G-LAB

G-CNA 课程

讲师：沈老师

局域网技术

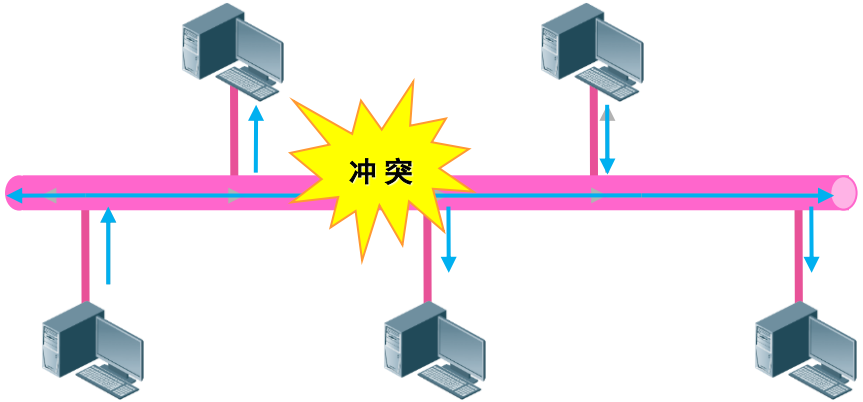
1. 以太网协议介绍
2. 局域网交换机的通讯原理?
3. VLAN-TRUNK
4. Vlan间通信
5. 局域网环路避免技术

以太网概述

- 最初的以太网使用粗同轴电缆为传输介质，为共享式以太网，会产生冲突
- 以太网利用CSMA/CD算法解决共享信道内的信道争用和冲突问题
- 以太网的发展：
  - 20世纪70年代产生于施乐公司
  - 1978年，DEC公司、Intel公司和Xerox拟定了一个针对10Mbps以太网的标准，成为DIX标准
  - 1983年，DIX标准演变成IEEE 802.3标准
  - 随着以太网技术的发展，百兆、千兆、万兆的标准相继出台

共享信道内的冲突问题

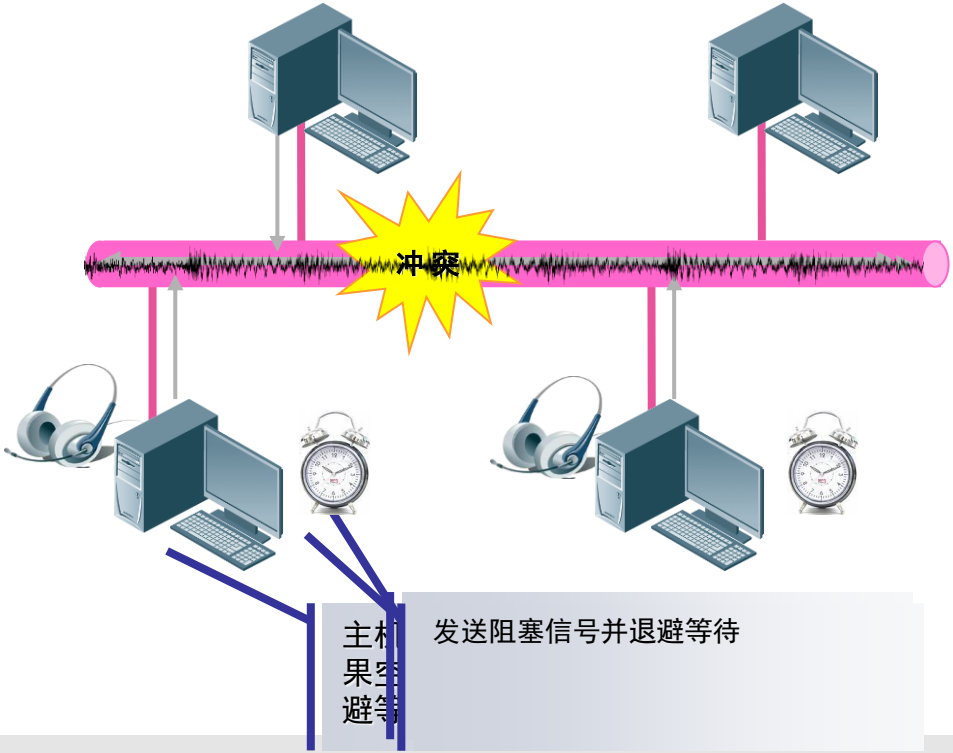
- 任意时刻信道只能传输一路数据
- 每台主机发出的数据可以被其他所有主机所接收
- 如果有两台主机同时发送数据，则产生冲突
- 这些主机所处的范围称为冲突域。



CSMA/CD

- CSMA/CD：带有冲突检测的载波侦听多路访问（Carrier Sense Multiple Access/Collision Detect）
  - 载波侦听：发送节点在发送数据之前，必须侦听传输介质（信道）是否处于空闲状态。
  - 多路访问：具有两种含义，既表示多个节点可以同时访问信道，也表示一个节点发送的数据可以被多个结点所接收。
  - 冲突检测：发送节点在发出数据的同时，还必须监听信道，判断是否发生冲突

CSMA/CD



CSMA/CD

- 需要最小帧长度64Byte的限制，以便冲突能够被检测到
- 优点：
  - 原理简单，技术上容易实现，不需集中控制，不提供优先级控制
- 缺点：
  - 在网络负载增大时，发送时间增长，发送效率急剧下降

常见以太网技术标准

名称	介质	距离	速率	拓扑
10Base-5	同轴电缆	500m	10Mbps	总线型
10Base-2	细同轴电缆	185m	10Mbps	总线型
10Base-T	3类非屏蔽双绞线	100m	10Mbps	星型
100Base-TX	5类非屏蔽双绞线	100m	100Mbps	星型
100Base-FX	光纤	412m	100Mbps	星型
1000Base-SX	短波光纤	260m	1Gbps	星型
1000Base-LX	长波光纤	440m (多模) 5000m (单模)	1Gbps	星型

以太网技术发展

- Xerox公司开发以太网获得巨大成功。1978年，DEC公司、Intel公司和Xerox拟定了针对10Mbps以太网标准，称为DIX标准。经过两次修改以后，1983年变成IEEE 802.3标准。
- 10BASE5
  - 最早使用粗同轴电缆以太网，称为10BASE5。其中10代表以Mbps为单位速度，BASE使用基带传输，BASE后面代表传输介质。此处“5”指电缆最大长度（不使用中继器）。其含义是：运行在10Mbps速率上、使用基带，支持分段长度为500 m。
- 10BASE2
  - 使用细同轴电缆以太网。细缆比粗缆更容易弯曲，使用T型接头也更可靠，造价低，容易安装。但细同轴电缆每一段最大长度只有185 m，每一段只能容纳30台机器。
- 10BASE-T
  - 由于同轴电缆这，故障监测、电缆断裂、电缆超长、接头松动等故障都易造成网络瘫痪，这导致星形拓扑结构产生。星型拓扑结构网络中所有结点都连接到集线器（hub）上。使用双绞线，此种以太网也就被称为10BASE-T，T代表双绞线。

以太网技术发展

- 10BASE-F
  - 双绞线传输距离有限，人们开发出10BASE-F以太网，F代表光纤。使用光纤作为传输介质成本很高，这种以太网具有良好抗噪声性能和安全性（防窃听），传输距离也很远（上千米），适用于远距离楼与楼之间连接。
- 100BASE-T4
  - IEEE 802.3组织委员会于1995年推出802.3u标准，即快速以太网（Fast Ethernet）。为了向后兼容以太网，该标准保留原来帧格式、接口，和10BASE-T一样使用集线器和交换机作为连接设备，传输介质除3类双绞线和光纤外，还增加5类双绞线。
  - 使用3类双绞线快速以太网称为100BASE-T4，使用5类双绞线快速以太网被称为100BASE-TX，使用光纤快速以太网则称为100BASE-FX，F代表光纤。
- 千兆以太网（gigabit Ethernet）
  - 1998年6月IEEE802.3组织委员会推出了千兆以太网（gigabit Ethernet）规范802.3z。以太网速度提升10倍，仍与现有以太网标准保持兼容。

