



The project plan is the most important indicator plan. The brief introduction reflects the project achievement status of the company. The project plan needs to be formulated in strict accordance with the process

**PROJECT SOLUTIONS**

**数据通信笔记**

姓名：于国哉

通信：就是信息传递是指人与人、人与物、物与物之间通过某种媒介和行为进行的信息传递与交流。

网络通信：数据传递是指终端设备之间通过计算机网络进行的通信。

数据通信网络：由路由器、交换机、防火墙、无线控制器、无线接入点，以及个人电脑、网络打印机、服务器等设备构成的通信网络。

TCP：一种面向连接的、可靠的传输接收结果有响应传输层通信协议。

PDU：应用层数据，传输层是数据段，网络层是数据包，数据链路层是数据帧

封装：添加头部和尾部信息

解封装：头部尾部添加的信息去掉，剩下的部分

端口号：区分不同应用层协议。知名端口号<1023

报文：统称，整体信息

TCP窗口字段作用：流量的控制

数据包逐跳转发

数据链路层用的最多的协议是以太网

# 以太网交换基础

## **什么是以太网：**共享介质的广播域网络

* CSMA/CD的工作原理可简单总结为：先听后发，边发边听，冲突停发，随机延迟后重发。（解决数据发送冲突）
* 交换机中的hub（集线器）只会转发信号不会处理信号
* 工作在物理层

**冲突域：**冲突影响的范围大小 。一个hub整体是一个冲突域.冲突是因为有共享介质

## MAC地址

* 一个MAC地址有48 bit，6 Byte。MAC地址通常采用“十六进制&-”表示
* 一个制造商在生产制造网卡之前，必须先向IEEE注册，以获取一个长度为24bit (3字节)的厂商代码，也称为OUI，后24bit由厂商自行分派

终端的是OUI，组播、广播是非OUI

* 发广播的数据包用广播的IP地址，发广播的数据帧用广播的MAC地址
* 电脑工作在应用层，向下兼容；hub工作在物理层
* 封装数据帧的时候调用Mac地址。单播第8个比特位是0，组播第8个比特位是1
* 没有Mac地址封装不了数据帧

广播是二层交换协议的广泛使用

## ARP（Address Resolution Protocol，地址解析协议）

ARP（Address Resolution Protocol，地址解析协议）是根据IP地址获取数据链路层地址的一个TCP/IP协议。该协议属于数据链路层，服务于IP，但因为与IP相关联，也可以说它是网络层协议。

**原理：**

1. 先从本地arp缓存，是否有目标Mac信息
2. 缓存无记录时，发送arp广播请求，全网查找目标Mac
3. 收到目标设备的arp回复报文，先放入arp缓存
4. 封装成完整数据帧

**注意：**

* 请求是广播的数据帧，响应是单播的数据帧
* Arp缓存表默认300秒，
* 以太网数据帧协议类型0800 IP；0806 ARP

## 物理层

### 网线

* 种类：4对8根，橙白橙、蓝白蓝、棕白棕、绿白绿
* 线序：13；26做调换
  1. 直通线（568B）

橙白 橙 绿白 蓝 蓝白 绿 棕白 棕

* 1. 交叉线（568A）

绿白 绿 橙白 蓝 蓝白 橙 棕白 棕

* 线序使用

相同设备用交叉线，PC和路由器是同种设备

不同的设备用直通线。

注意：一般网线总长度小于100米

端口自协商：自动调整端口速率，适配下面连接的终端（短距离使用）

端口自适应：自动调整端口的引脚，适应线序

* 网线质量

含铜量越高，导电性越好，线质量越好，越硬，越不好做

* 网线要求

百兆线要求：1、2、3、6线通即可

千兆线要求：8根线全通

万兆线要求：8根线全通，地线也必须通

* 网线线标含义

1、品牌

可以根据这个标识来核查是否是购买的品牌，谨防无良商家调包，以次充好。一般箱线（不带水晶头）品牌的标识后面会印上公司官网的网址。

2、网线种类

目前市场上的网线基本分为：五类网线（CAT5）、超五类网线（CAT5e）、六类网线（CAT6）、超六类网线（CAT6A）、七类网线（CAT7）等。

3、制作网线标准

AWG是美制电线标准的简称，AWG值是导线厚度（以英寸计）的函数。

  直径为24AWG，约为0.511mm。

4、屏蔽类型

根据屏蔽类型网线分为：非屏蔽（UTP）、单屏蔽（FTP）、双屏蔽（SFTP）。屏蔽主要是为了减少信号干扰，保障信息安全。

5、使用场景

solid LAN cable代表线缆是实心的线芯，在局域网的环境中使用。

6、米数标记

在实际布线场景中，米数标记是最实用的，并只出现在箱线的标识上。NA无特殊意义，仅仅是为了更好地将米数标识和前面标识隔开，方便快速查看。

7、跳线的特有标记

跳线，即自带水晶头，因为水晶头的接法分为T568A和T568B，所以跳线会将水晶头的接法做标记。

 TIA/EIA代表网线水晶头接法的标准，一般缩写为“T”。

**每根网线的具体作用**

第一根线（白绿/绿线）：称为发送线（TX+），它用于发送数据信号。在一对绞线中，TX+是正极，它负责传输数据的正信号。

第二根线（绿线）：称为发送线（TX-），它与第一根线相配对，用于发送数据信号。在一对绞线中，TX-是负极，它负责传输数据的负信号。

第三根线（白橙/橙线）：称为接收线（RX+），它用于接收数据信号。在一对绞线中，RX+是正极，它负责接收数据的正信号。

第四根线（蓝线）：称为中断线（SQ-），在八芯网线中通常不使用，因此它的作用较小。

第五根线（白蓝/橙线）：称为中断线（SQ+），它与第四根线相配对，在八芯网线中同样较少使用。

第六根线（白棕/棕线）：称为接收线（RX-），它与第三根线相配对，用于接收数据信号。在一对绞线中，RX-是负极，它负责接收数据的负信号。

第七根线（棕线）：称为中断线（D+），在八芯网线中通常不使用，它的作用很小。

第八根线（白棕/棕线）：称为中断线（D-），它与第七根线相配对，同样较少使用。

总结起来，八芯网线的每根线都有其特定的作用：

* 第一根与第二根线：发送数据信号。
* 第三根与第六根线：接收数据信号。

第四根与第五根线、第七根与第八根线：通常不使用，可以认为是冗余线。

使用八芯网线传输数据时，一对绞线用于传输数据的正信号，另一对绞线用于传输数据的负信号。这种差分传输方式可以减少信号干扰，并提高数据传输的稳定性和可靠性。此外，使用八芯网线还可以支持全双工通信，即同时发送和接收数据信号。

### 光纤

* 光纤接口：SC大方头 FC圆头 ST卡扣 LC小方头
* 分类:

单模光纤：同一时间只有一束光在光纤内传播（必须成对使用）

适合超远距离传输

用激光发射器做光源

多模光纤：同一时间有多束光在光纤内传播（可以单根使用）

适合近距离传输

用发光二极管做光源

注意：

单模光纤配单模光模块，连接的时候要对应，两者要相匹

### 设备管理

#### 带内管理

使用普通的网络接口，执行远程管理

#### 带外管理

使用专门的管理口（console)，配合专用的配置线，近距离管理。所有设备都有console配置口，专门用来管理设备；客户端需要使用console配置线，插入设备console口，管理。通常用来对新设备做配置

#### console线管理设备的步骤

1. 下载并安装console线的驱动
2. 连接设备
3. 打开系统中的设备管理器，查看USB模拟的串口编号
4. 打开配置软件，如：xshell、CRT、putty、等

连接方式选：serial串口方式

串口号=com端口号（通过设备管理器查看）

波特率=9600

## 各层主要协议详解

### 总体概览

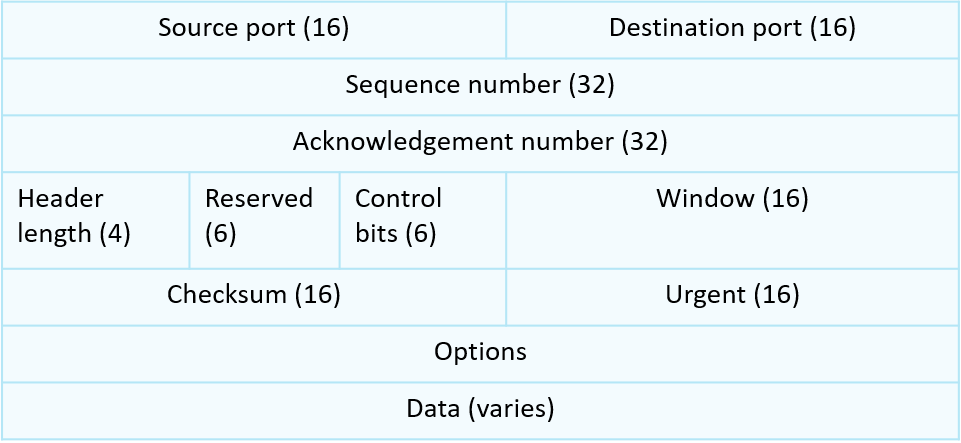


* 1. 应用层，对应用程序提供接口。
  2. 表示层，进行数据格式的转换，以确保一个系统生成的应用层数据能够被另外一个系统的应用层所识别和理解。
  3. 会话层，在通信双方之间建立、管理和终止会话。
  4. 传输层，建立、维护和取消一次端到端的数据传输过程。控制传输节奏的快慢，调整数据的排序等等。
  5. 网络层，定义逻辑地址；实现数据从源到目的地的转发。
  6. 数据链路层，将分组数据封装成帧；在数据链路上实现数据的点到点、或点到多点方式的直接通信；差错检测。
  7. 物理层，在媒介上传输比特流；提供机械的和电气的规约。

### 传输层

作用：建立、维护端到端的数据传输

利用端口号来确认双方使用的应用程序



TCP头部

Source Port：源端口，标识哪个应用程序发送。长度为16比特。

Destination Port目：的端口，标识哪个应用程序接收。长度为16比特。

Sequence Number：序号字段。TCP链接中传输的数据流每个字节都编上一个序号。序号字段的值指的是本报文段所发送数据的第一个字节的序号。长度为32比特。

Acknowledgment Number：确认序列号，是期望收到对方下一个报文段数据的第1个字节的序号，即上次已成功接收到的数据段的最后一个字节数据的序号加1。只有Ack标识为1，此字段有效。长度为32比特。

Header Length：头部长度，指出TCP报文头部长度，以32比特（4字节）为计算单位。若无选项内容，则该字段为5，即头部为20字节。

Reserved：保留，必须填0。长度为6比特。

Control bits：控制位，包含FIN、ACK、SYN等标志位，代表不同状态下的TCP数据段。

RST标志位，中断标志位

Window：窗口TCP的流量控制，这个值表明当前接收端可接受的最大的数据总数（以字节为单位）。窗口最大为65535字节。长度为16比特。

Checksum：校验字段，是一个强制性的字段，由发端计算和存储，并由收端进行验证。在计算检验和时，要包括TCP头部和TCP数据，同时在TCP报文段的前面加上12字节的伪头部。长度为16比特。

### 网络层

作用：转发数据包、确认双方的IP地址

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Header Length | | Type of Service | Total Length | | |
| Identification | | | | Flags | Fragment Offset | |
| TTL | | Protocol | | Header Checksum | | |
| Source IP Address | | | | | | |
| Destination IP Address | | | | | | |
| Options | | | | | | Padding |

IPV4头部

IP Packet（IP数据包），其包头主要内容如下：

Version：4 bit，4：表示为IPv4；6：表示为IPv6。

Header Length：4 bit，首部长度，如果不带Option字段，则为20，最长为60。

Type of Service：8 bit，服务类型。只有在有QoS差分服务要求时，这个字段才起作用。 差分服务 优先级

Total Length：16 bit，总长度，整个IP数据包的长度。

Identification：16 bit，标识，分片重组时会用到该字段。

Flags：3 bit，标志位。

Fragment Offset：12 bit，片偏移，分片重组时会用到该字段。

Time to Live：8 bit，生存时间。 防止环路，防止无限循环，每次转发减一 255-1 、254-1

Protocol：8 bit，协议号：上一层协议。指出此数据包携带的数据使用何种协议，以便目的主机的IP层将数据部分上交给哪个进程处理。

协议常见值：

1: ICMP, Internet Control Message；

2: IGMP, Internet Group Management；

6: TCP , Transmission Control Protocol；

17: UDP, User Datagram Protocol。

Header Checksum：16 bit，首部检验和。

Source IP Address：32 bit，源IP地址。

Destination IP Address：32 bit，目的IP地址。

Options：可变，选项字段。

Padding：可变，填充字段，全填0。

**UDP**

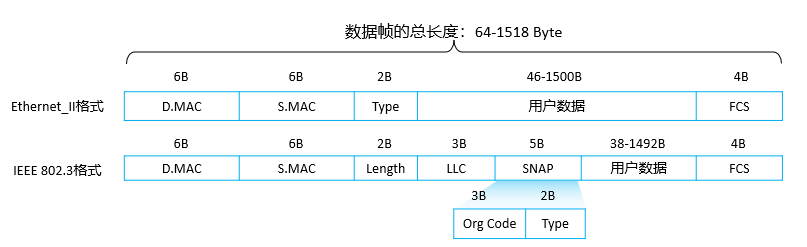
只有一种安全验证设置：校验和

作用：检测UDP报文在传输过程中是否有错，有错就丢弃

### 数据链路层

作用：数据封装成数据帧，实现点到点、点到多点的通信

利用Mac地址，确认双方的身份



以太帧格式

DMAC：6字节，目的MAC地址，IPV4为6字节，该字段标识帧的接收者。

SMAC：6字节，源MAC地址，IPV4为6字节，该字段标识帧的发送者。

Type：2字节，协议类型。常见值：

0x0800：Internet Protocol Version 4 (IPv4)

