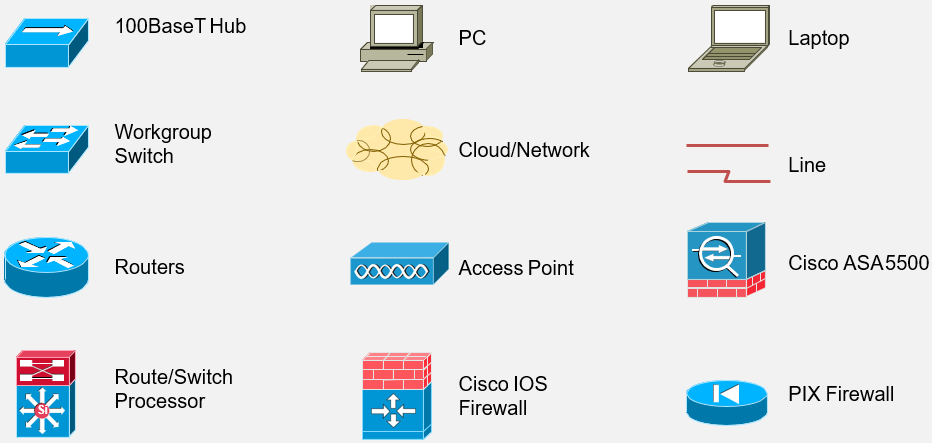
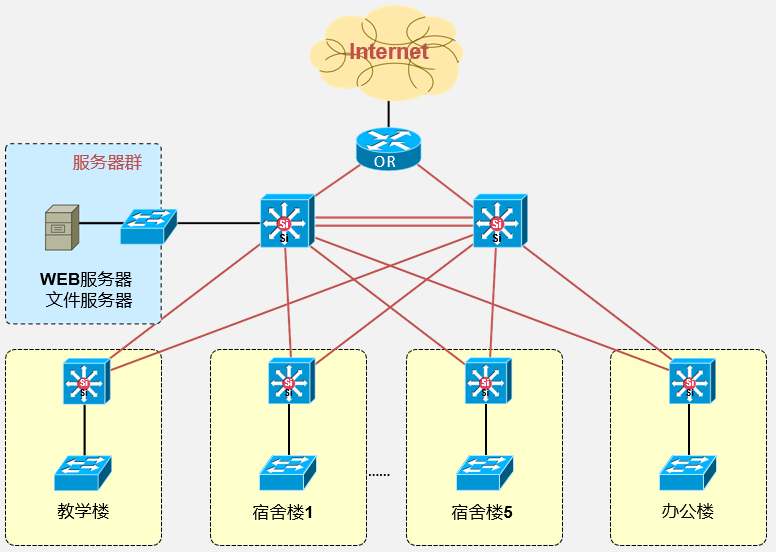
# 1.0计算机网络概述