以太网技术发展

- 万兆以太网
  - 2002年7月，IEEE通过万兆以太网标准802.3ae。初始万兆以太网仅采用全双工与光纤技术，同年11月间，IEEE就提出铜缆实现万兆以太网建议，并成立专门研究小组。
  - 万兆以太网仍属于以太网家族，保持着和其他以太网技术兼容，不需要修改以太网MAC子层协议或帧格式，能够与10M/100M或千兆位以太网无缝地集成在一起直接通信。万兆以太网技术适合于企业和运营商网络建立交换机到交换机连接（如在园区网），或交换机与服务器之间互连（如数据中心）。
- 百万兆以太网
  - 2007年IEEE又提出802.3ba标准，目标设计40Gbps或100Gbps以太网。
  - 以太网技术发展30多年，逐渐成为主流局域网建设标准。以太网之所以有如此强大生命力，和它简单分不开。简单带来可靠、廉价、易于维护等特性，在网络中增加新设备非常容易；另外以太网和IP协议能够很好配合。而TCP/IP已经在以太网得到广泛应用。

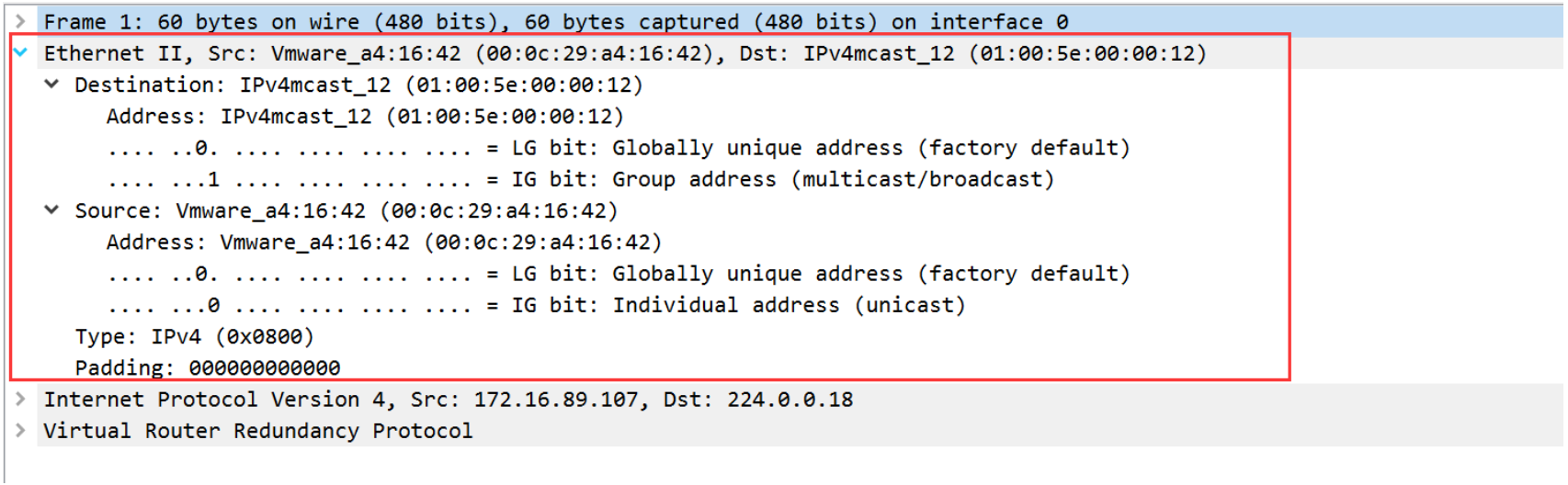
以太网帧格式

- 历史上出现过多种以太网帧格式
  - 1980年，DEC、Intel、Xerox制订了DIX Ethernet I的标准
  - 1982年，DEC、Intel、Xerox又制订了DIX Ethernet II的标准
  - 1982年，IEEE开始研究Ethernet的国际标准802.3，定义了802.3 SAP帧格式
  - 1983年，Novell基于IEEE的802.3的原始版开发了专用的Ethernet帧格式
  - 1985年，IEEE推出IEEE 802.3规范，后来为解决Ethernet II与802.3帧格式的兼容问题，推出折衷的802.3 SNAP格式
- 现在最常见的是：Ethernet II、802.3 SAP和SNAP

