

# CCNA 学习总结-原理篇

## 第一部分：OSI 参考模型

**OSI 参考模型：**Open System Interconnection，是一个开放式的七层模型，上三层称之为高层，下四层称之为低层。它只是一个参考模型，用来将互联网络进行层次划分，方便各厂商根据各层标准制定设备。

**Application Layer：**应用层，OSI 模型中的第七层，主要负责确定通信伙伴，为特性的应用程序提供功能。典型的 TCP/IP 应用包括：文件传输协议 FTP、简单文件传输协议 TFTP、简单邮件传输协议 SMTP、超文本传输协议 HTTP、自举协议 BOOTP、动态主机配置协议 DHCP。

**Presencation Layer：**表示层，OSI 模型中第六层，主要负责完成各种不同的数据、视频、语音、图像的格式与传输格式之间的相互转换来提供通信服务。该层的标准有文本——ACS、图像——TIFF、JPEG、GIF、PICT、声音——MIDI 等。

**Session Layer：**会话层，OSI 模型中第五层，主要负责在应用程序之间建立、管理和终止设备或主机之间的会话。该层的协议有：网络文件系统 NFS、结构化查询语言 SQL、远程过程调用 RPC、X Windows 系统、Apptalk 会话协议 ASP、DNA 会话控制协议 SCP。

**Transport Layer：**传输层，OSI 模型中第四层，数据格式为段，主要负责端到端的可靠与不可靠的数据传输，包括流量控制和错误恢复。TCP 提供可靠地数据传输，UDP 提供不可靠地数据传输，像 TFTP、SNMP、NFS、DNS、RIP 都是用 UDP 协议提供不可靠传输。

**Network Layer：**网络层，OSI 模型中第三层，数据格式为分组(包)，主要负责两个端系统之间提供连通性和路径选择，两端系统可能处于不同网络上。网络层协议包括：Internet 协议 IP、Novell 的互联网分组交换 IPX、地址解析协议 ARP、反向地址解析协议 RARP、Internet 控制消息协议 ICMP。

**Data-link Layer：**数据链路层，OSI 模型中第二层，数据格式为帧，主要负责在物理线路上提供可靠地数据传输，它主要关心物理寻址、网络拓扑结构、线路规范、错误通知、有序帧传输和流量控制。数据链路层协议包括：以太网、IEEE 802.3、令牌环、IEEE 802.5、HDLC、PPP。

**Physical Layer：**物理层，OSI 模型中的最底层，数据格式为比特，通过在终端之间激活、保持、释放物理链路，该层定义了电气、机械、程序和功能规范。该层标准包括：10BaseT、V.35、RS-232。

## 第二部分：桥接和交换

传统的集线器共享一个冲突域，使用带有冲突检测的载波监听多路访问机制，但仍然造成带低带宽、高冲突的网络环境。为了减少网络拥堵的一个方法就是尽可能的使用交换机来替代集线器。交换机每个物理端口都是一个冲突域，但他们所有端口处于一个广播域，交换机每个端口独享专有带宽，进而大大增加了其转发速度。

### 全双工/半双工

全双工：在同一时刻既可以发送也可以接收数据，全双工方式使六安路吞吐量增加一倍，在一条全双工的连接上不会发生冲突，因为冲突与内只有两台设备。

半双工：在同一时刻要么发送、要么接收数据，一旦出现即发送又接收，就会产生冲突。连接到集线器的主机必须采用半双工的工作方式，因为他们必须能够检测何时发生了冲突。

### 两种主要的交换方式：贯穿式，储存转发式

储存转发式交换在交换机内讲一个以太网帧从另外一个端口发送出去之前复制全部的帧到缓冲区，把真校验序列 FCS 与自己的计算结果进行比对，如果匹配再转发出去，否则丢弃。

贯穿式分为快速转发方式和无碎片转发方式，快速转发方式在读取到帧的目的地址后就查找 MAC 表，立即从适当的端口转发出去。无碎片转发方式比快速转发慢，比储存转发快，它在接收帧的 64 字节口再开始转发，因为冲突帧应该在帧的前 64 字节，它在转发前去掉了这部分冲突。思科交换机默认的转发方式就是无碎片式。

