第 3 章　校园网设计方法和实现过程

在校园网设计和实施过程中，需要解决如何通过无线局域网接入移动终端的问题，如何通过以太网安全机制防御 ARP 欺骗攻击和源 IP 地址欺骗攻击的问题，以及如何通过安全路由防御路由项欺骗攻击的问题。

3.1　校园布局和设计要求

我们需要根据校园布局设计校园网的分层结构。对应分层结构，将建筑物分为教室、办公楼和主楼三个层次。

3.1.1　校园布局

校园布局如图 3.1 所示，楼与楼之间的距离为 1～2km，要求通过校园网实现各个楼之间互联。为简化起见，只要求将每一栋教室中的若干终端和数据中心中的若干服务器连接到校园网上，不考虑主楼和办公楼中的终端和服务器。教室中的终端包括固定终端和移动终端。

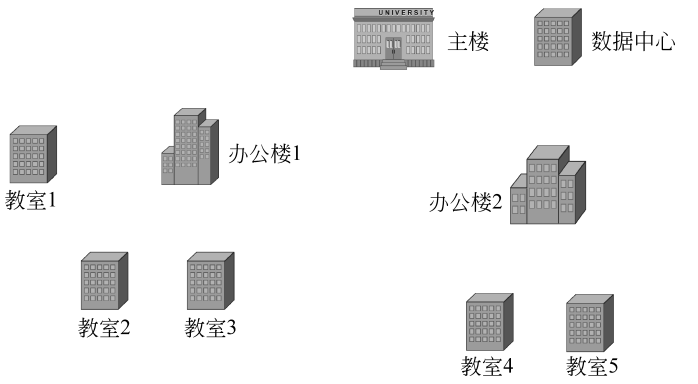

图 3.1　校园布局

3.1.2　需求分析

每一个教室存在三种类型的终端：一是上课用的固定终端，二是学生携带的移动终端，三是教师携带的移动终端。每一个教室设置 AP，由 AC 统一完成对 AP 的配置过程。移动终端通过 AP 接入校园网。数据中心设置 Web 服务器、DHCP 服务器、域名系统(Domain Name System，DNS)服务器、文件传输协议(File Transfer Protocol，FTP)服务器、E-mail 服务器、RADIUS(Remote Authentication Dial In User Service，远程鉴别拨入用户服务)服务器等。如果对移动终端接入过程实施统一鉴别，由 RADIUS 服务器完成统一鉴别过程。教

师和学生的移动终端以及固定终端都通过 DHCP 获取网络信息。教师移动终端、学生移动终端和固定终端属于不同的 VLAN，有着不同的资源访问权限。固定终端不能访问 E-mail 服务器，学生移动终端不能访问 FTP 服务器。

3.2　逻辑设计

逻辑设计阶段需要根据校园布局完成拓扑结构设计，根据需求分析结果导出数据通信系统和安全系统的功能和设计原则，完成设备选型。

3.2.1　网络拓扑结构

网络拓扑结构设计一是需要考虑布线系统的实施难度和成本，二是需要考虑放置和管理网络设备的方便性，三是需要考虑数据通信网络的设计要求。根据如图 3.1 所示的校园布局，设计出如图 3.2 所示的校园网拓扑结构。接入层设备放置在各个教室和数据中心，教室中接入层设备的功能是连接教室中的固定终端和 AP，数据中心中接入层设备的功能是连接数据中心中的服务器。汇聚层设备放置在两个办公楼中，汇聚层设备的功能一是连接核心层设备，二是连接分布在教室中的接入层设备。办公楼 1 中的汇聚层设备连接教室 1、教室 2 和教室 3 中的接入层设备。办公楼 2 中的汇聚层设备连接教室 4 和教室 5 中的接入层设备。核心层设备放置在主楼中，核心层设备的功能是连接放置在办公楼 1 和办公楼 2 中的汇聚层设备和 AC 以及连接数据中心中服务器的接入层交换机。

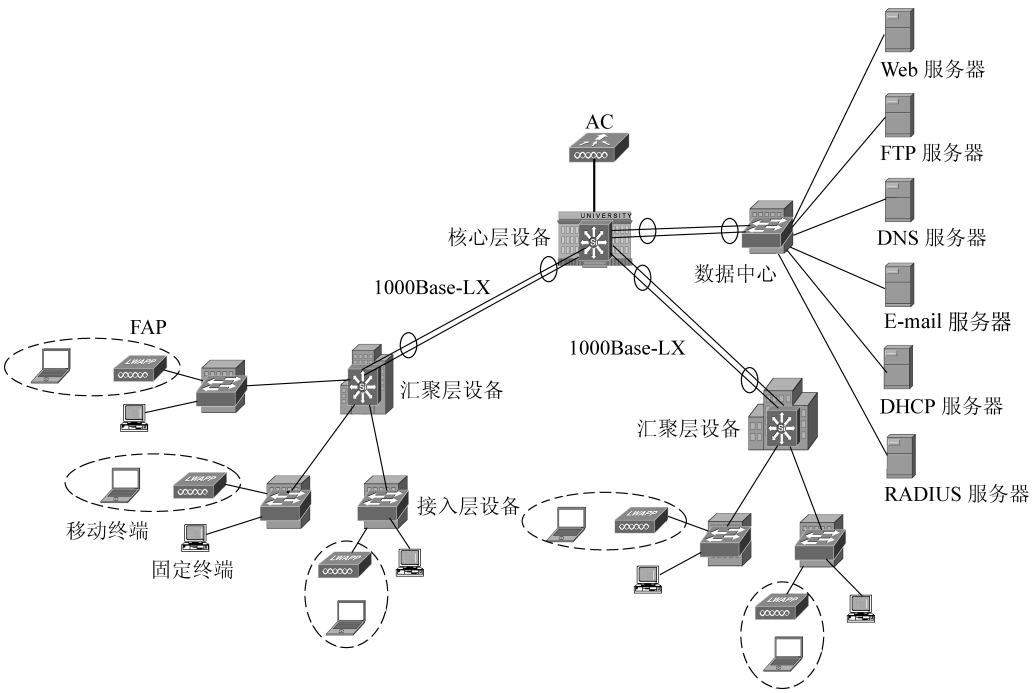

图 3.2　校园网拓扑结构

3.2.2 数据通信网络性能指标和设计原则

1. 数据通信网络性能指标

- 全双工、100Mb/s 链路连接终端。
- 全双工、1000Mb/s 链路连接 FAP。
- 全双工、1000Mb/s 链路连接服务器。
- 教室与办公楼之间提供全双工、1000Mb/s 链路。
- 办公楼 1 与主楼之间通过链路聚合技术提供全双工、2000Mb/s 物理连接。
- 办公楼 2 与主楼之间通过链路聚合技术提供全双工、2000Mb/s 物理连接。
- 数据中心与主楼之间通过链路聚合技术提供全双工、2000Mb/s 物理连接。
- 允许跨教室划分 VLAN。
- 允许按照应用和安全等级为服务器分配 VLAN。
- 完成各个 VLAN 的 IP 地址分配。
- 选择 OSPF 作为路由协议,将校园网作为单个 OSPF 区域。
- 按照安全系统要求建立端到端传输路径。
- 所有终端通过 DHCP 自动获取网络信息。

2. 数据通信网络设计原则

- 由于允许多个终端同时通过瘦 AP 接入校园网,因此接入层交换机通过 1000Mb/s 链路连接瘦 AP。
- 由于每一个接入层交换机连接 1 个固定终端和多个移动终端,因此接入层交换机通过 1000Mb/s 链路连接汇聚层交换机。
- 由于每一个汇聚层交换机连接多个接入层交换机,因此汇聚层交换机通过 2000Mb/s 链路连接核心层交换机。
- 为提高服务器访问速率,每一台服务器通过 1000Mb/s 链路连接数据中心交换机。由于数据中心交换机连接多台服务器,因此数据中心交换机通过 2000Mb/s 链路连接核心层交换机。

3.2.3 AC+瘦 AP 结构和设计原则

1. AC+瘦 AP 结构

分布在各个教室的 AP 是瘦 AP,瘦 AP 不需要通过人工逐一配置,而是由无线控制器(AC)统一配置。AC+瘦 AP 的一种典型结构如图 3.3 所示,AC 和瘦 AP 连接在同一个 VLAN 上,该 VLAN 通常是本地 VLAN,通过本地 VLAN 传输的 MAC 帧无须携带 VLAN ID。默认情况下,VLAN 1 是本地 VLAN。图 3.3 中的各个瘦 AP 首先需要通过广播发现 AC,获取自己的网络信息,建立与 AC 之间的隧道,然后由 AC 推送配置信息。每一个 AP 可以绑定多个 WLAN,每一个 WLAN 有着独立的服务集标识符(Service Set Identifier,SSID)和加密及鉴别方式。不同的 WLAN 可以绑定不同的 VLAN。这里,每

