项目三

网络交换技术

任务5　了解网络交换中常用的技术

5.1　项目导引

通过一段时间的学习，小张已经初步认识计算机网络中的常用设备，并且对交换机及路由器的可管理性有了一定的了解，并能进行一些基本的交换机与路由器的配置工作。为了更深入地学习网络技术，小张决定对计算机网络的基本知识再进行学习。先学习的内容是交换机在计算机网络中经常用到的技术。

5.2　项目分析

前面的几个任务主要学习计算机网络的结构与组成，企业网络体系结构、在计算机网络中常见的网络设备以及如何解决在构建企业网络时常常遇到的问题。接下来的任务是学习如何对网络进行管理与配置。

以太网是当今现有局域网采用的最通用的通信协议标准，我们通常说的交换机就是以太网交换机的简称。目前，基于OSI模型第二层的以太网技术包括标准以太网、快速以太网、千兆以太网和万兆以太网等。最初的10Mbit/s的标准以太网已经过时，在组建企业网络的时候可以不需要再考虑选择它。而且因为10/100/1000Mbit/s自适应以太网的成本已经较低，所以100Mbit/s快速以太网已经不是主流，已经成为非常普遍使用的网络技术，正在缓慢地淡出。本部分讨论设计和组建多层交换网络中实现交换机和模块之间互联的各种数据链路层技术。

5.3　技术准备

5.3.1　标准以太网10Mbps

开始以太网只有10Mbps的吞吐量，使用的是带有冲突检测的载波侦听多路访问

(CSMA/CD,Carrier Sense Multiple Access/Collision Detection)的访问控制方法。这种早期的 10Mbps 以太网称之为标准以太网,以太网可以使用粗同轴电缆、细同轴电缆、非屏蔽双绞线、屏蔽双绞线和光纤等多种传输介质进行连接。并且在 IEEE 802.3 标准中,为不同的传输介质制定了不同的物理层标准,如 10Base-T、10Base-5、10Base-2、10Base-F 等。

与 10Mbps 的标准以太网相比较,快速以太网和千兆以太网技术更加先进,并且具有更低的成本,所以 10Mbps 以太网现在已经不再使用,除非是在较旧的计算机网络中,或者需要连接老式设备,否则通常不在企业网络中使用 10Mbps 标准以太网。但在目前的智能家居网络中,使用 ADSL 宽带上网的人群中还时常出现这种应用。现在绝大多数的宽带用户网络最高只能提供 8-10Mbit/s 的带宽,所以就没有必要使用 100Mbps 快速以太网技术。

5.3.2 快速以太网

随着计算机网络的快速发展,传统的标准以太网技术已经不能满足快速增长的网络数据流量传输速度的需求。在 1993 年 10 月以前,对于要求 10Mbps 以上数据流量的局域网应用,只有光纤分布式数据接口(FDDI)可供选择,而它是一种价格非常昂贵的、基于 100Mpbs 光缆的局域网技术。由于价格昂贵,也只能用在企业网的主干,所以不能解决网络数据的传输问题。

1993 年 10 月,Grand Junction 公司推出了世界上第一台快速以太网集线器 Fastch10/100 和网络接口卡 FastNIC100,从而使快速以太网技术正式得以应用。随后 Intel、SynOptics、3COM、BayNetworks 等公司亦相继推出自己的快速以太网装置。与此同时,IEEE802 工程组也对 100Mbps 以太网的各种标准,如 100BASE-TX、100BASE-T4、全双工等标准进行了研究。1995 年 3 月 IEEE 宣布了 IEEE802.3u 100BASE-T 快速以太网标准(Fast Ethernet),就这样开始了快速以太网的时代。

从网络规划更实用的观点出发,还是应该使用快速以太网技术做为网络工作区终端设备接入技术。因其传输速率为 100Mbit/s,完全能满足目前的企业网络的数据传输。同时快速以太网技术还能向下兼容标准以太网,支持 10Base-T 的差错控制功能、帧格式和帧长度等。快速以太网在接口与传输介质等方面都可以实现向更新的以太网技术平滑地过渡,利用自适应技术,在千兆以太网的情况下它们能够有选择地支持自动协商到 10Mbit/s 和 100Mbit/s。

快速以太网设备通常支持全双工操作,它可以将有效带宽加倍到 200Mbit/s。在缺少自动协商的情况下,快速以太网默认支持半双工操作。

根据规范的定义,快速以太网可以运行在 UTP 和光纤上,快速以太网规范所定义的各种线缆类型和最大线缆长度如表 5-1 所示。

100BASE-TX:是一种使用 5 类非屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用两对双绞线,一对用于发送,一对用于接收数据。在传输中使用 4B/5B 编码方式,信号频率为 125MHz。使用同 10BASE-T 相同的 RJ-45 连接器。它的最大网段长度为 100 米。支持全双工的数据传输。

100BASE-T4:是一种可使用 3、4、5 类非屏蔽双绞线或屏蔽双绞线的快速以太网技术。100Base-T4 使用 4 对双绞线,其中的三对用于在 33MHz 的频率上传输数据,每一对均工作于半双工模式。第四对用于 CSMA/CD 冲突检测。在传输中使用 8B/6T 编码方式,信号频率为 25MHz。它使用与 10BASE-T 相同的 RJ-45 连接器,最大网段长度为 100 米。

100BASE－FX：是一种使用光缆的快速以太网技术，可使用单模和多模光纤（62.5/125μm）。多模光纤连接的最大距离为550米。单模光纤连接的最大距离为3000米。在传输中使用4B/5B编码方式，信号频率为125MHz。它使用MIC/FDDI连接器、ST连接器或SC连接器。它的最大网段长度为150m、412m、2000m或更长至10公里，这与所使用的光纤类型和工作模式有关，它支持全双工的数据传输。

100BASE－FX特别适合于有电气干扰的环境、较大距离连接、或高保密环境等情况下的适用。

表5-1　　快速以太网线缆标准和最大长度

标准	线缆分类	线缆最大长度	连接器
100BASE－TX	EIA/TIA 5类UTP	100m	RJ-45
100BASE－T4	EIA/TIA 3类-5类/5eUTP(全双工)	100m	RJ-45
100BASE－FX	多模光纤62.5/125 单模光纤	550m(半双工) 3000m(单模光纤)	ST、SC

5.3.3　千兆以太网

千兆以太网技术作为最新的高速以太网技术，给用户带来了提高核心网络的有效解决方案，这种解决方案的最大优点是继承了传统以太网技术价格便宜的优点。千兆技术仍然是以太网技术，它采用了与10M以太网相同的帧格式、帧结构、网络协议、全/半双工工作方式、流控模式以及布线系统。由于该技术不改变传统以太网的桌面应用、操作系统，因此可与10M或100M的以太网很好地配合工作。升级到千兆以太网不必改变网络应用程序、网管部件和网络操作系统，能够最大程度地保护投资。

此外，IEEE标准将支持最大距离为550米的多模光纤、最大距离为70千米的单模光纤和最大距离为100米的同轴电缆。千兆以太网填补了802.3以太网/快速以太网标准的不足。为了能够侦测到64Bytes资料框的碰撞，千兆以太网（Gigabit Ethernet）所支持的距离更短。

Gigabit Ethernet支持的网络类型如表5-2所示。

表5-2　　千兆以太网线缆标准和最大长度

标准	线缆分类	线缆最大长度
1000BASE－CX	铜质屏蔽双绞线	25m
1000BASE－T	5类非屏蔽双绞线	100m
1000BASE－SX	多模光纤62.5/125或50/125 使用波长780nm的激光	260m(使用62.5μm多模光纤) 550m(使用50μm多模光纤)
1000BASE－LX	单模光纤9/125 使用波长1300nm的激光	3000m
1000BASE－ZX	单模光纤9/125 使用波长1550nm的激光	70～100km

在企业网的设计中，如果没有使用万兆以太网链路，那么千兆网就可以设计在园区网络接入部位、建筑群子系统、园区主干网和数据中心的连接中。同时还可以考虑在所有可能之处尽

量采用多个千兆以太网接口进行冗余和负载均衡。在高带宽的企业网络和数据中心，万兆以太网已经成为连接交换机的最主要选择。

千兆以太网也非常适合于将高性能的服务器连接到网络中。高性能应用服务器或视频服务器通常会同时占用 3 到 4 条快速以太网连接。此外，随着服务器和服务器网卡处理能力和数据吞吐率的提高，以及在企业园区网内将服务器集中化的趋势，千兆以太网已经成为数据中心内部网络的必备之选。虚拟化等新技术的实现，更需要万兆甚至更高的数据传输速率。

此外，千兆以太网默认采用全双工操作，进而能够有效地利用 2Gbit/s 带宽。全部千兆以太网技术都要求自动协商，其中自动协商包括检测链路完整性和双工协商的方法。基于上述原因，与快速以太网相比较，吉比特以太网自动协商具有更大的兼容性和弹性。

5.3.4 万兆以太网

万兆以太网是指传输速度为 10Gbit/s 的以太网，其技术与千兆以太网类似，仍然保留了以太网帧结构。通过不同的编码方式或波分复用提供 10Gbit/s 传输速度。

以太网采用 CSMA/CD 机制，即带碰撞检测的载波监听多重访问。千兆以太网接口基本应用在点到点线路，不再共享带宽。碰撞检测，载波监听和多重访问已不再重要。千兆以太网与传统低速以太网最大的相似之处在于采用相同的以太网帧结构。万兆以太网技术与千兆以太网类似，仍然保留了以太网帧结构。通过不同的编码方式或波分复用提供 10Gbit/s 传输速度。所以就其本质而言，10G 以太网仍是以太网的一种类型。

万兆以太网于 2002 年 7 月在 IEEE 通过。10G 以太网包括 10GBASE－X、10GBASE－R 和 10GBASE－W。

10GBASE－X 使用一种特紧凑包装，含有 1 个较简单的 WDM 器件、4 个接收器和 4 个在 1300nm 波长附近以大约 25nm 为间隔工作的激光器，每一对发送器/接收器在 3.125Gbit/s 速度（数据流速度为 2.5Gbit/s）下工作。

10GBASE－R 是一种使用 64B/66B 编码（不是在千兆以太网中所用的 8B/10B）的串行接口，数据流为 10.000Gbit/s，因而产生的时钟速率为 10.3Gbit/s。

10GBASE－W 是广域网接口，与 SONET OC-192 兼容，其时钟为 9.953Gbit/s，数据流为 9.585Gbit/s。

万兆以太网能够为服务提供商和企业网络提供很多的应用。万兆以太网的主要作用就是多个千兆以太网和网段（例如，建筑物建筑群子系统）汇集在一起，进而组建高速主干网络。而某些技术也的确要求非常高的带宽，例如视频和海量数据存储。