### Vlan

Vlan 可以分离广播域，可以把一个 vlan 视作一个子网，vlan 技术的引入，抑制的广播风暴的产生，它将若干子网在逻辑上隔离开，避开不必要的 ARP 请求，以减少网络带宽和主机处理周期，总之 vlan 技术的应用，使我们组网更加灵活、安全。

### Vlan 干道协议：ISL、802.1Q

ISL：思科专有的交换机间链路协议，ISL 将一个新的 ISL 头标封装在数据帧的头部

802.1Q：IEEE 的标准方法，它在以太网帧中插入标签

### Vlan 中继协议：VTP

Vtp 的产生主要为了解决在 vlan 交换式网络运行中的潜在问题，减少 vlan 配置工作量。

VTP 三种模式：server、client、transparent。VTP 分为两个版本，版本 2 支持令牌环。

服务器模式：发送、转发 VTP 通告，与其他交换机同步 vlan 信息，可以增加、删除、修改 vlan 信息，vlan 配置保存在 NVRAM。

客户模式：发送、转发 VTP 通告，与其他交换机同步 vlan 信息，不能创建、修改、删除 vlan 信息，配置不保存到 NVRAM。

透明模式：只转发 VTP 通告，不与其他交换机同步 vlan 信息，可以创建、删除、修改 vlan 信息，vlan 配置保存到 NVRAM。

STP：为了实现交换网络的冗余设计，防止环路的产生，STP 协议由此运作开来。通过在逻辑上阻塞某些端口，构建一个无环路网络。

STP 的运行需要选举一个根桥，根桥上所有端口为指定端口，非根桥会选举一个根端口，该端口是到达根桥的最低成本路径。STP 根桥的选举考虑 BID：优先级和网桥的 MAC 地址，有着最低 BID 的网桥会被选举成为根桥。

STP 的端口状态：LSN、LRN、FWD、BLK、Disabled。非根桥根端口的选举根据路径成本来判定，具有成本最低的端口将被选举为根端口。

RSTP：快速生成树协议

RSTP 的端口类型和 STP 不同，分为：根端口、指定端口、替换端口、备份端口、禁止端口。

### 第三部分：被路由协议 IP

常用 IP 地址分为三大类：A、B、C。其中 A 类地址有 126 个网络数，每个网络能容纳 16777216 个主机，B 类地址有 16384 个网络，每个网络能容纳 65535 个主机，C 类地址有 2097152 个网络，每个网络能容纳 254 个主机。

私有地址

|                                |     |
|--------------------------------|-----|
| A: 10.0.0.0-10.255.255.255     | /8  |
| B: 172.16.0.0-172.16.255.255   | /16 |
| C: 192.168.0.0-192.168.255.255 | /24 |

子网划分

为了创建子网结构，必须通过从主机位进行借出比特，将主机比特位重新分配成网络比特位。解决某个数学问题的方法通常不止一种，划分子网的方法也不例外，本篇介绍一种方法仅供参考。



首先我们要确定你所设置的新的子网掩码将产生多少个子网？应该是 2 的 X 次方-2，其中 X 表示掩码的二进制位数，切记，是掩码的二进制的位数！-2 是去掉全 0 和全 1。

其次，我们要知道每个子网有多少个主机？应该是 2 的 X 次方-2，其中 X 代表主机的 2 进制位数，-2 是去掉全 0 全 1。

然后确定有效子网间隔是什么？256-新的 10 进制子网掩码、每个子网的广播地址，下一个子网号-1、每个子网的有效主机地址，子网号+1 到下一个子网号-2

综合一个例子，假如需要将 192.168.1.0/24 原 C 类网络划分成 30 个子网

首先确定向主机位借出多少比特位才够 30 个子网，发现 2 的 5 次方-2=30，那么就确定了需要向主机位借出 5 个比特位，新的子网掩码就是 255.255.255.248，每个子网的主机数 2 的 3(8-5)次方-2=6，有效子网间隔 256-248=8 那么 192.168.1.8 就是有效地子网间隔。

十进制、十六进制和二进制之间的转换

表 1：2 字节/16 比特数

|          |          |          |          |          |       |       |
|----------|----------|----------|----------|----------|-------|-------|
| $2^{15}$ | $2^{14}$ | $2^{13}$ | $2^{12}$ | $2^{11}$ | ..... | $2^0$ |
| 32678    | 16384    | 8192     | 4096     | 2048     | ..... | 1     |

