CCNA 培 训 讲 义

Sailing

Email:sailing_2000@163.net

2002 年 5 月　　上 海

目　　录

前　言

写一本适合喜欢 Cisco 网络新手的培训讲义，一直是我的一个想法。我接触网络有 7 个年头了，从最初的 Windows3.1、Novell Netware 下的网络建设开始，直到今天的以 Cisco 设备为主的大型网络，中间经历了与大多数人一样的学习过程。95 年在大学上计算机网络专业的研究生时，由于自己本科学的是卫星通信，可以说当时对计算机网络一点感觉都没有。当初计算机普及率跟现在是不能相提并论的，更别说网络了，那时能在导师手下，独用一台 486DX 已经可以在同学中招摇过市了。记得有一次在实验室导师让我将一个文件从另外一台机器拷到他的机器上，我折腾了半天也不会用，脑子里面的计算机网络知识除了 OSI，其它一点都没有帮上忙。当时我就觉得为什么在书本上学的那么多的理论知识，可到实际生活中却一点都用不上？也许，这也正是许多网络新手最初对网络的感觉——神秘、不可捉摸。

看到许多介绍网络知识的书本，感到它们要么是面广，泛泛而谈，看完之后原来是自己都会的东西；要么就是点深，讲了一大通理论和复杂的算法后，除了空白还是空白。

98 年参加单位超大型网络建设，接触了大量 Cisco 网络设备，

尤其是路由器。喜欢 Cisco 没有别的原因，就是因为简捷、好用、可靠，而且它也是一个将理论转换为实际的理想平台。对了，我不是 Cisco 任何形式的代理，我说的只是自己摸索 Cisco 设备的一些心得。

2001 年年初，与一个朋友聊天，得知他已是什么 CCNA 了，又告诉我什么是 CCNP、CCIE。以前也了解一些 Cisco 认证情况，但从来没有一个实际的全面的认识。于是，下定决心去考 CCNA，触摸一下认证的感觉。过了 CCNA 之后感觉到，CCNA 对自己的工作确实很有帮助，提高和纠正了自己在工作中的经验。好吧，再去考 CCNP，也过了。我从 CCNA 到 CCNP，全部是自己学习的，只是从网上 Down 了许多学习资料，而且也得到了许多人的帮助。CCNP 细化了 CCNA，将许多深奥的理论以浅显的方式表述出来，理顺和加深了自己对一些网络概念的理解。这里我觉得看英文版书要比看中文版书好。

当然，CCIE 是我的一个目标，但是费用是我的一个最大问题。我相信许多网络人的共同目标就是何时拿下 CCIE，与朋友们煮酒论英雄。

The Hardest Day Is Yesterday!这是一句美国西点军校的名言，它告诉我们要勇敢地面对明天，因为最困难的日子都过去了，还有什么不能坚持下去，希望就在前方。我想这就是我们在寒冷的 IT 冬天的最好的慰籍，在此献给所有 IT 同行们。

我在一个网络培训中心，做过 CCNA 讲师，用的是 ICND 教材。ICND 是 Cisco 公司的幻灯片形式的讲义，它没有展开网络知识，只是归纳出重要概念和纲目来。从严格意义上讲，它不能算是一个好的教材。所以我结合自己的实际情况和已有的一些资料，写了这本讲义。由于网络知识涉及面广，内容新，其中一定有不少不当之处和表达不清的地方，希望大家给我批评指正，就当是给一个朋友提个醒。

Sailing

2002 年 5 月 25 日　上海

第一章　CCNA 介绍

1.1 什么是 CCNA？

Cisco 认证分为三个层次，分别为 CCNA，CCNP，CCIE。

CCNA--Cisco 认证网络工程师(Cisco Certified Network Associator)，Cisco 初级认证。

CCNP—Cisco 认证资深网络工程师（Cisco Certified Network Professial），Cisco 中级认证。

CCIE—Cisco 认证互联网工程师 (Cisco Certified Internet Engineer)，Cisco 高级认证。

1.2 CCNA 学习内容及目标

从学习内容上可分为四大部分，主要内容包括：网络协议理论基础 OSI；TCP/IP 协议；广域网协议；局域网、广域网解决方案。涉及到的内容均为目前中小型网络解决方案中所必需的知识。

通过认证的 CCNA 工程师将具备如下技能:

- 安装、配置以及运行 500 个网络节点规模的 Cisco 网络系统
- 能够胜任 Internet/Intranet 的路由器管理能力

- CCNA 已获得全球 500 大企业的认可和接受
- 是各跨国公司和电子商务企业所急需的人才
- 移民及出国留学可获得技术加分，是升职加薪，寻找丰厚工作待遇的有力凭证

1.3 CCNA 学习基础

只要具有一定的英语基础和基本的计算机应用知识，拥有高中以上的学历就可开始 CCNA 的学习。CCNA 课程的特点是入门的起点不高，但随着课程的逐步深入，您将学习到更高层次的知识与技能，最后成为计算机网络应用的高级人才。因此，是否具有渴望掌握先进网络知识的愿望、积极的学习态度，以及希望从事计算机网络行业、成为高级网络人才的理想是能否学会 CCNA 课程的前提条件。当然，如果具有良好的基础，会达到事半功倍的效果。

1.4　考试申请

至少提前一天，个人到 Cisco 考试中心申请 CCNA 认证考试。

1.5　CCNA 目标人群

对 Cisco 产品或网络不太熟悉的客户、渠道经销商；对 Cisco 产品和服务不太了解的网络技术人员；中小型企业网的网络管理员；在中大型企业中执行桌面支持工作的网络技术支持人员；为小型企业环境提供网络设备安装和第一线支持的网络技术人员；希望获取 CCNA 授证的人员；希望获取 CCNP 授证的人员。

第二章 ICND 课程介绍

2.1 课程特点

介绍在多协议互连网络中配置 Cisco 交换机和路由器所需的概念、命令和*相关实验*。通过讲解、讨论、演示、练习(和*实验设计*)，能够为中小型企业确定和推荐最佳 Cisco 解决方案。该课程提供技术支持人员所需的关于 Cisco 产品安装、配置以及故障排除方面的知识。

2.2 课程目标

- 确定集线器、以太网交换机或路由器的最佳使用环境
- 确定多种互连的 Cisco 设备的网络中的地址、协议以及链路连接状态
- 根据给定的网络设计指标互连 Cisco 交换器和路由器
- 在路由器上正确配置各种路由协议和广域网技术
- 配置访问列表，对网络设备或网段的访问权限以及常规网络流量实施控制

- 检查 Cisco 交换机、路由器及其网络服务和协议的运作情况是否符合给定的网络指标

2.3 预备知识

参加 ICND 课程，应具有基本的网络概念，并且接触过 IP 或 IPX 网络。建议学员最好具有网络环境里的工作经验。详细的预备知识包括对如下内容的基本了解:

- 常用的网络术语和拓扑结构
- 基本的网络设备（例如集线器、网桥、路由器、交换机)
- 二进制和十六进制的运算及与十进制数字转换(最好掌握，但并非必须要求)
- OSI 网络模型
- 访问 Internet 或 intranet
- 应用 Windows 95/NT 运行多个应用程序

2.4 课程安排

课程时间为 5 天或 10 个晚上，具体如下:

课 次		内 容	备 注
第一天	第一晚	Chapter 1,2（介绍、OSI Model）	课程介绍、Internet 介绍；网络基础知识回顾（OSI 原理，TCP/IP 原理等）
	第二晚	Chapter 3,4(操作 IOS 命令)	
第二天	第三晚	Chapter 5(路由器组成)	网络互连配置；IOS 基本命令；网络环境管理的基本命令；交换机基本概念；
	第四晚	Chapter 6(交换机的工作原理)	
第三天	第五晚	Chapter 7(VLAN)	交换机 VLAN 、TCP/ IP 的配置； TCP/IP 的配置（续）
	第六晚	Chapter 8（IP 地址划分）	
第四天	第七晚	Chapter 9（路由协议）	RIP、IRGP、OSPF 路由协议工作原理
	第八晚	Chapter 10（ACL）	
第五天	第九晚	Chapter 12,13,14 (PPP,ISDN,FR）	WAN 的配置； ISDN 的配置；帧中继的配置等；
	第十晚	实验(实验配置见图)	

2.5 推荐书目

在考试之前，推荐几本好一点的 CCNA 学习用书，结合 ICND 会达到事半功倍的效果。

1、《思科网络技术学院教程》(上,下册)78 元，中文版，人民邮电出版社。特别适合初学者，内容通俗易懂。

3、考试: 《Cisco CCNA 认证考试(640-507)指南》83 元(含光盘)，中文版，人民邮电出版社。Cisco press 的考试用书，内容覆盖了考试的全部内容，也有许多内容，已经超出了 CCNA 的考试要求。

4、因为 Cisco 考试是全英文的，所以最好在考试之前，再仔细将研读英文版用书。目前较流行的英文版用书有: Troytech CCNA study guide 3.0（封面有一个骑士头像）

5、RouterSim 3.1——CCNA 路由交换模拟，强烈推荐。能完成 CCNA 学习中遇到的绝大部分命令。

6、Boson Test 3.XX——考试模拟器，强烈推荐。虽然里面没有所谓的真题，但试题内容全部覆盖了 CCNA 的内容，是考前巩固已学知识的利器。

7、Sybex 出版的 CCNA 学习用书推荐，我是用它过的 CCNA。

5、CCNA 官方培训幻灯片&Cisco CCNA study guide

第三章　Internetworking concepts overview

知识点：

1）OSI Reference Model

2）Cisco Network Model

3）OSI’s PDU Encapsulation（5 steps）

4)CSMA/CD

5)Connection-oriented services VS Connectionless Service

6)TCP’s Three-way Handshake

7)Physical address VS Logical address

8)Routing protocol Vs Routed protocol

9)Cisco products Selection

3.1 OSI Model 提出背景

在70年代，Internet网络得到了迅速的发展和应用，在当时的情况下已经变成一个非常巨大的网络。但是由于各种原因，许多网络的设计采用不同的硬件和软件，造成一个必然结果就是：不同的

网络之间互相不兼容，互相不能通信。为了解决这个问题，国际标准化组织ISO（International Organization for Standardization）认识到只有制定一个网络模型，才能让所有网络设计人员设计出的网络能够互相通信，协同工作。基于此， ISO于1984年提出OSI参考模型，即我们常讲到的OSI七层协议。

ISO（国际标准化组织）是一个代表了130个国家的标准化组织的集体，总部设在瑞士的日内瓦。ISO的目标是制定国际技术标准以促进全球信息交换和无障碍贸易。你可能认为该组织应被简称为“ISO ”，但“ISO ”并不意味着是一个首字母缩略字。实际上，在希腊语中，“ISO”意味着“平等”。通过这个词汇表达了组织对标准的贡献。

3.2 OSI 模型的提出意义

OSI模型的主要目的就是为不同的网络提供互相兼容、互相通信。在网络领域，我们虽然看不见一个网络中两个节点是如何通信的，亦可用一个模型对通信过程进行描述。通常用来描述网络通信的模型称为开放系统互连（OSI）模型。通过ICND的学习，您知道OSI模型的七层结构以及各层之间如何相互作用；每层具有的功能。当然，学习OSI模型不足以成为一个网络专家，但是熟悉OSI模型是你

成为网络专家的必要条件。

3.3 OSI 模型

在20世纪80年代早期，ISO即开始致力于制定一套普遍适用的规范集合，以使得全球范围的计算机平台可进行开放式通信。ISO创建了一个有助于开发和理解计算机的通信模型，即开放系统互连OSI模型。OSI模型将网络结构划分为七层：即物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层均有自己的一套功能集，并与紧邻的上层和下层交互作用。在顶层，应用层与用户使用的软件（如字处理程序或电子表格程序）进行交互。在OSI模型的底端是携带信号的网络电缆和连接器。总的说来，在顶端与底端之间的每一层均能确保数据以一种可读、无错、排序正确的格式被发送。*注意：组成网络部件的组合方式常被描述成它的“体系结构”。*“体系结构”这个词在网络领域，反映了这样一个事实，就像一幢建筑物，包括了许多不同的但被集成在一起的部件：电缆、服务器、协议、客户机、应用程序、网络接口卡等等。OSI模型是对发生在网络中两节点之间过程的理论化描述，它并不规定支持每一层的硬件或软件的模型，但你学习到的有关网络的每件事均能对应于模型中的一层。因此，不仅应了解各层的名字，而且应了解它们的功能及层之间相互作用的方法。

图3- 1 描绘了OSI模型层结构:

应用层(Application)
表示层(Presentation)
会话层(Session)
传输层(Transportion)
网络层(Network)
数据链路层(Data Link)
物理层(Physical)

图 3－1　OSI 模型层结构

3.3.1 物理层

物理层是OSI模型的最低层或第一层，该层定义网络连接机械电气性能；定义了Media type、Connector type、Signaling type；包括物理连网媒介，如电缆连线连接器。在物理层上传输的是“0”或“1”比特流。工作在这一层的典型网络设备为集线器（HUB）。术语“第一层协议”和“物理层协议”，均是指描述电信号如何被放大及通过电线传输的标准。

区别以下两个概念，Collision Domain VS Broadcast Domain。

***collision domain**

In Ethernet, the network area within which frames that have collided are propagated.Repeaters and hubs propagate collisions; LAN switches, bridges and routers do not.