目前万兆以太网主要应用于下列方面：

（1）实现服务器集群技术。

（2）汇聚多个千兆网段。

（3）用于数据中心、企业网主干或建筑群子系统。

（4）连接多个多层交换网络。

万兆以太网接口所支持的工作范围与传输介质类型如表 5-3 所示。

表 5-3　　万兆网的典型部署

万兆以太网物理层接口	典型部署	工作范围			
		多模光纤 62.5/125（FDDI 级别）	多模光纤 50/125（MMF）	单模光纤 10/125（SMF）	双绞线
10GBASE-CX4	数据中心	N/A	N/A	N/A	15m
10GBASE-SR	数据中心	28～33m	66～300m	N/A	N/A
10GBASE～LX4	园区或数据中心	300m	240～300m	N/A	N/A
10GBASE-LR	团区或城域网	N/A	N/A	10km	N/A
10GBASE-ER	城域网	N/A	N/A	40km	N/A
10GBASE-ZR	城域网或长途	N/A	N/A	80km	N/A
DWDM	城域网或长途	N/A	N/A	80km	N/A

5.3.5　千兆位接口转换器

GBIC(Gigabit Interface Converter，千兆位接口转换器)是千兆以太网端口所使用的业界标准的模块化光接口收发器。GBIC 的主要作用是将物理端口与光纤电缆相连接。它一头是一个通用的 GBIC 公头，另一头可以是传输电信号的 DB9、HSSDC、HSSDC2，也可以是传输光信号的 LC、SC。通用 GBIC 插入口插入到存储设备提供的 GBIC 母头中，它要求存储设备提供符合工业标准的 GBIC 母头，具体提供何种信号由 GBIC 的类型决定。

GBIC 支持热插拔，既有 SC 连接器的光纤使用标准形式的 GBIC，也有 LC 连接器的光纤使用 SFP(small form-factor pluggable，小型可插拔)形式的 GBIC。

目前 GBIC 基本被 SFP 取代，SFP 可以简单的理解为 GBIC 的升级版本。SFP 模块(体积比 GBIC 模块减少一半，可以在相同面板上配置多出一倍以上的端口数量。由于 SFP 模块在功能上与 GBIC 基本一致，也被有些交换机厂商称为小型化 GBIC(Mini-GBIC)。

5.4　项目实施

下面的项目是针对一个企业园区进行网络设计。我们先对项目进行一下分析，然后完成网络的初步设计，绘制拓扑图。更详细的设计与实现可以在期末实训阶段中进行。

1. 项目简介

某企业租用了 A、B 两幢大楼。A 楼用作企业办公，B 楼作为企业研发中心。A 楼共有 4 层每层大约有 200 个用户节点。A 楼 201 室用作企业的中心机房(数据中心)，要求配置服务器和网络设备的 UPS 系统。而 B 楼约有 20 个用户节点，且 B 楼 101 室是电信接入点。并且企业自己提供少许的公网 IP 地址，因此内部要使用私网 IP 地址。

企业对于网络有如下的要求：

(1)采用先进的网络通信技术完成企业网络的建设，连接 2 个相距较远的办公地点；

(2)为了提高数据的传输效率，在整个企业网络内控制广播域的范围；

(3)在整个企业集团内实现资源共享,并保证骨干网络的高可靠性;

(4)企业内部网络中实现高效的路由选择;

(5)在企业网络出口对数据流量进行一定的控制;

(6)能够使用较少的公网 IP 接入 Internet;

(7)对内网到外网的访问进行一定控制,要求不允许财务部访问互联网,业务部只能访问 WWW 和 FTP 服务,而综合部只能访问 WWW 服务,其余访问不受控制;

(8)数据中心的 WWW、FTP、EMAIL 能被外网访问。

2. 用户需求详细分析

需求 1:在接入层采用二层交换机,并且要采取一定方式分离广播域。

分析 1:在接入层交换机上划分 VLAN,可以实现对广播域的分离。划分业务部 VLAN10、财务部 VLAN20、综合部 VLAN30,并分配接口。

需求 2:核心交换机采用高性能的三层交换机,且采用双核心互为备份的形式,接入层交换机分别通过 2 条上行链路连接到 2 台核心交换机,由三层交换机实现 VLAN 之间的路由。

分析 2:交换机之间的链路配置为 Trunk 链路,三层交换机上采用 SVI 方式(switch virtual interface)实现 VLAN 之间的路由。

需求 3:2 台核心交换机之间也采用双链路连接,并提高核心交换机之间的链路带宽。

分析 3:在 2 台三层交换机之间采用端口聚合,以提高带宽。

需求 4:接入交换机的 access 端口上实现对允许的连接数量的控制,以提高网络的安全性。

分析 4:采用端口安全的方式实现。

需求 5:为了提高网络的可靠性,整个网络中存在大量环路,要避免环路可能造成的广播风暴等。

分析 5:整个交换网络内实现 RSTP,以避免环路带来的影响。

需求 6:三层交换机配置路由接口,与 Ra 和 Rb 之间实现全网互通。

分析 6:2 台三层交换机上配置路由接口,在 Ra 和 Rb 上分别配置接口 IP 地址。在三层交换机的路由接口和 Ra、Rb 的内部网络上启用 RIP 路由协议,实现全网互通。

需求 7:Ra 和 B 办公地点的路由器 Rb 之间通过广域网链路连接,并提供一定的安全性。

分析 7:Ra 和 Rb 的广域网接口上配置 PPP(点到点)协议,并用 PAP 认证提高安全性。

需求 8:Rb 配置静态路由链接到 Internet。

分析 8:2 台三层交换机上配置缺省路由,指向 Ra。Ra 上配置缺省路由指向 Rb。Rb 上配置缺省路由指向连接到互联网的下一跳地址。

需求 9:在 Rb 上用少量的公网 IP 地址实现企业内网到互联网的访问。

分析 9:用 NAT(网络地址转换)方式,实现企业内网仅用少量的公网 IP 地址到互联网的访问。

需求 10:在 Rb 上对内网到外网的访问进行一定的控制,要求财务部不允许访问互联网,业务部只允许访问 WWW 和 FTP 服务,而综合部只能访问 WWW 服务,其余访问不受控制。

分析 10:通过 ACL(访问控制列表)实现。

3. 网络拓扑设计

本设计的拓扑图如图 5-1 所示。

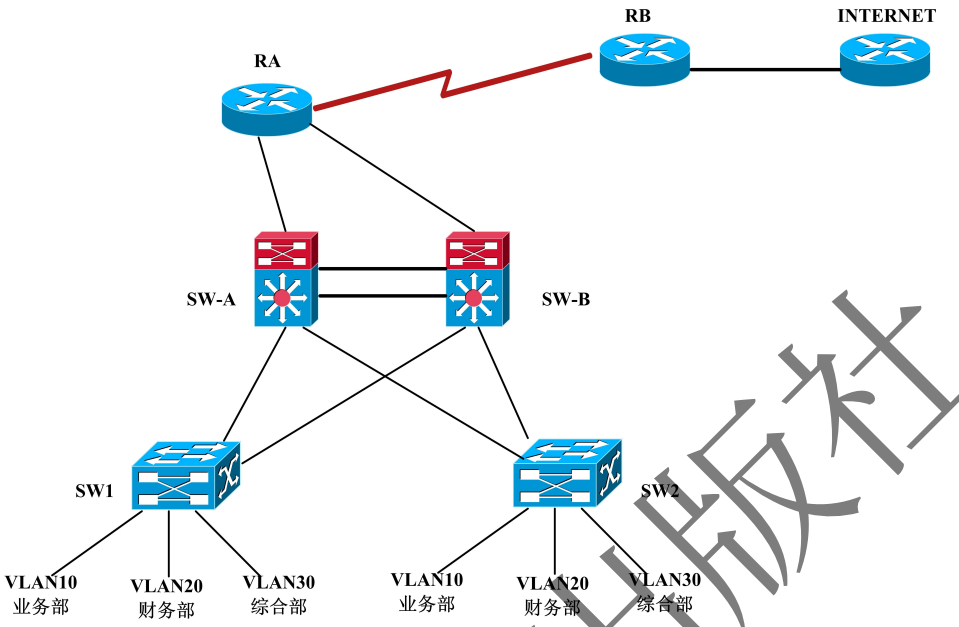

图 5-1　项目拓扑图

5.5　技术拓展

数据中心(Data Center)通常是指在一个物理空间内实现信息的集中处理、存储、传输、交换和管理。而计算机设备、服务器设备、网络设备、存储设备等通常认为是网络核心机房的关键设备。而关键设备运行所需要的环境因素,如供电系统、制冷系统、机柜系统、消防系统、监控系统等通常被认为是关键物理基础设施。

数据中心产生于业务的发展、管理的需要。如客户在银行的数据,原来分散在不用的业务系统中,如储蓄、信用卡、房贷、投资、车贷等。现在随着业务发展和竞争的需要,银行需要全面了解客户,才能更好交叉销售,更好地服务客户,这样就产生了整合不同业务系统中客户数据的需求。这个需求会导致数据存储量增大,数据处理能力更高,网络带宽更大,对数据的安全性要求更高,进而对机房条件、电源条件、人员和管理能力都有相应的提高。又如门户网络服务商,要为数量极大的客户提供一致的服务,以至于原来单一的任何型号计算机、存贮设备都无法满足其处理要求,这就需要集成多台计算机、存储设备、网络设备的能力,为客户提供服务。

由此就产生了认识数据中心第二个角度—技术能力。数据中心的业务或管理需求,导致数据或服务的集中,产生新的技术需求,即数据中心可能需要超过原来单一计算机和存储设备的处理需求。这就是为什么会有厂商称存储设备、服务器集群为数据中心。

由于数据集中、处理能力集中,数据中心影响面比原来大得多,因而也就要求更高的保障能力,包括机房管理、安全管理、灾难备份和电源备份。这是数据中心与原来企业信息基础设施的第三个不同之处,或第三个角度。

最后,也是第四个角度,是集中后的数据中心。处理能力和数据影响面极广,技术能力和保障能力要求高,必然也要求更高的管理能力。这种能力体现在队伍的建设,包括人员的备份;流

程的完整和严谨;考评和检查的落实。

5.6 本章小结

本章复习了局域网中最常用的以太网技术,了解了 100BASE-T、1000BASE-T、10GBASE-T 等技术,以及支持这种技术的一些网络产品。通过本章的学习,我们应该能对一些不是很复杂的企业网络进行设计与规划。

5.7 强化练习

1. IEEE 802.3 帧结构有哪几部分组成?
2. 以太网的物理层有几种标准?
3. 快速以太网有哪几种组网方式? 各有什么特点?
4. 千兆位以太网有哪几种标准?
5. 什么是 10/100Mpbs 自动协商?
6. 万兆以太网有哪些技术特色?
7. 万兆以太网物理层有哪几种?
8. 万兆以太网应用在哪些方面?
9. 组建以太局域网需要哪些设备?