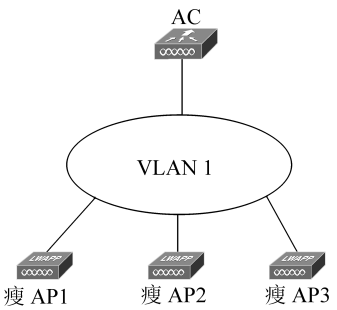

图 3.3 AC+瘦 AP 结构

一个 AP 绑定两个 WLAN，分别是连接学生移动终端的 WLAN 和连接教师移动终端的 WLAN。为平衡负载，将教室 1、教室 2 和教室 3 中瘦 AP 绑定的这两个 WLAN 分别关联 VLAN 2 和 VLAN 4，将教室 4 和教室 5 中瘦 AP 绑定的这两个 WLAN 分别关联 VLAN 3 和 VLAN 5。

2. 设计原则

- 将瘦 AP 和 AC 连接在同一个本地 VLAN。瘦 AP 加电后通过广播无线接入点控制和配置协议（Control And Provisioning of Wireless Access Points Protocol，CAPWAP）报文发现 AC，且封装 CAPWAP 报文的 MAC 帧不携带 VLAN ID。因此，为保证瘦 AP 广播的不带 VLAN ID 的 MAC 帧到达 AC，瘦 AP 和 AC 必须连接在同一个本地 VLAN 上。
- AC 自动为瘦 AP 分配网络信息。瘦 AP 分配 IP 地址后才能建立与 AC 之间的隧道。因此，在瘦 AP 发现 AC 后，由 AC 通过 DHCP 为瘦 AP 分配网络信息。

3.2.4　安全系统功能和设计原则

1. 安全系统功能

- 将交换机端口与 IP 地址和 MAC 地址对绑定，以防止源 IP 地址欺骗攻击和 ARP 欺骗攻击。
- 通过将教师移动终端、学生移动终端和固定终端接入不同的 VLAN 和将不同的服务器接入不同的 VLAN，建立如下访问控制策略。
  - 不允许学生移动终端访问 FTP 服务器，但允许访问其他服务器。
  - 允许教师移动终端访问所有服务器。
  - 不允许固定终端访问 E-mail 服务器，但允许访问其他服务器。
- 启动 OSPF 的安全路由功能，防止路由项欺骗攻击。
- 通过限制终端与服务器之间未完成的 TCP 连接数量，防止对服务器的 DoS 攻击。

2. 安全系统设计原则

- 由二层交换机通过 DHCP 侦听建立 DHCP 侦听库，通过 DHCP 侦听库建立交换机端口、IP 地址和 MAC 地址之间的关联。
- 将 AC 与瘦 AP 之间通信的网络与 VLAN 1 绑定，且 VLAN 1 是本地 VLAN。为平衡负载，将教室 1、教室 2 和教室 3 中连接学生移动终端的 WLAN 与 VLAN 2 绑定，连接教师移动终端的 WLAN 与 VLAN 4 绑定，将这三个教室的固定终端连接到 VLAN 6 上。同时，将教室 4 和教室 5 中连接学生移动终端的 WLAN 与 VLAN 3 绑定，连接教师移动终端的 WLAN 与 VLAN 5 绑定，将这两个教室的固定终端连接到 VLAN 7 上。
- 在三层交换机中启动防 OSPF 路由项欺骗攻击功能。
- 在三层交换机中设置无状态分组过滤器，实施不允许学生移动终端访问 FTP 服务器和不允许固定终端访问 E-mail 服务器的安全策略。

3.2.5　设备选型和配置

1. 设备选型依据

接入层设备选择二层交换机，汇聚层和核心层设备选择三层交换机。接入层设备选择

二层交换机的依据如下。

- 接入层需要具有 VLAN 划分功能。
- 接入层需要具有接入控制和防御 ARP 欺骗攻击、源 IP 地址欺骗攻击及伪造 DHCP 服务器攻击等功能。
- 终端和服务器需要提供全双工通信方式。
- 接入层一般不需要提供 VLAN 间路由功能。
- 由于接入层设备的量比较大,因此采用相对比较便宜的设备。

汇聚层设备选择三层交换机的依据如下。

- 需要汇聚层设备支持跨接入层设备的 VLAN 划分。
- 需要汇聚层设备实现 VLAN 间路由功能。
- 需要汇聚层设备实现资源访问控制功能。
- 需要汇聚层设备灵活分配连接核心层设备和接入层设备的链路的带宽。
- 需要汇聚层设备生成端到端 IP 传输路径。

核心层设备选择三层交换机的依据如下。

- 需要核心层设备具有高速转发 IP 分组的功能。
- 需要核心层设备灵活分配连接汇聚层设备的链路的带宽。

选择 AC+瘦 AP 结构的依据如下。

- 瘦 AP 分布在各个教室,人工逐一配置的工作量太大,而且容易发生配置不一致问题。
- 选择 AC+瘦 AP 结构使得瘦 AP 可以即插即用,降低了维护和更换瘦 AP 的工作量。
- 便于对瘦 AP 进行集中管理。

2. 设备配置

各个交换机的端口配置如表 3.1 所示,表中的交换机编号与图 3.4 中一致。假设每一个教室中的接入层交换机连接一个固定终端和一台瘦 AP,根据数据通信网络设计要求,每一台接入层交换机需要提供一个用于连接固定终端的 100Base-TX 端口、一个用于连接瘦 AP 的 1000Base-TX 端口和一个用于连接与办公楼之间的 1000Mb/s 的光纤链路的 1000Base-LX 端口。数据中心中的接入层交换机需要提供 6 个用于连接 6 台服务器的 1000Base-TX 端口。此外,需要提供 2 个 1000Base-LX 端口,这两个 1000Base-LX 端口通过端口聚合技术聚合为一个 2000Mb/s 的端口通道,用于实现与主楼核心层交换机之间的 2000Mb/s 的物理连接。

办公楼 1 中的汇聚层交换机需要提供 5 个 1000Base-LX 端口,其中 3 个 1000Base-LX 端口分别用于连接与教室 1、教室 2 和教室 3 中接入层交换机之间的 1000Mb/s 的光纤链路。2 个 1000Base-LX 端口通过端口聚合技术聚合为一个 2000Mb/s 的端口通道,用于实现与主楼核心层交换机之间的 2000Mb/s 的物理连接。

办公楼 2 中的汇聚层交换机需要提供 4 个 1000Base-LX 端口,其中 2 个 1000Base-LX 端口分别用于连接与教室 4 和教室 5 中接入层交换机之间的 1000Mb/s 的光纤链路。2 个 1000Base-LX 端口通过端口聚合技术聚合为一个 2000Mb/s 的端口通道,用于实现与主楼核心层交换机之间的 2000Mb/s 的物理连接。

主楼中的核心层交换机需要提供 6 个 1000Base-LX 端口和一个 1000Base-TX 端口。6 个 1000Base-LX 端口分成三组，每一组包含 2 个 1000Base-LX 端口。每一组的 2 个 1000Base-LX 端口通过端口聚合技术聚合为一个 2000Mb/s 的端口通道，三组共构成 3 个 2000Mb/s 的端口通道，分别用于实现与办公楼 1 中汇聚层交换机之间、与办公楼 2 中汇聚层交换机之间和数据中心中接入层交换机之间的 2000Mb/s 的物理连接。一个 1000Base-TX 端口用于连接 AC。

表 3.1　设备类型和配置

设备名称	类型	100Base-TX 端口	1000Base-TX 端口	1000Base-LX 端口
S1	二层交换机	1	1	1
S2	二层交换机	1	1	1
S3	二层交换机	1	1	1
S4	二层交换机	1	1	1
S5	二层交换机	1	1	1
S6	二层交换机		6	2
S7	三层交换机			5
S8	三层交换机			4
S9	三层交换机		1	6