***broadcast domain**

Set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames.

连接在HUB上所有计算机处于一个Collision Domain中，在Ethernet中，采用CSMA/CD(Carrier Sense Multiple Access/Collision Detect)技术，避免Collision的发生。具体见2-20页。

3.3.2 数据链路层

数据链路层是OSI模型的第二层，控制网络层与物理层之间的通信。此层数据叫作帧（FRAME）。数据链路层的主要功能是将从网络层接收到的数据分割成特定的可被物理层传输的帧（Frame），见图3 - 2 示出了802.3的数据帧图。

Preamble(6B)	Dest MAC(6B)	Source MAC(6B)	Len (2B)	Data(46-1500B)	FCS(4B)

图3-2 802.3 帧结构

工作在此层的网络设备有，如网桥或交换机。由于它们要对帧解码并使用帧将数据发送到正确的接收方，所以它们工作在数据链路层的。以太网(Ethernet)是应用数据链路层技术的一个实例。

在Data Link层，常会提到Physical Address，即MAC地址。MAC地址固化在网卡的ROM中，所以以简称Burned-IN Address。常见的写法为00-50-04-EE-24-B3。MAC地址分为两大部分，前24字节为厂商号（Oroganizationally Unique Identifer）加上后24字节的厂商自己分配号，目的就是为了保证在全世界不会出现同样地址的网卡。

3.3.3 网络层

网络层，即OSI模型的第三层，关系到子网的运行控制，主要功能是将网络地址翻译成对应的物理地址，并决定如何将数据从发送方路由到接收方。例如，一个计算机有一个IP地址10.34.99.12（TCP/IP）和一个物理地址（MAC）00-60-97-3E-97-F3。这种编址方案就好像说某某人的姓名和他的身份证号码相对应一样。即使还有其他许多人也叫某某，但他们的身份证号码是唯一的。

我们经常提到的IP地址，也称作Logical Address，就定义在网络层。IP地址32字节长，分为网络号部分和主机号两部分。常见IP地址的写法为：16.100.1.86。对IP地址的详细讨论见Chapter 8。

在网络层，要区别Routing Protocol与Routed Protocol两个概念。所谓的Routing protocol是指路由协议，如OSPF、RIP、IGRP。

而Routed Protocol是指IP或IPX协议。

网络层通过综合考虑发送优先权、网络拥塞程度、服务质量以及可选路由的花费来决定从一个网络中节点A 到另一个网络中节点B 的最佳路径。由于网络层处理路由，而路由器因为即连接网络各段，并智能指导数据传送，属于网络层。在网络中，“路由”是基于编址方案、使用模式以及可达性来指引数据的发送。

网络层协议还能补偿数据发送、传输以及接收的设备能力的不平衡性。为完成这一任务，网络层对数据包进行分段和重组。分段即是指当数据从一个能处理较大数据单元的网络段传送到仅能处理较小数据单元的网络段时，网络层减小数据单元的大小的过程。重组过程即是重构被分段的数据单元。工作在此层的网络设备有路由器或具有第三层交换功能的交换机。此层数据叫作数据包（Packet）。

3.3.4 传输层

传输层负责确保数据可靠、顺序、无错地从网络A点到传输到网络B点（A、B点可能在也可能不在相同的网络段上）。如果没有传输层，数据将不能被接受方验证或解释，所以传输层常被认为是OSI模型中最重要的一层。传输协议同时进行流量控制或是基于接

收方可接收数据的快慢程度规定适当的发送速率。

除此之外，传输层按照网络能处理的最大尺寸将较长的数据包进行强制分割。例如，以太网无法接收大于1500字节的数据包。发送方网络节点的传输层将数据分割成较小的数据片，同时对每一数据片安排一序列号，以便数据到达接收方节点的传输层时，能以正确的顺序重组。该过程即被称为排序。在网络中，传输层发送一个ACK（Acknowledgement应答）信号以通知发送方数据已被正确接收。如果数据有错，传输层将请求发送方重新发送数据。同样，假如数据在一给定时间段未被应答，发送方的传输层也将认为发生了数据丢失从而重新发送它们。工作在传输层的一种服务是TCP/IP协议族中的TCP(传输控制协议)，另一项传输层服务是IPX/SPX协议集的SPX。

在传输层，引入两个重要概念：面向连接服务和无连接服务，即Connection-Oriented Service 和 Connectionless Service。Connection-oriented 是在通信前先建立connection，这样保证了数据传输的Reliability。 而 Connectionless是不建立连接就传输，所以 connectionless 有更少的 overhead，但不能保证数据的Reliablity。所以我们传E-mail要用connection-oriented，而网上听歌因为速度更重要丢几个packets没关系可以用connectionless的protocol。在常见的protocol里面TCP是connection-oriented,

UDP 是connectionless。

对于TCP协议，要经过“三次握手“（Three-way Handshake）才能建立连接，再进行数据传输。

“三次握手”具体过程见图3-4:

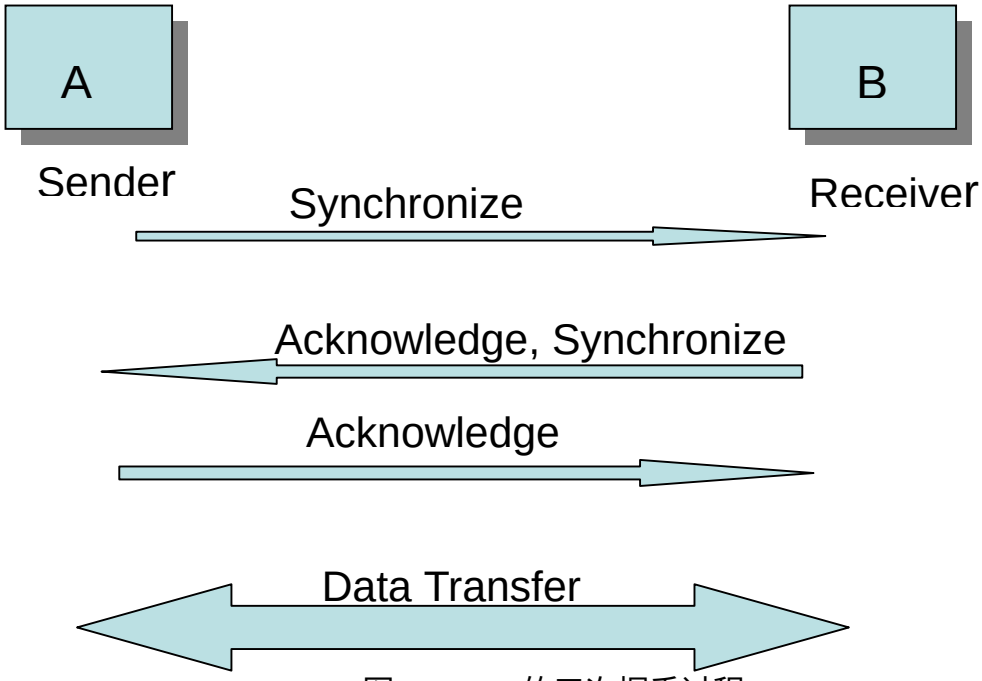


图3-4　TCP的三次握手过程

3.3.5 会话层

会话层负责在网络中的两节点之间建立和维持通信。术语“会话”指在两个实体之间建立数据交换的连接，常用于表示终端与主机之间的通信。会话层的功能包括：建立通信链接，保持会话过程

通信链接的畅通，同步两个节点之间的对话，决定通信是否被中断以及通信中断时决定从何处重新发送。当通过拨号向你的ISP请求连接到因特网时，ISP服务器上的会话层向你与你的PC客户机上的会话层进行协商连接。若你的电话线偶然从墙上插孔脱落时，你PC机上的会话层将检测到连接中断并重新发起连接。会话层通过决定节点通信的优先级和通信时间的长短来设置通信期限。

3.3.6 表示层

表示层如同应用程序和网络之间的翻译官，在表示层，数据将按照网络能理解的方案进行编码，这种编码也因所使用网络的类型不同而不同。表示层协议还对图片和文件格式信息进行解码和编码。

3.3.7 应用层

OSI模型的第七层是应用层。应用层负责对软件提供接口以使程序能使用网络服务。术语“应用层”并不是指运行在网络上的某个特别应用程序，如Microsoft Word ，应用层提供的服务包括文件传输、文件管理以及电子邮件的信息处理。程序可以独立运行，而不管发送数据时目标节点是否被连接到网络上。在宽带网设计中，经常会遇到第七层交换机，就工作在这一层，它主要起到应用

程序负载均衡作用。

3.4 OSI 数据封装

在OSI模型中的每一层都使用它自己的协议和接收设备的对等层通信。每一层通过协议数据单元（Protocol Data Unit）交换数据。PDU包括控制信息和数据两部分。在OSI模型中，将控制信息和数据绑定的过程称作封装（Encapsulation）。当某一层收到上一层PDU之后，它便进行封装过程，将收到的PDU当作本层PDU的数据部分，再加上本层的控制头信息和控制尾信息，形成本层的PDU，交给下一层处理。如图3-5所示:

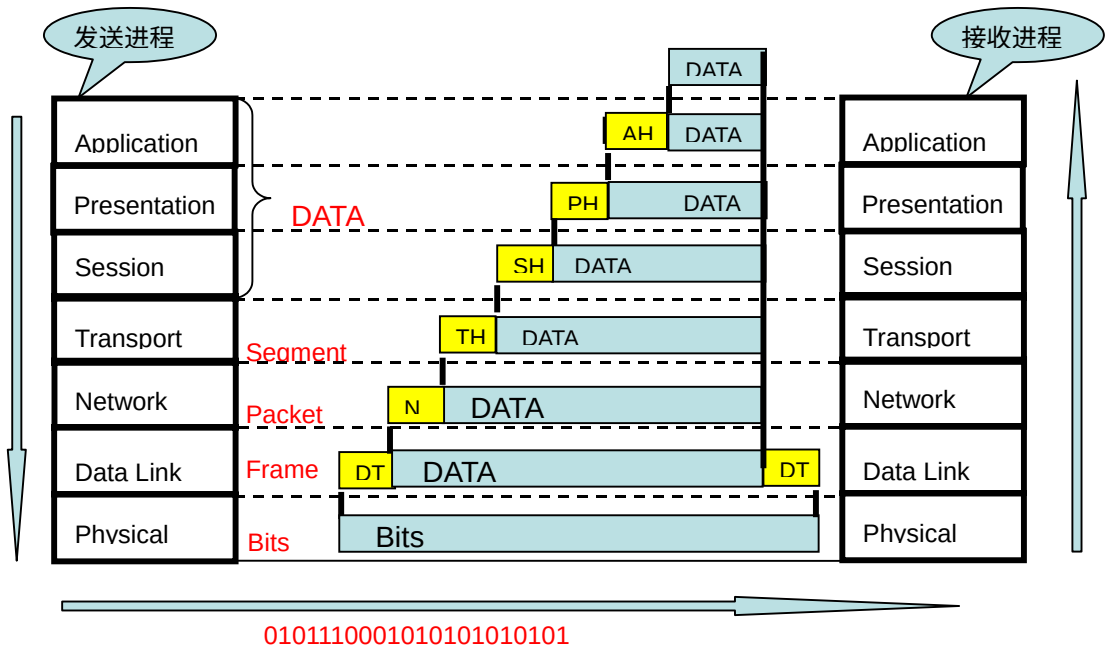


图3-5　OSI数据封装过程

概括来讲数据封装的五步为:

（1）User information is converted to data. (Application Layer)

（2）Data is converted to segments (Transport Layer)

（3）Segments are converted to Packets or Datagrams (Network Layer)

（4） Packets or Datagrams are converted to Frames (Data Link Layer)

（5） Frames are converted to bits. (Physical Layer)

3.5 Cisco　模型

为了简化网络设计和管理，Cisco公司提出一个三层模型来描述网络，这三层为:（2－6到2－9）

Core layer	快速交换层，高档交换机
Distribution layer	策略层，2—8页，路由器
Access layer	终端用户接入点，HUB或Switch

3.6 Cisco 产品选择

具体见从2-40到2-46页。Cisco公司为了简化产品选择工作，

编制一个Cisco Product Selection软件，可以到网上down。

第四章　Assembling and Cabling Cisco Devices、Operating and Configuring a Cisco IOS Device、Managing Your Network Environment

ICND的第三章、第四章、第五章节，主要讲解Cisco设备交换机和路由器以及Cisco　IOS的一些基本知识，突出实践经验，知识点分布得比较散乱，希望大家仔细看书。

4.1 Cisco 路由器

Cisco 路由器或分为固定配置和模块化两大类。路由器是cisco考试中最重要的概念。路由器有多个network interface，连接多个不同的subnet；路由器通过routing table 来决定packets 往哪边传，永远不可能往两个interface上传，万一遇到这种情况会把packet drop 掉；routing table 可以人工加，也可以使用routing protocol，如RIP 或OSPF动态维护routing table。路由器工作在OSI

3 Layer 、4 Layer。

4.1.1 路由器硬件构成

路由器有六大部分组成，分别为:

1）RAM——主要运行Cisco IOS和running configuration。

2）ROM——含有Microcode，用于路由器的启动和维护。

3）Flash——含有Cisco IOS Images，相当于PC机的硬盘。

4)NVRAM——Non-volatle RAM，非易失性RAM，用于储存配置文件，如startup-config文件和Config-register。

5）Config Register——控制Cisco路由器启动过程，具体见5-22。

6)Interface——主要有console port、AUX port、AUI port、serial port、BRI port、ethernet prot、fastethernet port。

console port: 本地配置端口。要用console cable (Cisco 的原装cable 是蓝色的)一头连在console port上，另一头连在PC机的COM口上，然后用HyperTerminal登录，进行配置。一般情况下Cisco 路由器都是用console port 进行配置的。这种情况也叫带内配置，Band-inside-config。con0代表第一个 console port。

AUX（auxiliary） port: 辅助port的意思就是用modem连接进行远程调试路由器。用处不是很大，在某些cisco路由器里面都没

有这auxilary port。

AUI port、ethernet port、fastethernet port：以太口或快速以太口，用于连接局域网。e0 代表第一个 ethernet port。如果是第一个fast ethernet 的话用fa0 来表示。

Serial port：分为固定配置和模块化配置两种情况。在模块化配置情况下，还需要购买WAN卡，如WIC(WAN interface card)。Serial port一般用s0代表第一个serial port。

BRI port：用于连接ISDN。

Cisco路由器的接口命名规则是按从右往左，从下往上的顺序排列的。比如有两个ethernet port，左边那个就是e1，右边那个就是e0。 如果这两个ethernet port 是上下排列的下面那个就是e0，上面那个就是e1。在有的router 里面一个network module solt 里面会有多个interface，这时候你可以用 e1/0，e1/1，e1/2 等符号来表示。

4.2 IOS (Internetwork Operating System)

正如Microsoft 的operating system 叫Windows，Cisco 的operating system 叫IOS，其实Cisco router 里面的chip都很便宜的大多数也就是486 的水平现在的Pentium computer也就卖几百美金，为什么这个小小的router就敢卖好几千的美金就应该是这个

IOS。如果说Microsoft是靠Windows 垄断了市场，那么说Cisco 是靠IOS 来垄断了市场真是一点都不为过。

4.2.1 IOS 界面

Exec 是 CLI (Command Line interface) 的，象MS-DOS、unix 里面的command line 都是 CLI 的。而Windows 是GUI (Graphic User Interface)。CLI 的特点是比较难学，但配置起来比较快。现在Cisco 也正在做Java 的GUI-based configuration software,但大家还是喜欢CLI 的件进行练习。

Cisco IOS有两种EXEC方式: user mode 和 Priviledge mode。在学习IOS命令的时候，一定要记住所使用的命令处于何种提示符下。在IOS中，经常会遇到以下提示符，如下表。

提示符	描述
Hostname>	User mode
Hostname#	Priviledge mode
Hostname(config)#	全局配置模式
Hostname(config-if)#	端口配置模式
Hostname(config-subif)#	子端口配置模式
Hostname(config-line)#	Line配置模式，如VTY、AUX、异步拨入
Hostname(config-router) #	动态路由协议配置，如RIP、IGRP、OSPF

4.2.2 常用 IOS 命令

在CCNA中，我们要掌握和熟记一些常用IOS命令。见下表。

命令	描述
Show version	查看IOS版本号
Show running-config	显示当前在内存中运行的配置信息
Show startup-config	显示保存于NVRAM中的配置信息
Show flash	显示FLASH内容，如IOS名称、大小
Show interface XX	查看端口状态
ip address 16.100.1.5 255.255.255.0	在端口上配置IP地址
Setup	进入菜单配置模式
Config terminal	进入全局配置模式
Hostname XX	修改路由器或交换机名称
Router(config)#line console 0 Router(config-line)#login Router(config-line)#password *XXXX*	配置进入console 口口令
Router(config)#line vty 0 4 Router(config-line)#login Router(connfig-line)password *XXXX*	配置Telnet进入口令
Router(config)#enable password *XXXX*	进入priviledge口令
Routet(config)#enable secret *XXXX*	代替enable口令
Clock rate 640000	在DCE端口设置通信速率为64K
Bandwidth 64	在show interface 命令中会表现出来，它设定路由协议所能使用的带宽，而非通信线路上的实际带宽。
Router(config-if)#no shutdown	使能一个端口
Show controller *serial 0*	查看某个端口的电缆类型为DTE或为DCE。
Show session	查看建立telnet会话个数
Show user	查看console口是否在使用；并列出所有telnet会话。
有关running-config、startup-config、tftp之间的转换关系，见ICND的5-27页。	
ip default-gateway 10.5.5.3	设定网关地址
?	帮助命令
Router> show history	- Shows command buffer
Router> terminal history size	- Set command buffer size
Router> terminal no editing	- Disable advanced editing features
Router> terminal editing	Re-enables advanced editing

注意: 在switch上配置IP只是为了利于远程管理。

4.2.3 外部配置方式

外部配置方式有:

1）console port

2)aux port

3)vty port－telnet

4)TFTP server

5)Web Browser

4.2.4 IOS 常用快捷键

Ctrl-W - Erases a word
Ctrl-U - Erases a line
Ctrl-R - Redisplays a line
Ctrl-A - Moves the cursor to the beginning of the current line
Ctrl-E - Moves the cursor to the end of the current line
Ctrl-F (or right arrow) - Move forward one character
Ctrl-B (or left arrow) - Move back one character
Ctrl-P (or up arrow) - Repeat previous command entry
Ctrl-N (or down arrow) - Most recent command recall
ESC+B - Move backward one word
ESC+F - Move forward one word
Ctrl-Z - Ends Configuration Mode and returns to the Privileged EXEC Mode.
TAB Key - Finished a partial command

4.2.5 Cisco CDP

Cisco Discovery Protocol是Cisco特有的（proprietary）用于收集直接相邻Cisco设备信息的管理工具。CDP工作在OSI模型的

Data link层，采用SNAP帧结构。默认情况下，CDP是enable的，CDP每60秒发送一次广播，它的hold-time是180秒。涉及CDP的有一些命令，有:

Router(config)#cdp run——启动CDP

Router(config-if)#no cdp enable——关闭CDP

Router(config)#cdp timer 30——设置CDP广播时间

Router(config)#cdp holdtime 120——设置CDP保留时间

Router#show cdp neighbors ——查看直接相邻设备五大类信息，如Device identifiers、Address list、Port identifier、Capabilities list、platform。

4.2.6 Configuration-Register

Configuration-Register用于控制路由器启动过程，其工作原理类似PC机中的CMOS。在默认情况下，它的值为0x2102，可以用show version命令来查看。Configuration-Register长为16Bit，其中低4 bit叫作boot field，设置不同的值，可以让路由器启动到不同的工作状态。具体为:

Boot field	Meaning
0x0(0000)	启动到Rom monitor状态，提示符为＞或rommon>
0x1(0001)	从ROM启动，提示符为router(boot)
0x2(0010)-0xF(1111)	正常启动，到NVRAM中查找boot命令。

Configuration Register Value及其含义:

```
---------------------------------------------------------------------
ConfigurationRegisterValue 含义
0x2102            缺省设置。
bit13=0x2000         Flash引导失败5次后，自动从Rom引导。
bit8=0x0100          关闭Break键。
Boot field=0x2        从Flash中引导正常运行模式。
0x2101
bit13=0x2000         Flash引导失败5次后，自动从Rom引导。
bit8=0x0100          关闭Break键。
Boot field=0x1        进入Boot Rom运行模式。Router(boot)>
0x142
bit8=0x0040          进入 Rom Monitor运行模式。>
Boot field=0x2        从Flash中引导正常运行模式。
```

4.2.7 口令恢复

由于各种原因，口令的丢失总是对工作造成不必要的影响。在这里，向大家介绍如何重新恢复Cisco 2509路由器口令。

准备工作：一台运行终端仿真程序（可以在Windows 95/98下启动超级终端）PC，串口（COM1/COM2）通过Cisco公司随机配备的console线与路由器Console口连接。

（1）路由器开机，30 秒内按 Ctrl + Break 键，出现提示符 “>"（如果没有出现该提示符，路由器重新开机，重复（1）步骤）。

（2）键入如下命令： ">o/r 0x142"。

（3）初始化路由器： ">i"。

（4）系统重新启动，屏幕显示系统配置对话:

"System configuraiton to get started?，键入 "no"，系统显示“Press RETURN to get started! "，按“Return"键，系统显示“Router>"。

（5）键入如下命令: "Router>enable"进入超级用户状态(系统不再需要你输入超级口令了); “Router # show startup – config"显示配置参数，特别要注意记住所看到的密码（你也可以通过enable serect "changepassword"命令更改超级用户口令）。

（6）键入如下命令恢复原来的寄存器:

"Router(config) # config – reg 0x2102" ;

"Router(config) # ctrl – z";

"Router(config) # wr"存盘。

（7）重新启动路由器，即可: “Router # reload"。

Module2-Interconnecting Catalyst Switches

第五章　Catalyst 1900 Switch Operations、Extending Switched Networks with Virtual LANs

知识点：

1）　Switch’s three main functions

2）　Broadcast Storm

3）　Switch Vs Bridge

4）　STP、STP’s ports

5）　Switch’s three forward way

6）　Vlan、Vlan’s Tagging

7）　Vlan Trunk Protocol(VTP)

8）　Some basic switch’s configurations

5.1 Switch(Bridge)技术

目前，运用于OSI Layer2上的主要技术有Ethernet、FDDI(Fiber Distributed Data Interface)、Token Ring。在CCNA中，我们主要考虑Ethernet。