如上所述,最常见的比特分组时 8bit，构成 1 个字节。但是有些时候，一个字节能容纳的最大值 255 不够用，这时，必须结合多个字节，可以用一个 16bit、24bit 而不是 3 个 8bit 数，比如将一个十进制数 6783 转换成二进制，由于采用一个 8 位组不够用，那么我们就采用一个 16 位组，根据表格可以得出 6783=0001101001111111。二进制转换十进制正好相反，将二进制数放入表中对应的位相加得出 10 进制数。

## ICMP

因特网消息控制协议，是 TCP/IP 的一个组件，解决了 IP 在发送数据中发生故障不进行通知的局限性，ICMP 不提供错误纠正，它唯一能错的只是向工作站报告错误。

## 第四部分：路由选择协议

协议就是基于多个标准的一组规则，它确定计算机如何穿越网络进行通信。协议描述了以下内容：

消息必须使用的格式

在某个特定活动中，计算机交换消息所必须使用的方式，比如穿越网络发送消息。

**被路由协议：**任何在网络层地址中提供足够信息，是分组能根据寻址方案，从一台 PC 转发到另一台 PC 的网络协议。被路由协议就是被路由选择协议路由的协议，它是被动的，它定义了分组中字段的格式，它使用路由选择表来转发分组，被路由协议包括：IP、IPX、AppleTalk、Digital DECnet。

**路由选择协议：**通过提供共享路由选择表信息的机制来支持被路由协议，路由协议的消息在路由器之间传送。TCP/IP 路由选择协议包括：RIP、OSPF、IGRP、EIGRP。路由器的两项关键功能：维护路由选择表并确保其他路由器知道网络拓扑的变化、当分组到达一个接口时，路由器必须是个路由选择表来确定向哪里发送分组。

路由选择协议度量值用于确定路由优良的值，使用各种标准组合来确定路由选择度量值，有跳数、带宽、延迟、可靠性、负载、成本。

**RIP：**距离矢量路由选择协议，IGP，用跳数来衡量度量值，周期性的每 30 秒发送器全部路由表给相邻的邻居路由器，即使网络中没有更新变化发生也会周期性的发送更新，因此收敛速度比较慢。RIP 有两个版本 RIPv2 在 RIPv1 版本基础上进一步支持了 CIDR、VLSM、支持 MD5、明文身份验证、使用组播地址传送路由选择更新。RIP 使用水平分割、抑制定时器、触发更新方式来防止路由选择环路，16 跳作为无穷大的能量值，认为不可达

**IGRP：**距离矢量路由选择协议，IGP，思科私有路由选择协议，默认用带宽和延迟来计算度量值，比 RIP 支持更多的跳数，故此支持更大的网络环境；**EIGRP：**IGRP 的增强版本，采用 DUAL 算法，收敛速度极快，通过发送增量的更新，对带宽提供高效的利用，支持 CIDR、VLSM，还能通过 PDM 模块，对多种网络层进行支持，如 IP、IPX、AppleTalk。EIGRP 也使用最大跳数，其值为 224，IGRP 为 255，而 RIP 是 15。EIGRP 在 IGRP 和 EIGRP 之间共享或重新分配的信息时自动的，只要两者使用相同的自治系统号。EIGRP 中邻居表是其最重要的表，每台 EIGRP 路由器维护一个列出毗邻路由器的邻居表，与 OSPF 的邻居表类似。拓扑表由自治系统中所有的 EIGRP 路由选择表构成，拓扑表包括：可行距离 FD=到每一个目的地的最低计算度量值、报告距离 RD=毗邻的邻居报告的到一个指定目的地的距离、接口信息、路由来源和路由状态。路由状态可标识为 P=被动的、A=活跃的。

**后继：**指被选中作为到达一个目的地所使用的主要路由的路由

**可行后继 FS：**是一条备份路由

EIGRP 主动的建议邻居关系，使用更小的 hello 分组，缺省每 5s 发送一次，与邻居建立毗邻关系

**OSPF：**

一种链路状态路由选择协议，通过发送 hello 分组来建议邻居关系，更适合大规模的网络。OSPF 支持广播型多路访问、非广播型多路访问 NBMA、点到点网络。OSPF 路由器进入 two-way 后，根据网络类型决定选举或不选举 DR、BDR OSPF 通过 5 种不同种类的分组来识别它们邻居并更新链路状态信息：