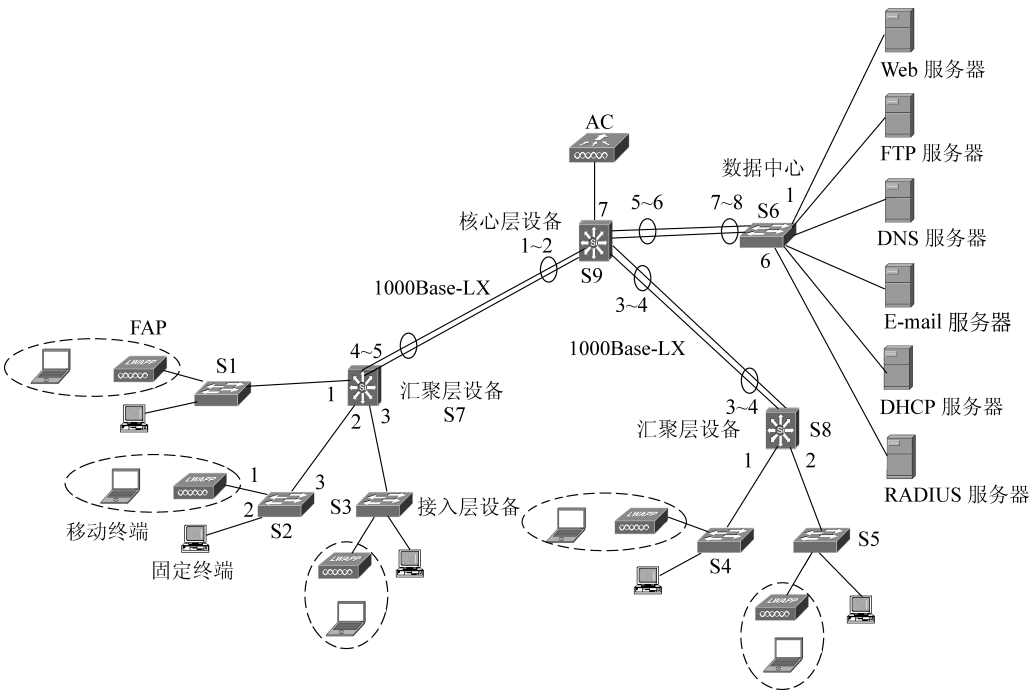

图 3.4　交换机端口分配方式

3.3 数据通信网络实现过程

数据通信网络实现过程涉及链路聚合、AC+瘦 AP 无线局域网结构、VLAN 划分、OSPF 配置及路由表生成过程等。

3.3.1 链路聚合

交换机 S6、S7、S8 和 S9 通过链路聚合技术建立端口通道,各个交换机建立的端口通道及该端口通道包含的交换机端口如表 3.2 所示。

表 3.2 各个交换机建立的端口通道及各个端口通道包含的交换机端口

交换机	端口通道	端口	交换机	端口通道	端口
S6	Port Channel 1	端口 7 和端口 8	S9	Port Channel 1	端口 1 和端口 2
S7	Port Channel 1	端口 4 和端口 5		Port Channel 2	端口 3 和端口 4
S8	PortChannel 1	端口 3 和端口 4		Port Channel 3	端口 5 和端口 6

3.3.2 AC 配置

AC 需要创建 4 个 WLAN,如表 3.3 所示。WLAN 1 用于连接教室 1、教室 2 和教室 3 中的学生移动终端,WLAN 2 用于连接教室 1、教室 2 和教室 3 中的教师移动终端,WLAN 3 用于连接教室 4 和教室 5 中的学生移动终端,WLAN 4 用于连接教室 4 和教室 5 中的教师移动终端。WLAN 1 与 VLAN 2 建立关联,WLAN 2 与 VLAN 4 建立关联,这两个 WLAN 需要绑定教室 1、教室 2 和教室 3 中的瘦 AP1、瘦 AP2 和瘦 AP3。WLAN 3 与 VLAN 3 建立关联,WLAN 4 与 VLAN 5 建立关联,这两个 WLAN 需要绑定教室 4 和教室 5 中的瘦 AP4 和瘦 AP5。

表 3.3 AC 需要创建的 4 个 WLAN 及相关参数

WLAN	绑定的 VLAN	SSID	鉴别机制	RADIUS 服务器	密钥	绑定的瘦 AP
WLAN 1	VLAN 2	1234561	WPA2	192.1.8.21	12345678	瘦 AP1、瘦 AP2、瘦 AP3
WLAN 2	VLAN 4	1234562	WPA2-PSK		1234567890	瘦 AP1、瘦 AP2、瘦 AP3
WLAN 3	VLAN 3	1234563	WPA2	192.1.8.21	12345678	瘦 AP4、瘦 AP5
WLAN 4	VLAN 5	1234564	WPA2-PSK		1234567890	瘦 AP4、瘦 AP5

AC 为了能够与瘦 AP 通信,需要与所有瘦 AP 位于同一个 VLAN 中,且该 VLAN 是本地 VLAN,这里将 VLAN 1 作为互联 AC 和瘦 AP 的 VLAN。由 AC 为该 VLAN 定义 IP 接口和配置 IP 地址,同时由 AC 创建本地 VLAN 对应的 DHCP 地址池,为所有瘦 AP 自动分配网络信息。AC 配置的 IP 地址和 DHCP 地址池如表 3.4 所示。

表 3.4　AC 配置的 IP 地址和 DHCP 地址池

AC 配置的 IP 地址	AC 配置的子网掩码	DHCP 地址池
192.168.1.1	255.255.255.0	192.168.1.100～192.168.1.150

3.3.3　VLAN 划分

1. 需要创建的 VLAN 及其功能

在如图 3.4 所示的校园网拓扑结构中创建 15 个 VLAN(VLAN 1 是默认 VLAN),这 15 个 VLAN 的功能如表 3.5 所示。

表 3.5　需要创建的 VLAN 及其功能

VLAN	功　　能
VLAN 1	用于所有瘦 AP 与 AC 之间交换 CAPWAP 消息
VLAN 2	用于连接瘦 AP1、瘦 AP2 和瘦 AP3 连接的学生移动终端
VLAN 3	用于连接瘦 AP4 和瘦 AP5 连接的学生移动终端
VLAN 4	用于连接瘦 AP1、瘦 AP2 和瘦 AP3 连接的教师移动终端
VLAN 5	用于连接瘦 AP4 和瘦 AP5 连接的教师移动终端
VLAN 6	用于连接交换机 S1、S2 和 S3 连接的固定终端
VLAN 7	用于连接交换机 S4 和 S5 连接的固定终端
VLAN 8	用于连接 Web 服务器
VLAN 9	用于连接 FTP 服务器
VLAN 10	用于连接 DNS 服务器
VLAN 11	用于连接 E-mail 服务器
VLAN 12	用于连接 DHCP 服务器
VLAN 13	用于连接 RADIUS 服务器
VLAN 14	用于实现三层交换机 S7 与 S9 互联
VLAN 15	用于实现三层交换机 S8 与 S9 互联

2. 各个交换机 VLAN 与交换机端口的映射

根据图 3.4 所示的交换机端口分配方式,得出表 3.6～表 3.11 所示的各个交换机 VLAN 与交换机端口之间的映射。交换机 S2 和 S3 的 VLAN 与交换机端口之间的映射与交换机 S1 相同,如表 3.6 所示。交换机 S5 的 VLAN 与交换机端口之间的映射与交换机 S4 相同,如表 3.7 所示。建立 VLAN 与交换机端口之间映射的原则如下:如果端口 X 被属于 VLAN Y 的交换路径经过,需要将端口 X 配置给 VLAN Y。如果端口 X 仅被单条属于 VLAN Y 的交换路径经过,端口 X 作为接入端口分配给 VLAN Y。如果端口 X 既被属于 VLAN Y 的交换路径经过,又被属于 VLAN Z 的交换路径经过,端口 X 作为主干端口被 VLAN Y 和 VLAN Z 共享。

属于同一 VLAN 的终端和设备之间需要建立交换路径,属于同一 VLAN 的终端和设备与创建该 VLAN 对应的 IP 接口的三层交换机之间也需要建立交换路径。由于所有瘦 AP 和 AC 属于 VLAN 1,需要建立所有瘦 AP 与 AC 之间的交换路径,因此属于 VLAN 1 的交换路径经过的交换机端口和端口通道如下:交换机 S1、S2、S3、S4 和 S5 的端口 1 和端口 3;交换机 S7 的端口 1、端口 2、端口 3 和端口通道 Port Channel 1;交换机 S8 的端口 1、端口 2 和端口通道 Port Channel 1;交换机 S9 的端口 7、端口通道 Port Channel 1 和端口通道 Port Channel 2。