可以说Ethernet 是运用最为广泛的一种局域网技术。1960年，Ethernet network architecture 起源于夏威夷大学，他们当时采用carrier sense multiple access/collision detection (CSMA/CD)技术。这一技术后来被IEEE802.3采用并细化。目前，Ethernet和IEEE 802.3 占有大部分LAN市场。今天，Ethernet常被用来代表采用carrier sense multiple access/collision detection (CSMA/CD)技术的LAN's。 Ethernet 和 IEEE 802.3 是两种特别相似的LAN技术。

第一、它们都采用CSMA/CD技术。

所谓的CSMA/CD就是：在CSMA/CD局域网中的工作站任何时候都可以访问网络，在发送数据之前，stations “侦听”网络是否被占用。如果网络被占用，它们将等待。如果没有被占用，stations 开始发送数据。当两个stations “侦听”网络没有被占用，并同时开始发送数据，便出现冲突（collision），这时两个stations的发达

都将被破坏。在等待一个随机时间后，两个stations重新开始transmit。

第二、它们都是广播网络（Broadcast networks）。

所谓的广播网络就是网络中的任何一个station 都可以看见所有数据帧，不论这些数据帧是不是发送给它们。

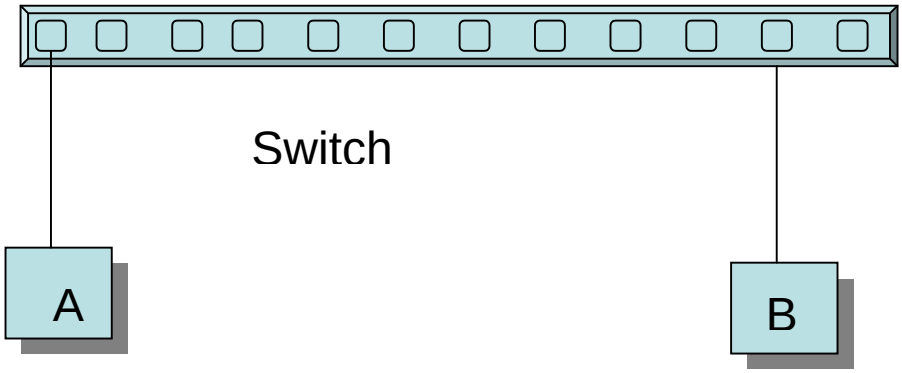
第三、它们之间的差别是非常微小的。Ethernet提供OSI模型的 Layer 1 和 Layer 2服务。而IEEE 802.3 则是描述OSI模型的Layer 1和Layer 2的MAC子层。

5.2 Switch 的三个功能

在讲述三个功能之前，首先回顾一下IEEE 802.3帧结构，见下图: (具体说明参见2－22页)

Preamble	Des MAC	Source MAC	Length	DATA	FCS

*功能一、Address Learning Function



首先，Switch负责维护MAC表。在Switch的Cache中，MAC表用来记录与之端口相连的PC的MAC地址以及与之对应的port。以上图为例，Switch初始化时，MAC表为空，此时如果PC A向PC B发送数据，Switch收到PC A的数据帧后，第一步抽取该帧中的”Source MAC”中值，并和对应的port号，保存到MAC表中。第二步，由于Switch不知道PC B连接在哪个port上（因为此时MAC表为空），它将Flooding该帧到其它所有port上。一旦PC B收到数据帧，发送响应数据给PC A，Switch收到后，采取以下工作。

第一、 抽取该帧中”Source MAC”中的值，并和对应的port，保存到MAC表中。

第二、 抽取数据帧中的”Dest MAC”中的值，并以此值查找MAC表中对应的port号。

第三、 如果查找成功，将此帧只转发到该port。如果不成功，则Flooding。

如上所述，在经过一段时间后，Switch将会在MAC表中保存所有连接的PC MAC地址及其对应的port号，并保留一定时间。如果某条记录在一定时间内没有被刷新，Switch将会删掉这条记录，以保证Switch的交换速度。

* 功能二、Forward/Filter Decision

MAC表建立完后，Switch收到一个数据帧，抽取 “Source MAC”

中的值，在MAC表中查找对应的PORT，查找成功后，Switch只向此PORT转发数据帧，而不向其它PORT转发，达到节省带宽目的。

* 功能三、Loop Avoidance

在大型网络中，任何网络的阻断都是不能容忍的，所以设计了类似6－9中的网络冗余结构。任何事物都具有矛盾的两方面，这种网络冗余结构，会造成Broadcast Storm 、Multiple frame copies和MAC表不稳定。

1） Broadcast Storm

见6－10

2） Multiple Frame Copies

见6－11

3） MAC table Instability

见6－12

5.3 Spanning-Tree Protocol(STP)

针对LOOP，必须采用某种方法使得冗余网络中的某个port处于断开状态，从而构不成循环网络。目前广泛使用的是STP，即Spanning-Tree Protocol。

STP最早是DEC公司开发出来，后来被802.1d所采用。在Cisco Catalyst Switch 中默认是802.1d。运行STP的交换机以一定的频率

（默认是每2秒）通过BPDU（Bridge Protocol Data Unit）互相交换信息。

STP的具体作用，参看6－14到6－22。

5.3.1 STP 的 Convergence 步骤

1.Elect one Root Bridge

在一个网络中，只能存在一个Root Bridge。具有最低Bridge ID的Switch就是Root Brideg。在Root Bridge上的所有port都是Designated ports，处于Forwarding状态。由于每2秒Switch交换Bridge ID，通过STA算法最终得出一个Root Bridge。当然其它Switch为Nonroot Bridge。Bridge ID由2个字节的Bridge Priority(32768)和6个字节的Bridge MAC组成。

2.Elect one Root Port per non-Root Bridge

各个non-Root Bridges参照到Root Bridge的path cost值的大小，选出NonRoot Bridge的Root port。Root port 工作于Forwarding状态。Path Cost 是一个可以累加的基于带宽的值，哪个port的path cost值越小，就是Root port。具体COST值定义见6－18。

3.Elect one Designated Port per segment

在Root Bridge基础上，再选择Designated Port。首先根据到Root Bridge的PORT具有最低path cost值。如果两个PORT具有相同的path

cost，再比较谁的Bridge ID低，谁低谁就是Designated Port，另外一个就是Non-Designated Port，处于Blocking 状态。

举例，见6－19。

5.3.2 Spanning-Tree Port States

在STP中，port 的状态共有5种。

1） Disabled

这种状态并非是STP状态，它是由于人为DOWN掉的。

2） Blocking

当PORT初始化时，处于该状态，在Blocking状态，port不能接收或发送数据，也不能向MAC表中添加MAC地址。它只能接收BPDU，以获取其它Switch信息。

3） Listening

当Switch认为该port将被选为root port或designated port时，该port将从Blocking向Listening状态转变，准备开始转发数据。处于此状态的PORT，不能接收或发送数据帧。当然能接收或发送BPDU。

4） Learning

经过一个Forward Delay之后，转为Learning状态。在此状态下，PORT只能接收数据帧，并向MAC表中添加。它也能接收或发送BPDU。

5） Forwarding

工作状态，即能接收或发送数据，也接收或发送BPDU。在正常情况下，PORT要么处于Forwarding状态，要么处于Blocking状态。

State	DATA Frame	BPDU
Blocking	NO	Receive only
Listening	NO	Receive or Send
Learning	Receive only	Receive or Send
Forwarding	Receive or Send	Receive or Send

5.3.3 Switch Vs Bridge、Switch 的转发模式

* 在ICND的6－23页，告诉大家如何区别Switch与Bridge。

Bridge	Switch
Primarily software based	Primarily hardware based(ASIC)
Up to 16 ports per bridge	More ports on a switch
One STP per bridge	Many STP per Switch

* Switch的转发模式有:

1） cut-through

Switch一旦检查到数据帧中Dest MAC字段，就转发，转发速度最快，效率最高，可靠性最低。

2） store-and-forward

Switch只有全部收到数据帧才转发，转发速度最慢，效率最低，可靠性最高。

3） fragment-free

在一般情况下，冲突发生在数据帧的前64字节内，所以在这种模式下，Switch读进数据帧的前64字节内容，才转发，转发速度中等，效率中等，可靠性中等。

5.4 Switch 的配置

在以Cisco Catalyst Switch 1900系列背景下，Switch的配置方法一般有三种: Menu、Web-based、IOS CLI。

在配置Switch时，需要注意的问题是在Switch上配置IP地址，只是为了远程管理用。

5.5 VLAN（虚拟局域网）

5.5.1 什么是 VLAN?

VLAN指一个或多个LAN上的一组设备，尽管它们处于不同的地方或位于多个不同的LAN段，但是它们仍然像在同一条线上通信。因为VLAN 基于逻辑连接而非物理连接，它们是非常灵活的。不属于同一VLAN的Switch端口，不共享广播，也就是说通过创建VLAN，可以将一个广播域划分为若干个小广播域，减少LAN中的广播流量，

提高网络效率。此外，虚拟网的划分对网络安全也有一定的意义，可以通过虚拟网隔离不同用户群之间的相互访问，并可以根据需要随时调整。

在CCNA中，我们主要考虑的是第二层交换机的VLAN。第二层交换机可以根据端口或者MAC地址划分虚拟网，第三层交换机则可以根据IP地址划分虚拟网，因此第三层交换机提供的虚拟网管理能够为用户提供更多的灵活性。构建大中型网络一定会涉及虚拟网的划分，用户应根据网络应用的需要选择具有相应虚拟网功能的交换机产品。

VLAN的可以按照地点、职能部门、功能组来划分。在1900上配置VLAN有两种方法:

* 静态(Static)－per port

网络管理员人工配置，这种方法适合中小型网络。

* 动态(Dynamic)- per mac

对于大型网络，网络管理员不可能对所有Switch进行配置和管理。采用动态方法，必须使用VMPS（VLAN Membership Policy Server）。

VLAN提供以下好处:

•Reduced administration costs from solving problems associated with moves and changes——减少管理费用

As users physically move they just have to be re-patched and

enabled into their existing
VLAN
•Workgroup and network security——增加安全性
You can restrict the number of users in a VLAN and also prevent another user from joining a VLAN without
prior approval from the VLAN network management application.
•Controlled Broadcast activity——控制广播流量
Broadcasts are only propagated within the VLAN. This offers segmentation based on logical constraints.
• Leveraging of existing hub investments——易于升级网络
Existing hubs can be plugged into a switch port and assigned a VLAN of their own. This
segregates all users on the hub to one VLAN.
•Centralized administration control——易于集中管理
VLANs can be centrally administrated.

5.5.2 Frame Tagging(帧封装技术)

当不同VLAN数据帧在交换机中传输时，交换机需要识别这些数据帧归属于哪个VLAN。Frame Tagging技术就是在每个数据帧上加上一个唯一的ID，有时也称这种技术为VLAN ID或VLAN Color。Cisco的Frame Tagging是仅当数据帧通过Trunked Link时才起作用，意味着当数据帧离开Trunked Link时，Vlan Tag要被去除。每个交换机都必须识别出数据帧的ID，并决定如何归属这些数据帧。如果交换机还有另外一个Trunked Link，并且数据帧的ID不在此交换机的VLAN ID中，该交换机将此数据帧转发到另外一个Trunked Link上。

一旦数据帧到达一个Access Link，交换机就必须去除该数据帧的Vlan ID，终端设备收到的数据帧是不带有任何Vlan ID的。

目前，比较常见的Frame Tagging技术有:

1）802.10——用于FDDI VLAN，是Cisco 特有的。

2)LANE——用于ATM VLAN。

3) 802.1q——IEEE公布的标准VLAN Frame Tagging技术，它在802.3帧结构的Source MAC 和Length中插入一个4个字节长的ID字段，这种技术也称作internal tagging。

4)ISL(Inter-Switch Link)

ISL是Cisco特有的VLAN ID技术，它只能配置在用于Trunked Link的FastEthernet和Gigabit Ethernet端口上。与802.1q不同的是，它叫作external tagging，它在802.3帧的头尾封装识别字段。在头上加上26字节长的ISL Header，尾上加上4字节长的CRC。ISL Header的具体解释见7－7。

需要注意的是: ISL是由硬件ASIC完成的，速度快; ISL最多支持1024个VLAN。

5.5.3 VLAN Trunk Protocol(VTP)

Cisco创建VTP协议来管理交换网络中所有已配置的VLAN，维护全网一致性。通过VTP，网络管理人员可以增加、删除VLAN以及修改VLAN名称。所有这些变化都要通过VTP传播给网络中的所有交换机。VTP与Trunked Link没有任何关联，容易引起混淆。

各个交换机通过Trunked Link来传递VTP信息的。使用VTP来管理网络中的VLAN，首先必须要创建一具VTP server。所有共享VLAN信息的Switch都必须属于同一个Domain。一个Switch在同时只能属于一个Domain。

所谓VTP Domain就是一个网络中的多个相连的Switches。如果在网络中，只存在一个VLAN，就没有必要使用VTP。在一个VTP DOMAIN中，Switch有三种不同的VTP工作模式，分别为:

1）Server

VTP server mode 是所有Cisco交换机的默认工作方式。在一个VTP Domain中，至少需要一个Server在整个DOMAIN中广播VLAN信息。在此方式下你可以:

_ Create, add, or delete VLANs on a VTP domain.