天津 thinkmo 新盟教育

**Hello:** 与邻居建立和维护毗邻关系的分组

**数据描述分组 DBD:** 描述一个 OSPF 链路状态数据库的内容

**链路状态请求分组 LSR:** 请求相邻路由器发送其链路状态数据库中的特定项

**链路状态更新 LSU:** 向邻居路由器发送链路状态通告

**链路状态确认 LSACK:** 确认收到了邻居的 LSA

OSPF 的接口可能处于下列 7 种状态之一:

**DOWN:** 物理 down, OSPF 进程还没有与任何邻居交换信息

**Int:** 初始状态, 以固定的时间间隔发送 hello 分组, 与邻居建议关系。

**Two-Way:** 双向状态, 每台 OSPF 路由器都试图与统一 IP 网络中的所有邻居建立 two-way 状态。

**ExStart:** 准启动

**Exchange:** 交换, 在此状态下, 邻居路由器使用 DBD 分组来相互发送他们的链路状态信息

**Loading:** 加载, 在相互描述过自己的链路状态数据库后, 路由器使用 LSR 请求更完整的信息

**Full Adjacency:** 全毗邻, 加载结束后, 路由器变成全毗邻状态, 每台路由器都保存一张毗邻路由器列表=毗邻数据库

。

**IS-IS 中间系统到中间系统**

该协议是 OSI 协议栈中的动态链路状态路由协议, 因此它负责在 ISO 无连接网络服务 CLNS 环境下, 为无连接网络协议 CLNP 的数据分发路由选择信息。集成式 IS-IS 也是 IS-IS 的一种实现方式, 能完成对多种网络协议的路由选择。集成式 IS-IS 为 CLNP 路由标记上关于 IP 网络和子网的信息。

**BGP 边界网关协议**

是外部网关协议 EGP 的一个例子, BGP 在自主系统之间交换路由选择信息, 同时保证无环路的路由选择, 该协议是因特网上大公司和运营商使用的首要路由协议, BGP 基于网络策略来作为度量值标准, 使用不同的 BGP 路径属性来法定路径选择。

**比较距离矢量、链路状态、混合路由选择协议**

链路状态路由选择协议设计用于克服距离矢量协议的局限性, 链路状态路由选择协议对网络变化能做出迅速反应, 只在有变化时才触发更新, 并以很长的时间间隔, 发送周期性更新。



## 第五部分：广域网协议

广域网协议与服务主要包括：PPP、HDLC、Frame-relay、ISDN/LAPD、LAPB、ISDN DDR。

**HDLC：**HDLC 分为标准的和思科专有的，思科设备默认的封装是 HDLC。HDLC 成帧方式设计用于在不可靠的线路上提供可靠的传输，包括了用于流量和差错控制的信令机制，帧总是以一个 8 比特的标识字段开始和结束，该字段比特模式为 01111110。由 HDLC 派生的协议有 X.25 使用的平衡时链路接入过程 LAPB、ISDN 使用的 D 信道链路接入过程 LAPD 等。

**PPP：**PPP 使用分层体系结构，使用了 OSI 模型中的 3 层，物理层定义了用来实际的点到点连接，数据链路层的链路控制协议 LCP 用来建立和配置连接，网络层的网络控制协议 NCP 用来配置不同的网络协议。PPP 支持身份验证，提供两种验证方式：PAP、CHAP，PAP 为密码验证，CHAP 为咨询握手验证协议，使用 3 次握手机制，CHAP 使用 MD5 产生哈希函数来加密密码，安全性更高。

**ISDN：**综合业务数字网

目前使用 ISDN 的用户主要用于广域网备份、向远程办公者和小型企业办公室提供远程接入，它不像 DSL 技术那样将数字信号转换成模拟再进行传输，它直接传输数字信号。