对于 VLAN 2,需要建立瘦 AP1(交换机 S1 连接的瘦 AP)、瘦 AP2(交换机 S2 连接的瘦 AP)、瘦 AP3(交换机 S3 连接的瘦 AP)和创建 VLAN 2 对应的 IP 接口的三层交换机 S7 之间的交换路径。为允许由 AC 转发数据帧,还需要建立瘦 AP1、瘦 AP2、瘦 AP3 与 AC 之间的交换路径,因此属于 VLAN 2 的交换路径经过的交换机端口和端口通道如下:交换机 S1、S2 和 S3 的端口 1 和端口 3;交换机 S7 的端口 1、端口 2、端口 3 和端口通道 Port Channel 1;交换机 S9 的端口 7 和端口通道 Port Channel 1。属于 VLAN 4 的交换路径经过的交换机端口和端口通道与 VLAN 2 相同。

对于 VLAN 6,需要建立属于 VLAN 6 的固定终端和创建 VLAN 6 对应的 IP 接口的三层交换机 S7 之间的交换路径,因此属于 VLAN 6 的交换路径经过的交换机端口如下:交换机 S1、S2 和 S3 的端口 2 和端口 3;交换机 S7 的端口 1、端口 2 和端口 3。各个交换机其他 VLAN 与交换机端口之间的映射可以通过同样的分析方式导出。

表 3.6　交换机 S1 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口	VLAN	接入端口	主干端口
VLAN 1		端口 1、端口 3	VLAN 4		端口 1、端口 3
VLAN 2		端口 1、端口 3	VLAN 6	端口 2	端口 3

表 3.7　交换机 S4 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口	VLAN	接入端口	主干端口
VLAN 1		端口 1、端口 3	VLAN 5		端口 1、端口 3
VLAN 3		端口 1、端口 3	VLAN 7	端口 2	端口 3

表 3.8　交换机 S6 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口	VLAN	接入端口	主干端口
VLAN 8	端口 1	Port Channel 1	VLAN 11	端口 4	Port Channel 1
VLAN 9	端口 2	Port Channel 1	VLAN 12	端口 5	Port Channel 1
VLAN 10	端口 3	Port Channel 1	VLAN 13	端口 6	Port Channel 1

表 3.9　交换机 S7 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口
VLAN 1		端口 1、端口 2、端口 3、Port Channel 1

续表

VLAN	接入端口	主干端口
VLAN 2		端口 1、端口 2、端口 3、Port Channel 1
VLAN 4		端口 1、端口 2、端口 3、Port Channel 1
VLAN 6		端口 1、端口 2、端口 3
VLAN 14		Port Channel 1

表 3.10　交换机 S8 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口	VLAN	接入端口	主干端口
VLAN 1		端口 1、端口 2、Port Channel 1	VLAN 7		端口 1、端口 2
VLAN 3		端口 1、端口 2、Port Channel 1	VLAN 15		Port Channel 1
VLAN 5		端口 1、端口 2、Port Channel 1			

表 3.11　交换机 S9 的 VLAN 与交换机端口映射表

VLAN	接入端口	主干端口	VLAN	接入端口	主干端口
VLAN 1		Port Channel 1、Port Channel 2、端口 7	VLAN 10		Port Channel 3
VLAN 2		Port Channel 1、端口 7	VLAN 11		Port Channel 3
VLAN 3		Port Channel 2、端口 7	VLAN 12		Port Channel 3
VLAN 4		Port Channel 1、端口 7	VLAN 13		Port Channel 3
VLAN 5		Port Channel 2、端口 7	VLAN 14		Port Channel 1
VLAN 8		Port Channel 3	VLAN 15		Port Channel 2
VLAN 9		Port Channel 3			

3. VLAN 内的 MAC 帧传输过程

属于相同 VLAN 的两个终端之间能够通过 VLAN 内的交换路径实现以这两个终端的 MAC 地址为源和目的 MAC 地址的 MAC 帧的传输过程。

在图 3.5 中，每一个 VLAN 有单独的网桥转发属于该 VLAN 的 MAC 帧，每一个网桥有独立的转发表。假定各个与 VLAN 4 绑定的转发表已经通过地址学习过程建立了如图 3.5 所示的转发表，终端 B 发送给终端 H 的 MAC 帧的传输过程如下。

终端 B 发送给终端 H 的 MAC 帧以终端 B 的 MAC 地址 MAC B 为源 MAC 地址，以终端 H 的 MAC 地址 MAC H 为目的 MAC 地址。这里假定终端 B 已经加入与 VLAN 4 绑定的 WLAN，且瘦 AP1 的转发表中已经建立 MAC 地址为 MAC H。转发端口为瘦 AP1 以太网端口的转发项。因此，当瘦 AP1 通过无线局域网接收到该无线局域网 MAC 帧，确定将其通过以太网端口转发出去后，将该无线局域网 MAC 帧转换成以太网 MAC 帧并为该以太网 MAC 帧添加 VLAN ID＝4。该以太网 MAC 帧经过交换机端口 S1.1 进入交换机 S1，由于交换机端口 S1.1 是被 VLAN 1、VLAN 2 和 VLAN 4 共享的主干端口，且该以太网

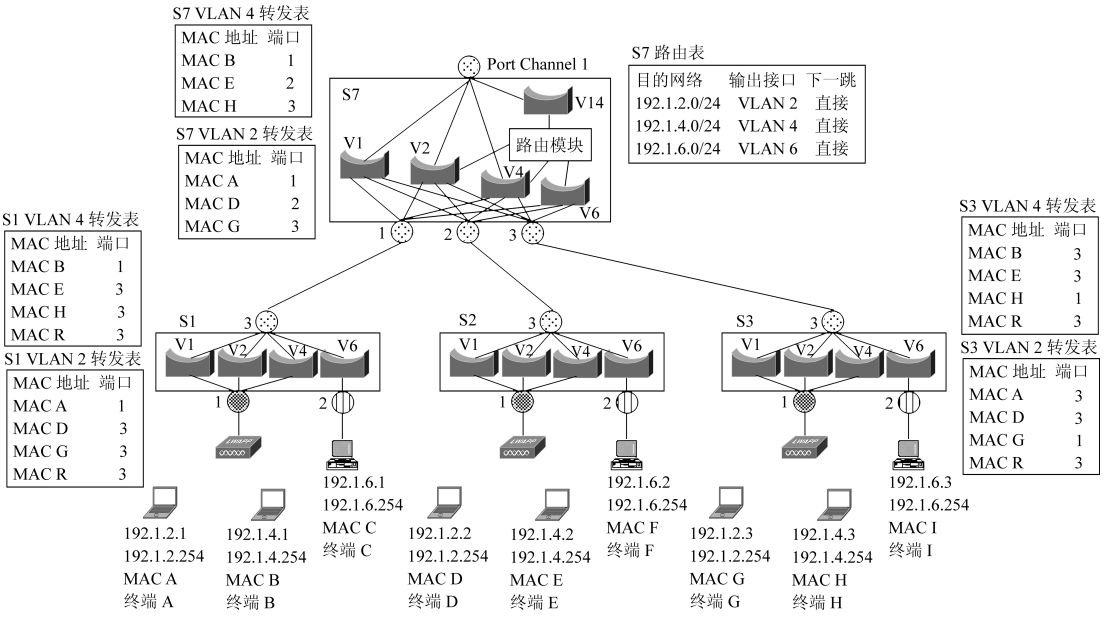

图 3.5　交换路径示意图

MAC 帧携带 VLAN ID=4,因此将其提交给与 VLAN 4 绑定的网桥(图 3.5 中用 V4 表示与 VLAN 4 绑定的网桥)。与 VLAN 4 绑定的网桥在自己的转发表中检索到 MAC 地址为 MAC H 的转发项,确定输出端口是端口 S1.3。由于端口 S1.3 是主干端口(也称为标记端口),因此从该端口输出的 MAC 帧携带 VLAN ID=4。

从端口 S1.3 输出的 MAC 帧经过端口 S7.1 进入交换机 S7,由于端口 S7.1 是被 VLAN 1、VLAN 2、VLAN 4 和 VLAN 6 共享的主干端口且 MAC 帧携带 VLAN ID=4,因此该 MAC 帧被提交给与 VLAN 4 绑定的网桥(图 3.5 中用 V4 表示与 VLAN 4 绑定的网桥)。与 VLAN 4 绑定的网桥在自己的转发表中检索到 MAC 地址为 MAC H 的转发项,确定输出端口是端口 S7.3。由于端口 S7.3 是主干端口(标记端口),因此从该端口输出的 MAC 帧携带 VLAN ID=4。