_ Change VTP information. Any change made to a switch in server mode is advertised to the entire VTP domain.

所有配置信息保存在NVRAM中。

2）Client

VTP clients接收来自VTP servers信息，发送和接收VTP更新数据。但是在此方式下，你不可以做任何修改。 No ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch about the new VLAN. If you want a switch to

become a server, first make it a client so that it receives all the correct VLAN information, then change it to a server.

3) Transparent

VTP transparent switches 不参与VTP DOMAIN的任何活动，但是在此工作方式下，它们仍然可以通过Trunked Link转发VTP Advertisements(只有VTP Version 2) 。工作于此方式的交换机独立于VTP Domain。在VTP transparent switches 上，仍然进行增加、删除、修改工作，而不影响其它交换机。所有配置信息保存在NVRAM中。

VTP的具体工作过程见7-10。

5.5.4 VTP Pruning

配置VTP Pruning可以减少一些不必要流量，诸如广播(broadcast)、多播(multicast)、甚至单播(unicast)，达到节省网络带宽目的。VTP限制这些数据只流向所需要的Trunk link。如果一个Trunk Link不需要这些广播，就没有必要再向此PORT发。举例来说，如果一个交换机上没有任何一个PORT配置给VLAN 5，这时如果有一个VLAN 5 的广播，那么这个广播就没有必要通过Trunk Link向这个交换机发。

默认情况下，VTP pruning 是Disabled，并且VLANs 2到1005是

可以pruning。在VTP SERVER上Enabling pruning意味着整个Domain中的所有交换机Enable Pruning。VLAN 1 是不能prune，因为VLAN1是作为管理用。

5.5.5 VLAN 配置

一般情况下，VLAN配置采取以下步骤:

1) Enable VTP(可选)

在VTP配置中，有以下参数需要配置:

*VTP Domain Name

*VTP mode

*VTP Pruning

*VTP Password

*VTP Trap—用于SNMP

Switch(config)#vtp {server|transparent|client} {domain *xxx*}
{trap{enable|disable}} {password *xxxx*}
{pruning {enable|disable}}

2) Enable Trunking

Switch(config-if)#trunk [on|off|desirable|auto|nonegotiate]

3) Create VLANs

在全局配置模式下，

Switch(config)#vlan *X* name *XXXX*

4) Assign VLAN to ports

Switch(config-if)#vlan-membership [static *X*|dynamic]

Module 3—Interconnecting Cisco Routers

第六章 Interconnecting networks with TCP/IP

知识点：

1) TCP/IP Overview

2) TCP/IP Three-way Handshake

3) ARP

4) Computing TCP/IP Address

5) ISL Configuration

6.1 TCP/IP 概述

TCP/IP协议簇是由DARPA于70年代开发的，后来又被伯克利研究所细化。由于OSI model太过理想化，一直没有被实现。TCP/IP因此成为目前工业标准。TCP/IP协议簇并不是静态的实体，它更像是一

个动态改变的互连网络协议的集合，这些协议不断推动了互连网络向前发展。作为事实上的标准，TCP/IP协议并不为任何供应商所拥有，但是任何供应商都支持它。由各种不同种类的计算机系统组成的互连网络需要互相通信，而TCP/IP正是代表了各种不同平台上的共同特性。

TCP/IP协议有五层，大致对应OSI参考模型。见图6-1。

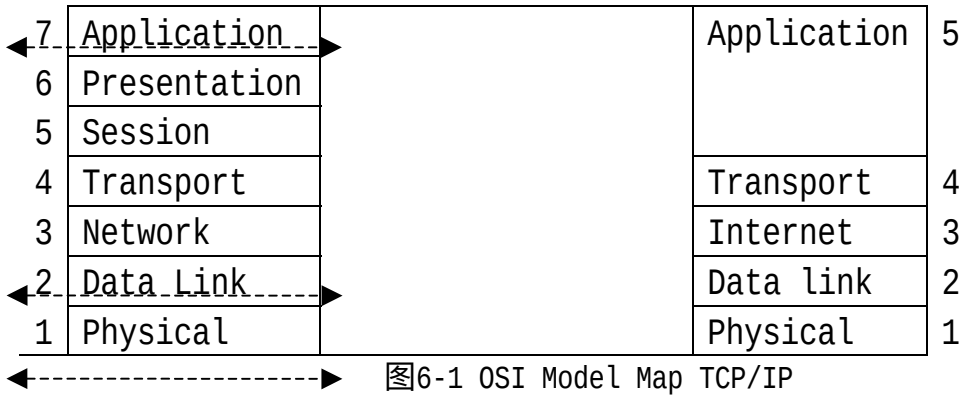


图6-1 OSI Model Map TCP/IP

下面对TCP/IP各层进行简单描述。

1) Application

此层提供各种应用服务，如FTP、E-Mail、Telnet、SNMP。

2) Transport

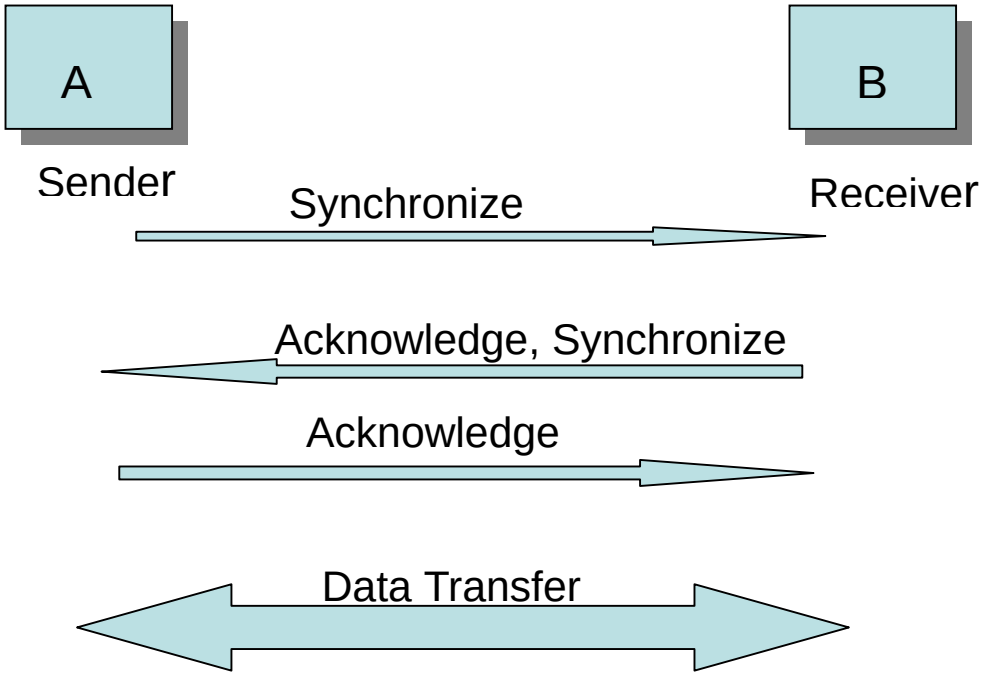
此层提供端到端的传输服务，有两大主要功能，一是Windowing流量控制技术；二是使用Sequence numbers 和 acknowledgement来保证传输可靠性。在此层有两个典型协议：TCP和UDP。

* TCP——TCP是一个面向连接、可靠的协议。在面向连接服

务中，连接是在数据传输之前就已经建立完成。TCP在终端应用程序间提供一条虚拟电路（Virtual Circuit），TCP负责将上层数据打包成segment进行传输；整合从下层收到的数据，交由上层处理。TCP数据段Segment的结构，见8－7。其中:

第一、TCP的PORT——TCP和UDP协议通过PORT或Socket号将数据交给上层协议处理。所谓的port就是用来在同一时间识别不同会话的一种机制。如在同一时间，我们可以进行FTP、TELNET、DNS、SNMP等会话，但是并不会出现互相冲突现象，这就是因为这些不同的服务的port不同。IANA规定Port号小于1024为Well known ports。大于1024可以动态分配。

第二、第二、TCP的三次握手——在前面章节中，我们曾经介绍过TCP的三次握手过程。



第三、Windowing Flow Control——Tcp使用Windowing技术来控制流量。Windowing的大小决定每一次接收方所能承受能力。当Windowning size设为1，意味着在发送每一个Segment都要被Acknowledgement。具体见8－11到8－13，要求记住。

*UDP——UDP是无连接、不确定、不可靠服务。它没有任何可靠性机制，只能依靠上层协议来维护传输可靠性。

3) Internet

Internet层相当于OSI的Network层，在此层上运行以下几种典型协议:

* IP——为数据传输寻找通路，它本身与数据传输无关。IP数据包结构见8－16。Protocol Field: TCP－6，UDP－17。

* ICMP——提供各种控制和消息功能，如：Destination Unreachable、Echo(Ping)等，具体见8－18。
* ARP——ARP用来解析或映射已知IP地址到MAC这样一个过程。在PC机中存在ARP Cache。如果一个目的PC机的MAC地址不存在，它就会启动ARP去寻找目的PC的MAC。
* RARP——RARP是ARP的反过程，已知MAC地址解析IP地址。这种技术常常用在无盘工作站中。

4) Data Link

5) Physical

6.2 IP 地址划分

6.2.1 基本知识

* 熟悉二进制和十进制的转换。如:

二进制	十进制
1111,1111	255
1110,0010	226
1101,1101	221
1100,0001	193
0111,1101	125
0101,0110	86

*标准IP地址分类——IP地址长32BIT，4个字节，分为两个部

分，前面是network，后面是host部分。对于计算机来言，它只懂得二进制语言，即所谓的“0”、“1”代码。但是，对于人的记忆来讲，不可能记住晦涩难懂的“0”、“1”代码写的IP地址。所以我们常将IP地址写成：XXX.XXX.XXX.XXX形式。举例：172.16.122.204，它的network部分是172.16；Host部分为122.204。

IP地址的分类是按照最高字节来划分的，见下表:

类别	8bits 8bits 8bits 8bits	可用地址数
A	Network Host Host Host	2＾24—2
B	Network Network Host Host	2＾16—2
C	Network Network Network Host	2＾8—2

D	Multicast	
E	Research	

A类	0000,0001-0111,1110	1-126	255.0.0.0
B类	1000,0000-1011,1111	128-191	255.255.0.0
C类	1100,0000-1101,1111	192-223	255.255.255.0
D类	1110,0000-1110,1111	224-239，用作Multicast	
E类	1111,0000-1111,1111	240-255，用作研究	
特殊用途	127.0.0.1	用作本机测试	
	10.0.0.1-10.255.255.254	用作私有地址	
	172.16.0.1-172.31.255.254		
	192.168.0.1-192.168.255.254		

* 计算机有效地址数——一旦IP地址的网络部分给定，就可以推算出在该网络中能拥有多少有效地址数。在进行计算之前，一定要知道两个原则:

1） IP地址的network部分或host部分不能全为“0”。

全为“0”特指为网络。

2） IP地址的network部分或host部分不能全为“1”。

全为“1”特指为广播地址。

依据此原则，举例说明:

1）172.16.2.2 255.255.0.0(也可写成172.16.2.2/16)

Network为172.16.0.0，Host为2.2

在该网络中有效IP地址范围为：172.16.0.1-172.16.255.254，共有2＾16－2个有效IP地址。大家可以练习8－28页的习题。

6.2.2 子网划分

通过划分子网，可以更加有效地使用网络地址，降低网络广播流量。在通常情况下，IP地址的network部分通过向host部分借用若干位，达到子网划分目的。在子网地址中，IP地址可以划分为network、subnet、host部分。

如172.16.0.0/16这样一个B类网络的network部分向host部分供借用8位，形成172.16.0.0/16这样254个子网。

Network=172.16，Subnet=0，Host=0

利用以下公式，可以计算subnet数和host数:

subnet数 = 2 ^ （ subnet位 ） - 2

Host数 = 2^(host位) - 2

可以再举N个例子。目的就是要学会计算subnet、IP地址范围、subnet的广播地址。

6.2.3 一些配置

1） router(config-if)#ip address 172.16.2.2 255.255.255.0

2） ISL configuration:

Router(config)#interface fastethernet0/0.1

```
Router(config-subif)#encapsultaion isl 1
```

详细可见8－54页。

第七章 Determining IP Routers

知识点：

1） Routing

2） Static Route

3） Dynamic Route

4） Default Route

5） Routing Protocol

6） Administrative Distance Vs Metric

7） Distance Vector 、its routing loop、loop Solution

8） Configure RIP or IGRP

7.1 什么是 Routing?