任务 6 企业级多层交换机的配置和排错

6.1 项目导引

交换机作为局域网中的核心设备之一,它的工作性能直接决定着网络的数据传输性能。可是,在长时间工作之后,交换机难免会遇到这样或那样的故障现象。为了及时解决故障现象,网络管理员时常会进行一些排错操作。

6.2 项目分析

在网络开始部署交换机之前,为了易于管理和排错,用户首先必须对交换机进行初始化配置。交换机的基本配置除了前面介绍的几个参数外,还有如下几个参数:

(1)时钟和 NTP(Network Time Protocol,网络时间协议)设置;

(2)Telnet 和 SSH(Secure Shell,安全外壳程序);

(3)DNS;

(4)系统日志。

为了能够方便管理和简化排错，交换机应当在初始安装的过程中配置上述参数。因用户的企业网络不同，还可能配置交换机的其他参数，例如 RMON 等。本教材将在后续章节讨论这些主题。

对于前面所列出的基本配置参数，它们也是在网络中部署交换机所必需的参数，并且可以进行带内管理和排错。

6.3　技术准备

6.3.1　时钟和 NTP 设置

NTP(Network Time Protocol 网络时间协议)是用来使计算机时间同步化的一种协议，它可以使计算机对其服务器或时钟源(如石英钟，GPS 等等)做同步化，提供高精准度的时间校正，且可以用加密确认的方式来防止恶毒的协议攻击。

在对交换机进行监控和排错的过程中，设置准确的日期和时间并能正确显示是十分必要的。而当意外事件发生的时候，能知道意外事件发生的确切时间也是至关重要。此外，对于企业网络中的所有网络设备，NTP 能够有助于同步它们的系统时钟。

在交换机上配置时间、日期和时区，需要使用下列命令，其中 clock set 命令具有两种可替换的格式：

```
clock set hh:mm:ss day month year
clock sat hh:mm:ss month day year
clock timezone zone hours-offset [minutes-offset]
```

clock set 命令是一条可执行的命令. clock timezoae 命令是一条全局配置命令。对于 clock timezone 配置命令，zone 代表缩写形式的时区. 例如 EST 和 PST；hours-offset 表示当前时区与 UTC(国际标准时间)的偏移小时数。

交换机配置时间和日期的命令如下：

```
命令：set time[day_of_week] [mm/dd/yy] [hh:mm:ss]
      set timezone[zone_name] [hours [minutes]]
```

例如，在交换机上配置时间、日期和时区的命令如下：

```
A503# clock set 20:26:00 Dec 24 2012
A503# show clock
20:26:12.345 UTCMon Dec 24 2012
A503# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
A503(config)#clock timezone gmc 8
```

此外，在 CISCO 交换机配置 NTP 服务器，以解决企业网络中路由器、交换机及 Windows 服务器、Linux 服务器等设备的时间同步问题。NTP(Network Time Protocol，网络时间协议)是基于 RFC1305 的协议，是一个跨越广域网或局域网的复杂的同步时间协议。一般情况下建议配置在路由器上，当然配置在其它设备上也是可以的。

配置 NTP 先要选择并确定一个 NTP 服务器，然后使用下面的 NTP server 命令来指定

NTP 服务器的地址。

命令:ntp server ip-address

例如:假设某 NTP 服务器的 IP 地址是 155.1.146.4,则命令如下:

```
A503(config)# ntp server 155.1.146.4
```

6.3.2 Telnet 和 SSH

交换机都支持通过 Telnet 和 SSH 进行管理访问。对于 Telnet 命令行访问,交换机需要先配置虚拟终端密码。对于带内访问,交换机需要配置 enable 密码。Telnet 以明文方式传递数据与密码,而 SSH 则不是以明文方式传递,所以 SSH 是 Catalyst 交换机带内连接 CLI 访问的优选方法。SSH 要求配置用户名和密码,并且能够有选择地使用集中安全访问的 RADIUS 和 TACACS+方法。

虚拟终端接口和全局配置命令:

命令:password password

```
enable password[levellevel]{password | [encryption-type] encrypted-password}
```

上述命令中,选项 encryption-type 指定采用 Cisco 专用算法对密码进行加密。

如果用户指定 encryption-type,那么就必须提供下一个参数作为加密密码。为简单起见,可以不使用选项 encryption-type,而只需要在配置 enable 命令的时候在命令行中输入未加密的密码。

为了能够在交换机上配置 enable 密码和虚拟终端密码,可以使用下列命令来产生更改密码:

命令:set password

```
set enablepass
```

例如:在交换机上配置 enable 口令和虚拟终端口令如下所示。

```
A503(config)# enable password lncc503        //设置 enable 密码是 lncc503
A503(config)# line vty 0 15                   //配置虚拟端口
A503(config-line)# password lncc503          //配置虚拟终端密码
```

交换机启用 SSH 需要使用如下命令产生 SSH 所需的密钥:

命令:crypto key generate rss

在不同版本的 Cisco IOS 软件中,除了 RSA 以外,还可以利用其他类型的密钥。

除了 crypto key generate 命令之外,启用 SSH 还需要全局配置命令 aaa new-model。通过使用该命令,将能够使用本地用户名和口令对设备访问的 SSH 会话进行认证,对 DNS 名称和虚拟终端进行配置。关于 aaa,我们将会在后续章节进行详细的讲述。

交换机中启用 aaa 的 SSH 配置如下:

```
ip domain-namelncc.edu                        //设置域名
aaa new-modle//启用 AAA 服务
username lncc503 password lncc503
crypto key generate rsa modulus 2048          //生成秘钥
The name for the keys will be:switch1.lncc.edut
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
```

```
How many bits in the modulus [512]: 1024      //指定 1024 位秘钥
% Generating 1024 bit RSA keys ...[OK]
username sshuser secret sshpassword           //指定 SSH 登录用户名和密码
ip ssh time-out 30                            //设定 SSH 超时值
no ip ssh version                             //启用 SSH V1 V2
aaa authentication login ssh local line none //设定 SSH 登录信息存储地址
ip access-list standard forssh                //定义 SSH 登录源地址
permit any
line vty 0 4
exec-timeout 30                               //设置线路登录超时值
login authentication ssh                      //指定验证登录用户信息存储地址
transport input ssh                           //设置线路登录模式为 SSH
access-class forssh in                        //应用访问列表
```

6.3.3　DNS

在交换机上配置 DNS 就能够将域名解析为 IP 地址，这样做的目的也是为了实现管理和排错，具体命令如下：

命令：ip name-serveraddress [address2...address8]

ip domain-namedomain

ip domain-lookupip name-serveraddress：最多能够为 DNS 解析查询而配置 8 个域名服务器。

ip domain-namedomain 命令，将可以指定交换机所在的域。

ip domain-lookup 命令，将能够启用 DNS 解析。

例如：在交换机上配置 DNS 命令如下：

```
A503(config)# ip domain-name dns.lncc.edu
A503(config)# ip name-server  202.199.184.11  202.199.184.12
A503(config)# ip domain-lookup
```

6.3.4　系统日志

系统日志是管理交换机的另外一种实用工具。默认情况下，交换机将关健信息记录到本地缓冲区中。具体命令如下：

命令：loggingip address

例如：在交换机上配置系统日志服务器命令如下：

```
A503(config)# loggingip address202.199.184.50
```

6.3.5　管理交换机配置

通过使用 copy 命令，能够将交换机的配置从一个存储部位或设备复制到另一个存储部位或设备，例如复制到 RAM、NVRAM 或 TFTF 服务器。

命令：copy　源位置　目标位置

例如：copy　running-config tftp

命令结果是:把 RAM 中的运行配置复制到 TFTP 服务器。管理交换机配置常用的几条命令如表 6-1 所示。

该命令将提示用户输入源文件名称、目标文件名称和 TFTP 服务器地址。

另外,为了更可靠地保存交换机的配置信息件,copy 命令还能够将运行配置复制到 NVRAM 中。

启动配置(start-config):它显示保存在 NVRAM 中的配置;

运行配置(running-config):表示当前运行在 RAM 中的配置。

表 6-1　　管理交换机配置常用的几条命令

命令	功能
copy running-config startup-conflg	把“运行配置”复制到“启动配置”
copy startup-config running-config	将“启动配置”复制到“运行配置”中
copy running-config tftp:	把“运行配置”复制到 TFTP 服务器
copy tftp running-config	把保存在 TFTP 服务器中的配置复制到“运行配置”中
erase startup-config	删除 NVRAM 中所保存的启动配置
write memory	保存到 NVRAM 中

举例:管理交换机上的配置文件命令如下:

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#copy startup-config tftp
Address or name of remote host []? 192.168.11.12
Destination filename [Switch-config]?
!!
3007 bytes copied in 1.028 secs (2925 bytes/sec)
```

6.3.6　基本排错实践

交换机的基本排错命令包括 show 和 debug 命令,其中 show 命令能够提供状态信息,而 debug 命令能够提供特定事件的实时信息。在排除任何异常故障的时候,总是首先使用 show 命令。除了 show 和 debug 命令之外,具有时间戳的日志信息也对监控和调试交换机非常有用。

1. show 和 debug 命令

在对网络异常、连接故障、性能问题和其他异常行为进行排错的时候,show 和 debug 是非常重要的工具。通过使用 show 命令,系统能够提供关于网络设备状态、邻接交换机和路由器、网络性能等静态信息的集合。show 命令能够帮助收集包括接口、节点、介质、服务器、客户端或应用的故障。在排错的过程中,很多场合都可能使用 show 命令,例如 show interface 命令能够收集错误统计信息。

通过使用 debug 命令,将提供下列信息流:接口所见到(或未见到)的流量、网络节点所产生

的错误信息、特定协议的诊断数据包、其它有用的状态排错数据等。为了确定事件或数据包是否工作正常，就需要 debug 命令来查看路由器或网络的进行运转情况。

在使用 debug 命令的时候，应当注意下列重要问题。

(1)debug 命令可能会产生大量与解决故障无关的的数据。

(2)如果使用 debug 命令，就可能加大 CPU 的开销，进而可能会影响网络设备的运转。

(3)在使用调试排错工具的时候，输出格式可能随着每种协议的不同而变化。

(4)某些 debug 命令可能会产生大量的输出结果。

(5)通过使用 debug 命令，可以获得网络流量和路由器状态的相关信息。最后，需要提醒的是，必须采取谨慎的态度来使用这些调试命令。

2. 排错时所使用的配置和命令

如果要正确测试，首先需要调试和日志消息的时间戳。知道事件发生时的时间帧和确切实例对性能问题的排错具有至关重要的意义。为了在的交换机上配置时间戳的调试和日志消息，需要使用下述全局配置命令：

```
service timestamps debug{datetime| uptime} [{msec} {localtime} {show-timezone}]
service timestamps log{datetime| uptime} [{msec} {localtime} {show-timezone}]
```

在配置调试和日志的时间戳的时候，还存在其他一些参数。通过上列命令中的 msec 和 localtime 选项，将可以使用交换机当前时间向所有的消息增加毫秒级的时间戳。

为了避免 CPU 出现利用率过高的情况，在启用调试之前注意 CPU 负载情况是必须的。为了能够在启用任何调试命令之前确定 CPU 的当前负载，需要使用下列命令：