0x0806：Address Resolution Protocol (ARP) 。

### 各层数据大小

数据段默认大小：1480字节，头部20字节，上层数据1460字节

数据包默认大小：1500字节，也叫MTU（最大传输单元），包头20-60字节

数据帧默认大小：1518字节，帧头18字节，帧尾4字节，上层数据1500字节

## 路由器、交换机接口类型

路由接口，可以直接配置接口

交换接口，必须在vlanif虚拟口配IP，物理接口要能传输该vlan的数据

1.6.1 链路聚合口-交换口变成路由口

Undo portSwitch

同种类型的口才能聚合，不同种类型的需要转换

## 交换机工作原理

* 学习数据帧的源Mac地址
* 转发数据帧的目的Mac地址（若目标Mac地址不在地址表中，则泛洪）

## 路由器工作原理

* 用多种手段完善路由表记录
* 检查目标网段是否在路由表中

路由表有记录，从指定接口单播转发

路由表无记录，直接丢弃

注意：

跨网段通讯的数据，在没有nat转换时，IP地址不变Mac地址变

在有nat转换时，IP地址变Mac地址变

## 使用域名网址访问服务器的原理

1. 先从本地DNS缓存查找相应记录
2. 缓存无记录时，向指定DNS服务器发出解析请求
3. 收到DNS服务器回复，先写入缓存
4. 向目标主机发起TCP三次握手连接
5. 向目标主机发起http协议的get请求，请求获取某个页面的完整内容
6. 收到目标主机的http回复报文，在浏览器中用html语音正确显示内容
7. 目标主机发送完毕后，执行TCP四次挥手过程，断开TCP连接

## 计算机通讯原理内容

1. 用各种方式获知目标IP
2. 判断源网段和目标网段是否为同一个网段

同网段时，需要获取目标Mac地址

不同网段，需要获取网关Mac地址

1. 利用ARP原理获取目标Mac地址

封装成数据帧，交给交换机转发处理

1. 利用交换机原理转发数据

源和目标IP为同网段时，数据帧直接发送到目标主机

1. 利用路由器原理转发数据

# IP路由基础

1.路由器隔离了广播域（路由器不转发数据帧），每一个接口连接一个不同的广播域

2.主机如何发现外部网络？通过路由

主机如何判断目的IP跟本地IP是不同地址？查路由表里的路由信息

## IP地址

**A类地址**

A类IP地址，第一段一字节数据表示网络号，剩下三段表示主机号。规定网络号最高位必须为0，则可以表示0000 0001-0111 1111，即126（除去全0和全1）个网络，剩下的3个字节数据可以表示2^24-2个主机。A类子网掩码255.0.0.0.

**B类地址**

B类IP地址，前两段2个字节数据表示网络号，剩下两段表示主机号。规定网络号最高位必须为10，则范围从10000 0000-10111111，即128-191，地址范围从128.0.0.0-191.255.255.255，共有2^14-2个网络，可以容纳2的16次方-2个主机。子网掩码255.255.0.0.

**C类地址**

C类IP地址，前三段3个字节数据表示网络号，剩下一段表示主机号。规定网络号最高位必须为110，则范围从1100 0000-1101 1111，即192-223，可以表示2^21-2个网络，可以容纳254个主机。子网掩码255.255.255.0

**D用于组播环境中**

**E用于科研机构**

A: 0 255.0.0.0

00000000.00000000.00000000.00000000 0.0.0.0

01111111.11111111.11111111.11111111 127.255.255.255

B：10 255.255.0.0

10000000.00000000.00000000.00000000 128.0.0.0

10111111.11111111.11111111.11111111 191.255.255.255

C：110 255.255.255.0

11000000.00000000.00000000.00000000 192.0.0.0

11011111.11111111.11111111.11111111 223.255.255.255

D：1110

11100000.00000000.00000000.00000000 224.0.0.0

11101111.11111111.11111111.11111111 239.255.255.255

E：1111

11110000.00000000.00000000.00000000 240.0.0.0

11111111.11111111.11111111.11111111 255.255.255.255

### 网络地址，广播地址，可用地址

网络地址：主机位全为0

广播地址：主机位全为1

可用地址：2n-2（n为主机位位数）

### 特殊IP地址

|  |  |  |
| --- | --- | --- |
| 特殊IP地址 | 地址范围 | 作用 |
| 有限广播地址 | 255.255.255.255 | 可作为目的地址，发往该网段所有主机（受限于网关）（特殊场景使用） |
| 任意地址 | 0.0.0.0 | “任意网络”的网络地址；“这个网络上这个主机接口”的IP地址 |
| 环回地址 | 127.0.0.0/8 | 测试设备自身的软件系统/测试自己的手段（自测）（不会出现在网络上） |
| 本地链路地址 | 169.254.0.0/24 | 当主机自动获取地址失败后，可使用该网段中的某个地址进行临时通信（特殊场景下出现的地址） |

### 子网划分

VLSM 可变长子网掩码技术。由于地址使用不合理，造成地址浪费，网络规划不合逻辑

划分步骤：

1、确定子网位：公式2n ≥需求数 n就是子网位的个数

2、根据子网位的结果，划分出相应的子网：

子网掩码中的网络位向主机位借位，确定每个子网中的可用地址

支持VLSM：可用划分子网

不支持VLSM：不能划分子网，只能按照IP分类规则使用（的是主类/有类网络）

主类/有类网络：只支持IP分类规则的网络

## IP选优原则

* 先判断路由优先级，越小越优先
  + 直连路由，路由优先级0
  + Ospf内部路由，路由优先级10
  + ISIS路由，路由优先级15
  + RIP路由，路由优先级100
  + Ospf外部路由，路由优先级150
  + Bgp路由，路由优先级255
* 优先级相同时，比较路径总开销cost，越小越优先

注意：

路由功能使用优先级判断时，一般数字越大越优先，但路由表中特殊

交换功能使用优先级判断时，一般数字越小越优先

CIDR：无类域间路由，打破了有类IP地址的划分

路由器有多个出接口的时候，默认路由慎用。

路由器产生的数据包，数据包的源IP默认是出接口的IP

Ping -A 192.168.0.1 172.16.0.1 改变数据包的源IP地址（带源地址ping）

默认路由不是静态路由，任何一个路由协议都会生成默认路由

在以太网环境中，静态路由的配置可以不写出接口，必须指明下一跳

ICMP：ping 、路由跟踪

VLAN：虚拟局域网。基于以太网，解决广播域太大的问题

在网络层如何测试网络的可达性？  **ICMP**

同层之间进行通信，上层利用下层的服务来通信。

端口可达：传输层

网络可达：网络层

Ping是ICMP协议下的一个应用程序

判断双方IP地址是否是同一个网段？

用自身IP地址与子网掩码的二进制同时进行与运算

用对方IP地址与子网掩码的二进制 估算

## 常见的网络层、传输层协议号

协议号1：ICMP协议

协议号4：IP协议

协议号6：TCP协议

协议号17：UDP协议

协议号41：IPV6协议

协议号50：ESP协议,叫安全封装载荷协议

协议号51：AH协议，叫认证头协议

协议号58：ICMPV6协议

注意：ESP和AH协议，主要用于VPN通讯

# 虚拟局域网 (VLAN, Virtual LAN)

## VLAN的定义

VLAN（Virtual Local Area Network，虚拟局域网）是一种将物理局域网划分成多个逻辑上独立的虚拟网络的技术。它可以实现将不同地理位置上的计算机通过逻辑方式连接在一起，并实现隔离和安全性。

## Vlan划分

### 静态vlan（基于接口的VLAN划分）

静态vlan指的是交换机接口与vlan是绑定、固定关系

根据交换机的接口来划分VLAN。

* 网络管理员预先给交换机的每个接口配置不同的PVID，将该接口划入PVID对应的VLAN。
* 当一个数据帧进入交换机时，如果没有带VLAN标签，该数据帧就会被打上接口指定PVID的Tag，然后数据帧将在指定PVID中传输。

缺省VLAN，PVID

Port VLAN ID，是接口上的缺省VLAN。

取值：1~4094。

### 动态vlan

其一根据数据帧的源MAC地址来划分VLAN。

* 网络管理员预先配置MAC地址和VLAN ID映射关系表。
* 当交换机收到的是Untagged帧时，就依据该表给数据帧添加指定VLAN的Tag，然后数据帧将在指定VLAN中传输。

映射表记录了MAC地址和VLAN ID的关联情况。

## 划分VLAN的作用

有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。由于VLAN隔离了广播风暴，也隔离了不同VLAN之间的通讯，因此，不同VLAN之间的通讯必须依靠路由器或者三层交换机来实现。

广播域：广播传播的范围；冲突域：在范围内同一时间只有一个设备能传输数据。

默认：交换机所有接口在同一广播域，路由器每个接口都是单独的广播域

## 以太网二层交换机接口类型

### Access接口

工作场景：通常用于交换机连接终端设备（主机、服务器）

特点：只允许某个vlan数据的接收和发送



### Trunk接口

工作场景： 通常用于交换机与交换机互联

特点：允许多个vlan数据的收发



### Hybrid接口

工作场景：既可以连接用户终端，也可以连接交换机/路由器

## Vlanif

交换机vlanif虚拟口接收vlan数据，跨vlan通讯

交换机跨vlan通讯原理：

物理口接收数据，添加vlan标记

数据发送到vlanif虚拟接口

查询路由表，找到出口对应的vlanif口

根据物理口与vlan对应关系，把数据发送到物理口

根据设置，携带或清除vlan标记，从物理口发出数据

注意：

交换机向路由器发送带vlan标记的数据时，必须用Trunk模式。此时路由器必须用子接口处理该数据。

交换机向路由器发送无vlan标记的数据时，尽量用access模式。此时路由器必须用物理接口处理该数据

## 端口组（多个端口批量操作）

### 永久端口组

Port-group aaa（起名）

Group-member e0/0/3 e0/0/4

### 临时端口组

Port-group Group-member e0/0/3 e0/0/4

配置的时候，一个命令，组里面的所有成员同时执行，退出后，临时端口组消失，配置不变。

# STP（spanning tree protocol）

## STP基本概念

STP是生成树协议的缩写，主要用于防止二层网络中的环路问题（三层网络中可以通过IP字段 TTL进行破环）

原理：先计算出无环的拓扑树，阻塞多余接口

### 为什么二层会环路

以太网帧中没有防环字段，帧在转发时没有TTL-1机制

### 二层环路带来的影响

* 广播风暴-------------------无休止运行，主机收到广播要交给CPU处理，影响主机性能，可能导致设备宕机
* MAC地址漂移-------------MAC地址振荡
* 单帧多次递交现象--------一般在同一Vlan中出现

**判断出现环路、广播风暴的依据：**

**交换机接口灯闪烁频率相同且极为频繁**

## STP端口角色的选举

### 标准STP协议的两种端口角色

根端口RP、指定端口DP、阻塞端口AP（非标准STP协议制定的）

标准的STP协议，端口角色只有两种，即RP和DP，没有对Block状态的端口进行角色的定义。但是在华为的设备上，STP协议将Block状态端口引用RSTP协议的AP端口角色来定义即AP端口是RSTP协议的端口角色，标准STP种并没有AP端口的定义，只是华为的STP用AP端口来表达端口的状态为Block

## BID与PID介绍

**BID：桥ID（包含交换机的优先级和交换机的MAC地址）**

优先级-----0~65535，缺省32768。并且优先级必须是4096的倍数-----越小越优先

MAC地址--选择交换机所有端口中最小的MAC地址做比较-------------越小越优先

**PID：端口ID（包含端口的优先级和端口编号）**

优先级-----0~255，缺省128。并且优先级必须是16的倍数-------------越小越优先

端口编号---------------------------------------------------越小越优先

## STP选举步骤

* 选举根桥，同一个二层网络根桥有且只有一个
* 其它交换机为非根桥，在非根桥上选举根端口（RP），每个非根桥交换机有且只有一个根端口，根桥上不存在根端口
* 在每条链路上选举一个指定端口（DP），每条链路有且只有一个指定端口（根端口和指定端口不能是同一个端口） 一台设备可以有多个指定端口
* 非根端口、非指定端口的端口，就称为阻塞端口（AP）

交换机启动后就自动开始进行生成树收敛计算，默认情况下，所有交换机在启动时都认为自己是根桥，自己的所有端口都为指定端口，这样BPDU报文就可以通过所有端口转发

### 选举根桥

**BID最小的交换机称为根桥（根桥可以被抢夺）**

* 比较桥优先级，越小越优
* 比较MAC地址，越小越优

### 选举根端口RP

**交换机上能够接收最好的BPDU报文的端口**

* 比较端口收到的BPDU报文中Root ID最小的，为根端口（同一根桥，Root ID是一致的）
* 比较路径开销，此开销为端口收到的最小路径开销，越小越优
* 比较对端的BID，选优先级高的
* 比较对端的PID，选择优先级高的
* 比较本端口的PID，选择优先级高的