所谓Routing就是一个数据包从一个地方到另一个地方这样一个过程。在网络中，路由器就是承担route功能的网络设备。为了达到Route目的，路由器必须知道以下关键因素:

* Destination Address

* Identifying sources of information

* Discovering routes

* Selecting routes

* Maintaining routing information

路由器将路由信息存在路由表中，路由器正是依靠路由表达到路由目的的。在路由器，可以通过“show ip route”查看路由表内容，如:

```
AS116-SH#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area   N1
       - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

     Gateway of last resort is not set

O E1 17.0.0.0/8 [110/249] via 16.1.8.17, 00:00:17, Serial0/0.1
     16.0.0.0/8 is variably subnetted, 332 subnets, 15 masks
O E2 16.121.113.24/30 [110/1] via 16.1.8.17, 00:00:17, Serial0/0.1
O E2    16.80.64.0/19 [110/20] via 16.1.8.17, 00:00:17, Serial0/0.1
O E2    16.16.0.0/14 [110/20] via 16.1.8.17, 00:00:17, Serial0/0.1
O IA    16.81.64.0/19 [110/155] via 16.1.8.17, 00:00:17, Serial0/0.1
O IA    16.80.1.64/30 [110/99] via 16.1.8.17, 00:00:17, Serial0/0.1
O IA    16.17.8.8/30 [110/208] via 16.1.8.17, 00:00:17, Serial0/0.1
  O       16.9.24.0/24 [110/50] via 16.1.8.17, 00:00:17, Serial0/0.1
  O       16.1.8.24/30 [110/96] via 16.1.8.17, 00:00:17, Serial0/0.1
  O       16.10.24.0/24 [110/51] via 16.1.8.17, 00:00:17, Serial0/0.1
  O       16.98.112.0/24 [110/122] via 16.100.31.2, 00:13:56, Serial3/0
  O E2    16.18.1.0/24 [110/20] via 16.1.8.17, 00:00:17, Serial0/0.1
  O E2    16.121.113.28/30 [110/1] via 16.1.8.17, 00:00:17, Serial0/0.1
```

7.2 路由分类

路由可以分为二大类:

* 静态路由——静态路由是一个单向路由，它由网络管理员手工配置到routing table中的。网络管理员配置网络中所有路由，一旦网络发生变化，必须手工改变和添加新路由。静态路由适合小型网络和Stub 网络。（所谓Stub网络就是只有一个进出网络的节点的网络。）

Static route configuration:

Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1

参数说明，见9－7。

Ip route Command	Description
172.16.1.0	目的网络
255.255.255.0	子网掩码
172.16.2.1	对端路由器IP地址
distance	
permanent	

默认路由（default route）是的一种特殊的静态路由。在Stub网络中，由于只存在唯一一个网络出入节点，也就是说所有数据包都使用一个路由。我们可以配置默认路由，将所有出入网络的数据包都从此路由通过。

Default route configuration:(见9－9)

Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

＊动态路由——动态路由是由路由协议动态获取的，当网络发生变化时，路由协议自动更新routing table。路由协议运行于网络层，选择路径和维护routing table。一旦一条路径决定下来，路由器就能路由routed protocol所产生的数据包。

区别以下两种名词:

Routed protocol: IP、IPX

Routing protocol: RIP、IGRP、OSPF

*Administrative Distance与Metric

在网络中，有时会存在多个路由协议和多条静态路由。如何给多种路由协议排定可信度，需要一个参数，那就是Administrative Distance。AD从0到255，其值越小说明这种路由协议的可靠度越高。

具体AD值分配如下（见9－12）:

Route Source	Default Distance
Connected interface	0
Static route address	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown/Unbelievable	255

routing metric

在网络中，如果存在多条并行路由，routing protocol使用**routing metric**选择一条最佳路由。**routing metric**保存在routing

tables中。 Metrics 包括 bandwidth， communication cost，delay，hop count，load，MTU，path cost，和reliability。

Routing protocol	Metric
RIP	Hop counts
IGRP	Bandwidth、delay、load，MTU、reliability。
OSPF	

7.3 路由协议分类

在一个autonomous system中，大部分IGP routing算法可以分为以下三大类:

* Distance vector——DV依靠Vector(direction)和Distance两个参数决定路由。
* Link state
* Hybrid routing

7.3.1 Distance Vector Routing Protocol

DV路由协议最大特点是路由器*定期*向直接相邻的路由器发送*全部*路由表内容。路由器一旦收到直接相邻路由器的路由表内容，就将此内容与本身路由表内容进行比对，发现更新内容时，不论其值正确或错误，修改或添加本身路由表内容，累加Administrative Distance值。所以也称DV为“Routing by Rumor”。目前，比较典

型的DV协议有Rip和IGRP。RIP有两特点: 1. Updates every 30 seconds (RIP) or 90 seconds (IGRP); 2. Hop/Metric-based route selection

7.3.2 最佳路由选择

如9－15页所示，我们可以在图中清晰地看到每个路由器的路由表内容。当在DV中，存在多条并行路由时，RIP使用Hop count作为routing metric选择一条最佳路由，9－16图所示。对于RIP来讲，使用Hop counts作为Routing metric并不是最好的，在9－16的图中，我们可以看到T1线路带宽要优于56K线路，但是RIP认为这两条路由的metric是一样，都是经过2跳。所以在IGRP中，所引入的metric就比RIP要复杂，它由Bandwidth、Delay、Load、Reliability、MTU组成，统称为Composite Metic。

7.3.3 维护路由表

在DV中，网络发生变化所产生的routing table updates必须按部就班地从一个路由器到另一个路由器，并且DV算法是定期将路由表的全部内容发送给直接相邻的路由器。当相邻路由器收到Updates后，和本身路由表内容进行比对。 有两种情况:

1） 新路由——METRIC + 1

2） 已存在路由——如果收到的路由要优于本身已存在的路由，则刷新，否则丢掉。

7.3.4 Routing Loop 的形成与克服

见9－18到9－22。解决办法有:

* Define a Maximum Hop count

如果hop 到15 的时候算成是infinity,就不会再advertise back了让对方router 里面的内容expire。

* Split Horizon——想象以下情况:

从哪个interface 来的就不advertise back 了，但split horizon并不能解决所有的问题因为有可能有R3。subnet1 的信息虽然不能传会R1 但会传到R3 R3 还会传到R1 的。

* Route Poisoning （Poison Reverse）

一般的如果subnet1 down 了的话一般不mention subnet1 down，但route poisoning 告诉附近的router subnet1 down 了，而不用象hold-down，要90 秒以后再hold down。

* Hold-Down Timers

根据invalid period，象90 秒以后hold-down。When learning about a failed route，ignore any new information about that subnet for a time equal to the hold-down timer Three events that will reset hold-down timer:

1).Hold-down timer expires

2). The router receives a processing task proportional to the number of links in the nternetwork

3). Another update is received indicating the network status has changed

* Triggered Updates

如果R1 刚advertise subnet1 的信息到R2 subnet2，对trigged updates 来说并不用等30秒再advertise，而是立即advertise。

7.3.5 配置 RIP 和 IGRP

用下面的命令config RIP:

Router#config t

```
Router(config)#router rip
RouterA(config-router)#network 1.1.1.0
RouterA(config-router)#^Z
RouterA#sh ip route
```

用下面的命令config IGRP

```
Router#config t
RouterA(config)#no router rip
RouterA(config)#router igrp 99
RouterA(config-router)#network 1.1.1.0
RouterA(config-router)#^Z
```

注意:

1） network命令所跟的网络是直接相连的classful网络。所谓Classful network是指标准的A类、B类、C类网络。

2） 对于IGRP来讲，要加上autonomous-system号；对RIP来讲，则不需要。

第八章　Basic IP Traffic Management with Access Lists

8.1 为什么要使用 ACL？

Cisco设计ACL有以下用途：一是增加网络安全性；二是控制网络流量；三是在ISDN中，定义所谓的"interesting traffic"以激起DDR；四是用作Traffic priority and custom queuing和route filtering。通俗地讲，ACL和黑名单很相似，只不过ACL可以针对用户，也可以针对某种服务。针对用户，就意味着可以让某些用户访问或不访问网络；针对服务，就意味着可以打开或不打开某些服务。

8.2 ACL 分类

目前ACL可以分为两大类:

类别	描述
Standard	Extended
Check source address	Check source and destination address
Generally permits or denies entire protocol suite	Generally permits or denies specific protocols

也可以按照以下分类:

类别	描述
Inbound Access-list	作用在进口上，可以有效地降低路由器负载
Outbound Access-list	作用在出口上，具体操作见10－8页

8.3 配置 ACL 原则

在配置ACL时，遵循以下原则:

1） 不同的号码表示不同的作用。

2） 在一个接口上、一个协议上、一个方向上，只能使用一条ACL。如果在一个接口上使用多个ACL，那么必须是针对不同协议的。

3） ACL作用是Top-down的。类似程序设计中的IF语句，从上到下依次执行，只要满足一个条件，就不再执行其它ACL条件，终止当前ACL。

4） 在所有ACL的最后一句是默认隐含的否认一切。所以在配置ACL时，要求至少一句ACL是允许的，否则将会造成所有数据包不能通过网络。

5） ACL只能限制流经路由器的数据包，而不能限制路由器本身所产生的数据包。

8.4 正确使用 Wildcard

在IP地址划分中，使用subnetmask来确定网络范围。在ACL中使用wildcard来确定IP或其它协议的访问控制范围。只不过与

subnetmask不同的是，在wildcard中:

0——IP地址相应位需要check

1——IP地址相应位不需要check

所以我们可以用以下公式来计算wildcard，

wildcard=255.255.255.255-subnetwork

有两个特例:

Host 172.16.100.100	172.16.100.100 0.0.0.0
any	0.0.0.0 255.255.255.255

举例:

请写出与172.30.16.0/24到172.30.31.0/24相匹配的wildcard。

解：由于172.30.16.0/24到172.30.31.0/24这一段范围，可以写成172.30.16.0/20，其它对应subnetmask=255.255.240.0，所以应用公式，得出该wildcard=255.255.255.255-255.255.240.0=0.0.15.255。

8.5 配置 Access-List

在配置ACL时，有两个命令要结合使用：一个是access-list；另一个是access-group。

第一步：在全局配置模式下，使用access-list命令设置一个或多个ACL条件。

标准IP ACL:

Router(config)#access-list *XX* {permit|deny} *source_address wildcard*

其中XX为1－99。

扩展IP ACL:

Router(config)#access-list *XX* {permit|deny} *protocol source source_wildcard destination destination_wildcard operator*