## 1.1设备图标



## 1.2拓扑

网络设备之间的互联，用来更加直观的表示各个网络设备之间的互联关系



## 1.3网络

1. **网络的概念：**

目前所指的网络即计算机网络，是由各种网络设备组成的IP数据传输网

1. **最简单的网络**

当两台主机通过网线进行连接，这就构成了一个最简单的网络。一个小型的局域网，该局域网中只有两台设备。

1. **HUB**

由于网线直连的两台设备可扩展性极低，如果要实现多主机互联，可能需要许多网线接口和互联网线。

由此便出现了HUB，可以将许多用户通过HUB连接在一起，构成一个局域网。

HUB是一层设备，他只简单的将比特流进行传输操作。

HUB提高了网络的可扩展性，但HUB存在数据传输冲突的问题。当局域网中同时有两个设备在同时发送信息，则会导致数据流的碰撞，从而使数据产生损毁，导致数据交换失败。

1. **交换机**

由于HUB可能会导致数据冲突问题，为了应对这一问题则产生了交换机。

交换机是二层设备，他主要起到以下作用：

1. 终端用户的接入
2. 隔离广播域
3. 起到最基本的一个安全功能
4. 二层链路的冗余、防环及负载均衡

同一网段的主机处于同一个广播域内，而二层交换机只能完成同一广播域内的数据通信，即使用交换机只能构成一个小规模的局域网，无法实现大规模设备数据通信

1. **路由器**

路由器工作在三层环境，他解决了二层交换机无法实现不同网段之间通信的问题。

路由器功能：

1. 路由协议的支持
2. 数据的转发、路径选择
3. 广播域的隔离、实现跨三层数据交互
4. 广域网接入、地址转换及基本的网络安全功能

路由器在购买之初，是不携带扩展办卡的，相应的扩展板卡插槽会被挡板覆盖。初始购买的路由器只存在最基本的数据传输接口，可以实现基本的数据传输功能。若要实现更多的接入和传输功能，则需要购买相应的板卡对设备接口进行扩充。

1. **园区网**

Cisco企业网络三层架构：

核心层：为汇聚层汇聚的数据提供有效、快速、合理的传输路径选择，同时对外网数据进行过滤，保障内网的数据安全。

汇聚层：汇聚接入层用户数据、提供服务器群的接入、实现设备冗余功能

接入层：提供更多的接口供用户接入网络

1. **区域网络互联（银行、高速收费等跨区域互联的连锁机构网络）**

一级行（省级）：接入企业数据中心，承担大量的数据查询访问工作，需要更高的网络负载能力（路由条目也相应的增加，这就需要采用合理的路由协议）

二级行（市级）：需要承担基础站点的网络数据传输，这便需要提高网络的负载能力

基础站点：对站点部门内的网络设备进行接入

1. **广域网、城域网、局域网**

局域网一般是私有网络，规模较小

园区网较局域网规模大，是对多个局域网进行互联之后的网络，多为私有网络

城域网园区网的互联，课理解为一个城市的网络，多由运营商来承担部署和维护

广域网是跨区域的网络链接，市级、省级一级州级、国家之间的网络互联

1. **网络工程**

对网络进行规划，部署并调试、维护网络设备，提供高性价比的网络搭建服务

## 1.3Question

1. 什么是网络？

# 2.0网络参考模型

## 2.1 OSI七层模型

* 1. 概念：

是由ISO国际标准化组织定义的，一个灵活、稳健、可操作性的网络模型。是用来帮助了解、设计网络体系结构的模型。

* 1. 目的：

为了规范不同系统之间的互联，使两个不同的系统能够更加容易的链接并进行通信，而不需要改变其底层的原理或软件结构。

* 1. 应用层

在七层中，应用层的规模最大，所产生的的协议也最多。

应用层的作用主要可以从三个视角来解释

用户：对于使用可入网终端设备的用户而言，应用层为用户提供了网络接入的支持。用户通过操作可入网应用程序，生成应用程序可识别的特定类型数据并交给下层经由网络进行传输。

开发人员：对于开发人员而言，应用层便是提供了网络接入的各种API接口，使得可以基于网络接口进行应用程序开发。

应用程序：应用层极大的一部分作用是规范应用程序之间交互数据时的数据格式，举例来讲就是如果使用QQ的两个用户之间要进行数据交互，则所传输的由QQ软件产生的数据就必须存在固定的数据格式。若数据格式不进行规范，在另一端接收到数据之后，由于格式不匹配，便会导致数据的读写产生错乱，从而造成数据传输失败。