### 选举指定端口DP

**链路上能够发送给根桥的最好BPDU的端口**

**对于根桥来说，其所有端口一般都为指定端口**

* 比较路径开销，此开销指的是端口发送出去的根路径开销，越小越优先（Eth端口开销默认为20000）
* 比较本端的BID，选优先级高的
* 比较本端的PID，选择优先级高的

根桥的端口都是指定端口，其状态是转发状态

## 5种端口状态

* 禁用（Disable）禁止任何报文收发
* 阻塞（Blocking）只收BPDU报文，其他报文禁止
* 侦听（Listening）收发BPDU报文，用户报文全禁止
* 学习（Learning）收发BPDU报文，只接收用户报文（为了学习源mac地址）不发送用户报文
* 转发（Forwarding）收发任何报文

**从阻塞到侦听需要20秒；判断正常链路故障无法联系根桥**

**从侦听到转发（侦听→学习，学习→转发各15秒）30秒**

## Stp 2种报文

* 配置BPDU：建立、维持无环结构（stp树形结构）

正常情况下，根桥发送、非根桥转发该报文

发送间隔：2s，根桥死亡时间默认20s

只有根桥发送配置BPDU，非根桥转发

* TCN BPDU：拓扑变更通知BPDU

## Stp生成树版本

* Stp
* RSTP：

优点：收敛速度快

缺点：所有vlan共用一个stp树，根桥压力大

AP →RP的备份；BP→DP的备份

* Mstp：特点vlan分流、根桥压力负载均衡。一般分2个生成树
* Pvst：思科公司专属stp协议
* Vbst：华为公司专属stp协议

Pvst和Vbst共同点：每个vlan都有单独的stp树

# Ospf（Open Shortest Path First，开放式最短路径优先）

## **基本概念**

动态路由协议。IPv4协议使用的是OSPF Version 2（RFC2328）；针对IPv6协议使用OSPF Version 3（RFC2740）。5种协议报文[hello、DD（Database Description）、LSR（Link State Request）、LSU（Link State Update）、LSA（Link State ACK）]，3种表项（OSPF邻居表、LSDB表和OSPF路由表），2种路由（DR、BDR）

工作过程一句话概括就是：ospf先建立邻居，互相发送hello报文；再发送LSA结束后形成LSDB；再基于LSDB计算路由从而形成路由表。

## 分类

### 按照使用位置

* IGP，内部网关协议，一般在私有网络使用

包含：ospf，RIP，ISIS

* EGP，外部网关协议，一般在运营商提供的公网使用

包含：BGP

### 按照运算机制、算法

* 距离矢量路由协议

包含：RIP

变种：路径矢量路由协议，包含bgp

判断最佳路由的依据：方向、跳数

RIP的最大跳数：15

* 链路状态路由协议

包含： ospf，ISIS

判断最佳路由的依据：开销

Ospf开销，可以手动配置，可以按公式计算

## Ospf状态机有7种

1. down
2. init 初始化状态
3. 2-way 双边状态（邻居状态）

------------------------前面都是hello报文

1. Ex-start 准启动状态、、、、用没有链路信息的DD报文确认双方的主从地位
2. Exchange 交换状态、、、、、从设备先发送带链路信息的DD报文

------------------------前面都是DD报文

1. Loading 加载状态-----发送LSR/LSU/LSA报文
2. Full 完整状态、、、、、、、、、双方路由器处于临接状态 （看到最多的是hello报文）

### Ospf各状态卡顿原因

1、卡在init状态:一方收不到另一方的hello包，如卡在认证

2、卡在2-way状态:没有做出DR/BDR选举，如果是DROther路由器则是正常状态

3、卡在exstart状态:接口mtu不匹配

4、卡在exchange状态:包的交互有问题

5、卡在1oading状态:lsa加载不完全会卡在Loading

## 5种协议报文

* Hello：（组播形式发送，目的IP地址是组播地址）
  + 发送、建立、维护邻居关系
  + 发送间隔：10s
  + 邻居死亡时间：4\*hello报文 、、、大多数的死亡时间=3\*hello时间
* DBD/DD（Database Description）（单播）
  + 作用：描述LSDB中已知的链路信息
* LSR（Link State Request）
* LSU（Link State Update）
* LSA（Link State ACK）

组播地址：224.0.0.5 所有ospf路由都接收

组播地址：224.0.0.6 只有DR、BDR路由器接收

## Ospf路由器

### 配置方式（必须有routerID）

1.手动配置

2.自动使用回环接口最大IP做routerID

3.没有回环则自动使用物理接口最大的IP做routerID

### 分类

1. 区域内路由器

路由器所有链路都在同一个区域

再细分2种

骨干路由器

非骨干路由器

1. 区域边界路由器

路由器链路宣告到2个或2个以上的区域

1. 自治系统边界路由器

自治系统：网络使用相同的路由协议

该类路由器必须运行2种或2个以上路由协议，其中必须有ospf协议

## DR/BDR路由器

* 使用场景：只有在接口类型是广播型、非广播型
* 竞选依据：手动配置的DR优先级越大越优先；DR优先级相同时，对比routerID，越大越优先
* 只允许DR、BDR与其他OSPF路由器建立邻接关系。DRother之间不会建立全毗邻的OSPF邻接关系，双方停滞在2-way状态。
* BDR会监控DR的状态，并在当前DR发生故障时接替其角色。

DR路由器作用：收集所有邻居信息

优点：减少临接数量、减少ospf报文数量

普通ospf路由器只与DR、BDR做临接关系

普通ospf路由器之间只做邻居关系

DR路由器选举在每个链路上都要选举

### 5.5.1 DR路由器选举

* 先比较接口的DR优先级，越大越优先

默认DR优先级是：1

* 优先级相同时，比较routerID，越大越优先

DR角色具有非抢占性

通常路由设备优先级越大越优先，交换设备优先级越小越优先

## 5.6 Ospf区域分为

通过区域，可以限制路由器进行路由学习的范围。只需要学习本区域内所有的链路信息

* 骨干区域：区域号必须是0
* 非骨干区域：

注意：非骨干区域之间通讯，必须经过骨干区域

区域划分，针对路由器的接口链路

## 5.7 Ospf宣告方式

1.在区域视图下 Network 网段 反向掩码

2.在区域视图下 Network 接口IP 0.0.0.0

3.在接口视图下，ospf enable 进程号 area 区域号（适合在IPV6中使用，ipv6的ospf

只有该方式才能宣告网段）

## 5.8 Ospf工作原理

1. 建立邻居关系
2. 交换链路信息，构建LSDB（包含全网的链路信息）
3. 利用SPF（最短路径算法）计算最佳路由
4. 最佳路由结果写入IP路由表

每个路由器必须拥有routerID

设置方式：

手动配置，没有手动，自动使用环回接口最大IP

没有环回口，自动使用物理接口最大IP

注意：

## 5.9 OSPF邻居关系不能建立的原因

1.设备物理接口状态和协议状态是down，没有up。

2.两端OSPF进程的Router ID一致。

3.两端OSPF区域ID不一致。

4.链接两端OSPF接口的网络类型不一致。

5.链路两端OSPF接口的IP地址不在同一网段或者IP地址的掩码不一致。

6.链路两端OSPF接口的IP地址所在网段没有包含在区域内配置的network内。

7.链路两端OSPF接口的DR优先级是0。

8.路由器之间OSPF有认证存在，认证模式或者或者口令不一致。

9.接口MTU不匹配

10.有访问控制列表ACL禁止了OSPF流量，或者接口被PASSIVE

11.OSPF的报文Hello/Hello dead 间隔不匹配

12.两端OSPF区域类型不同

**解决办法**

1. 检查邻居两端的接口物理和协议状态是否UP，状态是否稳定，接口是否有丢包，两边互ping大包是否能通。

若物理接口不Up或是不稳定（有振荡现象），请排查物理链路和链路层协议，确保物理和协议状态都是Up，并且接口无错误计数。可以通过ping测试，长ping测试是否存在丢包现象，ping大包（1500字节以上）测试是否存在大包不通的现象。

1. 检查链路两端OSPF进程的Router ID是否一致。

分别在链路两端的设备上执行命令display ospf [ process-id ] brief，查看OSPF进程的Router ID。RouterID尽量保证全网唯一，否则有可能邻居不能正常建立、路由信息不正确的问题。建议在设备上单独为每个OSPF进程配置全网唯一的Router ID。如果链路两端OSPF进程的Router ID一致，请在系统视图下执行命令ospf [ process-id ] router-id router-id，修改OSPF进程的Router ID以保证不冲突。修改OSPF进程的Router ID之后，必须在用户视图下执行命令reset ospf [ process-id ] process后，新配置的Router ID才会生效。

3.检查链路两端OSPF区域ID是否一致。

分别在链路两端的设备上执行命令display ospf [ process-id ] brief，查看OSPF的区域ID。如果链路两端的OSPF区域ID不一致，请在OSPF视图下执行命令area area-id，修改OSPF区域ID以保证一致。

4.检查链接两端OSPF接口的网络类型是否一致。

分别在链路两端的设备上执行命令display ospf [ process-id ] interface，查看OSPF接口的接口类型。一般情况下，链路两端的OSPF接口的网络类型必须一致，否则双方不能正常建立起OSPF邻居关系。当链路两端的OSPF接口的网络类型一端是广播网而另一端是P2P时，双方仍可以正常的建立起邻居关系，但互相学不到路由信息。当链路两端的OSPF接口的网络类型一端是P2MP而另一端是P2P时，双方仍可以正常的建立起邻居关系，但互相学不到路由信息。为了相互学到路由信息，此时需要在链路两端的OSPF接口上配置相同的Hello报文发送间隔和邻居失效时间。如果OSPF接口的网络类型不一致，请在运行OSPF协议的接口视图下执行命令ospf network-type { broadcast | nbma | p2mp | p2p }，修改OSPF接口的网络类型以保证一致。如果链路两端OSPF接口的网络类型都是NBMA，则必须在OSPF视图下执行命令peer ip-address [ dr-priority priority ]，配置NBMA网络的OSPF邻居。

1. 检查链路两端OSPF接口的IP地址是否在同一网段或者IP地址的掩码是否一致。

分别在链路两端的设备上执行命令display current-configuration interface interface-type interface-number，查看OSPF接口的IP地址。一般情况下，链路两端的OSPF接口的IP地址的掩码必须一致，否则双方不能正常建立OSPF邻居关系。但在P2MP网络中，可以通过在运行OSPF协议的接口视图下配置命令ospf p2mp-mask-ignore来使设备忽略对网络掩码的检查，从而正常建立OSPF邻居关系。如果OSPF接口的IP地址的掩码不一致，请在运行OSPF协议的接口视图下执行命令ip address ip-address { mask | mask-length }，修改OSPF接口的IP地址以保证掩码一致。

6.检查链路两端OSPF接口的IP地址所在网段是否包含在区域内配置的network内。

分别在链路两端的设备上执行命令display current-configuration interface interface-type interface-number，查看OSPF接口的IP地址；执行命令display current-configuration configuration ospf，查看OSPF进程的配置。满足下面两个条件，OSPF协议才能在接口上运行：接口的IP地址掩码长度≥network命令中的掩码长度。OSPF使用反掩码，例如0.0.0.255表示掩码长度24位。接口的主IP地址必须在network命令指定的网段范围之内。如果检查发现接口IP地址与配置的network不满足上述条件，请在运行OSPF协议的接口视图下执行命令ip address ip-address mask | mask-length }，修改接口的IP地址；或者在OSPF进程对应的区域视图下执行命令network，修改配置的网段，保证满足上述条件。

7.检查链路两端OSPF接口的DR优先级是否非零。

分别在链路两端的设备上执行命令display ospf [ process-id ] interface，查看OSPF接口的DR优先级。对于广播和NBMA类型网络，链路中至少要有一个OSPF接口的DR优先级不为0，这样才能正常选举出DR。否则两边的邻居状态只能达到2-Way。如果链路两端OSPF接口的DR优先级都为0，请在运行OSPF协议的接口视图下执行命令ospf dr-priority priority，修改OSPF接口的DR优先级以保证至少有一个接口的DR优先级不为0。

8.检查路由器之间OSPF是否有认证存在

执行命令display current-configuration 查看

9.接口MTU是否不匹配邻居建立过程中MTU需要匹配，通常MTU不匹配的情况下，邻居关系始终停留在EXSTART状态，MTU默认为1500,可以通过 命令：display interface +接口来查看，也可以通过Debug。

10.检查是否有访问控制列表ACL禁止了OSPF流量，或者接口被PASSIVE OSPF通常使用组播地址 224.0.0.5 来发送Hello包，如果被阻止，OSPF邻居无法建立。

检查命令有：display ip int bri , display cu , display ACL.