```
show processes
```

该命令能够显示当前正在运行的进程和 CPU 的总体利用率。当 CPU 利用率超过 70%的时候，不建议启用任何调试功能。

在启用和禁用调试的过程中，另外两条有用的命令是 no debug all 和 undebug all。这两条命令能够立即禁用所有的调试功能，进而避免产生更高的 CPU 利用率。

3. debug 命令的影响

通常情况下，如果某种异常情况导致需要进行调试工作，那么为了能够快速地诊断并解决问题，牺牲 CPU 的效率可能是理想的选择。这时，为了能够有效地使用调试工具，需要确定下列信息：

(1)排错工具对路由器性能的影响程度；

(2)最具针对性地选择和集中使用诊断工具；

(3)对于正在使用网络设备资源的其他进程，考虑如何尽量降低排错工作对它们的影响；

(4)为了使路由器能够在诊断结束之后恢复最高效的运转，考虑如何停止排错工具。

在使用 debug 命令的时候，应当考虑如下原则：

(1)最好在网络流量或用户少的时间内使用 debug 命令。

(2)应当以一种及时的方式从 debug 命令中获取信息，并且应当在调试完毕之后立即禁用 debug 命令，进而使得路由器能够恢复到正常的工作状态。

所有的 debug 命令都必须在特权模式下输入，并且大多数 debug 命令都不需要任何参数。但是，在将调试信息隔离到特定接口或特性的时候，调试参数就非常有用。

6.4 项目实施

1. 项目简介

本项目的拓扑图如图 6-1 所示，任务是通过 Console 端口对交换机进行初始配置；配置交换机的 IP 管理访问；配置 IP 服务，如 DNS、Telnet 和 SSH；将交换机的版本升级。

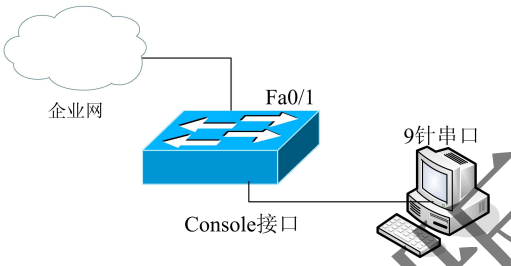

图 6-1 本项目拓扑结构图

2. 配置过程

(1)带外连接和配置交换机名称。

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname sw001
```

(2)配置交换机的 IP 连接。

```
sw001(config)#vlan 1
sw001(config-vlan)#exit
sw001(config)#interface vlan 1
sw001(config-if)#ip address10.1.118.103 255.255.255.0
sw001(config-if)#no shutdown
sw001(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
sw001(config-if)#exit
sw001(config)#interface fastethernet 0/1
sw001(config-if)#switchport access vlan 1
sw001(config-if)#no shutdown
sw001(config-if)#exit
sw001(config)#
```

(3)为交换机配置适当的默认网关。

```
sw001(config)#ip default-gateway 10.1.118.1
sw001(config)#exit
sw001#
```

(4)配置交换机支持 DNS 查找。

```
sw001(config)#ip name-server10.1.1.200
sw001(config)#ip domain-lookup
```

```
sw001(config)#exit
sw001#
```

(5)配置交换机特权和带内访问的密码。

```
sw001(config)#enable passworddalian
sw001(config)#line vty 0 4
sw001(config-line)#passworddalian
sw001(config-line)#exit
sw001(config)#
```

(6)配置 SSH 会话的本地用户名和密码。

```
sw001(config)#usernamedalian password dalian
```

(7)配置交换机支持 SSH,并禁用 Telnet 访问。

```
sw001(config)#aaa new-model                    //为 SSH 连接启用 AAA 认证
sw001(config)#ip domain-name dl.com            //以下命令配置交换机支持 SSH
sw001(config)#crypto key generate rsa
The name for the keys will be: sw001.dl.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

sw001(config)#                                 //以下配置交换机只支持 SSH 的带内访问
sw001(config)#line vty 0 15
sw001(config-line)#transport input ssh
sw001(config-line)#exit
sw001(config)#exit
sw001#
```

(8)配置交换机的时间设置、NTP 配置和系统日志配置。

```
sw001# clock set 20:26:00 Dec 24 2012
sw001# show clock
20:26:12.345 UTCMon Dec 24 2012

sw001#configure terminal
sw001(config)#clock timezone gmc 8
sw001(config)#ntp server 10.1.1.202
sw001(config)#exit
sw001#show ntp associations

sw001(config)#logging 10.1.1.199               //向系统日志服务器记录所有的默认信息
```

6.5 技术拓展

1. 交换机或路由器 IOS 的升级

在对能够正常启动的 Cisco 路由器的 IOS 进行升级时，建议将原有 IOS 文件备份下来，防止待升级的 IOS 文件存在问题不可用。

IOS 升级的具体步骤如下：

(1)在电脑上安装 TFTP 服务器软件，将要升级的 IOS 映象文件拷贝到相关的目录中(例：D:\)，并运行 TFTP 服务器软件，通过菜单设置 Root 目录为拷贝 IOS 映象文件所在目录(如 D:\)。假设该计算机的 IP 地址为 10.1.1.51；

(2)连接路由器的 Console 端口与 PC 机的 COM1，使用 PC 的超级终端软件访问路由器，将路由器的地址设置为 10.1.1.52(与计算机的 IP 地址同网段即可)。

设备连接如图 6-2 所示。

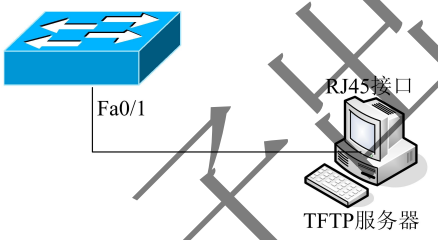

图 6-2 设备升级连接图

(3)查看并备份路由器中 IOS 映像文件。

查看目前 IOS 映象文件名的命令如下：

```
Router# dir flash:                    //查看目前 IOS 映象文件名，也可用 Show version
```

显示结果所示命令如下：

```
Router#dir flash:
Directory of flash:/

    3  -rw-   50938004     <no date>     c2800nm-advipservicesk9-mz.124-15.T1
.bin
    2  -rw-      28282     <no date>     sigder-category.xml
    1  -rw-     227537     <no date>     sigder-default.xml
64016384 bytes total  (12822561 bytes free)
```

备份 IOS 文件到 TFTP 的命令如下：

```
Router#copy flash tftp                          //备份 IOS 文件到 TFTP
Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 10.1.1.51    // TFTP 服务器地址
Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

50938004bytes copied in 324.071 secs (18509 bytes/sec)
```

(4)对路由器进行 IOS 升级。

```
Router#copy tftp flash
Address or name of remote host []? 10.1.1.51              // TFTP 服务器地址
Source filename []? c2800-i-mz.122-11.bin                 //需升级的新 IOS 映象文件名
Destination filename [c2600-i-mz.122-11.bin]?
Do you want to over write? [confirm]
Accessing tftp:// 10.1.1.51/c2600-i-mz.122-11.bin……
Erase flash:before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device…… eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ……erasedee
Erase of flash: complete
Loading c2600-i-mz.122-11.bin from10.32.10.1 (via Ethernet0/0): !!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5998292 bytes]
Verifying checksum…… OK(0xA0C0)
5998292 bytes copied in 318.282 secs(18846 bytes/sec)
```

2. 初始配置的排错技巧

本部分讨论首次配置交换机时所出现的几种常见的配置问题。

(1)不能够通过 Console 端口连接到交换机。

①验证是否使用直通电缆或反转电缆。

②确认终端配置是否与交换机控制台端口配置相匹配。控制台端口的默认设置是波特率 9600、数据位 8、无校验、停止位 1。

③确认连接交换机的计算机工作是否正常,必要时换另一台计算机再测试一下。

④检查交换机是否正常供电、是否正常工作。

(2)不能使用 Telnet 或 SSH 建立与交换机的 IP 连接。

①确认交换机和计算机的端口工作正常;输入 show interface 命令,从 CLI 界面验证连接交换机和计算机的交换机端口都处于“UP”状态。

②检查并确认将交换机连接到网络的端口采用正确的线缆,交换机间的连接通常采用交叉电缆。

③对于 SC 和 ST 类型接头的光纤连接.确认链路的发射端(TX)与链路另一端的接收端(Rx)正确地连接。

④通过使用 show interface 命令,确认相应的管理接口状态是否处于“UP”状态,并且是否配置正确。

⑤通过使用 show interface 命令,确认交换机端口 VLAN 成员身份是否正确。

⑥通过使用 show ip route 命令,验证默认网关配置或 IP 路由选择配置。

⑦对于通过远程访问软件(Telnet 或 SSH)与交换机建立连接的主机,确认其 IP 地址、子网掩码、默认网关、速度和双工设置都是正确的。

⑧如果涉及子网,验证主机所连接的交换机端口与主机是否位于相同的子网中。

⑨如果主机 IP 与与交换机的管理 IP 地址不在一个子网中,那么就需要确认交换机的默认网关与默认网关路由器是否位于相同的子网中。

⑩确认主机和相应交换机端口的速度和双工设置是否正确。将交换机和主机移动到不同的交换机端口,重新建立与交换机的连接。

6.6 本章小结

本章介绍了交换机的基本管理措施,即交换机的初始配置、管理 IP 地址的设置、交换机默认网关的设置、DNS 的设置、交换机的带内访问和带外访问的相关设置,简单介绍了交换的 SSH 配置,以及交换机的时间、NTP 和系统日志配置等内容。还介绍了 show、debug 命令在交换机查错中的应用。

6.7 强化练习

1. 在交换机上尝试使用 show、ping、trace、debug 等常用命令,并分析他们的功能?