协议：POP、FTP、HTTP、Telnet、SSH等

* 1. 表示层

表示层的主要功能是对应用层产生的仅能由应用程序识别的特定类型数据进行压缩、加密、格式化以及他们的逆化操作。

* 1. 会话层

建立虚连接并用来管理、区分和终止响应的网络服务进程。例如本地计算机任务管理器中，通过PID对本地网络服务进程进行区分、管理

* 1. 传输层

提供端到端的报文传输和差错控制。传输层主要定义了数据传输的可靠性，他在两个通信节点之间建立连接通道，并将上层得到的数据进行分片操作再交由下层来进行传输。

协议：TCP、UDP

* 1. 网络层

将上层来的数据从源端传送到目的端。在传输过程中提供逻辑编址和逻辑寻址功能，对数据传输过程中，通过哪些节点提供选择，即寻址方案。网络层会将上层分段后的数据进行打包处理并交由下层传输处理。

协议：IPV4、IPV6、IPX

* 1. 数据链路层

将上层打包的数据封装成帧，并提供节点到节点之间的传输。为节点到节点之间的传输方式提供标准。

数据链路层有两个子层：LLC子层和MAC子层

LLC子层负责提供网络层协议的识别、提供流控、比特流排序等工作

MAC子层提供物理寻址、逻辑拓扑、定义数据在介质上传输方式、线路控制等工作

协议：PPP、ATM、FR、HDLC、Ethernet2、802.3、令牌环

* 1. 物理层

将上层数据帧格式化为比特流并在物理介质上传输。定义了物理设备的工艺约定和规范，定义了传输媒介采用何种物理物理介质，并定义媒介的机械特性、光学特性等。

## 2.2 OSI在数据传输过程中的具体应用

假设两个PC编号为A、B需要进行通信，

数据的封装

1. 应用层：PC A建立网络虚连接并提供给用户通过操作终端与网络应用程序进行信息交互时使用，应用程序根据应用层协议产生相应格式的数据。
2. 表示层：PC A对数据进行格式化，格式化为统一的二进制文件，根据需求进行压缩和加密操作
3. 会话层：PC A通过管理虚连接来对网络服务进行控制，若用户关闭应用程序，便会将相应的虚连接进行关闭
4. 传输层：PC A 定义数据传输过程中的可靠性，若选择可靠传输，则与PC B之间建立端到端的实链接通道，将数据分片后加以TCP头部信息再经由通道进行传输
5. 网络层：PC A将分片后的数据再进行打包，并加以IP头部信息
6. LLC子层：PC A将打包后的数据再封装成帧，并加以LLC头部和三层协议识别尾部
7. MAC子层：PC A在LLC子层添加包头信息的基础上还要在添加MAC头部
8. 物理层：PC A将封装好的数据格式化为比特流，经由物理链路发出

数据的解封装

1. 物理层：在数据到达PC B之后，将比特流数据进行串行化，得到完整数据帧信息
2. MAC子层：解析数据帧的MAC头部，若与自己的MAC匹配则继续解析，若不匹配则丢弃（若为交换机会对数据包进行泛洪处理）
3. LLC子层：解析LLC头部和FCS帧校验序列，判断数据帧是否损坏、修改并识别三层协议。若帧校验不通过，则丢弃数据包
4. 网络层：解析数据包IP头部，并查看IP信息与自己的IP信息是否匹配，若匹配则继续解析，若不匹配则丢弃数据包（若为路由器则会查看本地路由表中是否有到达目的网段的路由条目，有则继续查表转发，无则查看缺省，无缺省则丢弃）
5. 传输层：解析TCP/UDP头部，如果是TCP头部，则核验TCP端口号与本地相应服务是否一致，若一致则继续解封装，若不一致则丢弃数据包。将系列接收到的数据段按照偏移值进行重组，得到完整的数据
6. 会话层：查看网络进程是否销毁，并交由相应的进程进行下一步的处理。
7. 表示层：将数据按照编码方式进行解码，按照需求进行解密、解压缩操作
8. 应用层：应用程序将数据提取后经过处理显示在输出设备中。一次网络数据传输完成。