11.OSPF的报文Hello/Hello dead 间隔不匹配

12.https://support.huawei.com/enterprise/zh/knowledge/EKB1000006403

## 5.10 动态路由引入其他路由写法

**写法1:专门引入其他路由**

Import route 其他路由协议

引入isis

import-route isis

引入静态路由

impO-route static

引入直连路由

import-route direct

**写法2:只能引入缺省路由**

default-route-advertise

# 链路聚合

## 聚合分类

### 手动聚合

所有聚合的物理口都能转发数据

### 自动聚合

物理口分2类：活动口、非活动口

处于活动口的物理接口转发数据

## 自动聚合的交换机有主从关系

主交换机的作用：确定活动口

主交换机竞选过程：

先比较系统优先级，越小越优先，系统默认（32768）

优先级相同时，比较Mac地址，越小越优先

主交换机选择活动口的过程：

先比较端口优先级，越小越优先（端口默认32768）

优先级相同时，比较接口号，越小越优先

注意：

链路聚合中的系统优先级和接口优先级数值，没有要求，合理即可

## 聚合口数据负载分担方式

### 基于数据包负载分担

每个数据包通过不同的链路发送

### 基于数据流负载分担

数据流：对应一次完整通讯

## 负载分担的调度算法

* 基于源IP的算法
* 基于目的IP的算法
* 基于源Mac的算法
* 基于源和目的IP的算法
* 基于源和目的Mac的算法

## 链路聚合命令

命令1：interface eth-trunk 1

Trunkport g 0/0/1 to 0/0/2

命令2：进入接口视图 eth-trunk 1

# 堆叠和集群

## 概念

多个物理设备组成1台高性能的虚拟设备

一般华为的s5720以上支持堆叠，一般关键位置的交换机使用堆叠，核心位置用集群

对交换机来说：堆叠可以多台，集群只支持2台

## 物联网交换机分类

1. 主交换机master

只有一台，管理所有的配置。把所有的配置、系统都会下发到备交换机、从交换机

1. 备交换机backup

只有一台，备份主交换机所有的配置、系统

1. 从交换机slave

可以有多台，负责数据转发

华为分为三类（主、备、从）；H3C分两类（主、备）

### 主交换机选举过程

1. 比较开机时间

开机时间小于20s ，认为开机时间一样

1. 开机时间相同，比较优先级，越大越优先
2. 优先级相同，比较Mac地址，越小越优先

## 堆叠分裂

堆叠分裂后的检测，需要把失败的堆叠系统所有接口关闭

### MAD

多主检测MAD（Multi-Active Detection）：一种检测和处理堆叠分裂的协议，链路故障导致堆叠系统分裂后，MAD可以实现堆叠分裂的检测、冲突处理和故障恢复，降低堆叠分裂对业务的影响。

#### 检测方式

* 直连检测

堆叠交换机单独准备检测线路

* 代理检测

利用正常数据通讯链路，通过与第三方设备通讯、检测

#### MAD冲突处理机制

使用MAD报文进行MAD竞争，竞争结果为堆叠系统处于Detect状态或者Recovery状态

* Detect：竞争成功，堆叠系统将处于正常工作状态。
* Recovery：竞争失败，堆叠系统将状态处于禁用状态，关闭除手动配置的保留端口以外的其它所有物理端口。

## 堆叠升级

堆叠升级方式有三种：智能升级、传统升级和平滑升级。

### 智能升级：

堆叠建立或者新的交换机加入堆叠时会自动和主交换机的版本进行同步。

### 传统升级：

和普通设备升级一样，指定下次启动版本，重启整个堆叠系统进行升级，会造成较长时间的业务中断。

### 平滑升级：

将堆叠系统划分成为active、backup区域，可以分区域升级，整个堆叠系统的上下行采用备份组网，主、备链路分别处于active、backup区域，可以实现升级时的业务不中断。

## 堆叠配置

### 堆叠ID，堆叠编号

可以手动配置，也可以由主交换机自动分配

默认的堆叠ID = 0

### 堆叠连接的接口

需要使用专用堆叠口，堆叠线

堆叠口至少万兆速率

堆叠使用虚拟网卡，实现堆叠数据的发送和接收

堆叠虚拟口必须是2个：stack-port n/1和stack-port n/2，n是堆叠ID

堆叠连线时，必须交换1的stack-port n/1，连接交换2的stack-port n/2。

### 堆叠连接的方式

1. 链式连接
2. 环形连接

建议连接，1个堆叠线故障，不影响所有交换机堆叠通讯

### 配置过程

1. 不要连线，单独配置堆叠信息
2. 先改堆叠ID
3. 再改堆叠优先级
4. 创建堆叠虚拟口，并添加物理口
5. 保存并关机，再连线
6. 按照优先级顺序，依次开机，必须保证前机堆叠启动完毕，再启动开机

## 堆叠配置命令

1、关闭物理接口 ---h3c要求的

物理接口至少是10G类型

interface Ten-GigabitEthernet 1/0/49

shutdown

interface Ten-GigabitEthernet 1/0/50

shutdown

2、创建堆叠虚拟口，物理口加入堆叠虚拟口

irf-port 1/1

port group interface Ten-GigabitEthernet1/0/49

irf-port 1/2

port group interface Ten-GigabitEthernet1/0/50

3、修改堆叠优先级和堆叠系统ID

irf member 1 priority 32

irf member 1 remember 2 --系统ID可以由主交换自动分配

4、开启物理接口

5、激活irf配置

irf-port-configuration active

6、所有交换机断电，连线

连线时，必须是：sw1的irf-port 1/1 连接sw2的irf-port 1/2

7、按照优先级从大到小，依次开机，必须保证前机启动完毕再启动后机

8、查看堆叠系统信息

display irf configuration

display irf

9、堆叠设备跨物理机配置聚合口

interface Bridge-Aggregation1

quit

interface GigabitEthernet1/0/1

port link-aggregation group 1

interface GigabitEthernet3/0/1

port link-aggregation group 1

display link-aggregation verbose

## 集群

集群：是高端的堆叠

### 概念

* 集群中的单台交换机称为集群成员交换机，按照功能不同，可以分为两种角色：

主交换机（Master）：主交换机，即Master，负责管理整个集群。

备交换机（Standby）：备交换机，即Standby，是主交换机的备份交换机。

* 集群ID：即CSS ID，用来标识成员交换机，集群中成员交换机的集群ID是唯一的。
* CSS Link：集群链路，专门用于组建集群，实现主交换机和备交换机之间数据通信。
* 集群优先级：即CSS Priority，主要用于角色选举过程中确定成员交换机的角色。优先级值越大优先级越高。

### 集群组建连接办法

* 使用主控板的集群口

主交换的主用主控板，是使用中的主控板

备交换的主用主控板，是首选的备用主控板

* 使用业务板的集群口

# ACL（Access Control List，访问控制列表）

## ACL概述;

ACL——访问控制列表是由一条或多条规则组成的集合。每条规则描述报文匹配条件（报文的源地址、目的地址、端口号等）的判断语句，设备基于这些规则进行报文匹配，可以过滤出特定的报文。

## ACL两大作用：

访问控制——配置一张ACL列表，列表包含设置好的规则，之后所有的流量按照对应的规则进行执行，允许，拒绝。

抓取感兴趣流量——ACL的另一个作用就是和其他服务结合，ACL负责按照事先规定的规则抓取流量。而其他服务对匹配到流量执行相应的动作。

## 应用层常见的协议端口号

http协议： TCP 80

https协议： TCP 443

FTP协议：控制端口 TCP 21（客户端连接、控制指令）

数据端口，主动型FTP服务器用TCP 20

被动型FTP服务器用TCP随机口（大于1024）

SSH协议：TCP 22

Telnet协议：TCP 23

协议RDP（远程桌面协议）：TCP 3389

MySQL数据库端口号：TCP 3306

Mmssql数据库端口号：TCP 1433

Oracle数据库端口号：TCP 1521

DHCP服务器端口号：UDP 67

DHCP客户端端口号：UDP 68

DNS服务器端口号：UDP 53，接收客户端查询数据用的端口

TCP 53，负责2个DNS服务器同步数据

## ACL分类

### 基本ACL

* 规则链编号:2000~2999。仅使用报文的源IP地址、分片信息和生效时间段信息来定义规则。
* 只能通过源IP来识别数据（源IP可以分为3类）
  + 源网段 写法：网段 反向掩码
  + 单个源IP 写法：IP地址
  + 任意源IP 写法：any

### 高级ACL

* 规则链编号:3000~3999。可使用IPv4报文的源IP地址、目的IP地址、IP协议类型、ICMP类型、TCP源/目的端口号、UDP源/目的端口号、生效时间段等来定义规则。
* 识别数据方式：源或目标IP、源或目标端口、协议

数据五元组：源[IP地址](https://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80/150859?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BA%94%E5%85%83%E7%BB%84/_blank)，[源端口](https://baike.baidu.com/item/%E6%BA%90%E7%AB%AF%E5%8F%A3/8743496?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BA%94%E5%85%83%E7%BB%84/_blank)，目的IP地址，目的端口和传输层协议

## ACL工作原理

1.检查数据是否匹配第一条规则，匹配时，按照规则设定，允许或拒绝通过

2.不匹配第一条，则检查是否匹配后续规则

3.匹配某条规则，按照该规则处理数据，不再检查后续规则，该操作也叫命中即停止

4.不匹配任何规则时，按照默认规则处理（华为默认规则是放通一切）

匹配原则：一旦命中即停止匹配。

## ACL的匹配顺序

华为设备支持两种匹配顺序：自动排序（auto模式）和配置顺序（config模式）。缺省的ACL匹配顺序是config模式。

自动排序，是指系统使用“深度优先”的原则，将规则按照精确度从高到低进行排序，并按照精确度从高到低的顺序进行报文匹配。

配置顺序，系统按照ACL规则编号从小到大的顺序进行报文匹配，规则编号越小越容易被匹配。——这个就是我们前面提到的匹配顺序。

如果后面又添加了一条规则，则这条规则会被加入到相应的位置，报文仍然会按照从小到大的顺序进行匹配。

## ACL应用步骤

1.创建规则链

2.规则链内创建各种具体规则

3.在各个功能内部应用

交给traffic-filter功能在接口上过滤数据，分inbound（入方向）、outbound（出方向）方向不要搞错！

ACL用于识别数据，需要在其他功能应用

# AAA

## 概述

Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

## 常见架构

包括用户、NAS（Network Access Server）、AAA服务器（AAA Server）。

## 认证方式

不认证，本地认证，远端认证。

## 授权方式

不授权，本地授权，远端授权。

## 计费方式

不计费，远端计费。

## 网络设备的权限划分

* 权限等级0：一般叫来宾级，基本没有任何能力
* 权限等级1：监控级，能查看设备的基本信息，大多数的display无法查看
* 权限等级2：管理级，能查看所有配置，能修改部分配置
* 权限等级3-15：超级管理级，能做任何操作

## 实现协议

RADIUS：Remote Authentication Dial In User Service，[远程用户](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%94%A8%E6%88%B7/1858887?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)拨号认证系统由RFC2865，RFC2866定义，是应用最广泛的[AAA协议](https://baike.baidu.com/item/AAA%E5%8D%8F%E8%AE%AE/0?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)。AAA是一种管理框架，因此，它可以用多种协议来实现。在实践中，人们最常使用远程访问拨号用户服务（Remote Authentication Dial In User Service，RADIUS）来实现AAA。

RADIUS是一种[C/S结构](https://baike.baidu.com/item/C/S%E7%BB%93%E6%9E%84/4868476?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)的协议，它的[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF/101081?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)最初就是[NAS](https://baike.baidu.com/item/NAS/0?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)（Net Access Server）[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)，任何运行RADIUS客户端软件的计算机都可以成为RADIUS的客户端。[RADIUS协议](https://baike.baidu.com/item/RADIUS%E5%8D%8F%E8%AE%AE/1331757?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)认证机制灵活，可以采用PAP、[CHAP](https://baike.baidu.com/item/CHAP/0?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/RADIUS/_blank)或者Unix登录认证等多种方式。RADIUS是一种可扩展的协议，它进行的全部工作都是基于Attribute-Length-Value的向量进行的。RADIUS也支持厂商扩充厂家专有属性。

# Nat（Network Address Translation，网络地址转换）

## Nat简介

NAT英文全称是“Network Address Translation”，中文意思是“网络地址转换”，它是一个IETF(Internet Engineering Task Force, Internet工程任务组)标准，允许一个整体机构以一个公用IP（Internet Protocol）地址出现在Internet上.顾名思义，它是一种把内部私有网络地址（IP地址）翻译成合法网络IP地址的技术

## 出口路由器必须配置的功能

Nat、ACL、缺省路由（下一跳指向运营商）

缺省路由必须引入到内部的动态路由环境

## Nat分类

1.SNAT（源地址转换）

(1)特点：把数据包中的源IP转换

(2)用法：一般在从内→外的上网行为中

2.DNAT（目标地址转换）

(1)特点：把数据包中的目标IP转换

(2)用法：一般在从外→内的服务器

## 转换方式

### 静态nat

* 特点：私网IP和公网IP是固定的一对一转换
* 使用场景：

政府、部分公司为内部服务器使用该nat，允许外网用户访问；一般只会针对对外开放的服务器。

静态nat可以实现双向地址转换

### 动态nat

* 特点：私网IP和公网IP是临时的一对一转换

### NAPT（属于SNAT转换）

* 特点：多个私网IP可以对应一个公网IP

但出口的公网IP不能做nat转换，，即需要2个公网IP

### EasyIP（属于SNAT转换）

* 特点：多个私网IP可以对应一个公网IP

可以用出口的公网IP做nat转换，即需要1个公网IP

### Nat server（属于DNAT转换）

注意：路由器使用公网端口号，区分内部服务器和具体业务

无论哪种nat配置，路由器都会生成nat映射表记录

作用：为了正确回传数据

查看命令：display nat session all

注意：

NAPT、Easyip 只允许从内→外通讯

Nat server 用于从外→内服务。外网用户访问时，需要用公网IP公网端口号组合

# 网络服务与应用

## FTP（File Transfer Protocol，文件传输协议）

### 概述

FTP采用典型的C/S架构（即服务器端与客户端模型），客户端与服务器端建立TCP连接之后即可实现文件的上传、下载。

### 传输模式

#### ASCII模式

传输文本文件（TXT、LOG、CFG ）时会对文本内容进行编码方式转换，提高传输效率。当传输网络设备的配置文件、日志文件时推荐使用该模式。

#### Binary（二进制）模式

非文本文件（cc、BIN、EXE、PNG），如图片、可执行程序等，以二进制直接传输原始文件内容。当传输网络设备的版本文件时推荐使用该模式。

### 工作方式

#### 主动模式（PORT）

FTP客户端首先和FTP Server 的TCP21端口建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送PORT命令。PORT命令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的TCP 20端口发送数据。FTP server必须和客户端建立一个新的连接用来传送数据。