Ethernet II标准的帧格式

- 类型/长度字段的值大于或等于0x0600时，表示上层数据使用的协议类型，例如0x0806表示ARP请求或应答，0x0800表示IP协议；

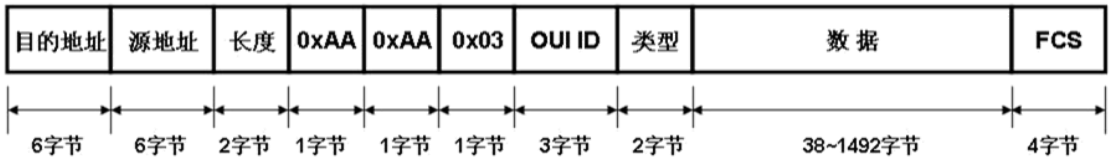
Ethernet II标准的帧格式



802.3 SAP和SNAP标准的帧结构

- 类型/长度字段的值小于0x0600时，表示以太网用户数据的长度
- 需要LLC子层的封装以指明上层协议类型

(a) 802.3 SAP 帧结构



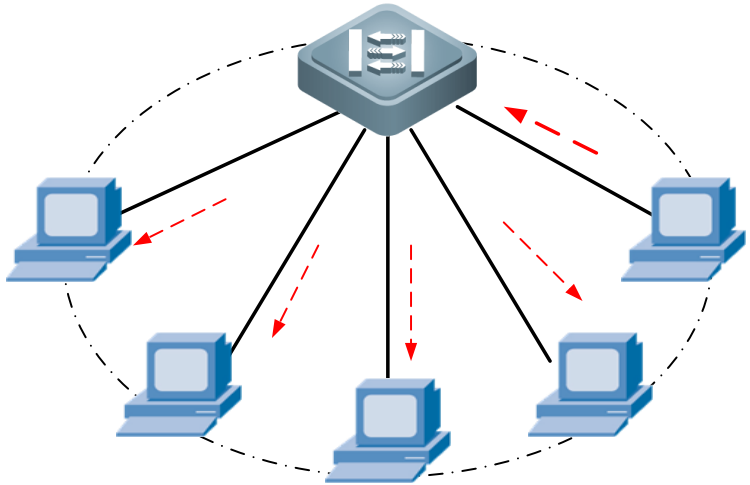
(b) 802.3 SNAP 帧结构

802.3 SAP和SNAP标准的帧结构

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
IEEE 802.3 Ethernet
  Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
      Address: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: aa:bb:cc:00:30:00 (aa:bb:cc:00:30:00)
      Address: aa:bb:cc:00:30:00 (aa:bb:cc:00:30:00)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Length: 38
    Padding: 0000000000000000
Logical-Link Control
  DSAP: Spanning Tree BPDU (0x42)
      0100 001. = SAP: Spanning Tree BPDU
      .... ...0 = IG Bit: Individual
  SSAP: Spanning Tree BPDU (0x42)
      0100 001. = SAP: Spanning Tree BPDU
      .... ...0 = CR Bit: Command
  Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x3)
Spanning Tree Protocol
```

以太网广播和冲突

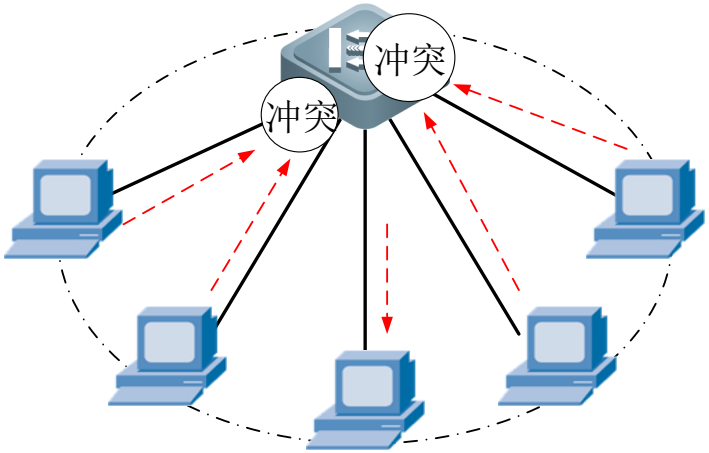
- 一般把网络中能接收任何一设备发出的广播帧的所有设备的集合，称为**广播域（broadcast domain）**。



广播域

以太网广播和冲突

- **冲突域**
  - 在以太网传输中，如果网络上两台计算机同时通信，就会发生冲突。共享介质上所有节点在竞争同一带宽传输信息时，都会发生冲突。这个冲突范围就是冲突域（**collision domain**）。

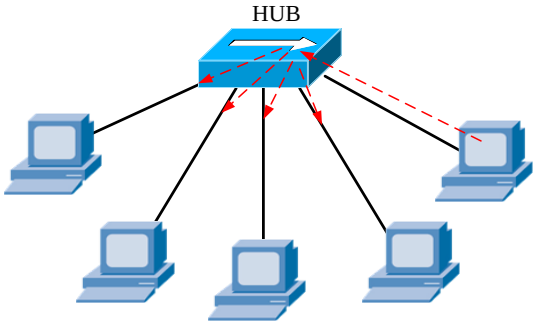


交换技术基础

- **什么是交换技术**
  - 交换技术是将用户发送来数据，按一定规格，把数据分割为许多小段的数据分组，在每个分组数据上增加标识，形成分组头，用以指明该分组发往何地址，后面增加控制信息。在一条物理线路上采用动态复用技术，同时传送多个数据分组。

交换技术基础

- **二层交换设备**
  - **集线器(Hub)**
- 早期以太网采用总线型拓扑，后来向星型拓扑结构发展过程中，集线器起着关键作用。
- 集线器英文“Hub”是“中心”意思，对接收到信号进行再生整形放大，以扩大网络传输距离，同时把所有节点集中在以它为中心的节点上。工作于OSI参考模型第一层，即“物理层”。

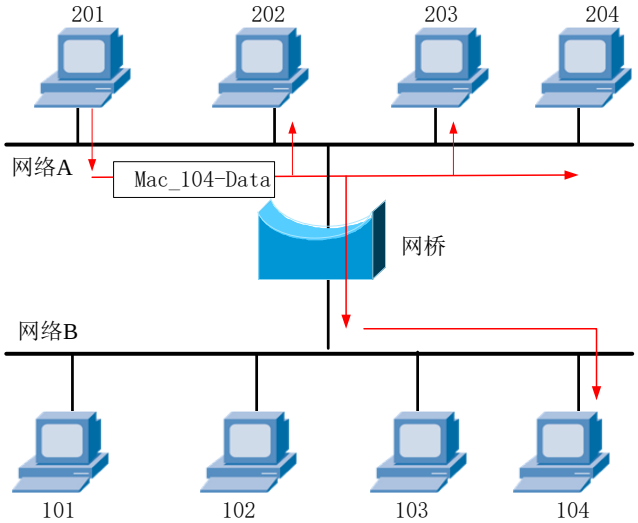