从端口 S7.3 输出的 MAC 帧经过端口 S3.3 进入交换机 S3,由于端口 S3.3 是 VLAN 1、VLAN 2、VLAN 4 和 VLAN 6 共享的主干端口且 MAC 帧携带 VLAN ID=4,因此该 MAC 帧被提交给与 VLAN 4 绑定的网桥(图 3.5 中用 V4 表示与 VLAN 4 绑定的网桥)。与 VLAN 4 绑定的网桥在自己的转发表中检索到 MAC 地址为 MAC H 的转发项,确定输出端口是端口 S3.1。由于端口 S3.1 是主干端口(标记端口),因此从该端口输出的 MAC 帧携带 VLAN ID=4。

瘦 AP3 通过以太网端口接收到该以太网 MAC 帧,由于该以太网 MAC 帧携带的 VLAN ID=4,确定转发给与 VLAN 4 绑定的 WLAN,因此将该以太网 MAC 帧转换成无线局域网 MAC 帧后,发送给与 VLAN 4 绑定的 WLAN。

3.3.4　VLAN IP 地址分配

1. IP 地址分配过程

IP 地址包括两种分配。

一是需要为每一个 VLAN 分配一个网络地址，网络地址包含的有效 IP 地址数随 VLAN 不同而不同。例如与接入学生移动终端的 WLAN 绑定的 VLAN 2、与接入教师移动终端的 WLAN 绑定的 VLAN 4 和连接固定终端的 VLAN 6，由于需要接入较大量的终端，因此网络前缀位数取值 24，有效 IP 地址数＝2^8－2＝254。划分数据中心中的服务器所产生的 VLAN，由于每一个 VLAN 只连接一台服务器，因此只需要两个有效 IP 地址，一个用于分配给服务器，一个用于分配给该 VLAN 对应的 IP 接口。因此，网络前缀位数取值 30，有效 IP 地址数＝2^2－2＝2。互联三层交换机的 VLAN 由于只需要分别为在两个三层交换机上创建的 IP 接口分配 IP 地址，因此网络前缀位数取值 30。图 3.6 给出了为每一个 VLAN 分配的网络地址。

二是需要为每一个 IP 接口分配 IP 地址。对于连接移动终端、固定终端和服务器所产生 VLAN，该 VLAN 对应的 IP 接口就是连接在该 VLAN 上的移动终端、固定终端或服务器的默认网关地址。为某个 VLAN 对应的 IP 接口分配的 IP 地址和子网掩码确定该 VLAN 的网络地址。如表 3.12 所示，一旦为 VLAN 2 对应的 IP 接口分配 IP 地址和子网掩码 192.1.2.254/24，则 VLAN 2 对应的网络地址为 192.1.2.0/24，连接在 VLAN 2 上的终端的默认网关地址为 192.1.2.254。各个 VLAN 对应的 IP 接口的 IP 地址和子网掩码如表 3.12 所示。在三层交换机 S7 中创建 VLAN 2、VLAN 4、VLAN 6 和 VLAN 14 对应的 IP 接口并为 IP 接口分配 IP 地址和子网掩码后，三层交换机 S7 建立如表 3.13 所示的直连路由项。三层交换机创建某个 VLAN 对应的 IP 接口的前提是，在该三层交换机中创建了该 VLAN 且至少有一个端口（或端口通道）被配置给该 VLAN。当然，该端口既可作为接入端口（非标记端口）也可作为主干端口（标记端口）配置给该 VLAN。

2. VLAN 间的数据传输过程

VLAN 间的数据传输过程是指两个连接在不同 VLAN 上的终端之间的数据传输过程，如图 3.5 中终端 A 和终端 B 之间的数据传输过程。

（1）源和目的终端配置网络信息。每一个连接在 VLAN 上的终端和服务器需要配置 IP 地址、子网掩码和默认网关地址，IP 地址和子网掩码确定的网络地址必须与分配给该 VLAN 的网络地址相同，且该 IP 地址没有分配给连接在同一 VLAN 中的其他终端和服务器。默认网关地址是分配给该 VLAN 对应的 IP 接口的 IP 地址，如图 3.5 中终端 A 分配的 IP 地址、子网掩码和默认网关地址分别是 192.1.2.1/24 和 192.1.2.254。

（2）发送终端获取接收终端的 IP 地址。发送终端向接收终端传输数据前，必须获取接收终端的 IP 地址。例如终端 A 向终端 B 传输数据前，终端 A 必须获取终端 B 的 IP 地址 192.1.4.1。

（3）发送终端确定与接收终端不在同一个 VLAN 上。发送终端通过用自己的子网掩码与接收终端的 IP 地址进行“与”操作求出接收终端的网络地址，如果接收终端的网络地址与自己的网络地址不同，则确定接收终端与自己不在同一个 VLAN 上。终端 A 的网络地址为 192.1.2.0/24，用子网掩码 255.255.255.0 与终端 B 的 IP 地址 192.1.4.1 进行“与”操作，得到结果 192.1.4.0。由于 192.1.4.0/24 不等于 192.1.2.0/24，因此确定终端 A 和终端 B 不在同一个 VLAN 上。

（4）发送终端解析出 IP 接口的 MAC 地址。对于 VLAN 间的数据传输过程，发送终端首先把 IP 分组发送给自己的默认网关。由于默认网关是发送终端所连接的 VLAN 所对应

的IP接口,因此发送给默认网关的IP分组必须封装成以发送终端的MAC地址为源MAC地址、以默认网关的MAC地址为目的MAC地址的MAC帧,发送终端连接的VLAN必须将这样的MAC帧传输给该VLAN对应的IP接口。在图3.5中,终端A发送给三层交换机S7 VLAN 2对应的IP接口的MAC帧必须转发给S7中的路由模块。每一个三层交换机用一个(或若干个)特殊的MAC地址表示接收端是三层交换机中的路由模块。因此,如果三层交换机接收到解析IP接口地址的ARP请求帧,则用该特殊MAC地址作为该IP接口的MAC地址,在图3.5中,统一用MAC地址MAC R作为三层交换机S7的特殊MAC地址。因此,终端A解析IP地址192.1.2.254得到的MAC地址是MAC R。

(5) 发送终端向IP接口传输IP分组。发送终端构建以自己的IP地址为源IP地址、以接收终端的IP地址为目的IP地址的IP分组,并且将IP分组封装成以发送终端的MAC地址为源MAC地址、以IP接口的MAC地址为目的MAC地址的MAC帧,通过连接IP接口的VLAN将MAC帧发送给IP接口。对于终端A至终端B的数据传输过程,终端A构建以192.1.2.1为源IP地址、以192.1.4.1为目的IP地址的IP分组,并且将IP分组封装成以MAC A为源MAC地址、以MAC R为目的MAC地址、以瘦AP1的MAC地址为接收端MAC地址的无线局域网MAC帧,通过WLAN 1将无线局域网MAC帧发送给瘦AP1。瘦AP1将该无线局域网MAC帧转换成以太网MAC帧,携带VLAN ID=2,并且发送给交换机S1。交换机S1通过端口S1.1接收到该MAC帧,将其提交给与VLAN 2绑定的网桥。与VLAN 2绑定的网桥在自己的转发表中检索到MAC地址为MAC R的转发项,确定输出端口是端口S1.3。由于端口S1.3是主干端口(标记端口),因此从该端口输出的MAC帧携带VLAN ID=2。从端口S1.3输出的MAC帧经过端口S7.1进入交换机S7,由于该MAC帧的目的地址是三层交换机S7用于标识路由模块的特殊MAC地址,因此S7将其提交给路由模块。

(6) 路由模块转发IP分组。三层交换机S7中的路由模块从MAC帧中分离出IP分组,用IP分组的目的IP地址192.1.4.1检索路由表,找到匹配的路由项<192.1.4.0/24,VLAN 4,直接>,确定通过VLAN 4将该IP分组发送给终端B。路由模块通过ARP地址解析过程获取终端B的MAC地址MAC B,重新将IP分组封装成以IP接口的MAC地址MAC R为源MAC地址、以终端B的MAC地址MAC B为目的MAC地址的MAC帧,并且将该MAC帧提交给与VLAN 4绑定的网桥。