#### 被动模式（PASV）

在建立控制通道的时候和Standard模式类似，当客户端通过这个通道发送PASV命令的时候，FTP server打开一个位于1024和5000之间的随机高位端口并且通知客户端在这个端口上传送数据的请求，然后FTP server将通过这个端口进行数据的传送，这个时候FTP server不再需要建立一个新的和客户端之间的连接。

### FTP的作用

路由交换利用FTP，可以保存配置文件

### FTP服务器保存路由配置步骤

路由器save保存配置

用dir命令查看路由器保存的配置文件名

使用put命令+文件名进行上传

## 远程管理

### Telnet（Telecommunication Network Protocol）

起源于1969年的ARPANET，是一种最早的Internet应用，Telnet提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，然后再通过Telnet的方式远程登录到网络上的其他主机上去，而不需要为每一台主机都连接一个硬件终端，然后对设备进行配置和管理。

### SSH（Secure Shell）

安全外壳协议是一种在不安全网络上用于安全远程登录和其他安全网络服务的协议。

### Telnet和SSH的区别

#### 安全性

* SSH是一种加密的协议，可以向服务器传输加密的数据，以防止数据被窃听或篡改。
* Telnet是一种明文协议，所有的数据都是以明文形式传输，所以对于敏感信息的传输是不安全的。

#### 身份验证

* SSH支持多种身份验证方式，如使用用户名和密码、SSH密钥等。
* Telnet只支持基于用户名和密码的身份验证。

#### 端口

* SSH使用的端口号是22，
* Telnet使用的端口号是23。

#### 功能

* SSH比Telnet更强大，除了远程登录外，SSH还支持文件传输、端口转发、远程命令执行等功能。
* Telnet只能提供基本的远程登录功能。

## DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）

### 概述

通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配IP地址，使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。

### DHCP的作用

### 为客户机分发IP地址，子网掩码，网关，DNS服务，租期等参数

### 工作原理

1. 客户端发送DHCP discover 广播包，找DHCP服务器
2. DHCP服务器用DHCP offer 单播包回复客户端，报文中携带客户端可用的IP地址且DHCP服务器把IP地址锁定
3. 客户端发送DHCP request 广播包，确认使用哪台服务器提供的地址
4. 选定的DHCP服务器发送DHCP ack 单播包和客户端签订IP租约

注意：如果DHCP服务器没有可分配的IP时，用DHCP nck单播包回复

### 客户端IP续租过程

1. 租期达到50%，客户端用DHCP request 单播包，向特定的DHCP服务器续租
2. 租期达到87.5%，客户端用DHCP request 广播包，向所有的DHCP服务器续租
3. 租期达到100%，客户端释放IP，重启开始获取IP4个过程

注意：客户端获取不到IP或IP冲突时，客户端自动使用169.254.x.x网段地址，客户端会每隔5分钟，经历IP获取的4个过程

### 配置模式

#### 接口DHCP模式

在接口下配置，客户端获取的IP，必须和接口IP在同网段；网关IP=接口IP

DNS服务器IP需要手动配置

#### 全局DHCP模式

在系统视图下创建地址池，并设置分配的IP网段

网关IP和DNS服务器IP，需要手动配置

注意：无论何种模式，DHCP配置改动，客户端必须更新租约才能获取变化

### 中继服务器

#### 使用场景

客户端用广播查找同网段中的DHCP服务器，如果客户端与DHCP在不同网段，客户端需借助DHCP中继服务器。

#### 作用

客户端跨网段访间DHCP服务器获取ip 。三层设备可以充当DHCP中继服务器

#### 配置步骤

1. 系统视图开启DHCP功能
2. 连核终端的接口启用DHCP中继
3. 指定DHCP服务器ip
4. DHCP服务器必须要有客户端的路由信息

### DHCP的优点

* 可靠的 IP 地址配置。DHCP 可以最大程度地减少由手动 IP 地址配置引起的配置错误（例如拼写错误），或者由于将一个 IP 地址同时分配给多台计算机而导致的地址冲突。
* DHCP 提供了以下功能来减少网络管理工作：
  + 集中的和自动化的 TCP/IP 配置。
  + 能够从一个中心位置定义 TCP/IP 配置。
  + 能够通过 DHCP 选项分配一系列其他 TCP/IP 配置值。
  + 高效处理必须频繁更新的客户端的 IP 地址更改，例如，移动到无线网络上不同位置的便携式设备的 IP 地址更改。
  + 使用 DHCP 中继代理转发初始 DHCP 消息，从而无需在每个子网上使用 DHCP 服务器。

### 与WiFi路由器有关的DHCP

WiFi路由器背板分2种接口类型

WAN口，连接光猫、运营商

LAN口，连接内部PC

用WiFi路由器做网线数量扩展

如果连接的是WAN口，需要在WiFi路由器配置界面，把WAN口IP设置为自动获得

如果连接的是LAN口，需要在WiFi路由器配置界面，关闭内置DHCP

WiFi路由器内置DHCP默认开启，只对LAN口有效

## [DNS（Domain Name System，域名解析系统）](https://blog.csdn.net/hy199707/article/details/135526090)

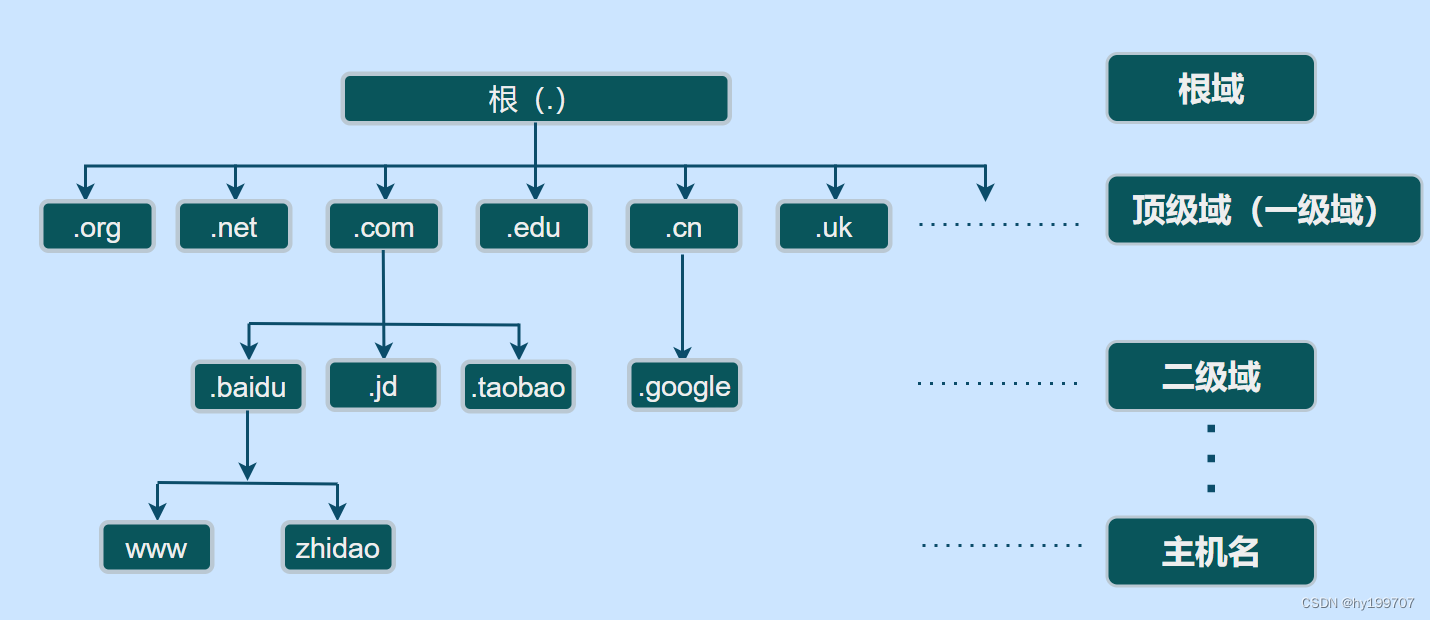
### 定义

DNS解析是指当用户或应用程序通过浏览器、电子邮件客户端等访问某个域名时，系统会通过DNS协议查询对应的IP地址的过程。这个过程涉及从本地缓存、递归DNS服务器到权威DNS服务器等一系列查询操作，最终获取到域名映射的实际IP地址。

### DNS解析的作用

1. 易于记忆与访问
2. 分布式管理
3. 负载均衡和冗余备份
4. 地理位置优化
5. 安全性和稳定性增强

### 域名体系结构



### 查询方式

#### 递归查询

**用于客户机向 DNS 服务器查询。**

递归查询要求DNS服务器必须向客户端返回一个最终结果，即域名对应的IP地址。如果DNS服务器本身没有该域名的记录，则它会代表客户端发起一系列查询，直到找到权威DNS服务器并获得最终答案，将返回的查询结果提交给客户机。

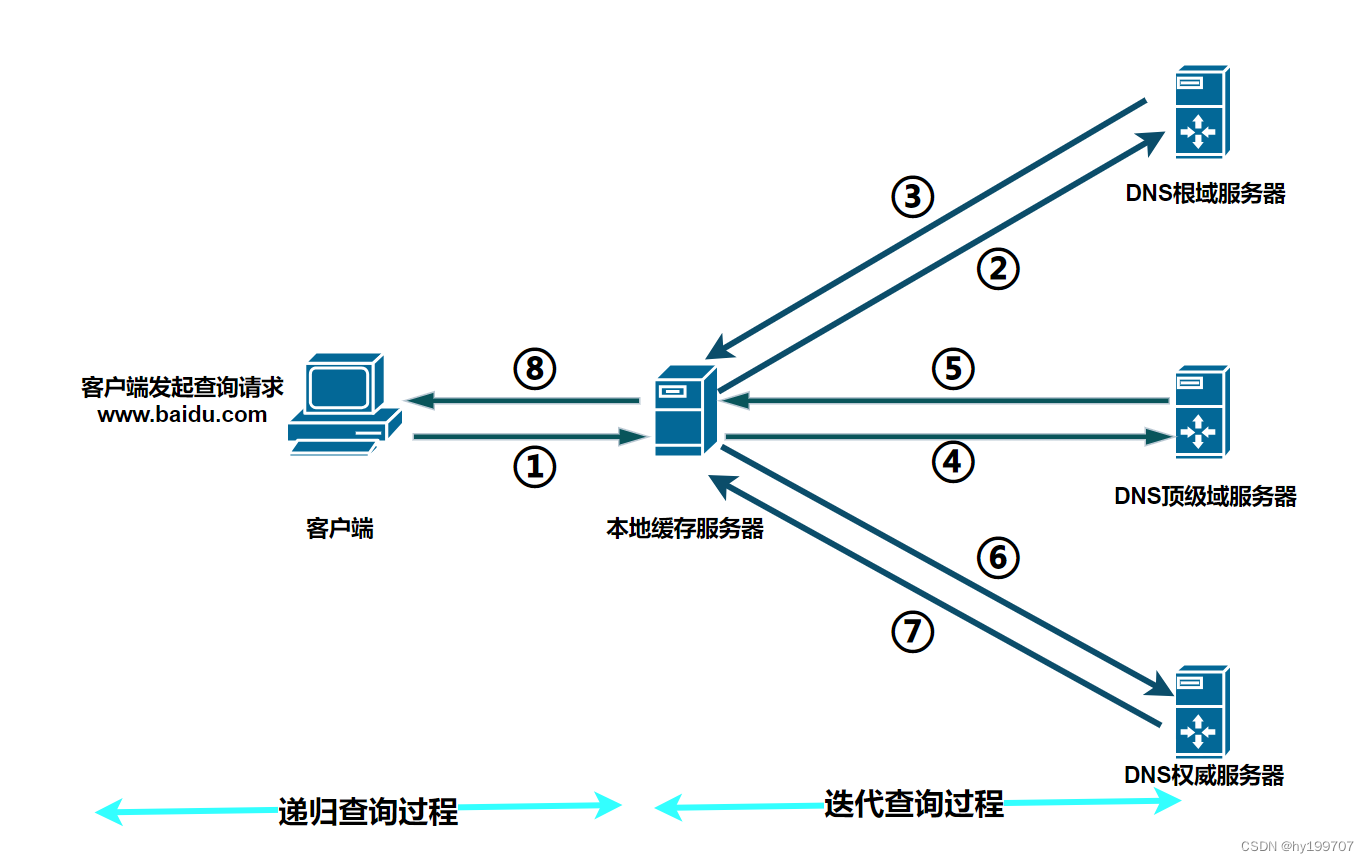
#### 迭代查询

**用于 DNS 服务器向其它 DNS 服务器查询。**

在迭代查询中，当DNS服务器接收到查询请求时，它并不会承诺直接给出最终答案，而是提供其他可以查询的DNS服务器地址。这意味着DNS服务器会告诉客户端“我无法给你答案，但你可以去问这个DNS服务器”，并将指向更接近答案的下一级DNS服务器地址发送给客户端，客户机再向这台DNS服务器提交请求，依次循环直到返回查询的结果为止。