交换技术基础

- **二层交换设备**
  - **网桥（Bridge）**
- 网桥是数据链路层设备，网桥具有智能化，能识别信号中携带MAC地址，因此能创建两个或多个LAN分段，其中每一个分段都是一个独立冲突域。网桥将两个相似网络连接起来，能解析接受到数据帧信息，按地址对帧信号进行转发，过滤LAN中冗余通信流，使得本地通信流保留在本地，而只转发属于其他局域网分段的通信流。

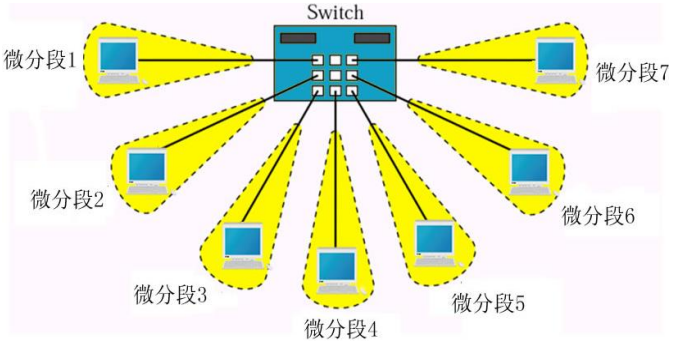
交换技术基础

- 二层交换设备
  - 网桥（Bridge）



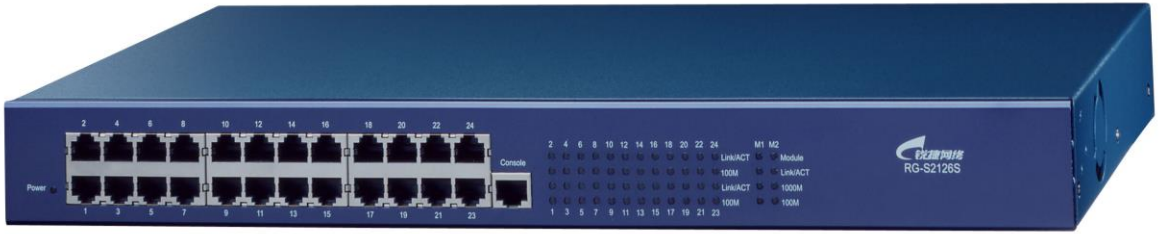
交换技术基础

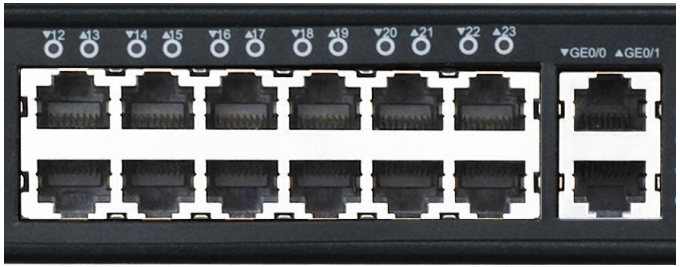
- 二层交换设备
  - 交换机（Switch）
- 普通交换机也叫第2层交换机，或称为LAN交换机，替代集线器优化网络传输效率。像网桥一样，交换机也连接LAN分段，利用一张MAC地址表来分流帧，从而减少通信量，但交换机的处理速度比网桥要高得多。

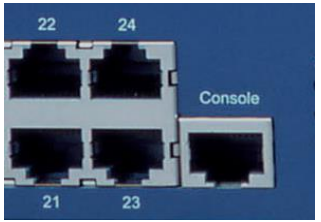


认识交换机设备

- 认识交换机端口







认识交换机设备

- 认识交换机组件
  - CPU芯片
- 交换机的CPU主要控制和管理所有网络通讯的运行，理论上可以执行任何网络功能。

认识交换机设备

- **认识交换机组件**
- **ASIC芯片**
- 交换机的ASIC芯片，是连接CPU和前端接口的专门的硬件集成电路，并行转发数据，提供高性能的基于硬件的功能特性，主要提供接口数据的解析、缓冲、拥塞避免、链路聚合、VLAN标记、广播抑制、ACL、QOS等功能。

衡量交换机性能的参数

- 背板带宽
- 包转发率
- 线速交换
- 支持VLAN 数量
- MAC地址表

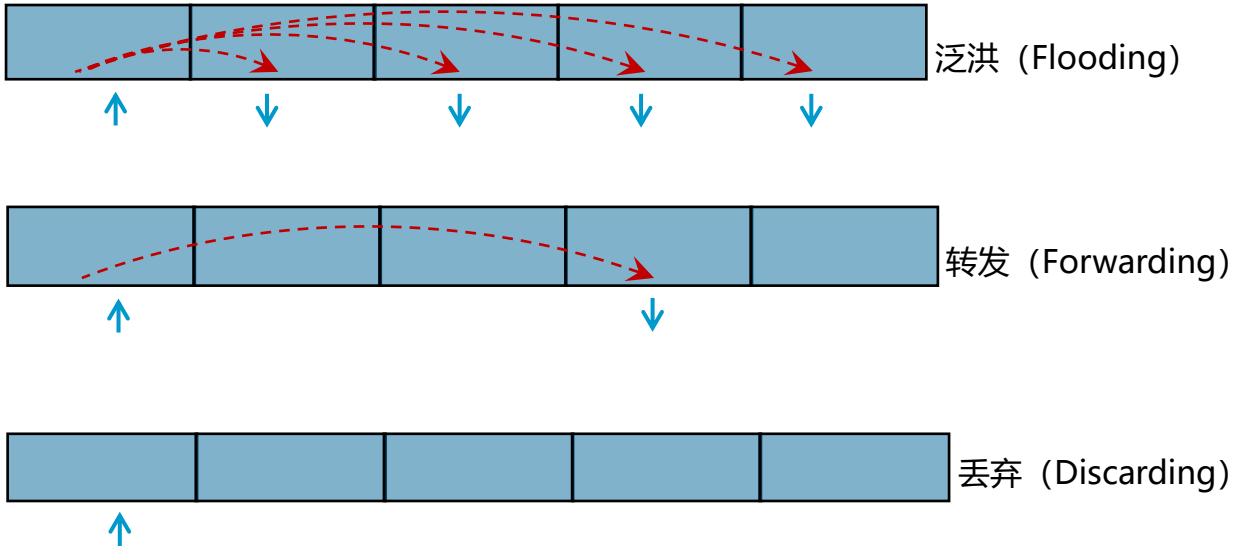
局域网技术

1. 以太网协议介绍
2. 局域网交换机的通讯原理?
3. VLAN-TRUNK
4. Vlan间通信
5. 局域网环路避免技术

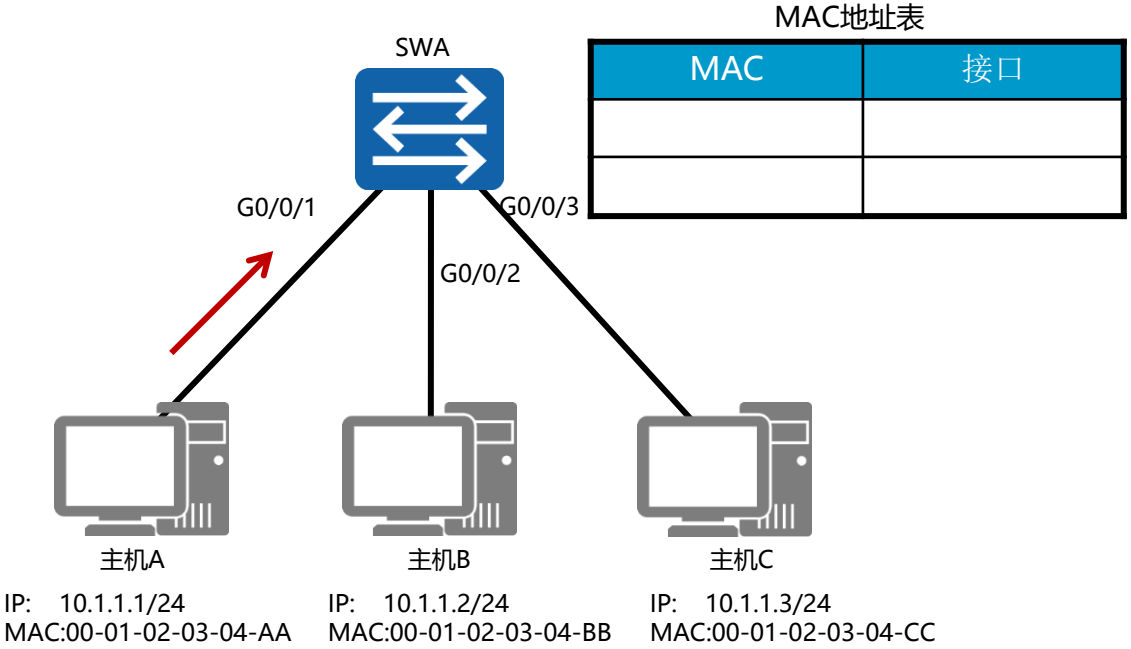
交换机工作原理

- 根据数据帧中的目标MAC地址，在端口之间进行帧转发
- 交换机的三项主要功能：
  - MAC地址表学习
  - 转发/过滤数据帧
  - 消除第二层环路
- MAC地址表：存储地址到端口的映射关系

交换机的转发行为

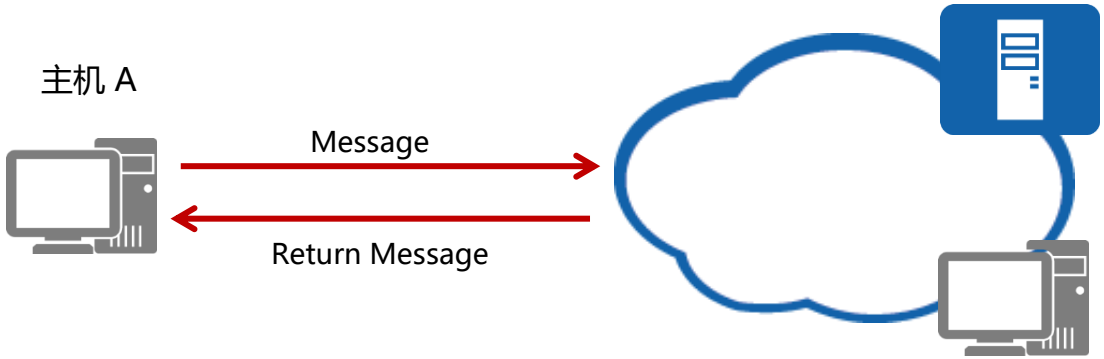


交换机初始状态



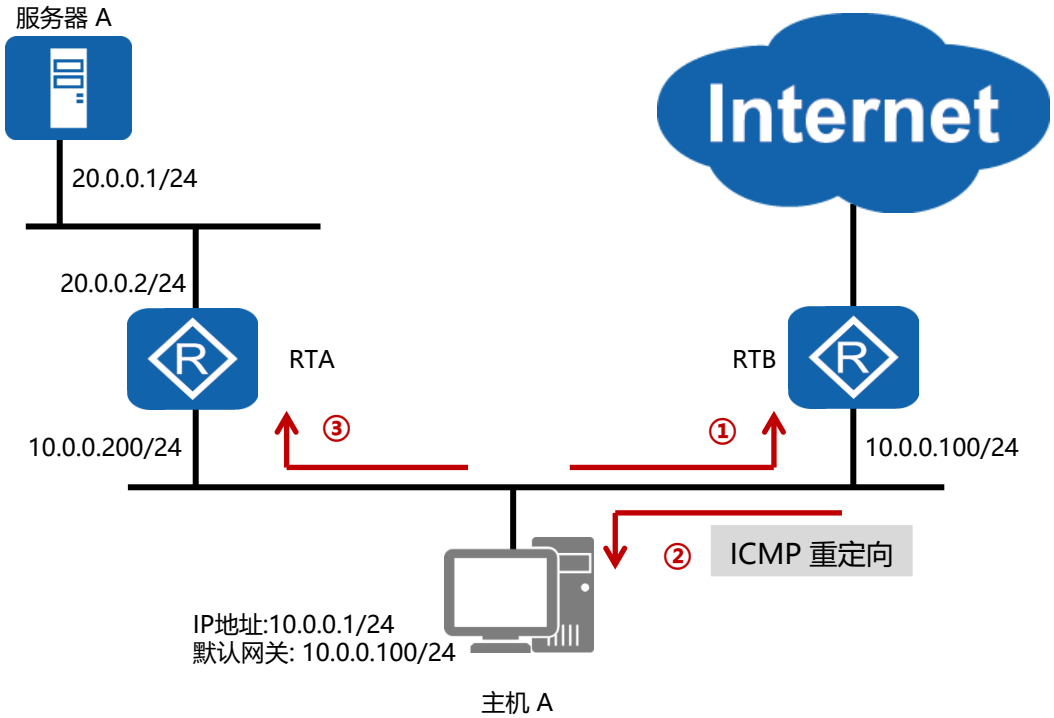
- 初始状态下，交换机MAC地址表为空。

ICMP



- ICMP用来传递差错、控制、查询等信息。

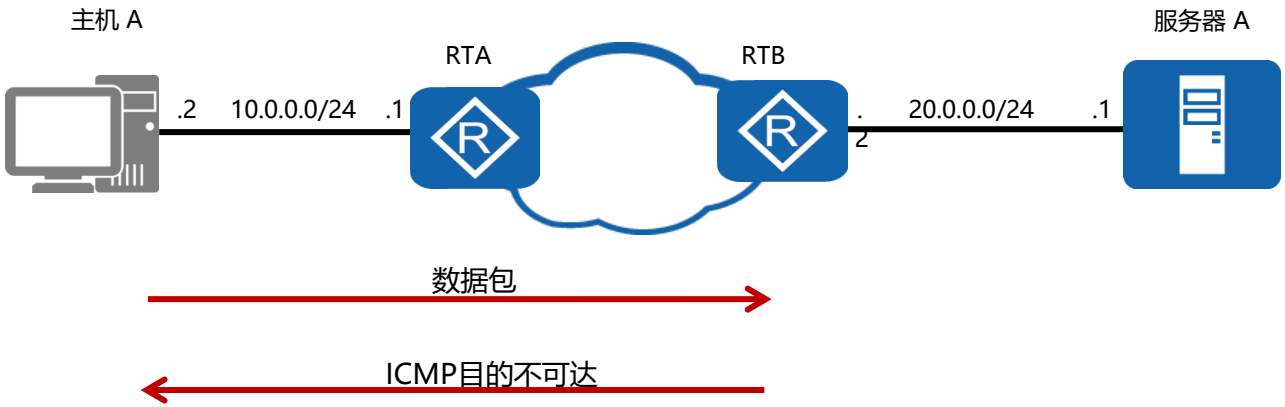
ICMP重定向



ICMP差错检测

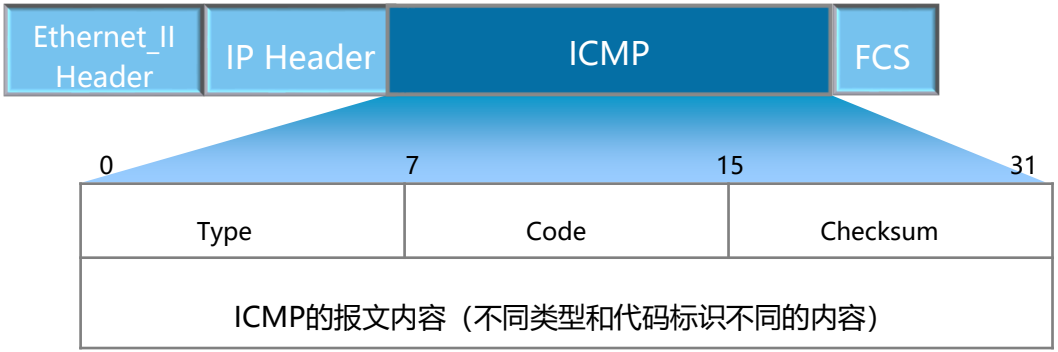
- ICMP Echo Request和ICMP Echo Reply分别用来查询和响应某些信息，进行差错检测。

ICMP错误报告



- 当网络设备无法访问目标网络时，会自动发送ICMP目的不可达报文到发送端设备。

ICMP数据包格式



- Type表示ICMP消息类型，Code表示同一消息类型中的不同信息。

ICMP消息类型和编码类型

类型	编码	描述
0	0	Echo Reply
3	0	网络不可达
3	1	主机不可达
3	2	协议不可达
3	3	端口不可达
5	0	重定向
8	0	Echo Request

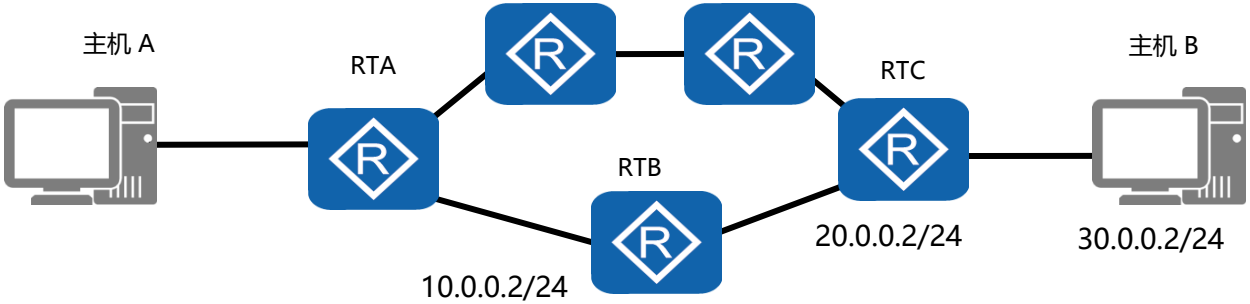
ICMP应用-Ping