(7) IP接口向目的终端发送IP分组。三层交换机S7中与VLAN 4绑定的网桥在自己的转发表中检索到MAC地址为MAC B的转发项,确定输出端口是端口S7.1。由于端口S7.1是主干端口(标记端口),因此从该端口输出的MAC帧携带VLAN ID=4。从端口S7.1输出的MAC帧经过端口S1.3进入交换机S1,由于端口S1.3是被VLAN 1、VLAN 2、VLAN 4和VLAN 6共享的主干端口且MAC帧携带VLAN ID=4,因此该MAC帧被提交给与VLAN 4绑定的网桥。与VLAN 4绑定的网桥在自己的转发表中检索到MAC地址为MAC B的转发项,确定输出端口是端口S1.1。由于端口S1.1是主干端口,因此从该端口输出的MAC帧携带VLAN ID=4。从端口S1.1输出的MAC帧到达瘦AP1,瘦AP1将其转换成无线局域网MAC帧,通过WLAN 2发送给终端B。终端B从MAC帧中分离出IP分组,实现IP分组从终端A至终端B的传输过程。

值得强调的是三层交换机 S7 的作用。在终端 B 至终端 H 的 MAC 帧传输过程中，三层交换机 S7 完全等同于二层交换机，根据 MAC 帧携带的 VLAN ID 和 MAC 帧的目的 MAC 地址完成 MAC 帧从端口 1 至端口 3 的交换过程。在终端 A 至终端 B 的 IP 分组传输过程中，三层交换机 S7 既实现 IP 分组路由功能，又实现 MAC 帧转发功能。当 S7 通过端口 1 接收到 MAC 帧时，由于 MAC 帧的目的 MAC 地址是用于表明接收端是路由模块的特殊 MAC 地址，因此 S7 直接将 MAC 帧提交给路由模块。由路由模块从以表明接收端是路由模块的特殊 MAC 地址为目的 MAC 地址、VLAN ID＝2 的 MAC 帧中分离出 IP 分组，并且重新将 IP 分组封装成以 MAC B 为目的 MAC 地址、VLAN ID＝4 的 MAC 帧。由 S7 二层交换功能完成根据 MAC 帧携带的 VLAN ID 和 MAC 帧的目的 MAC 地址确定 MAC 帧输出端口并将 MAC 帧通过端口 1 转发出去的过程。

3.3.5　OSPF 建立路由表的过程

1. 直连路由项

根据表 3.12 所示的内容为各个 IP 接口分配 IP 地址和子网掩码后，分配给各个 VLAN 的网络地址如图 3.6 所示。三个三层交换机 S7、S8 和 S9 中自动生成的直连路由项如表 3.13～表 3.15 所示。三层交换机自动生成直连路由项后，可以实现直接连接的 VLAN 之间的通信过程，如三层交换机 S7 实现的 VLAN 2 和 VLAN 4 之间的通信过程。如果需要实现两个连接在不同三层交换机上的 VLAN 之间的通信过程，各个三层交换机需要通过路由协议建立用于指明通往没有与其直接连接的 VLAN 的传输路径的路由项。

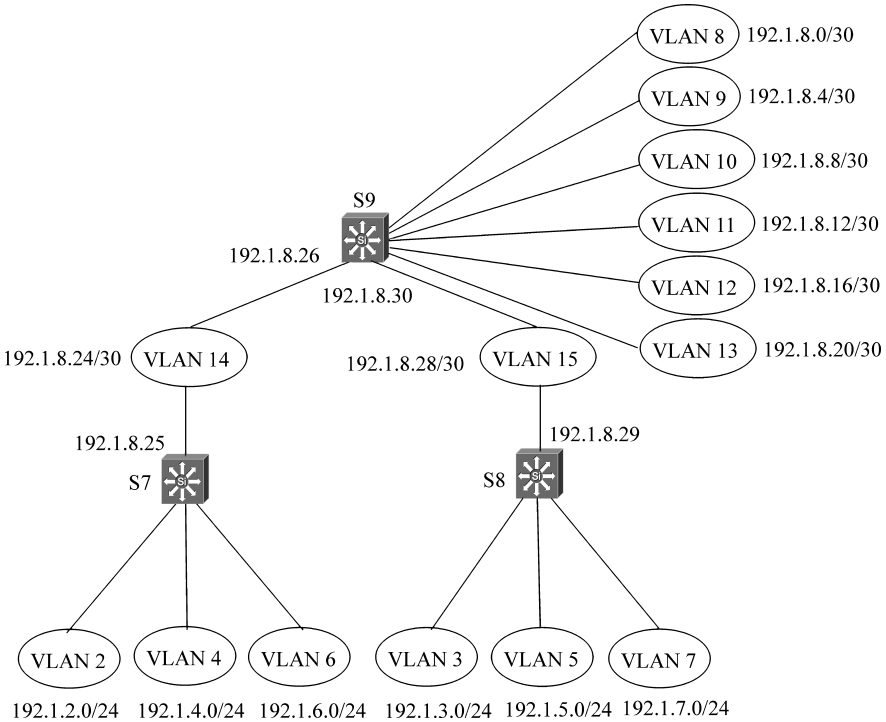

图 3.6　VLAN IP 地址分配结果

表 3.12　IP 接口分配的 IP 地址

设备名称	IP 接口	IP 地址	设备名称	IP 接口	IP 地址
S7	VLAN 2	192.1.2.254/24	S9	VLAN 8	192.1.8.2/30
S7	VLAN 4	192.1.4.254/24	S9	VLAN 9	192.1.8.6/30
S7	VLAN 6	192.1.6.254/24	S9	VLAN 10	192.1.8.10/30
S7	VLAN 14	192.1.8.25/30	S9	VLAN 11	192.1.8.14/30
S8	VLAN 3	192.1.3.254/24	S9	VLAN 12	192.1.8.18/30
S8	VLAN 5	192.1.5.254/24	S9	VLAN 13	192.1.8.22/30
S8	VLAN 7	192.1.7.254/24	S9	VLAN 14	192.1.8.26/30
S8	VLAN 15	192.1.8.29/30	S9	VLAN 15	192.1.8.30/30

表 3.13　三层交换机 S7 的直连路由项

目的网络	输出接口	下一跳	目的网络	输出接口	下一跳
192.1.2.0/24	VLAN 2	直接	192.1.6.0/24	VLAN 6	直接
192.1.4.0/24	VLAN 4	直接	192.1.8.24/30	VLAN 14	直接

表 3.14　三层交换机 S8 的直连路由项

目的网络	输出接口	下一跳	目的网络	输出接口	下一跳
192.1.3.0/24	VLAN 3	直接	192.1.7.0/24	VLAN 7	直接
192.1.5.0/24	VLAN 5	直接	192.1.8.28/30	VLAN 15	直接

表 3.15　三层交换机 S9 的直连路由项

目的网络	输出接口	下一跳	目的网络	输出接口	下一跳
192.1.8.0/30	VLAN 8	直接	192.1.8.16/30	VLAN 12	直接
192.1.8.4/30	VLAN 9	直接	192.1.8.20/30	VLAN 13	直接
192.1.8.8/30	VLAN 10	直接	192.1.8.24/30	VLAN 14	直接
192.1.8.12/30	VLAN 11	直接	192.1.8.28/30	VLAN 15	直接

2. OSPF 配置

OSPF 配置的内容：一是在各个三层交换机的 IP 接口上启动 OSPF 路由进程；二是为各个三层交换机的 IP 接口分配相同的区域标识符，表明所有三层交换机的 IP 接口属于同一个 OSPF 区域；三层交换机完成上述配置后，通过发现与其直接连接的网络(VLAN)和其他三层交换机的 IP 接口，建立自身链路状态。表 3.16 所示的三层交换机 S7 的链路状态，其内容包括直接连接的网络 192.1.2.0/24、192.1.4.0/24、192.1.6.0/24 和 IP 地址为 192.1.8.25 的 IP 接口。一般情况下，传输速率小于或等于 100Mb/s 的链路的链路代价采用默认值，端口通道及传输速率大于 100Mb/s 的链路的链路代价通过手动配置确定。

各个三层交换机建立自身链路状态后，通过泛洪链路状态通告(LSA)向其他三层交换

机发送自身链路状态，使得每一个三层交换机建立如表 3.16 所示的链路状态数据库，链路状态数据库给出同一 OSPF 区域内所有 IP 接口连接的网络和相邻的其他 IP 接口。

表 3.16　链路状态数据库

S7 链路状态					
邻居	邻居接口 IP 地址	链路代价	邻居	邻居接口 IP 地址	链路代价
S9	192.1.8.26	1	192.1.4.0/24		1
192.1.2.0/24		1	192.1.6.0/24		1
S8 链路状态					
S9	192.1.8.30	1	192.1.5.0/24		1
192.1.3.0/24		1	192.1.7.0/24		1
S9 链路状态					
S7	192.1.8.25	1	192.1.8.8/30		1
S8	192.1.8.29	1	192.1.8.12/30		1
192.1.8.0/30		1	192.1.8.16/30		1
192.1.8.4/30		1	192.1.8.20/30		1