ISDN 的两种接口：BRI、PRI

**BRI：**2B+D 2 个 64kbit/s 的 B 信道和一个 16kbit/s 的 D 信道

**PRI：**北美 23B+D、欧洲、澳大利亚和世界上其他地区 30B+D，前者等同于 T1，后者等同于 E1。

ISDN 也有一个三层模型，物理层定义了接口规范，数据链路层的 LAPD 协议定义 D 信道的控制信息和信令能够正确发送和接收。网络层使用 Q.931 来定义 B 信道的传输。ISDN 还定义了不同功能的参考点，比如非 ISDN 终端设备 TE2、ISDN 终端设备 TE1、TE1 与客户端交换设备 NT2、本地环路终结器 NT1。

其中参考点定义了设备连接间的接口标准：

**R：**非 ISDN 设备与终端适配器 TA 的连接点

**S：**连接到用户交换设备 NT2 上的参考点

**T：**其电子特征和 S 接口相同

**U：**连接到 ISDN 中心网络交换机的参考点

Frame-relay



天津 thinkmo 新盟教育

帧中继技术由 X.25 网络演变而来，由于其在光线介质上传输，去除了差错、流量控制，比 X.25 提供更高的速率。帧中继是一个公共网络，在一条线路上进行传输的不止自己公司的数据，是一种廉价的解决方案。

帧中继的术语包括：

**DLCI：**数据链路标识符，它是源和目的设备之间的表示逻辑电路的一个数值，一般由 ISP 分配。

**LMI：**本地管理接口，它是用户端设备 CPE 和帧中继交换机之间的信令标准，负责管理设备间的连接、维护设备间的连接状态。

**CIR：**承诺信息速率，服务提供商提承诺提供的最大数据量

**PVC：**由运营商配置的永久式虚电路

**SVC：**在有数据发送时才产生的交换式虚电路，在没有数据时会自动断开

## 第六部分 扩展 IP 地址

NAT

网络地址转换，缓解因特网 IP 地址不足，保护内网数据安全。NAT 分为静态、动态和 PAT(端口复用)。静态为内网地址与外网地址一对一转换，动态需要分配地址池，端口复用使用一个 IP 地址，不同的端口号，将内网 IP 转换成公网 IP。

BOOTP、DHCP

BOOTP、DHCP 都是自动为客户端 PC 分配 IP 地址，但 BOOTP 与 DHCP 最大的不同是，BOOTP 不是动态的，他通过事先定义条目，而 DHCP 提供动态分配机制，该机制循序客户端分配一个具有有限租期的 IP 地址。

## 第七部分 ACL

ACL

访问控制列表，它提供以一种安全机制，通过定义一连串的规则来允许或禁止某些符合这规则的特性通过路由器。分为标准、扩展、命名 ACL。

标准 ACL 根据源地址进行控制，扩展 ACL 根据源地址、目的地址、源 TCP/UDP 端口号、





目的端口号、协议进行控制。命名 ACL 提供了以个便捷之处，它允许在 ACL 条目创建后删除某条语句，如果基于代码的 ACL 将删除基于该代码的所有语句。一般情况下，定义标准 ACL 都是应用在离源出口最近，扩展 ACL 离目标最近。

## 第八部分 Cisco 设备、IOS 和网络基础

当我们第一次对路由器或交换机等设备进行配置之前，通常都会对该设备现有的 IOS 进行备份，那么将会用到 cisco 的 TFTP 软件，也可以将运行中的配置拷贝到 TFTP 服务器，在使用超级终端时，可以对配置文件进行管理，通过依次点击超级终端界面的传送、捕获文字、指定捕获文件的文本名称、点击开始，然后在设备中输入 `sh run`，最后在界面中点击停止就可以对配置文件进行拷贝到文本中，在文本中去掉不必要的文字，以备日后将配置文件拷贝到设备中。

思科路由器、交换机具备丰富的命令行帮助特性，详细可以参考其他文档。

`shw version` 命令可以查看设备的：

1. IOS 版本信息
2. 自举 ROM 版本
3. 启动 ROM 版本
4. 设备正常运行时间
5. 上次重新启动的方式
6. 系统映像文件和位置
7. 设备的平台
8. 配置寄存器的值

以上全部内容均为 CCNA 内容中一些知识点的总结，虽然本着尽量把 CCNA 中所有知识点概括出来的态度去做，但也避免不了出现一些纰漏，欢迎大家提出问题。