```
<PCA>ping ?
STRING<1-255> IP address or hostname of a remote system
-a            Select source IP address, the default is the IP address of
the
              output interface
-c            Specify the number of echo requests to be sent, the default
is
              5
-d            Specify the SO_DEBUG option on the socket being used
-f            Set Don't Fragment flag in packet (IPv4-only)
-h            Specify TTL value for echo requests to be sent, the default
is
              255
-i            Select the interface sending packets
……
```

ICMP应用-Ping

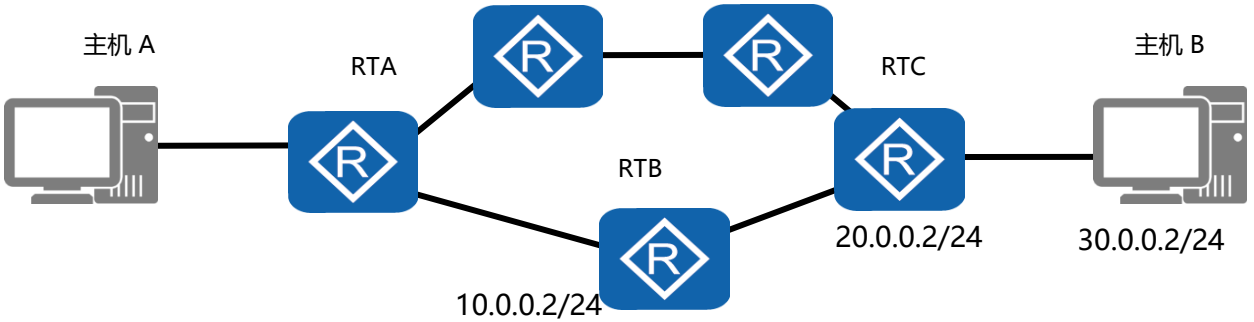
```
[PCA]ping 10.0.0.2
  PING 10.0.0.2 : 56  data bytes, press CTRL_C to break
    Reply from 10.0.0.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/88/340 ms
```

ICMP应用-Tracert