2. 某交换机的配置命令如下,根据命令后面的注释,填写空缺内容完成配置命令。

(1)

```
Switch (config) # _____ 将交换机命名为 Sw1
Sw1 (config) # interface vlan 1
Sw1 (config) # _____ 设置交换机的 IP 地址为 192.168.1.1/24
Sw1 (config) # no shutdown
Sw1 (config) # _____ 设置交换机默认网关地址
```

(2)

```
Sw1 (config) # interface range fastethernet0/20 进入组配置状态
Sw1 (config-if-range) # _____ 设置端口工作在访问接入模式
Sw1 (config-if-range) # _____ 设置端口 1～20 为 VLAN10 成员
```

(3)

```
SwitchA (config)# _____ 进入端口 3 配置模式
SwitchA (config-if)# _____ (设置当前端口为 Trunk 模式)
SwitchA (config-if)# _____ (设置允许所有 VLAN 通过)
SwitchA (config-if)#exit
```

(4)

```
Switch(config)# _____ (进入端口 7 的配置模式)
Switch(config-if)# _____ (设置端口为静态 VLAN 访问模式)
Switch(config-if)# _____ (把端口 7 分配给 VLAN10)
Switch(config-if)#exit
Switch(config)#exit
```

3. 请阅读下列 Switch A 的配置信息，在(　　)处解释该语句的作用。

```
Switch>enable                                (        )
Switch#config terminal                       (        )
Switch(config)#hostname SwitchA              (        )
Switch(config)#end                           (        )
SwitchA #
SwitchA #vlan database                       (        )
SwitchA #(vlan)#vtp server                   (        )
SwtichA #(vlan)#vtp domain vtpserver         (        )
SwitchA #(vlan)#vtp pruning                  (        )
SwitchA #(vlan)exit                          (        )
```

任务 7　设计 Cisco 多层交换网络

7.1　项目导引

当前，网络拥塞负荷问题日益严重，在此情况下，一边要将局域网进行有效的升级，另一边还要为维持局域网的运行而继续投入，这就向网络设计者提出了苛刻的要求。为了解决这些问题出现了多层交换网络技术。

对于局域网体系结构来说，多层交换网络技术结合了局域网交换技术和路由技术的优点，很大程度上提高了性价比。而且多层交换技术还是一个具有良好扩充性的解决方案。

7.2　项目分析

要完成多层交换网络的设计工作，首先需要了解多层交换网络的基本概念和组建多层网络的软、硬件设备；其次，还需要掌握多层网络设计的思想和关键技术。解决了这些问题，就可以完成多层交换网络的设计工作。

7.3　技术准备

7.3.1　多层交换技术简介

多层交换技术也被称做第三层交换技术或 IP 交换技术，是相对于传统交换概念而提出的。传统的交换技术是在 OSI 网络参考模型中的第二层—数据链路层上完成数据交换的，而多层交换技术是在第三层—网络层上实现了数据包的高速转发。简单地说，多层交换技术就是数据链路层上的数据帧交换技术与网络层上的数据包转发技术相结合。

多层交换技术的出现，解决了局域网中网段划分后网段中子网必须依赖路由器进行管理的

问题，同时也解决了由于传统路由器低速、复杂所造成的网络瓶颈问题。当然，多层交换技术并不是网络交换机与路由器的简单堆叠，而是二者的有机结合，形成一个集成的、完整的解决方案。

随着技术的发展，又出现了更高层的网络交换技术。例如：基于传输层的第四层交换技术和基于应用层的第七层交换技术。

理解多层交换技术首先要知道以下几个概念：

1. 硬件交换与软件交换

硬件交换是指通过专门的硬件组件（ASIC）在第二层到第七层上处理数据包的行为。

软件交换是指通过 CPU 实现传统的数据帧转发的行为。

二者相比较来看，硬件交换技术处理交换和路由通信流量的速度更快，具有更高性能和可用性。硬件交换在整个交换体系中更加易于扩展，ASCI 不会受到内存的限制。

2. 第二层交换技术

第二层交换技术是基于硬件的桥接技术，ASIC 负责处理数据帧的转发，交换机所转发的数据帧不会被修改。第二层交换技术的特点是：具有接近线速的性能；具有低延迟、可扩展的优点。

3. 第三层交换技术

第三层交换技术，又名 IP 交换技术，是在 OSI 参考模型的网络层中进行数据转发的交换技术。在原有二层交换技术基础上包含了三层路由转发功能，使用路由协议来进行最优转发决策。

第三层交换技术是基于硬件的路由选择技术，对数据包的处理程序和传统路由器相似。

三层交换技术的主要作用是高效的划分网段，打破了以前子网必须由路由器进行管理的局面，这种技术使工程的成本大大降低，能够提高信息处理的效能，打破了以往的网络瓶颈。

但是，三层交换技术并不是想象的那样简单，应用三层交换技术的过程中还需注意使多层交换机与路由器有机的结合在一起，才能充分发挥第三层交换技术的优势。

7.3.2 多层交换设备简介

1. 基于 IP 的多层交换设备

以太网多层交换设备具有多个交换端口，从逻辑上可以被看成是一个带三层转发功能的二层交换设备。同时它与第三层的数据转发模块采用高速互联。在数据通讯时，如果网上站点属于同一子网，则采取第二层转发方式；否则采用第三层转发方式。

2. 基于 IP/IPX 多层交换设备

目前在企业局域网内除了应用 IP 协议以外，Novell 的网络交换协议（IPX）也有非常广泛的应用。如果在局域网中同时使用了 IP 协议和 IPX 协议，并且选择把一个交换式局域网分成多个分离的广播域的方案，那就需要多层交换机具有同时支持 IP 和 IPX 的第三层转发技术，这样的多层交换机就是基于 IP/IPX 的多层交换设备。

3. 多层交换机的性能

早期采用二层交换设备组建网络，二层交换设备是基于硬件的方式进行数据包的转发，实现起来相对来说比较容易。这是因为二层交换机的转发策略是基于一个简单的 MAC 地址查

询表，而且在转发过程中不会改变数据包的内容。

如果需要进行三层的数据包转发时，可以采用路由器设备。但是路由器成本较高，且转发效率也不尽如人意。其原因主要有：

(1)一个路由器中数据包转发决策过程远比局域网交换机复杂的多；

(2)在路由器端每一个数据包必须经过数据包过滤器进行安全检查；

(3)路由器的大部分或全部数据包转发处理由软件来实现，使得性能价格比较低。

如果一个第三层转发功能模块完全由硬件实现，那么多层交换机无论在第二层还是在第三层进行交换都会表现出相同的高性能。如果第三层转发功能由软件方式实现，则多层交换机的转发数据性能不会优于路由器。

7.3.3　安全系统的构建

为了提高网络的安全系数，可以适当的减少网络各个部分的相关性，这样也会使得网络的可管理性加强，通常在构建网络的时候可以把网络划分成三个层次：

1. 核心层

核心层主要包含网络的主干部分。核心层的主要工作任务是负责汇聚各节点之间的互联，以及完成数据的高效交换转发，同时完成路由的分配。核心层主要功能包括：

(1)在广域网内面向各个交换区域提供连接信息；

(2)提供访问广域网的访问方法；

(3)尽可能实现高效的信息交换转发。

2. 汇聚层

汇聚层是核心层与接入层的分界点，主要的工作任务是将接入业务进行集中处理。除了处理数据之外，还负责把数据通过高速接口传递到核心层。汇聚层主要的功能包括：

(1)接入部门并聚合 VLAN；

(2)数据的路由；

(3)控制安全级别。

汇聚层可以将大量的交换组与无线局域网汇聚在一起并连接到网络中，通常在汇聚层使用的是千兆链路，这将减少千兆以太网的端口连接数，大大的降低网络建设的成本。

3. 接入层

接入层是用户被允许接入的网络连接点。该层通过过滤或者应用访问控制列表的方法控制用户的流量。在接入层可以通过提供各种标准接口把数据接入到网络中。同时可以完成 MAC 地址中的 VLAN 成员或者数据的过滤工作，使数据交换工作分工明确。

7.4　项目实施

1. 项目描述

通过一个具体模型来认识多层交换网络。

2. 拓扑结构

拓扑图如图 7-1 所示。

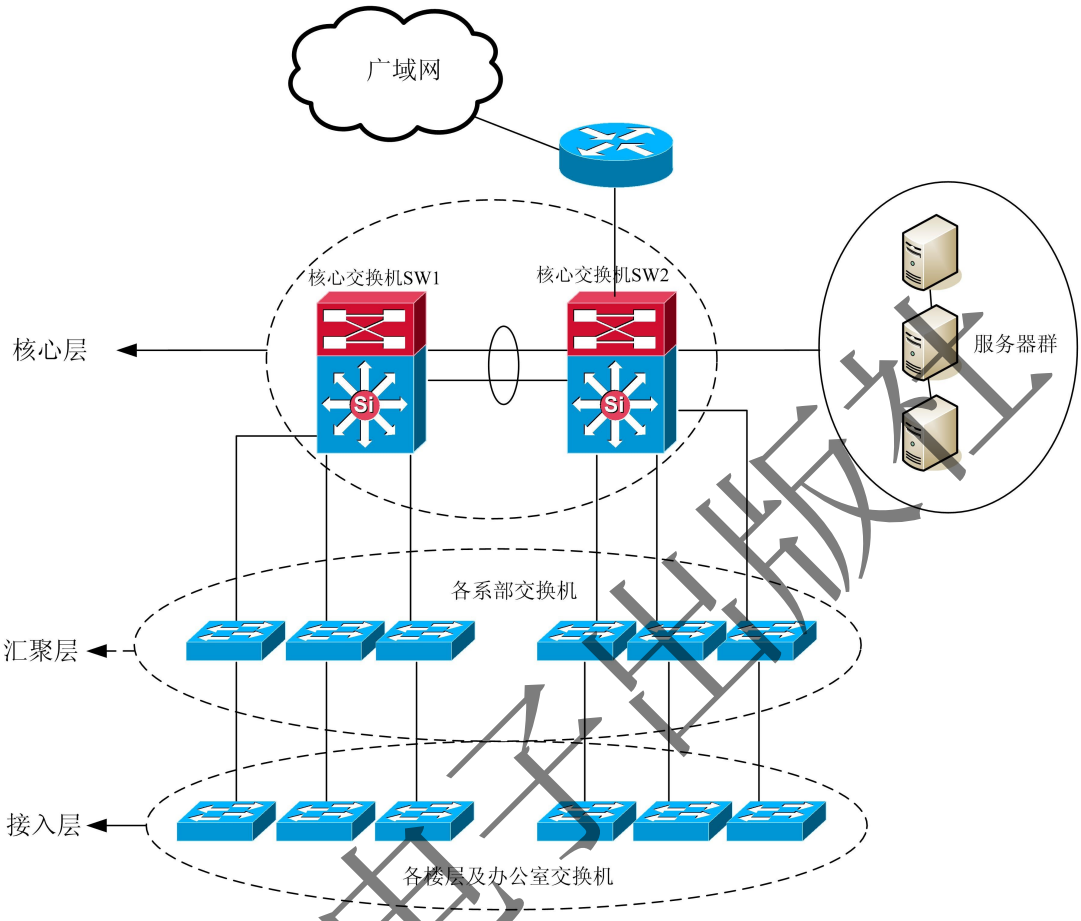

图 7-1 典型三层交换网络

3. 结构说明

项目以一个典型的校园网为例。校园网内 6 个系部交换机通过链路层连到核心层交换机上。

校园网核心交换机可以选用思科 3560、4500、6500 等系列的交换机；汇聚层交换机可以选取思科 3560、3750 等系列交换机；接入层可以选择思科 2600 等系列交换机。

7.5 本章小结

本章主要介绍了如何构建 Cisco 多层交换网络。通过介绍多层交换技术和多次交换设备，了解多层交换网络技术特点和主要结构。经过后面知识的学习可以合理的设计和组建多层交换网络。

7.6 强化练习

1. 什么是硬件交换？什么是软件交换？二者有什么区别？

2.如何设计多层交换网络的安全性能？设计时把网络分为哪几层？各层的功能特点是什么？

任务8　配置交换机端口安全和认证登录

8.1　项目导引

公司网络近期出现了很多安全问题，有些员工随意使用集线器等工具将一个上网端口增至多个，或者使用自己的笔记本电脑连接到公司的网路中。类似的情况都会给公司的网络安全带来不利的影响。公司领导要求对公司网络进行严格控制，不允许外来电脑随意接入公司网络，同时也要防止公司内部的网络攻击和破坏行为。