## 2.3 TCP/IP

应用层：对应于OSI的应用层、表示层和会话层

主机到主机层：对应OSI传输层

Internet层：对应OSI网络层

网络接入层：对应OSI数据链路层和物理层

## 2.4 OSI与TCP/IP的区别

1. OSI用于理论研究，TCP/IP用于实际环境
2. OSI不支持跨层分装，TCP/IP支持跨层封装
3. OSI支持各种网络层协议，TCP/IP仅支持IP协议栈（IPV4和IPV6）

## 2.5 Question

1. 什么是IP，IP的作用？
2. 什么是广播域、冲突域？
3. 什么是广播、组播、单播？
4. 什么是格式化？

# 3.0协议

## 3.1 TCP

### 3.1.1 协议详情

传输层协议

传输控制协议，是一种面向连接的可靠传输协议

* 1. 面向连接：

面向连接由三次握手来实现。

* 1. 三次握手：

SYN

SYN+ACK

ACK

隐式确认机制

* 1. 端口号：

（1）作用

* 对本地不同的网络服务进程进行区别
* 将本地和对端的端口号进行绑定，建立一条数据传输通道

（2）端口号范围：1-65535

（3）静态端口号：1-1023（端口号和流量之间一一对应且绑定）

（4）动态端口号：1024-65535（端口号和流量之间一一对应不绑定）

例如：telnet（TCP服务）23 SSH（TCP服务）22

HTTP（TCP服务）80 RIP（UDP服务）520

HTTPS（TCP服务）443 DNS 53

FTP（TCP服务）21 TFTP（UDP服务）69

* 1. 序列号和确认号
  2. 可靠传输：

确认、重传、流控（滑动窗口机制）、排序

### 3.1.2 协议封装

|  |  |  |  |
| --- | --- | --- | --- |
| Source port (16) | | | Destination port (16) |
| Sequence number (32) | | | |
| Acknowledgement number (32) | | | |
| Header length (4) | Reserved (6) | Control bits (6) | Window (16) |
| Checksum (16) | | | Urgent (16) |
| Options (0 or 32 if any) | | | |
| Data (varies) | | | |

### 3.1.3 Question

1. 如何保证面向连接？
2. 什么是三次握手？
3. 什么是端口号，端口号的范围及分类？
4. TCP如何保证可靠传输？
5. 什么是滑动窗口机制？

## 3.2 UDP

### 3.2.1 协议详情

传输层协议

用户数据报协议，是一种非面向连接的不可靠传输协议

### 3.2.2 协议封装

|  |  |
| --- | --- |
| Source port (16) | Destination port (16) |
| Length (16) | Checksum (16) |
| Data (if any) | |

### 3.2.3 Question

1. 如何使用UDP并保证数据传输可靠性？
2. TCP、UDP区别和用途？

## 3.3 IPV4

### 3.3.1 协议详情

网络层协议

32位二进制组成，采用点分十进制进行书写

IPV4地址的网络位和主机位是由掩码决定的

掩码：

功能：为逻辑寻址功能提供服务

构成：由连续的1和连续的0构成

IPV4地址分类

A类：0XXX XXXX . 1-126 掩码为255.0.0.0 /8

B类：10XX XXXX . 128-191 掩码为255.255.0.0 /16

C类：110X XXXX . 192-223 掩码为255.255.255.0 /24

D类：1110 XXXX . 224-239 组播地址 无掩码

E类： 1111 XXXX . 240-255 科研地址，保留

其中A/B/C类地址为单播地址，工程中可用

* 私有地址

由于IPV4地址受限，我们需要大量的使用私有地址来解决地址不足的问题。一般私有地址在局域网中使用。

A类私有地址10.X.X.X/8

B类私有地址172.16.X.X/16-172.31.255.255/16

C类私有地址192.168.X.X/24

### 3.3.2 协议封装

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version (4) | Header Length (4) | Priority & Type of Service (8) | Total Length (16) | |
| Identification (16) | | | Flags (3) | Fragment offset (13) |
| Time to live (8) | | Protocol (8) | Header checksum (16) | |
| Source IP Address (32) | | | | |
| Destination IP Address (32) | | | | |
| Options (0 or 32 if any) | | | | |
| Data (varies if any) | | | | |