3. 最终路由表

每一个三层交换机根据表 3.16 所示的链路状态数据库，构建用于指明通往没有与其直接连接的网络的传输路径的路由项，生成最终路由表。三层交换机 S7、S7 和 S9 的最终路由表如表 3.17～表 3.19 所示。

表 3.17　三层交换机 S7 的路由表

目的网络	输出接口	下一跳	链路代价	目的网络	输出接口	下一跳	链路代价
192.1.2.0/24	VLAN 2	直接	0	192.1.8.0/30	VLAN 14	192.1.8.26	2
192.1.4.0/24	VLAN 4	直接	0	192.1.8.4/30	VLAN 14	192.1.8.26	2
192.1.6.0/24	VLAN 6	直接	0	192.1.8.8/30	VLAN 14	192.1.8.26	2
192.1.8.24/30	VLAN 14	直接	0	192.1.8.12/30	VLAN 14	192.1.8.26	2
192.1.3.0/24	VLAN 14	192.1.8.26	3	192.1.8.16/30	VLAN 14	192.1.8.26	2
192.1.5.0/24	VLAN 14	192.1.8.26	3	192.1.8.20/30	VLAN 14	192.1.8.26	2
192.1.7.0/24	VLAN 14	192.1.8.26	3	192.1.8.28/30	VLAN 14	192.1.8.26	2

4. 端到端传输过程

终端 A 分配如图 3.5 所示的 IP 地址、子网掩码和默认网关地址。如果各个 IP 接口分配了表 3.12 所示的 IP 地址，Web 服务器只能分配 IP 地址、子网掩码和默认网关地址 192.1.8.1/30 和 192.1.8.2。终端 A 如果向 Web 服务器发送数据，则它构建以 192.1.2.1 为源 IP

表 3.18　三层交换机 S8 的路由表

目的网络	输出接口	下一跳	链路代价	目的网络	输出接口	下一跳	链路代价
192.1.3.0/24	VLAN 3	直接	0	192.1.8.0/30	VLAN 15	192.1.8.30	2
192.1.5.0/24	VLAN 5	直接	0	192.1.8.4/30	VLAN 15	192.1.8.30	2
192.1.7.0/24	VLAN 7	直接	0	192.1.8.8/30	VLAN 15	192.1.8.30	2
192.1.8.28/30	VLAN 15	直接	0	192.1.8.12/30	VLAN 15	192.1.8.30	2
192.1.2.0/24	VLAN 15	192.1.8.30	3	192.1.8.16/30	VLAN 15	192.1.8.30	2
192.1.4.0/24	VLAN 15	192.1.8.30	3	192.1.8.20/30	VLAN 15	192.1.8.30	2
192.1.6.0/24	VLAN 15	192.1.8.30	3				

表 3.19　三层交换机 S9 的路由表

目的网络	输出接口	下一跳	链路代价	目的网络	输出接口	下一跳	链路代价
192.1.8.0/30	VLAN 8	直接	0	192.1.8.28/30	VLAN 15	直接	0
192.1.8.4/30	VLAN 9	直接	0	192.1.2.0/24	VLAN 14	192.1.8.25	2
192.1.8.8/30	VLAN 10	直接	0	192.1.4.0/24	VLAN 14	192.1.8.25	2
192.1.8.12/30	VLAN 11	直接	0	192.1.6.0/24	VLAN 14	192.1.8.25	2
192.1.8.16/30	VLAN 12	直接	0	192.1.3.0/24	VLAN 15	192.1.8.29	2
192.1.8.20/30	VLAN 13	直接	0	192.1.5.0/24	VLAN 15	192.1.8.29	2
192.1.8.24/30	VLAN 14	直接	0	192.1.7.0/24	VLAN 15	192.1.8.29	2

地址、以 192.1.8.1 为目的 IP 地址的 IP 分组，并且将该 IP 分组封装成以终端 A 的 MAC 地址为源 MAC 地址、以表明接收端是 S7 路由模块的特殊 MAC 地址为目的 MAC 地址的 MAC 帧，通过 VLAN 2 内交换路径将该 MAC 帧发送给 VLAN 2 对应的 IP 接口。S7 路由模块根据该 IP 分组的目的 IP 地址检索路由表，确定与路由项＜192.1.8.0/30，VLAN 14，192.1.8.26＞匹配，将该 IP 分组重新封装成以表明发送端是 S7 路由模块的特殊 MAC 地址为源 MAC 地址、以表明接收端是 S9 路由模块的特殊 MAC 地址为目的 MAC 地址的 MAC 帧，通过 VLAN 14 内的交换路径将该 MAC 帧发送给交换机 S9 中 VLAN 14 对应的 IP 接口。S9 路由模块根据该 IP 分组的目的 IP 地址检索路由表，确定与路由项＜192.1.8.0/30，VLAN 8，直接＞匹配，将该 IP 分组重新封装成以表明发送端是 S9 路由模块的特殊 MAC 地址为源 MAC 地址、以 Web 服务器的 MAC 地址为目的 MAC 地址的 MAC 帧，通过 VLAN 8 内的交换路径将 MAC 帧发送给 Web 服务器。

3.4　安全系统实现过程

安全系统实现过程涉及 DHCP 侦听信息库建立过程、安全路由实现过程和分组过滤器配置过程等。

3.4.1　启动接入交换机的 DHCP 侦听功能

1. 建立 DHCP 侦听信息库

校园网中所有移动终端和固定终端通过 DHCP 自动从 DHCP 服务器中获取网络信息，终端获取的网络信息如图 3.7 所示。为防御源 IP 地址欺骗攻击和 ARP 欺骗攻击，在接入交换机 S1、S2、S3、S4 和 S5 中启动 DHCP 侦听功能。启动 DHCP 侦听功能后，一旦终端通过 DHCP 自动获取如图 3.7 所示的网络信息，则接入交换机 S1、S2、S3、S4 和 S5 中建立分别如表 3.20～表 3.24 所示的 DHCP 侦听信息库。侦听信息库中为每一个连接到接入交换机的终端创建一项终端信息绑定项。

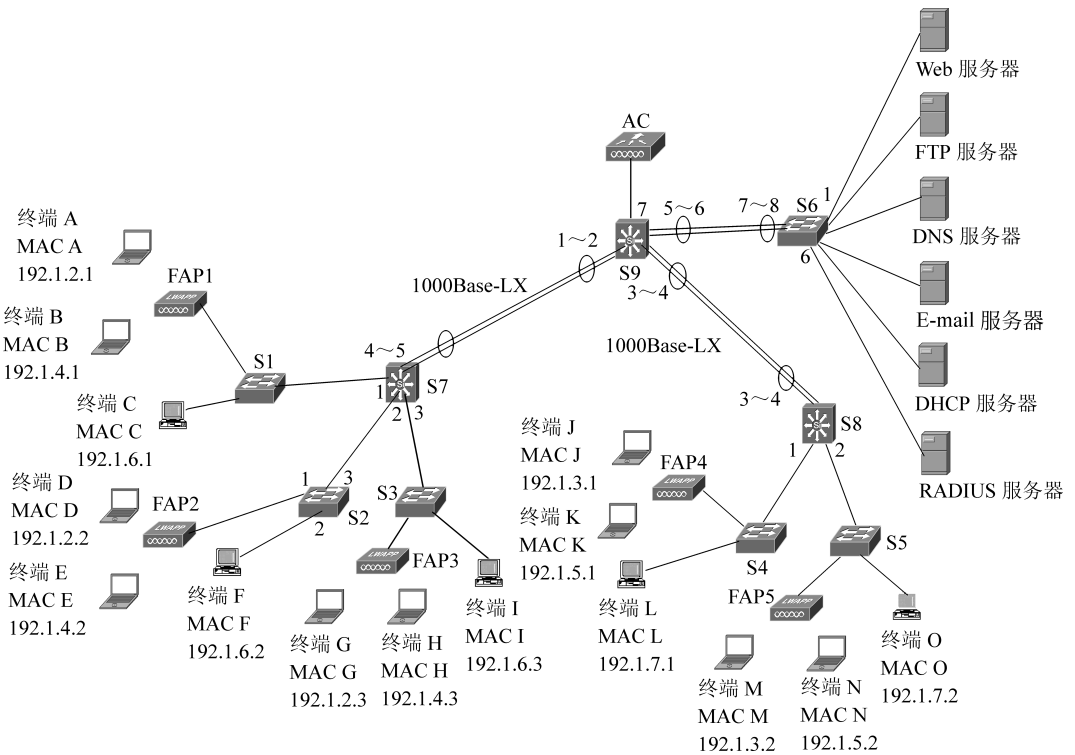

图 3.7　端口安全机制

表 3.20　交换机 S1 的 DHCP 侦听信息库

交换机端口	MAC 地址	IP 地址	VLAN
端口 1	MAC A	192.1.2.1	VLAN 2
端口 1	MAC B	192.1.4.1	VLAN 4
端口 2	MAC C	192.1.6.1	VLAN 6