8.2　项目分析

从公司目前的情况分析，主要的安全威胁行为有以下两种情况：

(1)未经授权的用户主机随意连接到企业的网络中。如员工自带一台笔记本电脑，在不经管理员同意的情况下，拔下某台主机的网线插在自己带来的电脑上，然后连入到企业的网路中。这会带来很大的安全隐患。如果员工带来的电脑带有病毒，病毒会通过企业内部网络进行传播，或者通过外带电脑非法复制企业内部的资料等等。

(2)未经批准采用集线器等设备随意增加上网端口数量。有些员工为了增加网络终端的数量，会在未经授权的情况下，将集线器、交换机等设备插入到办公室的网络接口上。这样会导致这个网络接口对应的交换机接口流量增加，从而导致网络性能的下降。

这两种行为需要严格限制，配置交换机端口安全和配置交换机登录认证是有效的解决方案。

8.3　技术准备

8.3.1　交换机端口安全

端口安全可以基于MAC地址来对网络流量进行控制和管理。例如通过把MAC地址与端口绑定来限制端口通过的MAC地址的数量，这样可以达到控制端口接入设备的数量；另外还可以在具体的端口限制某些MAC地址的帧流量通过。

注意：端口安全可以是基于2层的安全，即MAC地址绑定。也可以是基于3层的端口安全，即MAC地址与端口绑定以及MAC地址与IP地址绑定。

端口安全能够基于主机MAC地址来控制流量通过。单个端口能够允许若干个MAC地址流量通过。根据交换机型号的不同，允许的最大MAC地址数也不相同。配置端口安全的步骤

如下：

1. 在端口上启用端口安全(端口安全属性默认是关闭的)

命令格式如下：

```
Switch(config)# int f0/1 //进入要设置的端口
Switch(config-if)# switchport mode access //设置端口模式
Switch(config-if)# switchport port-security //启用端口安全
```

2. 绑定 MAC 地址

我们通常说的 MAC 地址与交换机端口绑定其实就是交换机端口安全功能的核心。我们可以配置一个端口只允许一台或者几台确定的设备访问交换机，可以根据 MAC 地址确定哪些设备可以访问交换机。

允许访问交换机的设备的 MAC 地址可以手工配置，也可以从交换机自动“学习”到。当一个未批准的 MAC 地址试图访问安全端口的时候，交换机采取措施禁止访问。

具体绑定 MAC 地址时可以采用三种模式：

(1)静态可靠的 MAC 地址：这种模式是在交换机接口模式下手动配置，这个配置会被保存在交换机 MAC 地址表和运行配置文件中，保存配置以后交换机重新启动数据不丢失，配置命令如下：

```
Switch(config-if)# switchport port-security mac-addressMac 地址
```

(2)动态可靠的 MAC 地址：这种模式是交换机默认的方式。交换机动态学习 MAC 地址，但是这个配置只会保存在 MAC 地址表中，不会保存在运行配置文件中，交换机重新启动后，这些 MAC 地址表中的 MAC 地址自动会被清除。

(3)粘性可靠的 MAC 地址：这种类型下，可以手动配置 MAC 地址和端口的绑定，也可以让交换机自动学习来绑定。这个配置会被保存在 MAC 地址表和运行配置文件中。如果保存配置，交换机重启动后不用再重新自动学习 MAC 地址。虽然这种模式也可以手动配置，但是 Cisco 官方并不推荐这样做。配置命令如下：

```
Switch(config-if)# switchport port-security mac-address sticky
```

注意：在上面这条命令配置完成并且该端口学习到 MAC 地址后，会自动生成一条配置命令：

```
Switch(config-if)# switchpor port-security mac-address stickyMac 地址
```

这也就是为何在这种模式下 Cisco 不推荐手动配置 MAC 地址的原因。

3. 设置安全端口最大连接数

通过 MAC 地址来限制端口流量，此配置允许一个 Trunk 口最多通过若干个 MAC 地址的流量，超过限定的数值时，来自新的主机的数据帧将丢失。

如果将最大端口连接数设为 1，并且为该端口配置一个安全地址，则连接到这个端口的工作站(其地址为配置的安全地址)将独享该端口的全部带宽。设置了安全端口上安全地址的最大连接数以后，可以用以下方式加满端口上的安全地址：

(1)手工配置安全端口的所有安全地址。

(2)端口自动学习地址，这些自动学习到的地址将变成该端口上的安全地址，直到达到最大数。

安全端口最大连接数配置命令示例如下：

```
Switch(config-if)# switchport port-security maximum 1 //指定最大连接数为 1
```

4. 指定安全违例行为(默认行为是永久性地关闭端口)

配置命令如下：

```
Switch(config-if)switchport port -security violation protect|restrict|shutdown
```

当超过设定 MAC 地址数量的最大值，或访问该端口的设备 MAC 地址不是这个端口绑定的 MAC 地址，或同一个 VLAN 中一个 MAC 地址被配置在几个端口上时，就会引发违反 MAC 地址安全，这个时候采取的措施有三种：

(1)protect：当安全 MAC 地址数量达到了端口所允许的最大 MAC 地址数的时候，交换机会继续工作，但将把来自新主机的数据帧丢弃，直到删除足够数量的 MAC 地址使其低于最大值。

(2)restrict：交换机继续工作，向网络管理站(SNMP)发出一个陷阱 Trap 通告。

(3)shutdown：交换机将永久性或在特定时间周期内关闭端口，端口进入“err-disable”状态，并发送 SNMP 的 Trap 陷阱通告。

注意：如果端口进入“err-disable”状态后，要恢复正常必须在全局模式下输入命令“errdisable recovery cause psecure-violation”开启，或者可以手动的输入 shut 命令关闭端口，再输入 no shut 命令。

8.3.2　交换机登录认证

未经授权的主机随意连接到企业的网络中会对企业网络带来很大的安全隐患，为了防止这种情况的发生，可以采用登录认证的方式来进行限制。

1. 802.1x 简介

802.1x 协议是基于 C/S 模式的访问控制和认证协议。它可以限制未经授权的用户和设备通过接入端口访问 LAN/MAN。在获得交换机或 LAN 提供的各种业务之前，802.1x 对连接到交换机端口上的用户或设备进行认证。在认证通过之前，802.1x 只允许 EAPoL(基于局域网的扩展认证协议)数据通过设备连接到交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

802.1x 身份验证协议最初用于无线网络，后来在普通交换机和路由器等网络设备上开始使用。它基于端口来对用户身份进行认证，即当用户的数据流量企图通过配置了 802.1x 协议的端口时，必须进行身份的验证，认证通过则允许其访问网络。802.1x 协议为二层协议，对设备的整体性能要求不高，可以有效降低建网成本。

2. 802.1x 验证的特点

基于端口的 802.1x 身份验证涉及 3 种设备：

(1)客户(Client)。

应用 802.1x 请求网络对其进行身份验证的工作站。

(2)身份验证服务器(Authenticationserver)。

负责验证交换机转发的客户请求。目前身份验证服务器通常采用安装了 EAPoL 扩展协议的 RADIUS 服务器。

(3)交换机。

负责将客户请求转发给身份验证服务器，并在客户通过身份验证后授予其访问网络的权

限。在 802.1x 运行期间，交换机实际上相当于一个代理。

交换机端口的状态决定了客户是否能够访问网络。端口最初处于未经授权(unauthorized)状态。在这种状态下，除 802.1x 协议数据包外，端口不允许任何入站通信流和出站通信流通过。当客户通过身份验证后，端口将切换到授权(authorized)状态，允许来自客户的通信流通过。如果交换机请求客户表明其身份(由证明方发起的)，而客户不支持 802.1x 协议，则端口将继续保持未经许可状态，客户就不能访问网络。相反地，当启用了 802.1x 的客户连接到端口，并向交换机发送 EAPoL 启动帧来启动身份验证过程(由请求方发起)，而交换机没有运行 802.1x协议，则交换机无法响应客户，此时客户将开始发送数据帧，就像端口处于许可状态一样。

配置 802.1x 身份验证协议，首先需要在全局启用 AAA 认证，这个和在网络边界上使用 AAA 认证没有区别，只不过认证的协议换成 802.1x；其次需要在相应的端口上启用 802.1x 身份验证，建议在所有的端口上启用 802.1X 身份验证，并且使用 RADIUS 服务器来管理用户名和密码。

802.1x 的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离，由 RADIUS 服务器和交换机利用不可控的逻辑端口共同完成对用户的认证与控制。业务报文直接承载在正常的二层报文上通过可控端口进行交换，通过认证之后的数据包是无需封装的纯数据包。可以使用现有的后台认证系统降低部署的成本，并有丰富的业务支持。

8.4 项目实施

8.4.1 交换机端口安全项目

1. 项目描述

在公司内交换机上配置端口安全，限制个人自带电脑接入公司网络，保证公司内部网络接入的安全，防止针对交换机 MAC 地址的攻击。

2. 拓扑结构

拓扑图如图 8-1 所示。

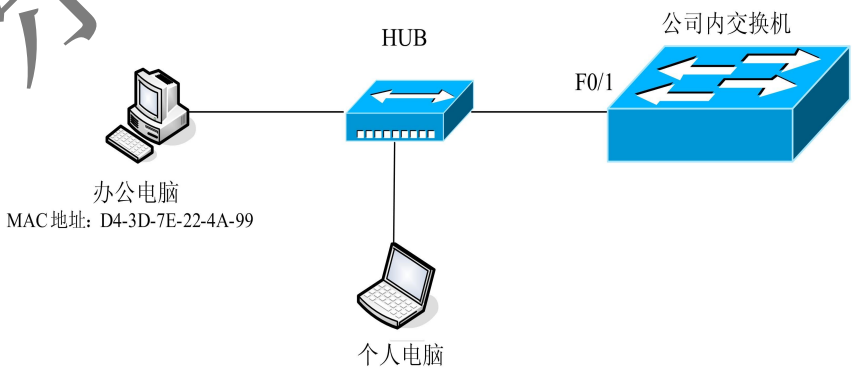

图 8-1 实现交换机端口安全

3. 配置与实现

(1)查看交换机 MAC 地址表。

```
Switch#show mac-address-table
Vlan    MacAddress          Type            Ports
1       0004.9a54.52c7      DYNAMIC         Fa0/1 //外来个人电脑
1       d43d.7e22.4a99      DYNAMIC         Fa0/1 //办公电脑
```

(2)配置端口安全。

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#shutdown //配置端口安全之前先关闭端口
Switch(config-if)#switchport mode access //在动态操作模式下,不能启用端口安全功能
Switch(config-if)#switchport port-security //启用端口安全
Switch(config-if)#switchport port-security maximum 1 //修改端口允许接入设备最大数为 1
Switch(config-if)#switchport port-security mac-address d43d.7e22.4a99 //设置允许接入设备的 MAC 地址为办公电脑的 MAC 地址
Switch(config-if)#switchport port-security violation shutdown //设置违例处罚方式
```

(3)验证。