```
<RTA>tracert ?
STRING<1-255>  IP address or hostname of a remote system
-a             Set source IP address, the default is the IP address of
the
               output interface
-f             First time to live, the default is 1
-m             Max time to live, the default is 30
-name          Display the host name of the router on each hop
-p             Destination UDP port number, the default is 33434
-q             Number of probe packet, the default is 3
-s             Specify the length of the packets to be sent. The default
               length is 12 bytes
……
```

ICMP应用-Tracert

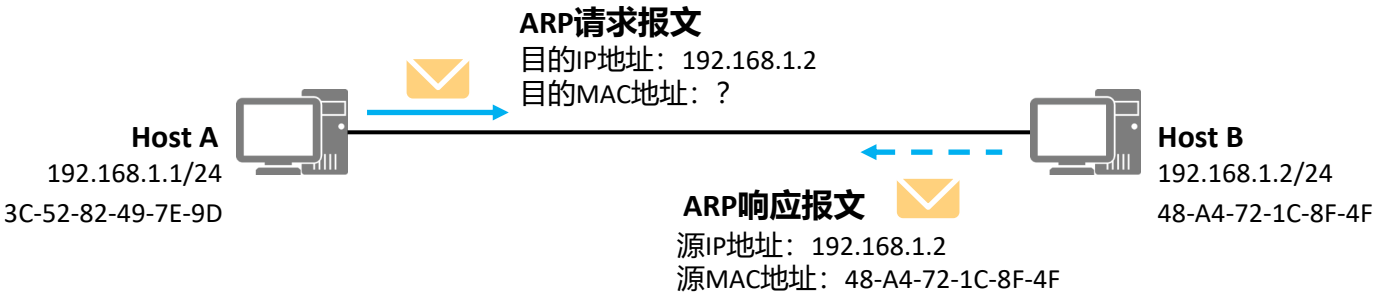