简而言之，在递归查询中，DNS服务器承担了所有查询工作，而客户端只需要等待最终结果；在迭代查询中，客户端或其代理DNS服务器需要进行多次查询操作，逐步逼近答案。

### DNS域名解析过程



1.客户端向本地缓存服务器或自定义服务器发出请求，有结果直接返回信息，没有则进行下一步

2.向根服务器发出请求，根服务器无法解析

3.根服务器反馈信息，让本地缓存服务器寻找顶级域服务器

4.向顶级服务器发出请求，顶级服务器无法解析

5.顶级域服务器反馈信息，让本地缓存服务器寻找二级域服务器

6.向二级域服务器发出请求，二级域服务器可以解析，那它就是该地址的权威服务器

7.二级域服务器（权威服务器）向本地服务器返回解析结果

8.本地缓存服务器得到结果后向客户端反馈信息

一旦本地DNS服务器获得了www.baidu.com的IP地址，它不仅将这个结果返回给客户端，还会将其缓存在本地，以便未来对该域名的请求可以直接使用缓存的结果。客户端拿到IP地址后，就可以通过TCP/IP协议栈建立与目标服务器的连接，从而访问网站或服务。

## [HTTP（Hypertext Transfer Protocol，超文本传输协议）](https://blog.csdn.net/SunshineTan/article/details/104511085/)

### 特点

1. 基于TCP/IP通信协议。
2. 默认端口80，可以改为8080或者其他端口。
3. 客户端/服务端（C/S）的架构模型：请求响应模型，一次请求对应一次响应
4. HTTP是无连接的，即限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接。采用这种方式可以节省传输时间。
5. HTTP是媒体独立的：只要C/S知道如何处理的数据内容，任何类型的数据都可以通过HTTP发送。客户端以及服务器指定使用适合的MIME-type内容类型。
6. 无状态：每次请求之间相互独立，不能交互数据。

### URL（UniformResourceLocator, 统一资源定位符）

是一种特殊类型的URI，包含了用于查找某个资源的足够的信息URL, 是互联网上用来标识某一处资源的地址。

### HTTP方法

#### DELETE（删除）

场景：用于删除资源

#### GET（获取）

场景：获取资源。

#### OPTIONS（预检请求）

场景：OPTIONS 方法的首要目的是 Priflight Request（预检请求）。

浏览器必须先使用OPTIONS方法发起一个预检请求，从而获知服务器是否允许该跨域请求：如果允许，就发送带数据的真实请求；如果不允许，则阻止发送带数据的真实请求。

#### POST（新增）

场景：提交、添加资源。大量检索参数的获取资源。

#### PUT（修改）

场景：PUT 与 PATCH 方法都是用于更新资源。

#### PATCH（局部更新）

场景：PUT 与 PATCH 方法都是用于更新资源；PATCH是对 PUT 方法的补充，用来对已知资源进行局部更新 。

#### HEAD

场景：获取报头信息，例如检查 cache 是否被修改，是否过期？

#### TRACE

场景：回显服务器收到的请求，主要用于测试或诊断。

#### CONNECT

场景：HTTP/1.1 协议中预留给能够将连接改为管道方式的代理服务器。

#### REST API规范

### HTTP状态码

1\*\* 指示信息，表示请求已接收，继续处理

2\*\* 成功，操作被成功接收并处理

3\*\* 重定向，需要进一步的操作以完成请求

4\*\* 客户端错误，请求包含语法错误或无法完成请求

5\*\* 服务器错误，服务器在处理请求的过程中发生了错误

### HTTP与HTTPS

#### 区别

http和https使用的是完全不同的连接方式,用的端口也不一样,前者是80,后者是443。http的连接很简单,是无状态的。HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全。

HTTPS是一种通过计算机网络进行安全通信的传输协议。HTTPS经由HTTP进行通信，但利用SSL/TLS来加密数据包。HTTPS开发的主要目的，是提供对网站服务器的身份认证，保护交换数据的隐私与完整性。

#### 注意

SSL（安全套接层，secure sockets layer）

TLS（传输层安全，transport layer security），是SSL的继任者。

安全层其实就是在明文的上层和TCP层之间加上一层加密，这样就保证上层信息传输的安全。

### HTTP工作原理

1. 客户端连接到Web服务器

一个HTTP客户端，通常是浏览器，与Web服务器的HTTP端口（默认为80）建立一个TCP套接字连接。例如，http://www.oakcms.cn。

1. 发送HTTP请求

通过TCP套接字，客户端向Web服务器发送一个文本的请求报文，一个请求报文由请求行、请求头部、空行和请求数据4部分组成。

1. 服务器接受请求并返回HTTP响应

Web服务器解析请求，定位请求资源。服务器将资源复本写到TCP套接字，由客户端读取。一个响应由状态行、响应头部、空行和响应数据4部分组成。

1. 释放连接TCP连接

若connection 模式为close，则服务器主动关闭TCP连接，客户端被动关闭连接，释放TCP连接;若connection 模式为keepalive，则该连接会保持一段时间，在该时间内可以继续接收请求;

1. 客户端浏览器解析HTML内容

客户端浏览器首先解析状态行，查看表明请求是否成功的状态代码。然后解析每一个响应头，响应头告知以下为若干字节的HTML文档和文档的字符集。客户端浏览器读取响应数据HTML，根据HTML的语法对其进行格式化，并在浏览器窗口中显示。

例如：在浏览器地址栏键入URL，按下回车之后会经历以下流程：

a. 浏览器向 DNS 服务器请求解析该 URL 中的域名所对应的 IP 地址;

b. 解析出 IP 地址后，根据该 IP 地址和默认端口 80，和服务器建立TCP连接;

c. 浏览器发出读取文件(URL 中域名后面部分对应的文件)的HTTP 请求，该请求报文作为 TCP 三次握手的第三个报文的数据发送给服务器;

d. 服务器对浏览器请求作出响应，并把对应的 html 文本发送给浏览器;

e. 释放 TCP连接;

f. 浏览器将该 html 文本并显示内容;

## NTP（Network Time Protocol）

### 定义

NTP是用来使计算机时间同步化的一种协议，全称是Network Time Protocol。它可以使计算机对其服务器或时钟源做同步化，可以提供高精准度的时间校正。它可以在大规模的设备范围内同步矫正时间到几ms级别的精度，在网络稳定的局域网内，精度甚至可以达到微秒级别。

### NTP工作原理

NTP通过原子钟、天文台、卫星或者互联网上获取准确的时间来源，并通过不同的等级对服务器进行分层来同步时间。按照离外部UTC时间源的远近，NTP将服务器归入不同的层(Stratum)中，最顶层为有外部UTC接入的Stratum-1，而Stratum-2就会从Stratum-1获取时间，以此类推，最大层数为15层。因此，层数越大时间准确度相对越低，层数16表示未同步。

### 系统时钟的同步流程

1. NTP客户端在T1时刻发送一个NTP请求报文给NTP服务器，该请求报文携带离开NTP客户端时的时间戳T1。
2. NTP请求报文到达NTP服务器，此时NTP服务器的时刻为T2。
3. NTP服务器处理之后，于T3时刻发出NTP应答报文。该应答报文中携带离开NTP客户端时的时间戳T1、到达NTP服务器时的时间戳T2、离开NTP服务器时的时间戳T3。
4. NTP客户端在T4时刻接收到该应答报文。

### NTPD

NTPD程序是一个操作系统守护进程，它将系统时钟同步到远程NTP时间服务器或本地参考时钟，是RFC 5905定义的NTPv4的完整实现，同时兼容RFC 1305定义的v3以及RFC 1059和RFC 1119定义的v1和v2。该程序可以在多种模式下运行，包括客户机/服务器、对称和广播模式等

### 9.6.5 全球知名的NTP服务器地址：

1. pool.ntp.org：这是一个全球分布的时间服务器网络，可以从中选择最接近你的服务器进行同步。
2. time.nist.gov：美国国家标准与技术研究院的NTP服务器。
3. time.google.com：Google提供的NTP服务器。
4. time.windows.com：微软提供的NTP服务器。

# [WLAN](https://blog.csdn.net/wh940830165/article/details/137856701)

## 概念

WLAN即Wireless LAN（无线局域网），是指通过无线技术构建的无线局域网络。WLAN广义上是指以无线电波、激光、红外线等无线信号来代替有线局域网中的部分或全部传输介质所构成的网络。

## 组网架构

### 有线侧

AP上行到Internet的网络使用以太网协议

#### AC - AP组网方式（二层组网和三层组网）

二层是指AP和AC之间是二层组网，三层是指AC和AP之间是三层组网；

二层组网AP可以通过二层广播，或者DHCP过程，即插即用上线；

三层网络下，AP无法直接发现AC，需要通过DHCP或DNS方式动态发现，或者配置静态IP。

AP用广播查找AC。若AP和AC不在同一个网段只能用单播通讯，AP需要知道AC地址

借助DHCP的参数：option43，指明AC的地址，让AP获得AC的IP

注意：ap数量大时，无论ac和ap是否在同网段，建议配置option43

#### AC连接方式（直连式组网和旁挂式组网）

直连式组网：直连式组网可以认为AP、AC与上层网络串联在一起，所有数据必须通过AC到达上层网络。直连式组网中AC同时扮演AC和汇聚交换机的功能，AP的数据业务和管理业务都由AC集中转发和处理。

旁挂式组网：旁挂式组网，AC旁挂在AP与上行网络的直连网络中，不再直接连接AP。旁挂式组网，AC旁挂在AP与上行网络的直连网络上，AP的业务数据可以不经AC而直接到达上行网络 。

注意：相邻AP无线覆盖面需要叠加，但需要注意信道不要冲突

相邻AP的信道差值大于等于5

#### CAPWAP（Control And Provisioning of Wireless Access Points Protocol Specification，无线接入点控制和配置协议）

该协议定义了AC如何对AP进行管理、业务配置，即AC与AP间首先会建立CAPWAP隧道，然后AC通过CAPWAP隧道来实现对AP的集中管理和控制。

CAPWAP是基于UDP进行传输的应用层协议。

默认CAPWAP通讯的目的IP是广播地址，要求AC和AP在同网段

功能：

AP与AC间的状态维护。

 AC通过CAPWAP隧道对AP进行管理、业务配置下发。

当采用隧道转发模式时，AP将STA发出的数据通过CAPWAP隧道实现与AC之间的交互。

#### POE与POE交换机

PoE：是指通过以太网网络进行供电，也被称为基于局域网的供电系统PoL或有源以太网

 PoE允许电功率通过传输数据的线路或空闲线路传输到终端设备。

 在WLAN网络中，可以通过PoE交换机对AP设备进行供电。

#### AC和AF的高可靠性

都需要配置VRRP

##### AC高可靠性

2个ac用vrrp虚拟ip和ap通讯，需要修改2项：

dhcp的option43参数需要指向vrrp虚拟ip

ac的capwap隧道配置不能用vlanif接口，改用vrrp虚拟ip

2个AC必须手动配置所有内容，ac的配置必须一致

高可靠性如果只靠VRRP实现，主AC故障后，AP需要重新在备用AC注册、获取配置

高可靠性还需要用到 HSB（热备份）

HSB的作用；同步ap信息

HSB分2部分配置：

a、建立HSB服务

作用：建立HSB连接

b、建立HSB组

作用：同步ap信息、用户入网信息、dhcp信息

HSB配置步骤：

a、先配置VRRP，给HSB准备环境

b、创建HSB服务，主备AC间建立备份通道

c、创建HSB组，绑定vrrp和指定同步内容

d、启动HSB

注意：HSB也分主备设备，主设备=vrrp的master

##### AF（防火墙）的高可靠性

必须满足一定条件：2个AF必须物理配置、系统版本完全一致

a、准备心跳线

作用：监视对端是否存活

通常使用物理直连

b、AF高可用工作模式有2种

1)主备模式

2)负载分担模式，也叫主主模式

c、AF高可用可以自动同步一些配置：安全策略、NAT策略、策略使用的操作对象、会话表等

##### vlan pool，vlan池

作用：在大量终端环境中，自动把终端分散到不同的业务vlan，降低广播包数量和影响范围

调度方式，有2种调度算法：

a、顺序分配算法，也叫轮询

用户上线按顺序加入不同的业务vlan，获取不同网段ip

好处：各个业务vlan的用户数一致

缺点：用户重新上线会加入其他vlan

b、hash算法

根据用户的mac地址hash计算，分配到不同的业务vlan

好处：用户始终加入固定的业务vlan

缺点：各个业务vlan的用户数有差距

##### 准入控制

作用：入网前先做认证，通过后才能入网

准入控制认证方式：

a、802.1X认证

PC需要安装专门的软件

b、mac认证

需要手动把设备mac地址，添加到认证服务器

c、portal认证，即web页面认证

### 无线侧

STA到AP之间的网络使用802.11协议。

#### FAT AP (胖AP)架构

适用于家庭，独立工作，需单独配置，功能较为单一，成本低。独立完成用户接入、认证、数据安全、业务转发和QoS等功能。

#### AC+FIT AP (瘦AP)架构

适用于大中型企业，需要配合AC使用，由AC统一管理和配置，功能丰富，对网络维护人员的技能要求高。用户接入、AP上线、认证、路由、AP管理、安全协议、QoS等功能需要同AC配合完成。