```
Switch#show mac-address-table
Vlan      MacAddress        Type        Ports
1      d43d.7e22.4a99      DYNAMIC    Fa0/1 //办公电脑
```

当外来个人电脑接入交换机后可以通过命令查看端口状态：

```
Switch#show interface fastEthernet0/1
```

显示端口状态为：

```
FastEthernet0/1 is down,line protocol is down(err-disabled) //端口已经被 shutdown
```

8.4.2　交换机登录认证项目

1. 项目描述

公司的网络管理员为了防止有公司外部的用户将电脑接入到公司网络中,造成公司信息资源受到损失,要求公司员工的电脑在接入到公司网络之前进行身份验证,只有具有合法身份的用户才可以接入到公司网络。

2. 拓扑结构

交换机认证登录拓扑图如图 8-2 所示。

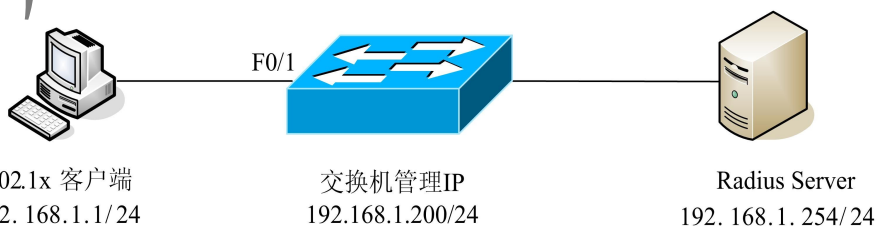

图 8-2　交换机认证登录拓扑图

说明:RADIUS 服务器要求支持标准 RADIUS 协议,此处使用第三方 RADIUS 服务器软件 WinRadius。

3. 配置与实现

(1)安装 RADIUS 服务器。

下面以一台运行 WindowsServer2003 的独立服务器为例进行介绍,先将该计算机的 IP 地址按照拓扑图 8-2 中所示配置为 192.168.1.254。

首先,在“控制面板”中双击“添加或删除程序”,在弹出的对话框中选择“添加/删除 Windows 组件”,在弹出的“Windows 组件向导”中选择“网络服务”组件,单击“详细信息”,勾选“Internet 验证服务”子组件,确定,然后单击“下一步”进行安装,直到成功安装 RADIUS 服务器。

RADIUS 服务器安装好之后,需要为所有通过认证才能够访问网络的用户在 RADIUS 服务器中创建账户。这样,当用户的计算机连接到启用了端口认证功能的交换机上的端口上时,启用了 IEEE802.1x 认证功能的客户端计算机需要用户输入正确的账户和密码,才能够访问网络中的资源。

创建账户的方法省略(参考 win2003server 系统创建用户账户的方法即可)。

注意:在添加用户之前,必须要提前做的是,打开“控制面板”→“管理工具”→“本地安全策略”,依次选择“账户策略”→“密码策略”,启用“用可还原的加密来储存密码”策略选项,如图 8-3 所示。

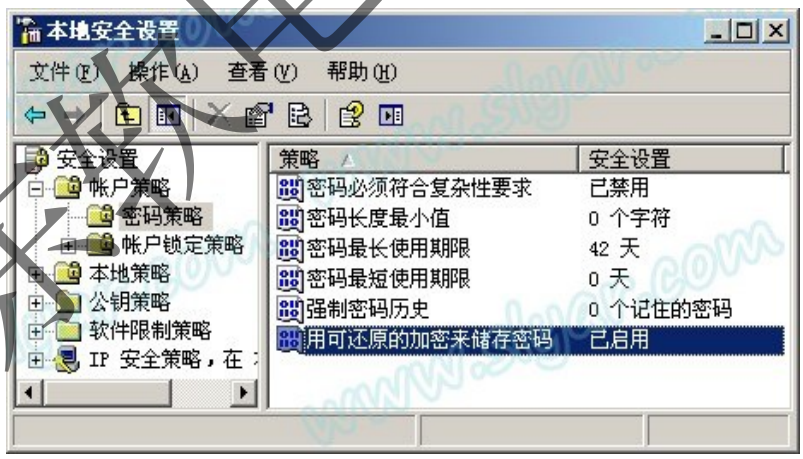

图 8-3 设置密码安全策略

如果不进行此项设置,以后在认证的过程中将会出现错误提示,如图 8-4 所示。

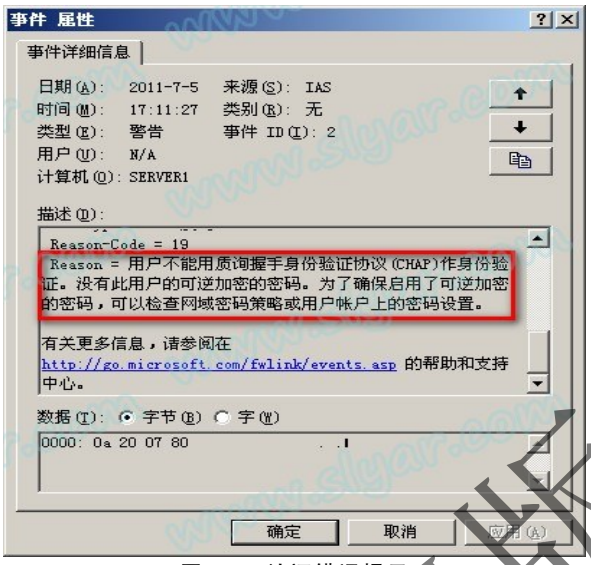

图 8-4　认证错误提示

添加用户账户“abc”，设置密码“123456”。为了便于以后进行统一管理，此处可以创建用户组“802.1x”将用户“abc”加入到组中(以后如果还需要添加用户账户，可以继续添加进此工作组内)。

在 RADIUS 服务器的“Internet 验证服务”窗口中，需要为交换机以及通过该交换机进行认证的用户设置远程访问策略。具体方法如下：

新建远程访问策略，右键单击“远程访问策略”，选择“新建远程访问策略”，如图 8-5 所示。

图 8-5　新建远程访问策略

选择配置方式，这里我们使用向导模式，如图 8-6 所示。

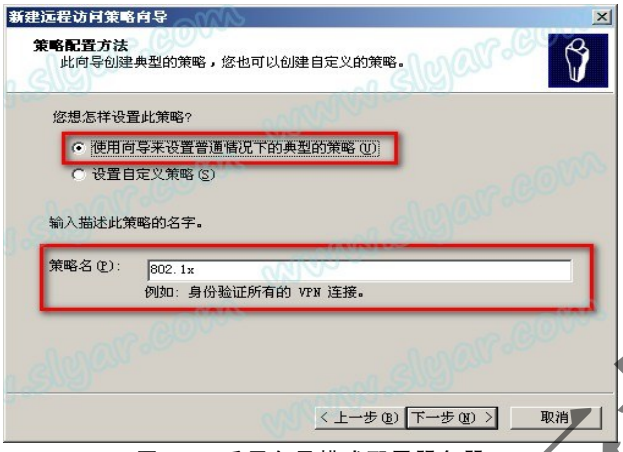

图 8-6 采用向导模式配置服务器

选择访问方法为“以太网”，如图 8-7 所示。

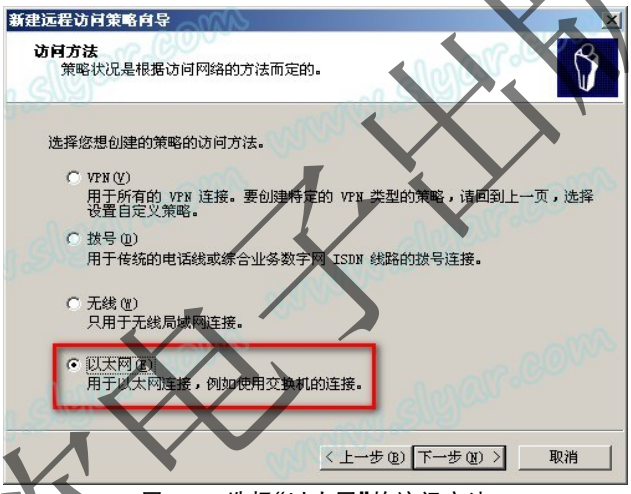

图 8-7 选择“以太网”的访问方法

选择授权方式，将之前添加的“802.1x”用户组加入许可列表，如图 8-8 所示。

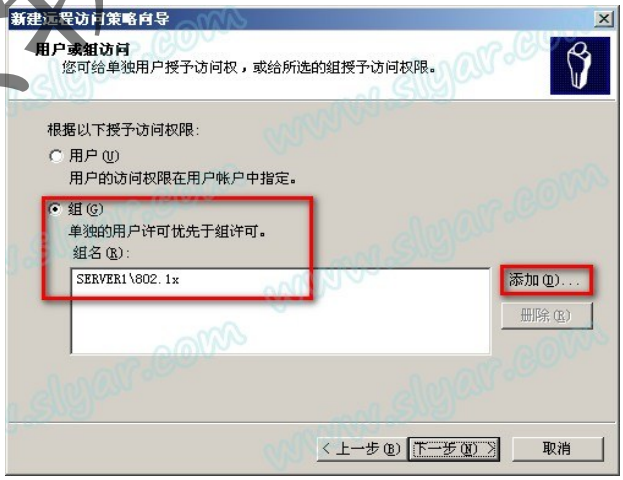

图 8-8 将工作组加入许可列表

选择身份验证方法“MD5-质询”，如图 8-9 所示。

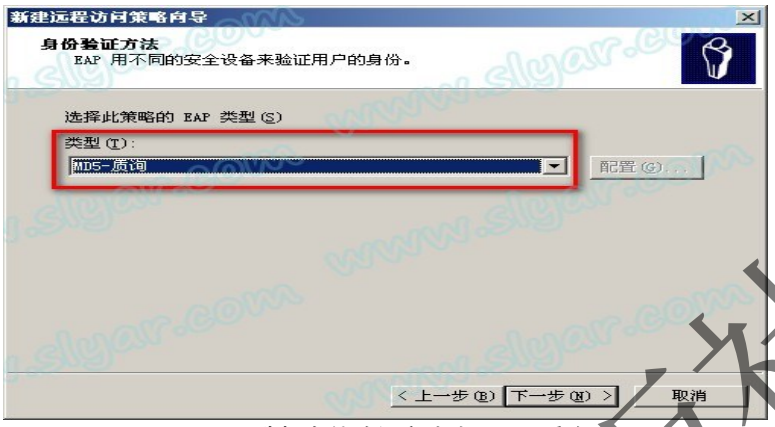

图 8-9　选择身份验证方法为“MD5-质询”

在远程访问策略中只保留新建的访问策略，删掉其他策略，如图 8-10 所示。

图 8-10　删除多余的访问策略

(2)创建 RADIUS 客户端。

说明：这里要创建的 RADIUS 客户端，是指拓扑图中的交换机设备，在实际应用中也可以是 VPN 服务器、无线 AP 等，并不是用户端的计算机。RADIUS 服务器只会接受由 RADIUS 客户端设备发过来的请求，为此需要在 RADIUS 服务器上来指定 RADIUS 客户端。具体步骤如下：

新建 RADIUS 客户端。鼠标右键单击“RADIUS 客户端”，选择“新建 RADIUS 客户端”，如图 8-11 所示。

图 8-11　新建 RADIUS 客户端

按照向导,设置 RADIUS 客户端的名称和 IP 地址。客户端 IP 地址即交换机的管理 IP 地址 192.168.1.200。

设置共享密钥和认证方式。认证方式选择“RADIUSStandard”,此处秘钥必须与交换机上设置的秘钥相同,这里设置秘钥为“123456”,如图 8-12 所示。

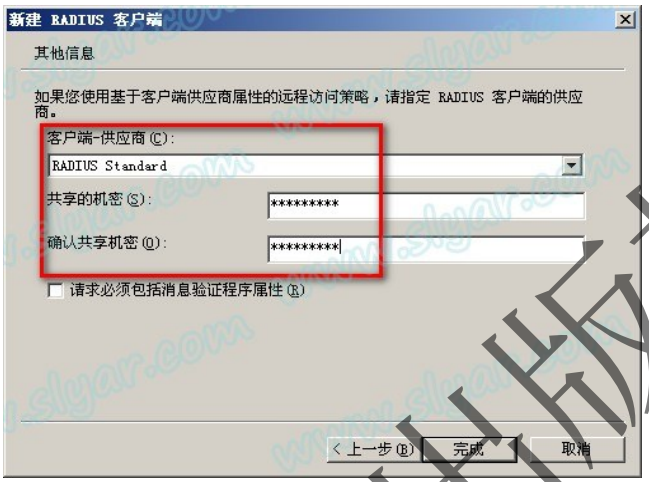

图 8-12　设置共享秘钥

(3)在交换机上启用认证机制。

配置之前先进行连通性测试,在客户端主机上 ping 服务器地址,此时可以 ping 通。

配置交换机 802.1x 认证:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.200 255.255.255.0 //配置交换机管理 IP 地址
```

