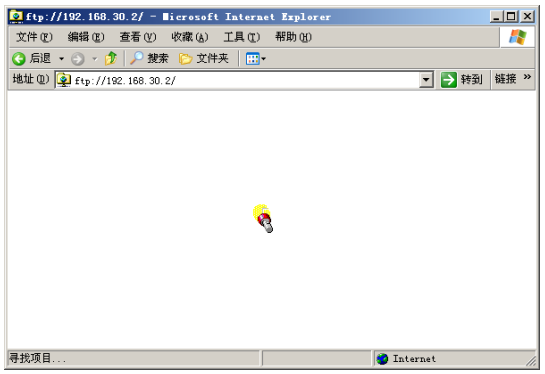

图 2-22　PC2 不能正常访问 FTP 服务

2.2.7　高级 ACL 任务总结

针对某公司办公区网络改造任务的内容和目标，根据需求分析进行了实训的规划和实施，通过本任务进行了路由器高级访问控制列表 ACL 的配置实训。