```
<RTA>tracert 30.0.0.2
Tracert to 30.0.0.2(30.0.0.2), max hops:30, packet length:40,
press CTRL_C to break
 1 10.0.0.2 130 ms  50 ms  40 ms
 2 20.0.0.2 80 ms  60 ms  80 ms
 3 30.0.0.2 80 ms  60 ms  70 ms
```

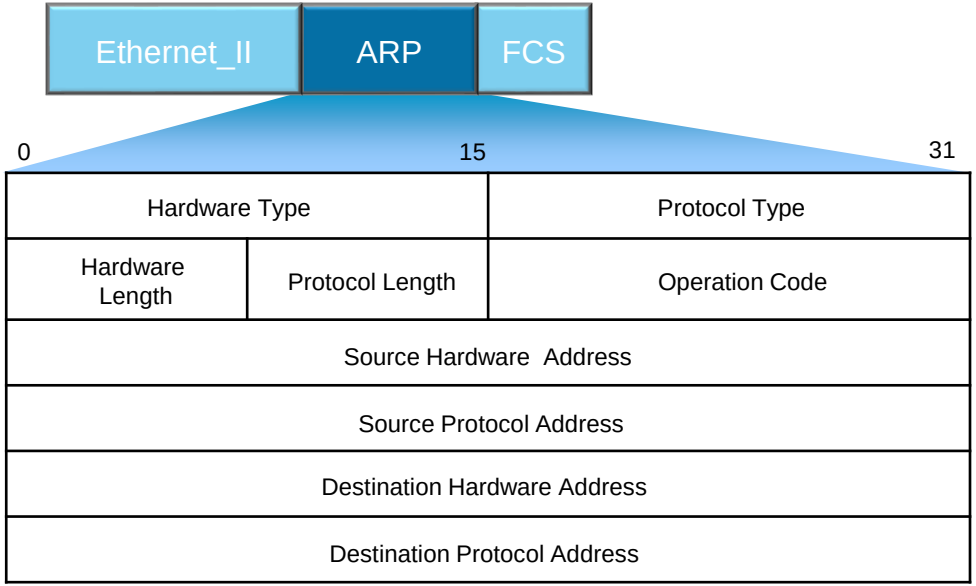
- Type表示ICMP消息类型，Code表示同一消息类型中的不同信息。

地址解析协议（ARP）

- ARP（Address Resolution Protocol）地址解析协议：
  - 根据已知的IP地址解析获得其对应的MAC地址。

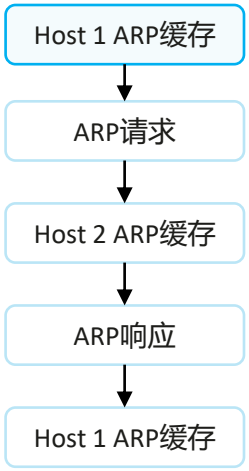


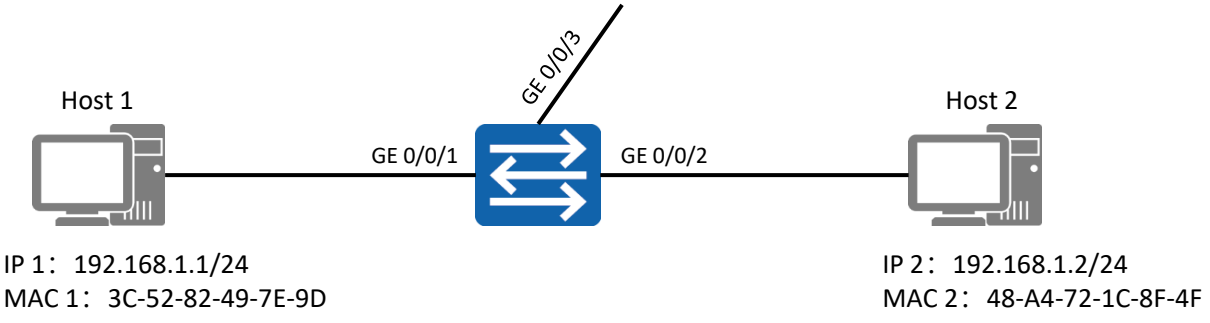
ARP数据包格式



- ARP报文不能穿越路由器，不能被转发到其他广播域。

ARP的工作原理（1）





1

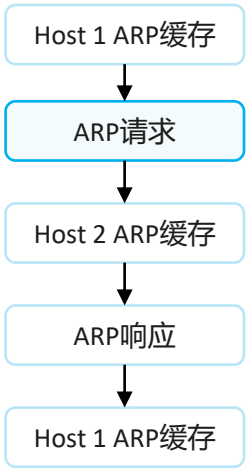
```
Host 1>arp -a
Internet Address    Physical Address    Type
```

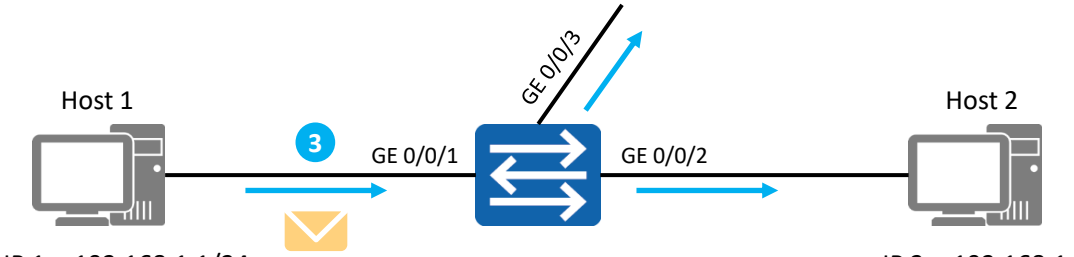
ARP缓存表为空

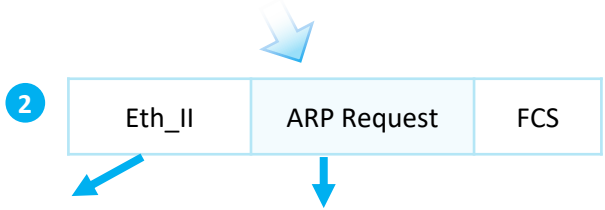
Step 1：

- 在发送数据前，设备会先查找ARP缓存表。
- 如果缓存表中存在对方设备的MAC地址，则直接采用该MAC地址来封装帧，然后将帧发送出去。如果缓存表中不存在相应信息，则通过ARP来获取。

ARP的工作原理（2）







目的MAC：
FF-FF-FF-FF-FF-FF
源MAC：
MAC 1

操作类型：ARP Request
发送端MAC： MAC 1
发送端IP：IP 1
目的端MAC：00-00-00-00-00-00
目的端IP：IP 2

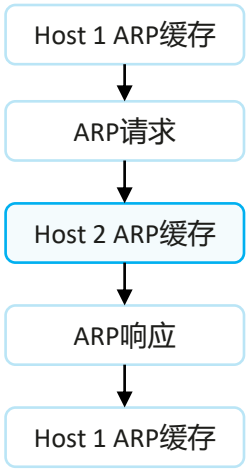
Step 2：

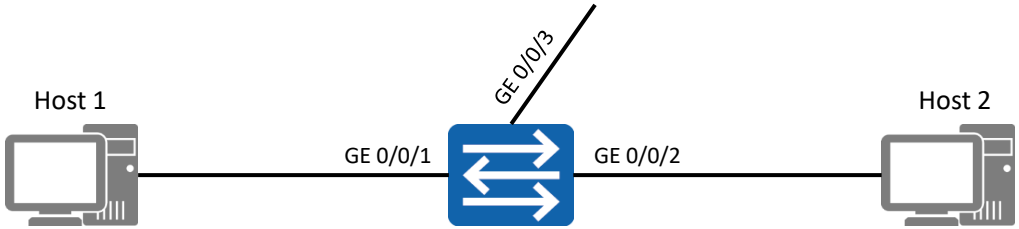
- 主机1通过发送ARP Request报文来获取主机2的MAC地址。
- 由于不知道目的MAC地址，因此ARP Request报文内的目的端MAC地址为0。

Step 3：

- ARP Request是广播数据帧，因此交换机收到后，会对该帧执行泛洪操作。

ARP的工作原理（3）





IP 1：192.168.1.1/24
MAC 1：3C-52-82-49-7E-9D

IP 2：192.168.1.2/24
MAC 2：48-A4-72-1C-8F-4F

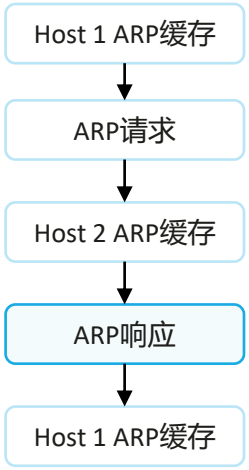
Step 4：

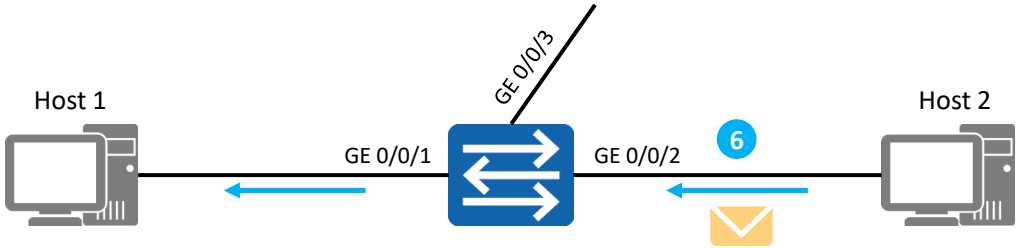
- 所有的主机接收到该ARP Request报文后，都会检查它的目的端IP地址字段与自身的IP地址是否匹配。
- 主机2发现IP地址匹配，则会将ARP报文中的发送端MAC地址和发送端IP地址信息记录到自己的ARP缓存表中。

4

```
Host 2>arp -a
Internet Address      Physical Address      Type
192.168.1.1           3C-52-82-49-7E-9D     Dynamic
```

ARP的工作原理（4）



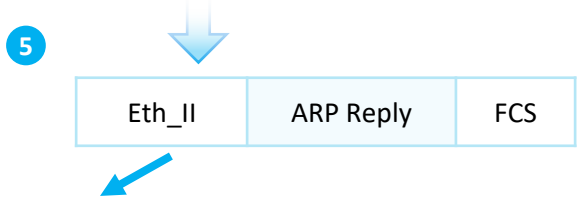


Step 5：

- 主机2通过发送ARP Reply报文来响应主机1的请求。
- 此时主机2已知主机1的MAC地址，因此ARP Reply是单播数据帧。

Step 6：

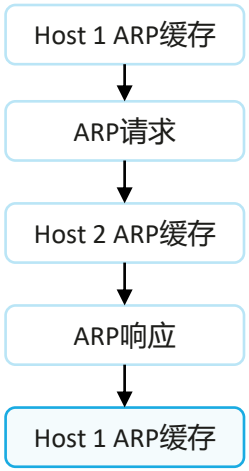
- 交换机收到该单播数据帧后，会对该帧执行转发操作。

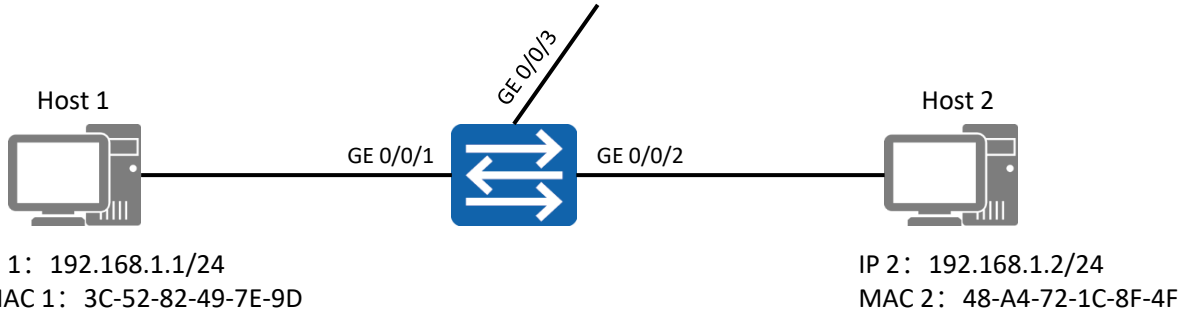


目的MAC：MAC 1
源MAC：MAC 2

操作类型：ARP Reply
发送端MAC： MAC 2
发送端IP：IP 2
目的端MAC： MAC 1
目的端IP：IP 1

ARP的工作原理（5）





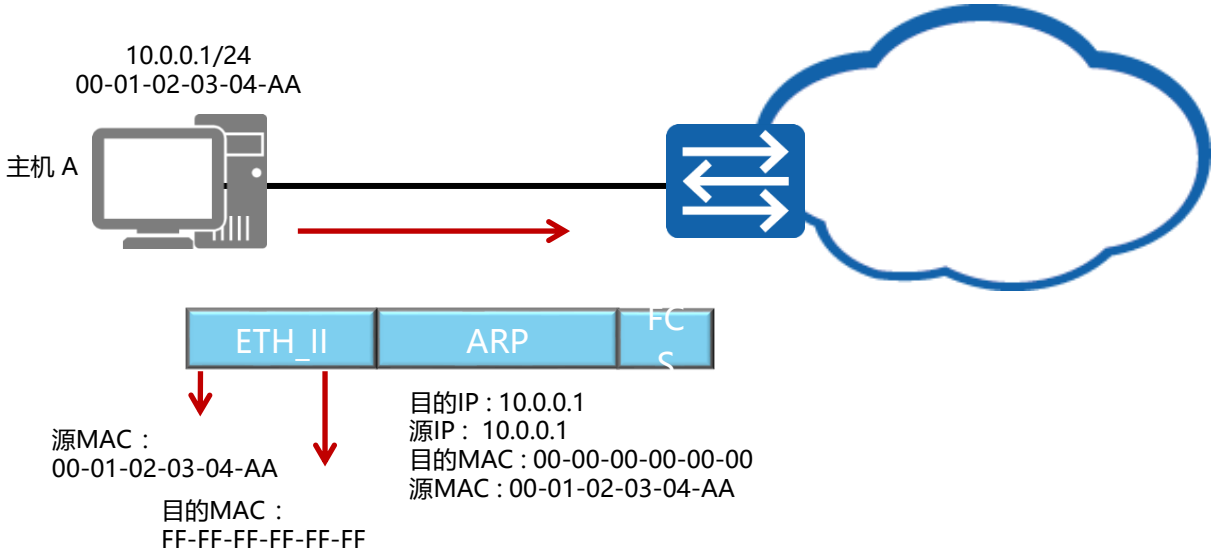
7