注意:此处配置交换机管理 IP 是为了保证交换机能和 RADIUS 服务器通信。

```
Switch(config)#aaa new-model //开启 3A 认证
Switch(config)#aaa authentication dot1x default group radius //选择 RADIUS 服务器认证方式
Switch (config)#dot1x system-auth-control //启用全局 dot1x 认证
Switch(config)#radius-server host 192.168.1.254 //配置 RADIUS 服务器的 IP 地址
```

注意:此处有可选 auth-port 参数表示配置 RADIUS 服务器的认证和授权端口号,默认情况下 RADIUS 服务器的认证和授权端口号为 UDP1812;acct-port 参数表示配置 RADIUS 服务器的计费端口号,默认情况下 RADIUS 服务器的计费端口号为 UDP1813。

```
Switch(config)#radius-server key 123456 //配置交换机与服务器之间的共享密钥
```

注意:此处配置的密钥要与 RADIUS 服务器上配置的一致。

```
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#dot1x port-control auto //启用 F0/1 端口的 802.1x 认证,模式为自动
Switch(config-if)#end
```

此时可以进行验证,由于 F0/1 端口启用了 802.1x 认证,在客户端计算机没有经过认证的情况下无法 ping 通服务器。

(4)测试 802.1x 认证接入。

注意:802.1x 默认是不启动的,可在服务中手动打开 Wired AutoConfig 服务。

在客户端计算机上，打开本地连接属性对话框，在本地连接的“验证”标签栏中启用 IEEE 802.1x 验证，EAP 类型设置为“MD5-质询”，其余选项可不选，如图 8-13 所示。

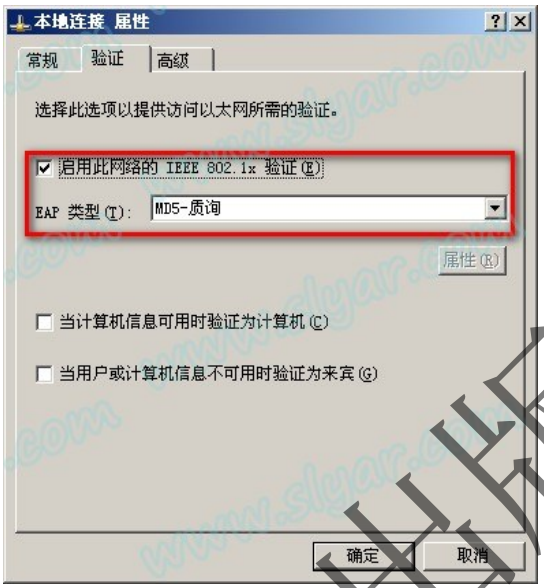

图 8-13　启用 IEEE802.1x 验证

如果之前配置没有问题，过一会即可看到右下角弹出要求进行验证的提示框，如图 8-14 所示。

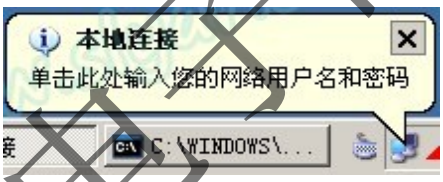

图 8-14　提示验证

点击之后会弹出登录框，要求输入用户名和密码。输入之前配置的用户名“abc”，密码“123456”，点击确定。

验证完成以后，可以进行测试，在客户端计算机上 ping 服务器 IP 地址，ping 通则证明验证成功。还可以通过“控制面板”→“管理工具”→“事件查看器”→“系统”子选项观察 802.1x 的验证日志。

8.5　技术拓展

8.5.1　配置端口安全的注意事项和保护特性

1. 注意事项

在对某个端口配置端口安全的时候，有以下注意事项：

(1)安全端口不能在动态的 Access 口或者 Trunk 口上配置。也就是说在对端口配置 port-secure 属性之前必须保证端口模式是 Access 模式。

(2)安全端口不能是一个被保护的端口。

(3)安全端口不能是 SPAN 的目的地址。

(4)安全端口不能属于 GEC 或 FEC 的组。

(5)安全端口不能属于 802.1x 端口。如果在安全端口试图开启 802.1x,就会有报错信息,而且 802.1x 会被关闭。同样如果试图改变开启的 802.1x 的端口为安全端口,也会出现错误提示信息,安全性设置不会改变。

2. 端口安全提供的保护特性

端口安全能够提供如下多种保护特性,例如:基于主机 MAC 地址允许流量、基于主机 MAC 地址限制流量、在端口上阻塞单播扩散、避免 MAC 扩散攻击、避免 MAC 欺骗攻击等。

8.5.2 802.1x 补充说明

1. 802.1x 和其他认证方式的区别

除了 802.1x 认证以外还有其他一些常用的认证,表 8-1 说明了它们之间的对比关系。

表 8-1　　各种认证方式的对比说明

	802.1x	PPPOE	WEB 认证
是否需要安装客户端软件	是	是	否
业务报文效率	高	低,有封装开销	高
组播支持能力	好	低,对设备要求高	好
有线网上的安全性	扩展后可用	可用	可用
设备端的要求	低	高	较高
增值应用支持	简单	复杂	复杂

2. 802.1x 应用环境

(1)交换式以太网络环境。

对于交换式以太网络中,用户和网络之间采用点到点的物理连接,用户彼此之间通过 VLAN 隔离,此网络环境下,网络管理控制的关键是用户接入控制,802.1x 不需要提供过多的安全机制。

(2)共享式网络环境。

当 802.1x 应用于共享式的网络环境时,为了防止在共享式的网络环境中出现类似“搭载”的问题,有必要将 PAE(端口访问实体)由物理端口进一步扩展为多个互相独立的逻辑端口。逻辑端口和用户/设备形成一一对应关系,并且各逻辑端口之间的认证过程和结果相互独立。

在共享式网络中,用户之间共享接入物理媒介,接入网络的管理控制必须兼顾用户接入控制和用户数据安全,可以采用的安全措施是对 EAPoL 和用户的其它数据进行加密封装。

3. 802.1x 认证的优点

(1)简洁高效:采用以太网技术内核,保持了 IP 网络无连接特性,不需要进行协议间的多层封装,去除了不必要的开销和冗余;消除网络认证计费瓶颈和单点故障,易于支持多业务和新兴流媒体业务。

(2)容易实现:可在普通 L3、L2、IPDSLAM 上实现,网络综合造价成本低,保留了传统 AAA 认证的网络架构,可以利用现有的 RADIUS 设备。

(3)安全可靠:在二层网络上实现用户认证,结合 MAC、端口、账户、VLAN 和密码等;绑定技术具有很高的安全性,在无线局域网网络环境中 802.1x 结合 EAP－TLS 和 EAP－TTLS,

可以实现对 WEP 证书密钥的动态分配，克服无线局域网接入中的安全漏洞。

(4)行业标准：IEEE 标准，和以太网标准同源，可以实现和以太网技术的无缝融合，几乎所有的主流数据设备厂商在其设备，包括路由器、交换机和无线 AP 上都提供对该协议的支持。在客户端方面，微软 WindowsXP 和 Linux 操作系统都提供了对该协议的支持。

(5)应用灵活：可以灵活控制认证的颗粒度，用于对单个用户连接、用户 ID 或者是对接入设备进行认证，认证的层次可以进行灵活的组合，满足特定的接入技术或者是业务的需要。

(6)易于运营：控制流和业务流完全分离，易于实现跨平台多业务运营，少量改造传统包月制等单一收费制网络即可升级成运营级网络，而且网络的运营成本也有望降低。

4. 802.1x 认证的安全性分析

802.1x 协议中，有关安全性的问题一直是 802.1x 反对者攻击的焦点。实际上，这个问题的确困扰了 802.1x 技术很长一段时间，甚至限制了 802.1x 技术的应用，但技术的发展为这个问题给出了答案：802.1x 结合 EAP，可以提供灵活、多样的认证解决方案。

8.6　本章小结

本节内容主要讲述了如何通过设置交换机端口安全和 802.1x 登录认证等方式，来控制未经授权的用户主机随意连接到企业的网络中以及未经批准采用集线器等设备随意增加上网端口数量的行为。

通过学习交换机端口安全配置方法和认证登录的应用可以解决公司交换机接入的安全问题，解决公司网络存在的安全隐患。

8.7　强化练习

1. 简单描述交换机端口安全。

2. 交换机端口安全违例处罚有哪几种行为？各自的特点是什么？

3. 802.1x 认证登录的基本模式是什么样的？

4. 802.1x 认证登录过程主要涉及到哪些设备？它们在整个认证登录过程中的角色和工作特点是什么？

任务 9　配置 PVLAN 提高公司网络安全性和利用率

9.1　项目导引

随着公司业务发展，公司网络对数据通信的安全性提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性。

公司以前的解决方法是给每个用户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，