其中XX为100－199。

具体解释见10－27。

第二步：在接口配置状态下，使用access-group命令激活第一步所产生的access-list 条件。

Router(config-if)#ip access-group *xx* {in|out}

其中的XX要和access-list命令中的XX要一致。

研究几个ACL例子可以更好地说明ACL的功能，见10－19到10－21；10－27到10－30。

正如在本章前面所讲到的，ACL的放置位置也会影响网络。Cisco推荐的方法为:

* Place extended access lists close to the source
* Place standard access lists close to the destination

见10－33。

在10－31页向大家介绍如何使用命名方法配置IP ACL。

8.5.1 使用 ACL 控制 VTY 访问

配置ACL控制VTY的访问，10－25。

```
Router(config)#access-list 12 permit 192.89.56.0
0.0.0.255
Router(config)#line vty 0 4
Router(config-line)#access-class 12 in
```

第九章 Establishing serial point-to-point Connections

知识点：

1） WAN

2） HDLC and its configuration

3） PPP and its PAP、CHAP

9.1 WAN（广域网）

WAN不同于LAN，最大的区别在于通信距离上。LAN一般是在短距离范围内，如几百米范围内，一栋建筑物或两个相邻的楼宇间。而WAN在距离上一般要远远大于LAN，几公里，几十公里，甚至上百公里、千公里，所造成的通信投资是非常巨大的，和LAN的投资不是一个数量级。但是随着LAN技术的发展，它们之间的差距也越来越小。

目前，WAN连接方式有三种:

＊Leased Line——租用一条专用通信线路，端到端连接起来，其它同步最高带宽为E3（45M）。由于这种连接方式的通信投资费用是很大的，在设计这种方案时，要特别注意。在Leased Line方

式中，OSI第二层可以运行HDLC、PPP、SLIP。

＊Circuit-switched——在我们日常生活中，最常被用到，如电话网，ISDN。在此种方式中，在发送方和接收方之间，必须存在一条电路才能保证双方通信。在其OSI第二层可以运行PPP、SLIP、HDLC。

＊Packet-switched——在Packet-switched系统中，网络设备共享单独一条端到端链路传输数据。通信双方使用一条虚拟电路（Virtual Circuit）进行通信。运行的服务有：X.25、Frame Relay、ATM。

9.1.1 几种常用术语

在配置WAN时，通信服务商常用一些术语，见12-5。

* Customer Premises Equipment
* Demarcation
* Local Loop(Last Mile)
* Central Office Switch
* Toll Network

9.2 几种 WAN 典型 OSI 第二层封装协议

正如在LAN中，大家都要遵守802.3之类协议一样，当数据离开

路由器进入WAN流通时，也要遵守OSI第二层协议。只不过这些服务要具体问题具体对待，不同的设备和不同的连接服务需要不同的封装协议。在实际配置WAN时，要及时地与通信服务商沟通，才能少走弯路，减少不必要的扯皮。常见的第二层WAN协议有:

* HDLC—High-Level Link Control——在点对点、专线、电路交换的WAN中，默认封装协议就是HDLC。当连接双方都是Cisco路由器时，最常使用的也是HDLC。它是ISO所定义的一种Bit-oriented synchronous data link layer protocol。

Bit-oriented: Class of data link layer communication protocols that can transmit frames regardless of frame content 。 Unlike byte-oriented protocols, bit-oriented protocols provide full-duplex operation and are more efficient and reliable。

Byte-oriented: Class of data-link communications protocols that use a specific character from the user character set to delimit frames. These protocols have largely been replaced by bit-oriented protocols.

HDLC的帧结构如下图:

Flag	Address	Control	DATA	FCS	Flag

基于ISO所定义的标准HDLC的环境中，不支持在一条线路上运

行多个OSI第三层协议。而在Cisco的设备中，支持在一条线路上同时可以运行多个OSI第三层协议，如IP、IPX、AppleTalk。这是由于Cisco自己改造ISO的HDLC，见下图:

Flag	Add	Control	*Protocol Field*	DATA	FCS	Flag

* PPP——在同步或异步通信线路上，提供端到端连接。与HDLC不同，PPP支持在一条线路上运行多个第三层协议，如IP、IPX。除此之外，PPP还具有安全措施，如PAP或CHAP。
* SLIP——同PPP，不过已经基本上被PPP所代替。
* X.25——X.25是早期在公用分组交换网络使用的典型的Packet-switched协议，它是CCITT在70年代开发的。由于当时的通信线路质量相当不好，所在在X.25的数据链路层设计了大量的克服传输错误的措施，这样一来限制传输速度，所以现在大多数X.25网络工作在64KBPS。X.25支持SVC(Switched Virtual Circult)和PVC(Permant Virtual Circuit)。

SVC（交换式虚电路）： 是在一台PC向网络发送分要求与远程PC通信时建立。一旦建立好连接，分组就可以在上面传输，通常按次序到达，如果双方通信结束，自动拆除这条SVC。

PVC（永久式虚电路）： 在用法上和SVC相同，只不过它是客户和通信服务商达成的协议建立连接，它一直存在，不随着通信双方是否使用线路而建立和拆除。

X.25在物理层的协议称作X.21，用于定义主机和网络之间物理的、电子的和程序上接口。

* Frame Relay——它是X.25的替代产品，是第二代X.25，它去除了在X.25中的针对线路质量不好所设计的错误控制措施，提供了通信速度，在FR中，错误控制由第三层处理。更详细地介绍FR，见下面章节。
* ATM——即Asynchronous Transfer Mode。它是Cell Relay的国际标准，可以提供多种服务，如Voice、Video、Data and so。由于它采用固定长度（53字节）的信元作为传输单位，它可以充分依靠硬件来处理，减少传输延迟，大大提供传输速度，可以达到E3、T3。

9.3 PPP

PPP可以定义在如下物理接口上：Asynchronours Serial、HSSI、ISDN、Synchronous Serial。PPP又可以分两个子层：(见12－12)

NCP（Network Control Protocol）封装多个网络层协议接口，如IPCP、IPXCP、and so on.

LCP（Link Control Protocol）在WAN数据链路上起到协商、建立等控制操作，如用户认证、数据压缩、错误侦察、多链路(Multiplelink)等功能。在CCNA中只讨论用户认证PAP和CHAP。

建立PPP session需要经历三个阶段: (见12-14)

1、 Link establishment phase

在此阶段，会话双方发送LCP数据包以进行配置参数，如最大接收单元、数据压缩，或测试数据链路。

2、 Authentication phase(optional)

第一阶段建立后，进入此阶段，不过此阶段是可选的。PPP支持两种authentication协议: PAP、CHAP。

3、Network-layer protocol phase

PPP的最后一个阶段，在此阶段PPP双方发送NCP数据包选择和配置一个或多个网络层协议，如IP、IPX。一旦网络层配置完毕，就进入数据传输。

9.3.1 PAP 和 CHAP

当你需要PPP authentication时，可以选择PAP和CHAP。一般情况下，优先选用CHAP。

	选用的时机不同	认证强度不同
PAP	只能在initial link establishment	Two-way Handshake、明文
CHAP	Initial link 和在link建立后的任一阶段	Three-way Handshake、加密
	见12－15到12－16。	

9.4 配置 PPP

见12－21，这是一个非常典型PPP配置。要注意的是在一个路由器上的hostname一定要和另外一个路由器上的username的要一致；口令也要一致。

第十章　Completing an ISDN BRI Call

知识点：

1）　what is ISDN?

2）　ISDB BRI

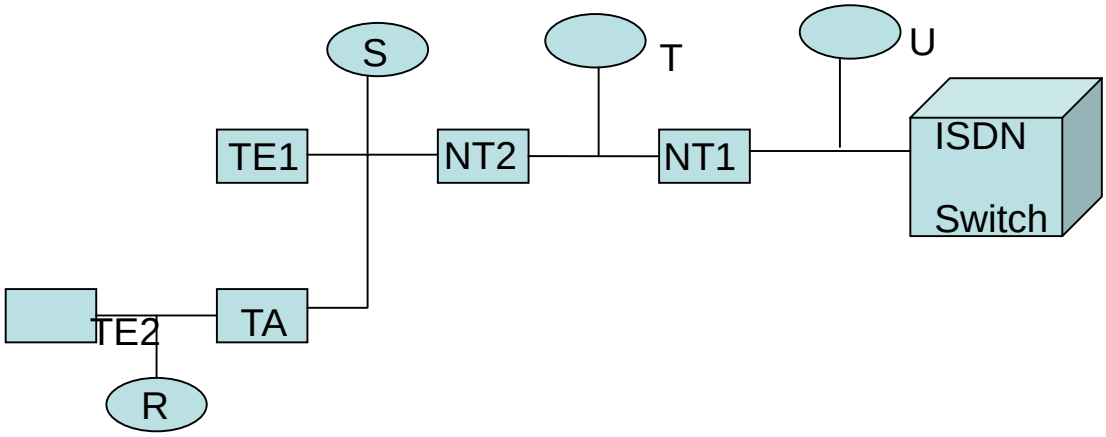
3）　ISDN functions and reference points

4）　ISDN DDR

10.1 ISDN

一个多世纪以来，主要的国际电信基础设施一直是公用的Circuti-Switched电话系统，它是为模拟话音传输而设计的，已经不能满足现代通信的需要。预计到大量的用户需求端到端的数字服务，世界各地的电话公司和电信部门于1984年在CCITT的号召下聚在一起，起草建立一个全新的完全数字化的电路交换电话系统，即ISDN，它是Integrated Services Digital Network的缩写。简而言之，就是要在普通电话线上运行话音、数据、图象等综合服务。

CCITT定义了应用于ISDN中的设备叫Function。在不同Function间的连接点叫Reference Point。见下图:



描述如下:

Function	Device type	Description
TE1	Terminal Endpoint1	ISDN兼容设备
NT2	Network Endpoint2	用户端的汇接点
NT1	Network Endpoint1	将BRI singal转换为ISDN可以识别的信号的设备
TE2	Terminal Endpoint2	非ISDN兼容设备
TA	Terminal Adapter	将非ISDN兼容设备接入ISDN的转换设备

Reference	Description
R	TA与TE2
S	TE1与NT2
T	NT2与NT1
U	NT1与ISCN Switch

10.2 ISDN 三种协议

有E、I、Q系列协议，分别定义不同内容。见13-4。

10.3 ISDN 的两种接入方法

ISDN定义两种接入方法：BRI和PRI。在CCNA中重点为BRI。

ISDN定义7种标准化信道，其中与CCNA关系最大的是B信道和D信道。B信道为64KBPS的数字PCM信道，用于话音或数字；D信道为16KBPS或64KBPS的数字信道，用于控制信令。

BRI	2B+1D=2*64K+1*16K=144KBPS
PRI	(北美和日本)23B+1D=23*64K+1*64K—T1
	(欧洲)30B+1D=30*64K+1*64K—E1

10.4 配置 ISDN

第一步、Specify the ISDN Switch type

router(config)#isdn switch-type *XXXX*

router(config-if)#isdn switch-type *XXXX*

第二步、(可选)Setting SPIDs

设置第一个B信道:

router(config-if)#isdn spid1 *spid-number*

设置第二个B信道:

router(config-if)#isdn spid2 *spid-number*

10.5 配置 DDR（按需拔号路由）

对于小规模用户来讲，只是某一时段或只当某些小业务量出现时才使用ISDN。如果全时段占用ISDN，所花费的投资是不可取的。

针对此种情况，Cisco设计的DDR功能可以节省用户费用。简单地说，DDR就是在双方路由器都是Cisco的基础上根据用户所需动态地建立通信连接。更为详细的DDR介绍，见CCNP的BCRAN课。

使用DDR有两种情况:

1） 是数据量小（small amounts of data）

2） 定期网络连接(Periodic connections)

10.5.1 配置 DDR 的步骤

配置DDR有以下五个操作。

1） 确定Route to destination

2） 定义Interesting packets

3） 配置拔号信息

4） 数据传输

5） 拆除链接

需要注意以下几点:

1) 如何定义Interesting packets，见13-19。

2) 如何配置拔号信息，见13-20、21。

3) 配置load-threshold、idle-timeout的意义。

第十一章 Establishing a Frame Relay PVC Connection

知识点：

1) Frame Relay

2) Configure Frame Relay

3) Configure Frame Relay subinterface

11.1 Frame Relay

Frame Relay 是一种高性能的流行的WAN封装协议，它作用于OSI的物理层和数据链路层。最初是针对ISDN来设计的，但是现在它已经支持多种网络接口。

Cisco Frame Relay支持以下协议: IP、DECnet、AppleTalk、 Xerox Network Service (XNS)、Novell IPX、 Connectionless Network Service (CLNS)、Transparent bridging。

普遍认为Frame Relay之所以比X.25效率更高、速度更快，是因为在X.25中所采取的纠错措施，而FR是在网络层，甚至更高层完成纠错功能。Frame Relay同X.25一样，也是通过virtual circuits实现的数据链路层的面向链接通信服务，这些VC是在packet-

switched network中的两个DTE间逻辑创建的，由DLCI号所标志。Frame Relay也使用PVC和SVC，但是大部分情况下仅仅使用PVC。

11.2 Frame Relay 术语

为了更好地理解Frame Relay术语，我们可以借用以下图示。

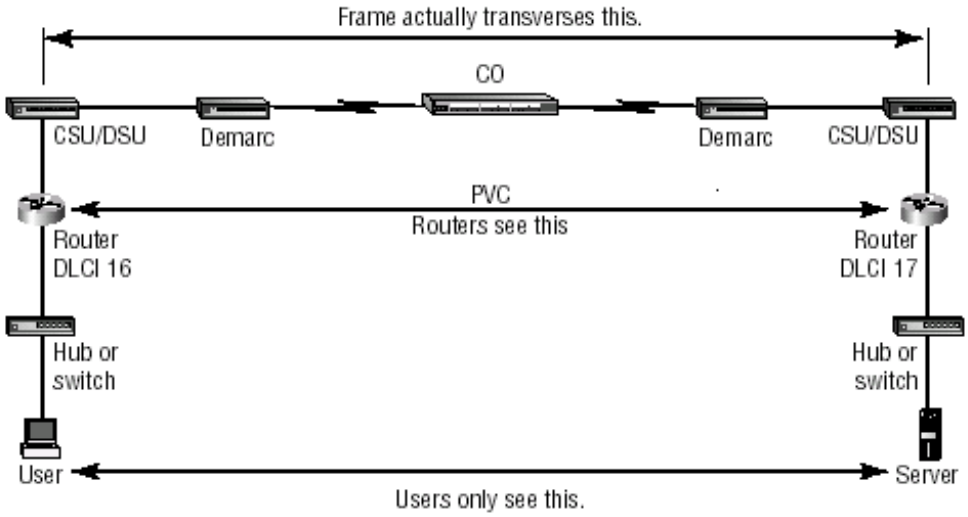


图11.1 Frame Relay technology and terms

在FR网络中最基本的想法是允许用户在两个DTE设备间通过DCE设备进行通信。对用户来讲根本不用关心FR是如何组织通信的，也不管两个通信的DTE间是如何连接的。上图表达出两个DTE是如何进行通信的。

1．在本地网络中，用户通过网关发送数据帧。

2．路由器抽取数据，并在路由表中查找到达目的网络路由。

3．查找成功后，路由器将会转发数据，否则丢掉该数据包。

4. The channel service unit/data service unit (CSU/DSU) 接收数字信号并且将其进行重新编码，以使Packet Switch Exchange (PSE)可以识别。PSE收到数字信号后，抽取其中的“1”和“0”。

5. The CSU/DSU 连接到demarcation (demarc)。Demarc is typically just an RJ-45 jack installed close to the router and CSU/DSU.

6. 一般情况下，Demarc 是一对双绞线连接到local loop。Local loop 连接到central office (CO)，有时也称作point of presence (POP)。

7. CO 收到frame后，通过Frame Relay “cloud”发送给它的目的网络。所谓的“cloud”就是若干个switching offices。switching offices可以通过IP-to-DLCI mapping查找目的IP地址和DLCI 号。

   Frame Relay mappings 可以静态地由网络管理员配置，也可以动态地Inverse ARP (IARP) protocol来创建。记住在数据通信之前，VC已经建立。

8. (1到6步骤的逆过程。) 一旦frame到达最靠近目的网络的 switching office 时，Frame通过local loop到达Demarc，然后到达CSU/DSU，最后router从frame中抽取packet， or datagram，并将packet放入新的LAN frame中送到目的主机。 在这里，我们看到user和server之间根本不需要知道，也没有必要知道Frame

通过Frame Relay network的所有过程。对用户来讲，远端server就象本地局域网资源一样使用。

结合上述内容，我们就比较容易理解Frame Relay常用术语了。常用的术语有:

1、 Local Access Rate

进入或离开FR网络时的时钟速度，也是连接FR网络的时钟速度。

2、 Virtual Circuit

在两个DTE间所建立的一条逻辑电路，并不是物理存在的电路。

3、 PVC

不管是否通信都存在的VC，称作PVC。在FR中，用show frame-relay pvc命令，查看PVC一般有以下三种状态:

Active	正常工作状态
Inactive	远端路由器可能没有正常工作
Deleted	本地路由器到FR交换机之间可能出现线路故障或本地路由器没有正常工作

4、 SVC

按需动态地建立或当传输完成后自动拆除的VC，称作SVC。

5、 DLCI

Data-Link Connection Identifier，它是Frame Relay 服务提供商分配的用来标志本地路由器和本地Frame Relay Switch间逻辑VC的号码，以区别网络中不同的VC。DLCI只具有本地

意义。Frame Relay Switch映射一对路由器间的DLCI号以创建一条PVC。见上图。

由于在一个Frame Relay接口上，可以连接多条virtual circuits，对连接在VC两端的IP设备来讲，需要将它们的IP与DLCI间建立映射。这种映射可以动态通过IARP，也可以手工通过map命令来建立。

Frame Relay 使用DLCIs和X.25 使用X.121 addresses具有同一功效。DLCI不但可以具有全局意义，也可以具有本地意义。所谓本地意义就意味着DLCI numbers不需要唯一，在不同端的两个DLCI numbers 可以一样。

配置如下:

```
RouterA(config-if)#frame-relay interface-dlci ?
        <16-1007> Define a DLCI as part of the current
        subinterface
RouterA(config-if)#frame-relay interface-dlci 16
```

6、 CIR——Committed Information Rate，Frame Relay Switch所同意的最低传输带宽，单位是b/s。对于Frame Relay来讲，在同一时刻要为多个用户提供服务，意味着将FR交换机费用分配到多个用户。FR要基于假设不是所有在同一时刻以不变的带宽传输数据这样一个原则收费。

Frame Relay非常适合突发性数据业务。不象专线用户要买服务， Frame Relay 为每一个用户提供一个专用带宽，用户可以在任何时刻调配使用这个带宽。Frame Relay provid-ers允许用户购买低于用户可能需要的带宽，这就叫Committed Information Rate (CIR)。举例来说，一个用户购买256K的带宽，但他的突发业务可达T1速度。CIR就意味着当用户以低于或等于CIR的带宽传输数据时，Frame Relay network 能够保证数据的正确转发，但是如果速率大于CIR，forward data for the PVC. However, if data rates exceed the CIR, Frame Relay network 就不能保证正确转发了。

7、Inverse ARP——利用它可以动态地映射本地DLCI号到对端网络层地址，如IP。

```
RouterA(config)#int s0.16 point-to-point
RouterA(config-if)#encap frame-relay ietf
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
```

如果采用手工静态配置映射，如下:

```
RouterA(config)#int s0
RouterA(config-if)#encap frame
RouterA(config-if)#int s0.16 point-to-point
RouterA(config-if)#no inverse-arp
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
RouterA(config-if)#frame-relay map ip 172.16.30.17 16 ietf  broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.18 17  broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.19 18
```

8、 Local Management Interface(LMI)——1990年，Cisco公司、StrataCom、Northern Telecom、和 Digital Equipment Corpora-tion联合开发了Local Management Interface (LMI)，也就是著名的the Gang-of-Four LMI 或 Cisco LMI。利用LMI可以使得互联网络设备非常容易地连接到FR中。 LMI是基于CPE device (router) 和frame switch之间的 signaling standard，它负责管理和维护这些设备的状态。LMI能提供以下信息:

Keepalives *Verify data is flowing*

Multicasting *Provides a local DLCI PVC*

Multicast addressing *Provides global significance*

Status of virtual circuits *Provides DLCI status*

默认情况下，LMI类型是”cisco”，也可以选用ANSI or Q.933A。Cisco设备可以自动适应Frame Relay Switch的LMI类型，如果没有启用自适应功能，你要询问FR提供商LMI的类型。

配置LMI如下:

RouterA(config-if)#**frame-relay lmi-type {** cisco| ansi| q933a**}**

Cisco	LMI defined by the Gang of Four (default)
ANSI	Annex D defined by ANSI standard T1.617
ITU-T (q933a)	Annex A defined by Q.933

9、 Forward Explicit Congestion Notification(FECN)与Backward Explicit Congestion Notification(BECN)

此两种参数，用于流量控制。当FR中的交换机阻塞时，它会向目的端设备发送FECN表示出现阻塞；向源端发送BECN，请求降低速率。

10、 Suninterface——在一个物理serial接口上，可以配置多个虚拟电路。每个虚拟电路就象一个单独接口一样，这就是*subinterface*s。

11.3 常用 FR 查看命令

Command	Description
Show Frame-Relay Lmi	查看本地路由器与FR交换机之间的LMI流量统计信息
Show Frame-Relay Pvc	列举所有已配置的PVC和DLCI号；提供PVC状态和流量统计；接收到的BECN和FECN的数目
Show Interface	检查LMI流量
Show Frame Map	列举所有网络层到DLCI的映射
Debug Frame Lmi	在检验FR连接问题时，帮助你决定路由器和FR交换机间是否交换正确LMI信息。

第十二章　实验部分

建立如下图实验环境：

其中：

Router A		Router B	
端口	IP/subnetMask	端口	IP/subnetMask
S0	192.168.1.1/30	S0	192.168.1.2/30
E0	192.168.2.5/24	E0	192.168.3.5/24
PC1		PC2	
IP/subnetMask	192.168.2.22/24	IP/SubnetMask	192.168.3.33/24

目的：

一、 Router A 与 Router B 的串口间用背对背连接；在两个局域网中分别设有一台 PC，为 PC1 和 PC2。

二、 要求正确配置 IP 地址与子网划分。

三、 要求 PC1(PC2)能 ping 到 PC2(PC1)。

四、 要求正确配置路由协议。

1、 配置动态路由。以 A 的 RIP 配置为例（IGRP 要注意使用 *autonomous system* 号）:

```
Router rip
Network 192.168.1.0
Network 192.168.2.0
```

2、配置静态路由。要求体会静态路由的单向性。

五、 要求配置

（1）Standard ACL 能阻止 PC1 防问 PC2 所在的网络。

在 B 上:

```
(config)#Access-list 10 deny host 192.168.2.22
(config)#Access-list 10 permit any
…
(config-if)#ip access-group 10 in
```

（2）Extended ACL 能阻止 PC1 ping PC2，阻止 PC1 telnet Router B 的 S0。在 B 上:

```
(config)#access-list 110 deny icmp host 192.168.2.22 any
(config)#access-list 110 deyn tcp host 192.168.2.22
```

```
any eq telnet(23)
(config)#access-list 110 permit ip any any
…
(config-if)#ip access-group 110 in
```

需要注意的问题:

1） 背对背情况下，在配置连接 DCE 电缆端的路由器的串口时，设置 DCE 命令，*clock rate 64000*。此命令有两条作用：一是手动设置 DCE 端；二是设置通信速率为 *64KBPS*。

2） ACL 配置过程中，要特别注意写上一条允许所有命令。另外在封锁 PC1 的 PING 后，PC2 也不能 PING 到 PC1 是因为 PC1 的 response 包被封锁。

3） 在端口配置过程中，不要忘记 *no shut* 命令。

4） 在任何一端的 S 口下使用 *no shut* 命令，会看到另一端状态由 *down* 到 *up*。