#### BSS (Basic Service Set)

无线网络的基本服务单元，通常由一个AP和若干STA组成，BSS是802.11网络的基本结构。由于无线介质共享性，BSS中报文收发需携带BSSID（MAC地址）。

#### 基本服务集标识符BSSID（Basic Service Set Identifier）

AP上的数据链路层MAC地址。

终端要发现和找到AP，需要通过AP的一个身份标识，这个身份标识就是BSSID。

为了区分BSS，要求每个BSS都有唯一的BSSID，因此使用AP的MAC地址来保证其唯一性。

#### 服务集标识符SSID（Service Set Identifier）

表示无线网络的标识，用来区分不同的无线网络。例如，当我们在笔记本电脑上搜索可接入无线网络时，显示出来的网络名称就是SSID。

如果一个空间部署了多个BSS，终端就会发现多个BSSID，只要选择加入的BSSID就行。但是做选择的是用户，为了使得AP的身份更容易辨识，则用一个字符串来作为AP的名字。这个字符串就是SSID。

#### 虚拟接入点VAP（Virtual Access Point）

是AP设备上虚拟出来的业务功能实体。用户可以在一个AP上创建不同的VAP来为不同的用户群体提供无线接入服务。VAP，叫虚拟AP，表示1个完整的无线配置、无线环境，每个物理AP可以有多个VAP。

## 无线配置步骤

1. 网络配置
2. AP上线。作用：AC识别AP
3. AC上配置无线功能（至少配置SSID、无线密码）

# 网络管理与运维

## 概念

网络管理是通过对网络中设备的管理，保证设备工作正常，使通信网络正常地运行，以提供高效、可靠和安全的通信服务，是通信网络的重要组成部分。

## 基本功能

1. 配置管理（Configuration Management）：配置管理负责监控网络的配置信息，使网络管理人员可以生成、查询和修改硬件、软件的运行参数和条件，并可以进行相关业务的配置。
2. 性能管理（Performance Management）：性能管理以网络性能为准则，保证在使用较少网络资源和具有较小时延的前提下，网络能够提供可靠、连续的通信能力。
3. 故障管理（Fault Management）：故障管理的主要目标是确保网络始终可用，并在发生故障时尽快将其修复。
4. 安全管理（Security Management）：安全管理可以保护网络和系统免受未经授权的访问和安全攻击。
5. 计费管理（Accounting Management）：记录用户使用网络资源的情况并核收费用，同时也统计网络的利用率。

## 管理方式

### 传统网络管理：

* Web网管方式：利用设备内置的Web服务器，为用户提供图形化的操作界面。用户需要从终端通过HTTPS（Hypertext Transfer Protocol Secure ，HTTPS 加密协定）登录到设备进行管理。
* CLI方式：用户利用设备提供的命令行，通过Console口、Telnet或SSH等方式登录到设备，对设备进行管理与维护。此方式可以实现对设备的精细化管理，但是要求用户熟悉命令行。
* 基于SNMP集中管理：SNMP（Simple Network Management Protocol，简单网络管理协议）。作用：收集设备运行的各种信息。
  + SNMP组成结构
    - 被监管设备，需要安装SNMP的代理程序
    - SNMP监控主机，收集被监控设备运行性能状态，通常保存在内置的MIB（信息管理库）
    - 查看客户端，查看监控主机收集到的设备信息一般通过浏览器访问监控主机。
  + SNMP版本划分
    - V1版，有5种报文类型
      * Get报文。作用：监控主机获取被监管设备信息。注意：v1版本中get内容是按照固定的顺序和格式获取
      * GetNext报文。获取下一项信息。
      * Response报文。作用：被监控设备回复自身的某项信息。
      * Set报文。作用：监控主机更改被监管设备的配置。
      * Trap报文。作用：被监控设备主动上报故障。
    - V2版本，在V1的基础上新增2种报文
      * GetBulk报文。作用：批量收集被监管设备信息
      * Inform报文。作用：和trap报文类似，但inform报文需要监控主机答复trap报文监控主机不需要回复。
    - V3版本，所有报文全部加密和身份验证

### 基于iMaster NCE的网络管理：

* iMaster NCE是集管理、控制、分析和AI智能功能于一体的网络自动化与智能化平台，包括四大关键能力：全生命周期自动化、基于大数据和AI的智能闭环、开放可编程使能场景化APP生态、超大容量全云化平台。
* iMaster NCE采用NETCONF（Network Configuration Protocol，网络配置协议）、RESTCONF等协议对设备下发配置，使用Telemetry监控网络流量。

# 广域网

## 概念

广域网是连接不同地区局域网的网络，通常所覆盖的范围从几十公里到几千公里。它能连接多个地区、城市和国家，或横跨几个洲提供远距离通信，形成国际性的远程网络。

## 广域网络设备基本角色

CE：用户端连接服务提供商的边缘设备。CE连接一个或多个PE，实现用户接入。

PE：服务提供商连接CE的边缘设备。PE同时连接CE和P设备，是重要的网络节点。

P：服务提供商不连接任何CE的设备。

## 运营商常见的协议

### PPP（Point-to-Point Protocol，点到点协议）

* 是一种常见的广域网数据链路层协议，主要用于在全双工的链路上进行点到点的数据传输封装。
* 只能用于点到点接口（串口），默认不能用于网口
* 该协议具有2种身份验证功能，

安全认证协议族PAP（Password Authentication Protocol，密码验证协议）

身份认证信息明文传输

CHAP（Challenge Handshake Authentication Protocol，挑战握手认证协议）

常用，认证信息密文

* 是协议簇，内部包含多种协议，分2层。

链路层协议，LCP（Link Control Protocol，链路控制协议），用于各种链路层参数的协商，例如最大接收单元，认证模式等。

网络层协议，NCP（Network Control Protocol，网络控制协议），用来和网络层其他协议互通。如IPCP（IP Control Protocol ，IP控制协议），用于各网络层参数的协商，更好地支持了网络层协议。

### PPPOE（PPP over Ethernet，以太网承载PPP协议）

是一种把PPP帧封装到以太网帧中的链路层协议。PPPoE可以使以太网网络中的多台主机连接到远端的宽带接入服务器。

作用：在普通网口运行PPP协议

常用于家庭宽带拨号上网

家庭宽带上行带宽=下行带宽/10

企业宽带上行带宽=下行带宽

### BGP（Border Gateway Protocol，边界网关协议）

BGP是一种实现自治系统AS之间的路由可达，并选择最佳路由的矢量性协议。

常用于运营商、IT大企业。也是动态路由协议，ospf重心是路由学习，bgp重心是路径控制

### MPLS（Multi-Protocol Label Switching，多协议标签交换）

主要用于VPN通讯、流量工程

VPN（Virtual Private Network，虚拟专用网）

企业中的作用：让互联网用户访问企业内部的资源

总部与分支之间互传数据

VPN可以企业自建，也可以购买运营商提供的MPLS服务

# SNMP，简单网络管路协议

作用：收集设备的运行信息

V1、v2缺点：明文传输‘

V3优点：密文传输

SNMP端口号：UDP161

v1的5种报文

Get报文，获取某种信息

Getnext报文，获取固定的下一项信息

Response报文，回复信息

Set报文，修改设备配置

Trap报文，故障、异常上报

# ipv6

## 概念：

IPV6地址由网络前缀和接口标识两个部分组成。网络前缀有n位，相当于IPv4地址中的网络ID；接口标识有（128-n）比特，相当于IPv4地址中的主机ID。网络前缀相当于IPV4中的网络位，用来标识和区分不同的网络范围，接口标识就还是在这个网络范围内去区分不同的主机。

## ipv6包头

* v6包头格式固定，基本包头+拓展包头。基本包头大小为40字节，扩展包头总是8 Byte长度的整数倍。扩展包的信息自动放在基本包头后面。扩展包头数据，除了“逐跳选项”扩展信息，需要每个路由器去读取，其他拓展信息路由器无需读取。
  + 扩展包头有6种类型

按照顺序固定不变：逐跳、目的选项、路由、分段、认证、封装、目的选项

只有目的选项扩展头可以用2次，其他只能用1次

只有逐跳扩展头，必须每个路由设备都要读取，其他扩展头只有源和目标设备读取

* v4包头中的分片信息被去除

v6的数据分片工作由发送端和接收端完成，中间路由器只转发不做任何分片操作。

Path MTU，叫做路径MTU

作用：发送到发送数据前，先探测整个链路最小的MTU，依次为依据进行拆包

## ipv6地址

### 格式

* IPv6地址的长度为128 bit。一般用冒号分割为8段，每一段16 bit，每一段内用十六进制表示。
* 简写要求：
  + 每一组是0000，可以用1个0表示
  + 多个连续的组，如果都是，用：：简写

注意: ：：只能简写一次

* 地址组成
  + 网络前缀，相当与v4的网络位

最长64位

* + 接口标识，相当于v4的主机位

一般都是64位

* + - 接口标识三种生成方法
      * 手工配置
      * 系统自动生成
      * 通过IEEE EUI-64规范生成
        + Mac地址转换成二进制格式
        + 正中间插入固定的16位长度内容：FFFE
        + 第7高位取反

### 分类

组播：

任播：接收方不是单一设备，接收离源最近的设备回复

单播：细分为3类

1. 全球单播地址

用于和运营商、互联网上通讯

相当于IPv4的公网IP

标准网段：200：：/3。但只用到2001：：/16和2002：：/16（用于v4到v6过渡）

1. 唯一本地地址

用于内部网络通讯

相当于IPv4的私网IP

标准网段：FC00：：/7。但只用到FD00：：/8

1. 链路本地地址

只能用在路由器的接口下，不能跨路由器的接口通讯

每一个使用IPv6的设备，必须配置、且自动配置的地址

标准网段：FE80：：/10

作用：邻居发现、ARP解析、v6地址无状态自动配置、动态路由源地址等

### 特殊地址

：：0/128缺省地址

：：1/128环回地址

### ipv6地址经历阶段

一个接口在发送IPv6报文之前要经历地址配置、DAD、地址解析这三个阶段

1. 用任何手段配置v6地址
2. 有v6地址后，自动执行DAD（重复地址检测）
3. 自动执行地址解析操作，代替arp协议，获取其他设备的Mac地址

注意：ipv6没有arp协议

接口配置ipv6时，ospfv3配置时，相邻路由器接口的ipv6地址可以不同网段

邻居间的

## ICMPv6

### 报文分类

**差错报文**：发现网络故障

差错消息用于报告在转发IPv6数据包过程中出现的错误，如常见的目的不可达、超时等等。

**信息报文：**获取网络信息

信息报文可以用来实现同一链路上节点间的通信和子网内的组播成员管理等。

### 新增功能

#### Path MTU发现

作用：发送数据包前，检测整条链路最小MTU

好处：路由器无需拆包、合包操作

#### 邻居请求、邻居确认。

邻居请求，用type135表示

邻居公告，用type136表示

作用：地址解析；实现DAD检测，代替arp协议

#### 路由器请求、路由器确认。

路由器请求，用type133表示

路由器公告，用type134表示

作用：v6地址无状态自动配置

## ipv6配置办法

1. 手动配置
2. IP地址有状态自动配置

IPv6地址分配服务器必须保存每个节点的状态信息，并管理这些保存的信息

1. IP地址无状态自动配置

不需要IPv6地址分配服务器保存和管理每个节点的状态信息的一种IPv6地址自动配置方式

[R1]interface GigabitEthernet 0/0/1

[R1-GigabitEthernet0/0/1]undo ipv6 nd ra halt

### IPv6无状态地址配置通过交互RS和RA报文完成

路由器公告报文RA

有2个关键标志位:

* M标志位，管理标志位，作用:终端使用有状态、无状态自动配置

M=0，表示使用无状态自动配置

M=1，表示使用有状态自动配置

* 0标志位，其他配置标志位

O=0，其他配置从路由器获得

O=1，其他配置从DHCPv6获得

## ipv6使用

* 阶段一：少数位置使用ipv6，绝大多数位置使用ipv4

使用隧道技术（隧道就是数据重新封装的技术）

GRE隧道（通用路由封装）：在原始IP包头前面，封装GRE头部，再封装新的IP包头

* 阶段二：大面积同时使用ipv6、ipv4

需要配置双栈技术

* 阶段三：全面删除ipv4，只使用ipv6

注意：ipv4和ipv6是独立的网络。如果要互通，需要配置NAT64功能

# NFV和SDN

## NFV

### 概念

NFV（Network Functions Virtualization ）是运营商为了解决电信网络硬件繁多、部署运维复杂、业务创新困难等问题而提出的。

### 关键技术--虚拟化、云化

虚拟化具有分区、隔离、封装和相对于硬件独立的特征，能够很好匹配NFV的需求。

### 架构

NFV架构分NFVI （Network Functions Virtualization Infrastructure，基础设施层）、 VNF（ Virtualized Network Function，虚拟化网络功能层）和MANO（Management and Orchestration，管理编排域），同还要支持现有的BSS/OSS（Business support system/ Operation support system）。

## SDN

### 概念

SDN（Software Defined Networking）即软件定义网络。 其核心理念通过将网络设备控制平面与数据平面分离，从而实现了网络控制平面的集中控制，为网络应用的创新提供了良好的支撑。