### 3.3.3 Question

1. 在网络中，是否可以直接使用私有地址接入互联网？

## 3.4 IPV6

### 协议详情

网络层协议

由128位二进制共16字节构成，采用点分十六进制书写

表示：

：：压缩：

地址：2001:0410:0000:0001:0000:0000:0000:45ff

压缩后：2001:0410:0000:0001::45ff

在压缩中，只能压缩一处的连续零，不能将多出的连续零进行压缩

压缩前导0：

地址：2001:0410:0000:0001:0000:0000:0000:45ff

压缩后：2001:410:0:1:0:0:0:45ff

：：压缩和压缩前导0可以同时使用：

地址：2001:0410:0000:0001:0000:0000:0000:45ff

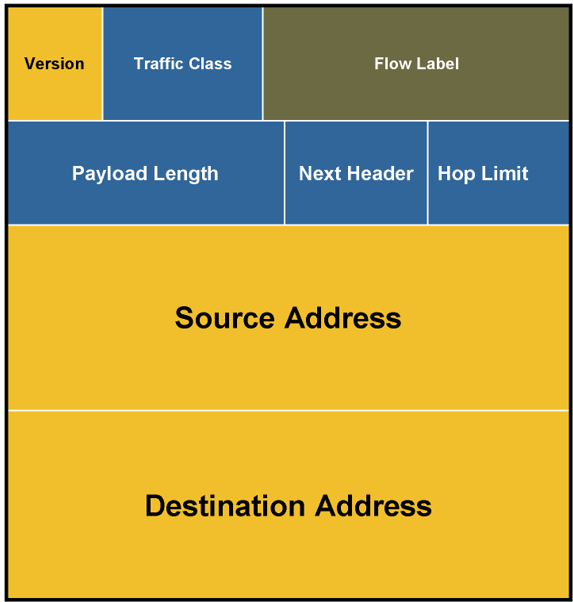
压缩后：2001:410:0:1::45ff

IPV6地址=前缀+接口标识

前缀类似于IPV4中的网络号，接口标识类似于IPV4中的主机号。前缀长度用类似于IPV4中掩码的形式表示

IPV6地址分类：

### 协议封装



### Question

## VLSM、CIDR

VLSM：可变长子网掩码技术

允许对主类网络的掩码进行再划分，也即常说的子网划分技术。

优点：可使地址更加合理的被使用，较少地址浪费的情况。

CIDR：无类别域间路由

对掩码的操作可以跨越主类网络掩码，主要用于网络汇总，减少了路由条目，增加了路由稳定性。

## ICMP

### 协议详情

网络层协议

用于检测网络中IP数据包是否能够正常到达目标地址，并回馈IP数据包被丢弃的原因。

ICMP协议基于IP协议工作，但不具备传输层的能力，故ICMP是网络层协议。

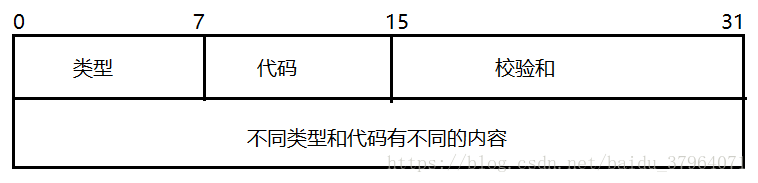
ping

ping是一个程序。一台主机向一个节点发送一个Type=8的ICMP报文，如果途中没有异常（例如被路由器丢弃、目标不回应ICMP或传输失败），则目标返回Type=0的ICMP报文，说明这台主机存在

traceroute/tracert

通过计算ICMP报文通过的节点来确定主机与目标之间的网络距离。

### 协议封装



|  |  |
| --- | --- |
| 字段类型 | 说明 |
| 类型 | 占一字节，标识ICMP报文的类型，从类型值来看ICMP报文可以分为两大类。第一类是取值为1~127的差错报文，第2类是取值128以上的信息报文 |
| 代码 | 占一字节，标识对应ICMP报文的代码。它与类型字段一起共同标识了ICMP报文的详细类型 |
| 校验和 | 这是对包括ICMP报文数据部分在内的整个ICMP数据报的校验和，以检验报文在传输过程中是否出现了差错（其计算方法与在我们介绍IP报头中的校验和计算方法是一样的） |