表 3.21　交换机 S2 的 DHCP 侦听信息库

交换机端口	MAC 地址	IP 地址	VLAN
端口 1	MAC D	192.1.2.2	VLAN 2
端口 1	MAC E	192.1.4.2	VLAN 4
端口 2	MAC F	192.1.6.2	VLAN 6

2. 防御 ARP 欺骗攻击

图 3.7 中终端 G 实施 ARP 欺骗攻击的过程如下：终端 G 故意发送将 IP 地址 192.1.2.1 与 MAC 地址 MAC G 绑定的 ARP 请求报文，使得在 VLAN 2 中的其他终端的 ARP 缓冲

表 3.22　交换机 S3 的 DHCP 侦听信息库

交换机端口	MAC 地址	IP 地址	VLAN
端口 1	MAC G	192.1.2.3	VLAN 2
端口 1	MAC H	192.1.4.3	VLAN 4
端口 2	MAC I	192.1.6.3	VLAN 6

表 3.23　交换机 S4 的 DHCP 侦听信息库

交换机端口	MAC 地址	IP 地址	VLAN
端口 1	MAC J	192.1.3.1	VLAN 3
端口 1	MAC K	192.1.5.1	VLAN 5
端口 2	MAC L	192.1.7.1	VLAN 7

表 3.24　交换机 S5 的 DHCP 侦听信息库

交换机端口	MAC 地址	IP 地址	VLAN	交换机端口	MAC 地址	IP 地址	VLAN
端口 1	MAC M	192.1.3.2	VLAN 3	端口 2	MAC O	192.1.7.2	VLAN 7
端口 1	MAC N	192.1.5.2	VLAN 5				

区中建立 IP 地址 192.1.2.1 与 MAC 地址 MAC G 的绑定项。一旦这些终端向 IP 地址为 192.1.2.1 的终端 A 发送 MAC 帧,MAC 帧的目的 MAC 地址错误地设置为 MAC G,该 MAC 帧就被交换式以太网转发给终端 G。

在接入交换机通过 DHCP 侦听建立如表 3.20～表 3.24 所示的 DHCP 侦听信息库后,如果接入交换机 S3 通过端口 1 接收到终端 G 发送的将 IP 地址 192.1.2.1 与 MAC 地址 MAC G 绑定的 ARP 请求报文,它便在如表 3.22 所示的 DHCP 侦听信息库中检索交换机端口为端口 1、IP 地址为 192.1.2.1、MAC 地址为 MAC G 的终端信息绑定项。由于接入交换机 S3 在 DHCP 侦听信息库中检索不到对应项,因此终端 G 发送的用于实施 ARP 欺骗攻击的 ARP 请求报文将被接入交换机 S3 丢弃,无法到达 VLAN 2 中的其他终端。

3. 防御源 IP 地址欺骗攻击

图 3.7 中终端 G 实施源 IP 地址欺骗攻击的过程如下:终端 G 将发送的 IP 分组的源 IP 地址设置成终端 H 的 IP 地址,以此获得终端 H 的访问权限。但在接入交换机通过 DHCP 侦听建立如表 3.20～表 3.24 所示的 DHCP 侦听信息库后,如果接入交换机 S3 通过端口 1 接收源 MAC 地址为终端 G 的 MAC 地址 MAC G 的 MAC 帧,且该 MAC 帧封装的 IP 分组的源 IP 地址为 192.1.4.3,则它将在如表 3.22 所示的 DHCP 侦听信息库中检索 MAC 地址为 MAC G、IP 地址为 192.1.4.3 的终端信息绑定项。由于接入交换机 S3 在 DHCP 侦听信息库中检索不到对应项,它将丢弃该 MAC 帧,因此终端 G 发送的用于实施源 IP 地址欺骗攻击的 IP 分组将被接入交换机 S3 丢弃。

3.4.2　启动安全路由功能

OSPF 安全路由功能包括三部分:一是指定区域内使用的鉴别机制,这里采用 HMAC-MD5 作为计算消息鉴别码(Message Authentication Code,MAC)的算法;二是要求属于该区域的接口发送的路由消息必须携带 HMAC;三是在连接两个相邻三层交换机的 IP 接口上配置相同的密钥。这里连接相邻三层交换机 S7 和 S9 的 IP 接口分别是三层交换机 S7 中 VLAN 14 对应的 IP 接口和三层交换机 S9 中 VLAN 14 对应的 IP 接口,这两个 IP 接口配置相同密钥 1234567890。连接相邻三层交换机 S8 和 S9 的 IP 接口分别是三层交换机 S8 中 VLAN 15 对应的 IP 接口和三层交换机 S9 中 VLAN 15 对应的 IP 接口,这两个 IP 接口

配置相同密钥 0987654321。

3.4.3　分组过滤器

1. 无状态分组过滤器的工作原理

无状态分组过滤器通过规则从 IP 分组流中鉴别出一组 IP 分组，然后对其实施规定的操作。

规则由一组属性值组成，如果某个 IP 分组携带的信息和构成规则的一组属性值匹配，则意味着该 IP 分组和该规则匹配。可对该 IP 分组实施相关操作，相关操作有正常转发和丢弃。

构成规则的属性值通常由下述字段组成。

- 源 IP 地址，用于匹配 IP 分组 IP 首部中的源 IP 地址字段值。
- 目的 IP 地址，用于匹配 IP 分组 IP 首部中的目的 IP 地址字段值。
- 源和目的端口号，用于匹配作为 IP 分组净荷的传输层报文首部中源和目的端口号字段值。
- 协议类型，用于匹配 IP 分组首部中的协议字段值。

一个过滤器可以由多个规则构成，IP 分组只有和当前规则不匹配时，才继续与后续规则进行匹配操作。如果与过滤器中的所有规则都不匹配，则对 IP 分组进行默认操作。IP 分组一旦和某个规则匹配，则对其实施相关操作，不再和其他规则进行匹配操作。因此，IP 分组和规则的匹配操作顺序直接影响该 IP 分组所匹配的规则，也因此确定了对该 IP 分组实施的操作。

无状态分组过滤器可以作用于端口的输入或输出方向，从外部进入无状态分组过滤器称为输入，离开无状态分组过滤器称为输出。如果作用于输入方向，每一个输入 IP 分组都和过滤器中的规则进行匹配操作，如果和某个规则匹配，则对其实施相关操作，如果实施的操作是丢弃，则不再对该 IP 分组进行后续的转发处理。如果过滤器作用于输出方向，则只有当该 IP 分组确定从该端口输出时，才将该 IP 分组和过滤器中的规则进行匹配操作。

2. 分组过滤器配置

校园网安全策略如下。

① 不允许学生移动终端访问 FTP 服务器，但允许访问其他服务器。

② 允许教师移动终端访问所有服务器。

③ 不允许固定终端访问 E-mail 服务器，但允许访问其他服务器。

根据校园网安全策略，在三层交换机 S7 VLAN 2 对应的 IP 接口的输入方向上配置以下分组过滤器。

① 协议＝IP，源 IP 地址＝192.1.2.0/24，目的 IP 地址＝192.1.8.5/32；丢弃。

② 协议＝IP，源 IP 地址＝192.1.2.0/24，目的 IP 地址＝0.0.0.0/0；正常转发。

在三层交换机 S8 VLAN 3 对应的 IP 接口的输入方向上配置以下分组过滤器。

① 协议＝IP，源 IP 地址＝192.1.3.0/24，目的 IP 地址＝192.1.8.5/32；丢弃。

② 协议＝IP，源 IP 地址＝192.1.3.0/24，目的 IP 地址＝0.0.0.0/0；正常转发。

在三层交换机 S7 VLAN 6 对应的 IP 接口的输入方向上配置以下分组过滤器。

① 协议＝IP，源 IP 地址＝192.1.6.0/24，目的 IP 地址＝192.1.8.13/32；丢弃。