### 三个特征

* 转控分离

所有网络设备都有2个操作平面

* + 控制平面，作用：配置设备
  + 数据转发平面，专用转发数据

转控分离的核心思想：设备的控制平面从设备脱离，在SDN服务器上集成所有的控制平面

* 集中控制

通过专门的服务器收集网络设备、各个链路的状态，并控制数据转发的路径

* 开放可编程接口

可以用各种编程语言编写前端程序

SDN服务器收集设备信息、下发转发路径，需要使用专用的通讯协议。如14.2.3

### OpenFlow

* OpenFlow是控制器与交换机之间的一种南向接口协议。它定义了三种类型的消息，Controller-to-Switch、 Asynchronous 和 Symmetric。每一种消息又包含了更多的子类型。
* OpenFlow交换机基于流表（Flow Table）转发报文。

流表中的2个关键信息：

* 匹配域

作用：匹配某些数据的依据

匹配数据的方式包括：源和目的IP、源和目的Mac、源和目标端口、入接口、vlan标签、vlan优先级、数据帧的协议类型

* 动作，作用：指导数据发送

### SDN设备转发数据原理

1. 先检查自身是否有对应的表记录

2. 自身没有流表记录，向SDN服务器发起请求

3. SDN服务器有相应的流表记录，直接下发到SDN设备

无相应流表记录，则利用已知的设备信息、链路信息，生成记录

# 命令简述

## 基本命令

G/0/0/0 槽位/板卡/端口号

进入登录界面

[Huawei]系统视图

< huawei >用户视图

<>system-view进入系统视图

<>Interface GigabitEthernet 0/0/1进入接口视图

<>quit 退出

[Huawei]interface e 0/0/0 #进入以特网接口0/0/0

[Huawei-Ethernet0/0/0]ip address 192.168.0.254 24 #给接口配置IP地址

[Huawei-Ethernet0/0/1]dis cu #查看设备的配置

[Huawei-Ethernet0/0/1]display this #查看当前视图的配置

<Huawei>save #最后保存

<Huawei>display interface e 0/0/0 查询e 0/0/0接口的地址

<Huawei>display ip routing-table #查看路由表

[Huawei]display ip routing-table protocol static #筛选查看静态路由协议的路由表、

## Vlan配置

[Huawei]vlan batch 10 20 #划分vlan10 vlan20

[Huawei-Ethernet0/0/1]port link-type access #修改接口类型

[Huawei-Ethernet0/0/1]port default vlan 10 #将接口划分到vlan10里面

Port trunk allow-pass vlan 10 20 #配置允许通过的列表，允许通过vlan10 20

Port trunk pvid vlan 10 #修改pvid的接口为10

## 子接口配置

[Huawei-Ethernet0/0/0.1] dot1q termination vid 10 #终结vlan10的标签

[Huawei -GigabitEthernet0/0/1.10]arp broadcast enable #开启arp广播

## Stp配置

Stp priority 数值 #修改优先级命令

stp root primary #设置为根桥

stp root secondary #设置为备份根桥

display stp brief #查看STP接口状态摘要

## Ospf配置

配置步骤：

* 创建并运行OSPF进程
* 创建并进入OSPF区域
* 运行指定的OSPF接口

[R3] ospf 1 router-id 3.3.3.3

[R3-ospf-1] area 1

[R3-ospf-1-area-0.0.0.1] network 3.3.3.3 0.0.0.0

[R3-ospf-1-area-0.0.0.1] network 10.1.23.0 0.0.0.3（反掩码）

[R3]dis ospf peer（查看邻居表）

[R3]Reset ospf process # 重启ospf进程

[R3]dis ospf error #ospf故障排除

[R3]dis ospf interface G0/0/1 #查看接口类型

[R3]dis ospf network-type #查看接口类型

[R3-ospf-1]default-route-advertise #引入缺省路由

## Nat配置（在出口配置）

### 静态nat

[接口视图]nat static global 122.1.2.1 inside 192.168.1.1

Global 公网 inside 私网

### Easy IP配置

[R1]acl 2000

[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255

[R1-acl-basic-2000]quit

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]nat outbound 2000

### NAPT

[R1]nat address-group 1 122.1.2.1 122.1.2.2（起终）

[R1]acl 2000

[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255

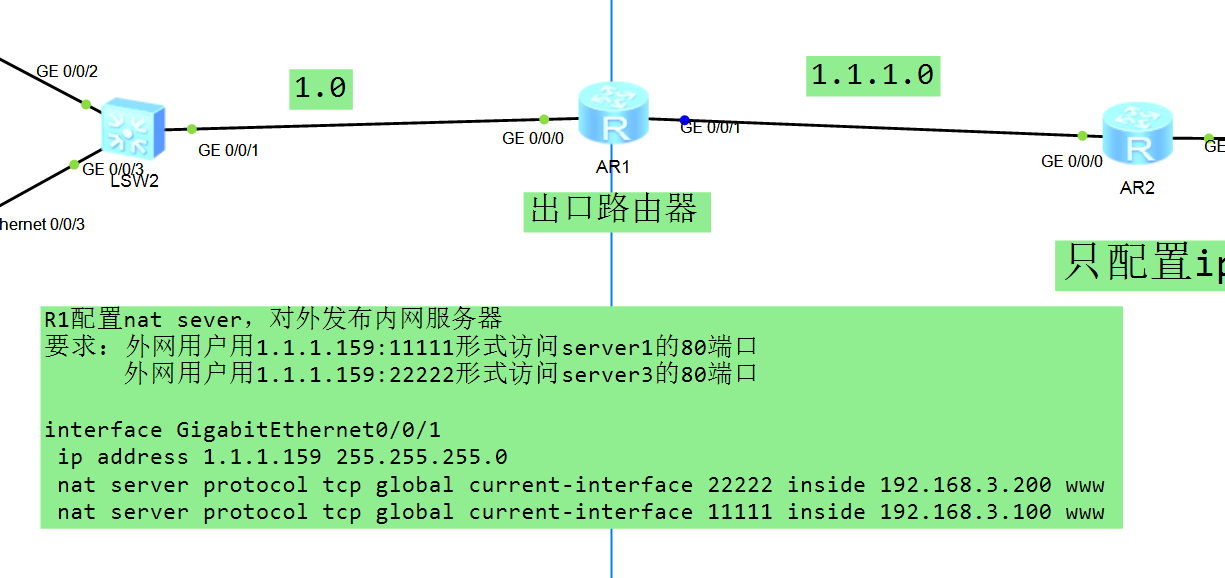
[R1-acl-basic-2000]quit

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1

### Nat server

[接口视图]Nat server protocol TCP global current-interface 80 inside 192.168.3.100 80



## FTP

Put命令，上传文件

Get命令，下载文件

Mkdir，新建文件夹

Cd，进入某个文件夹

## DHCP

客户端主动释放IP：ipconfig/release

客户端主动续租命令：ipconfig/renew

**接口配置**

[Huawei]dhcp enable

[Huawei]interface GigabitEthernet0/0/0

[Huawei-GigabitEthernet0/0/0]dhcp select interface

[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2

[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address 10.1.1.2

[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3

**全局配置**

[Huawei]dhcp enable

[Huawei]ip pool pool2

[Huawei-ip-pool-pool2]network 1.1.1.0 mask 24

[Huawei-ip-pool-pool2]gateway-list 1.1.1.1

[Huawei-ip-pool-pool2]dns-list 1.1.1.1

[Huawei-ip-pool-pool2]lease day 10

[Huawei-ip-pool-pool2]quit

[Huawei]interface GigabitEthernet0/0/0

[Huawei-GigabitEthernet0/0/1]dhcp select global

**中继配置（在vlanif接口视图配置）**

* 该vlanif必须是连接终端的
* 客户端跨网段获取IP时，必须要求DHCP服务器有可达的客户端网段

dhcp select relay --开启中继模式。

dhcp relay server-ip 192.168.1.1 --指定真实的dhcp服务器

## DNS

--display /displaydns（查看DNS缓存）

--Ipconfig /flushdns（清空DNS缓存）

## WLAN

AC与AP间通讯、AC控制AP的数据，使用管理vlan100

无线终端使用业务数据vlan101

三层交换g0/0/4口连接AC，g0/0/1口连接路由器，g0/0/2口连接二层交换

二层交换e0/0/1口连接三层交换，e0/0/2和e0/0/3连接AP

无线配置

1.网络配置

[SW1-3层交换]dis cu

vlan batch 2 100 to 101

#

interface Vlanif2 --配置ip连接路由器

ip address 192.168.2.2 255.255.255.0

#

interface Vlanif101

ip address 192.168.101.1 255.255.255.0

dhcp select interface --给无线客户机分配ip

#

interface GigabitEthernet0/0/1

port link-type access

port default vlan 2

#

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface GigabitEthernet0/0/4

port link-type access

port default vlan 100

#

ip route-static 0.0.0.0 0.0.0.0 192.168.2.1

<SW2-2层交换>dis cu

vlan batch 100 to 101

interface Ethernet0/0/1

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface Ethernet0/0/2

port link-type trunk

port trunk pvid vlan 100 --连接AP接口必须修改pvid，改成管理vlan

port trunk allow-pass vlan 2 to 4094

#

interface Ethernet0/0/3

port link-type trunk

port trunk pvid vlan 100

port trunk allow-pass vlan 2 to 4094

#

<AC6005>dis cu

#

vlan batch 100 to 101

#

dhcp enable

#

interface Vlanif100

ip address 192.168.100.100 255.255.255.0

dhcp select interface --给ap分配ip地址

#

interface GigabitEthernet0/0/1

port link-type access

port default vlan 100 --只接收AC、AP间管理vlan的数据

2.AP上线、AP注册

<AC6005>dis cu

capwap source interface vlanif100 --设置管理vlan

wlan

regulatory-domain-profile name aaa --新建国家模板

country-code cn --使用中国无线制度

ap-group name apzu --创建AP组

regulatory-domain-profile aaa --使用国家模板

ap auth-mode mac-auth --使用MAC确认合法AP

ap-id 1 ap-mac 00e0-fc88-3150 --第一个AP信息

ap-name ap1 --AP名字，可以不设

ap-group apzu --AP加入ap组

ap-id 2 ap-mac 00e0-fcad-1e30

ap-name ap2

ap-group apzu

3.无线各种配置

<AC6005>dis cu

wlan

security-profile name wxmm --创建安全模板

security wpa-wpa2 psk pass-phrase 123456789 aes --设置无线密码

ssid-profile name wxm --创建无线名称模板

ssid 1410 --设置无线名称

vap-profile name xnap --创建虚拟AP模板，组合无线配置

service-vlan vlan-id 101 --设置业务vlan

ssid-profile wxm --使用无线名称模板

security-profile wxmm --使用安全模板

forward-mode direct-forward --业务数据不传给ac，通过交换机直接向路由器转发

ap-group name apzu

vap-profile xnap wlan 1 radio 0 --使用2.4G无线信号

vap-profile xnap wlan 1 radio 1 --使用5G无线信号，可以和2.4G同时用，也可以单用1个

**修改射频功率：**

Wlan

Rrm-profile name default

Calibrate auto-txpower-select disable

q

q

Ap-group name ap组名

Radio 0/1 ----进入2.4G或5G无线射频配置视图

Eirp 数字 --手动调整射频功率的大小，控制无线覆盖面大小

**修改信号信道：**

Wlan

Rrm-profile name default

Calibrate auto-channel-select disable

q

q

Ap-group name ap组名

Radio 0/1 ----进入2.4G或5G无线射频配置视图

Channel 20mhz/40mhz-minus/40mhz-plus 信道编号

## SSH

### 配置步骤

1、开启SSH

[Huawei]stelnet server enable

2、3A认证配置登录账号

[Huawei]aaa

[Huawei-aaa]local-user bbb password cipher 123

[Huawei-aaa]local-user bbb privilege level 3

[Huawei-aaa]local-user bbb service-type ssh

3、账号SSH登录时使用密码验证

[Huawei]ssh user bbb authentication-type password

4、VTY界面允许SSH协议通过

[Huawei]user-interface vty 0 4

[Huawei-ui-vty0-4]authentication-mode aaa

[Huawei-ui-vty0-4]protocol inbound ssh ---vty只允许ssh远程

## Telnet配置

[Huawei]aaa

[Huawei-aaa]local-user aaa password cipher 123456

[Huawei-aaa]local-user aaa privilege level 3

[Huawei-aaa]local-user aaa service-type telnet ssh web--控制用户登录方式

[Huawei]user-interface vty 0 4

[Huawei-ui-vty0-4]authentication-mode aaa

## SNMP

[R1]snmp-agent -----启动SNMP客户端程序

[R1]snmp-agent sys-info version v3----版本

[R1]snmp-agent group v3 test privacy --test是组名，privacy表示使用安全设置

[R1]snmp-agent usm-user v3 R1 test authentication-mode md5 HCIA@Datacom123 privacy-mode aes128 HCIA-Datacom123 --R1是账号--test是组名--authentication-mode md5 身份认证密码--privacy-mode 数据加密密码

--------上面是监控主机询问配置

[R1]snmp-agent target-host trap-paramsname param v3 securityname sec privacy

[R1]snmp-agent target-host trap-hostname nms address 192.168.1.10 trap-paramsname param

[R1]snmp-agent trap source GigabitEthernet 0/0/1

[R1]snmp-agent trap enable

# 注意

* 动态协议宣告网段的作用

1. 让其他路由器学习该网段
2. 让对应的接口能收发动态协议报文

动态协议可以引用其他类型的路由信息，他们之间可以互相学习