类型字段：

|  |  |  |
| --- | --- | --- |
| 类型 | 代码 | 描述 |
| 0（回送应答） | 0 | Echo Reply——回显应答（Ping应答） |
| 3（目标不可达） | 0 | Network Unreachable——网络不可达 |
| 1 | Host Unreachable——主机不可达 |
| 2 | Protocol Unreachable——协议不可达 |
| 3 | Port Unreachable——端口不可达 |
| 4 | Fragmentation needed but no frag. bit set——需要进行分片但设置不分片比特 |
| 5 | Source routing failed——源站选路失败 |
| 6 | Destination network unknown——目的网络未知 |
| 7 | Destination host unknown——目的主机未知 |
| 8 | Source host isolated (obsolete)——源主机被隔离（作废不用） |
| 9 | Destination network administratively prohibited——目的网络被强制禁止 |
| 10 | Destination host administratively prohibited——目的主机被强制禁止 |
| 11 | Network unreachable for TOS——由于服务类型TOS，网络不可达 |
| 12 | Host unreachable for TOS——由于服务类型TOS，主机不可达 |
| 13 | Communication administratively prohibited by filtering——由于过滤，通信被强制禁 |
| 14 | Host precedence violation——主机越权 |
| 15 | Precedence cutoff in effect——优先中止生效 |
| 4（原点抑制） | 0 | Source quench——源端被关闭（基本流控制） |
| 5（重定向或改变路由） | 0 | Redirect for network——对网络重定向 |
| 1 | Redirect for host——对主机重定向 |
| 2 | Redirect for TOS and network——对服务类型和网络重定向 |
| 3 | Redirect for TOS and host——对服务类型和主机重定向 |
| 8（回送请求） | 0 | Echo request——回显请求（Ping请求） |
| 9（路由器公告） | 0 | Router advertisement——路由器通告 |
| 10（路由器请求） | 0 | Route solicitation——路由器请求 |
| 11（超时） | 0 | TTL equals 0 during transit——传输期间生存时间为0 |
| 1 | TTL equals 0 during reassembly——在数据报组装期间生存时间为0 |
| 12 | 0 | IP header bad (catchall error)——坏的IP首部（包括各种差错） |
| 1 | Required options missing——缺少必需的选项 |
| 13 | 0 | Timestamp request (obsolete)——时间戳请求（作废不用） |
| 14 |  | Timestamp reply (obsolete)——时间戳应答（作废不用） |
| 15 | 0 | Information request (obsolete)——信息请求（作废不用） |
| 16 | 0 | Information reply (obsolete)——信息应答（作废不用） |
| 17（地址子网请求） | 0 | Address mask request——地址掩码请求 |
| 18（地址子网应答） | 0 | Address mask reply——地址掩码应答 |

### Question

1. 简述ping过程
2. traceroute原理

## ARP

### 协议详情

网络层协议

地址解析协议，是根据IP地址获取物理地址的一个TCP/IP协议

### 协议封装

### Question

## DNS

用于提供域名解析服务，所谓域名解析就是通过请求的域名回复该域名对应的IP地址。

由于互联网中服务主机十分多，无法准确记住所有需要使用的服务器地址。故有了域名的感念，在互联网中的域名是唯一的，每一个域名对应一个服务器资源。

## VLAN

## Trunk

## VTP

## STP

## Static Route

## RIP

## OSPF

## ACL

## NAT