```
Host 1>arp -a
Internet Address      Physical Address      Type
192.168.1.2           48-A4-72-1C-8F-4F     Dynamic
```

Step 7：

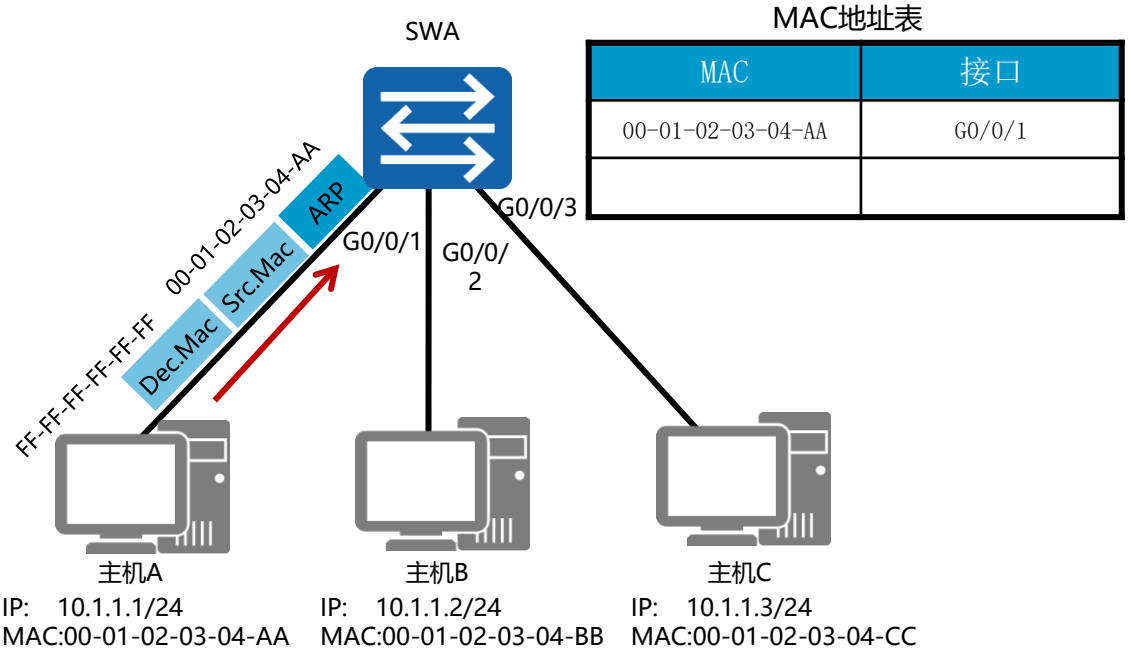
- 主机1收到ARP Reply以后，会检查ARP报文中目的端IP地址字段是否与自己的IP地址匹配。
- 如果匹配，会将ARP报文中的发送端MAC地址和发送端IP地址信息记录到自己的ARP缓存表中。

免费ARP



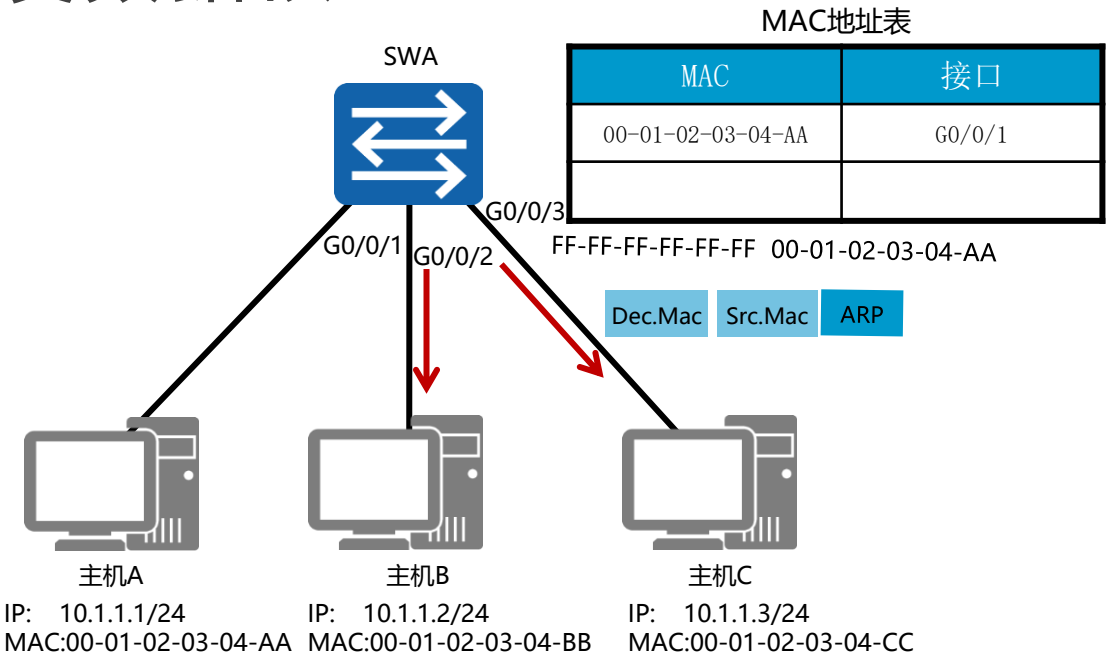
- 免费ARP可以用来探测IP地址是否冲突。

学习MAC地址



- 交换机将收到的数据帧的源MAC地址和对应接口记录到MAC地址表中。

转发数据帧

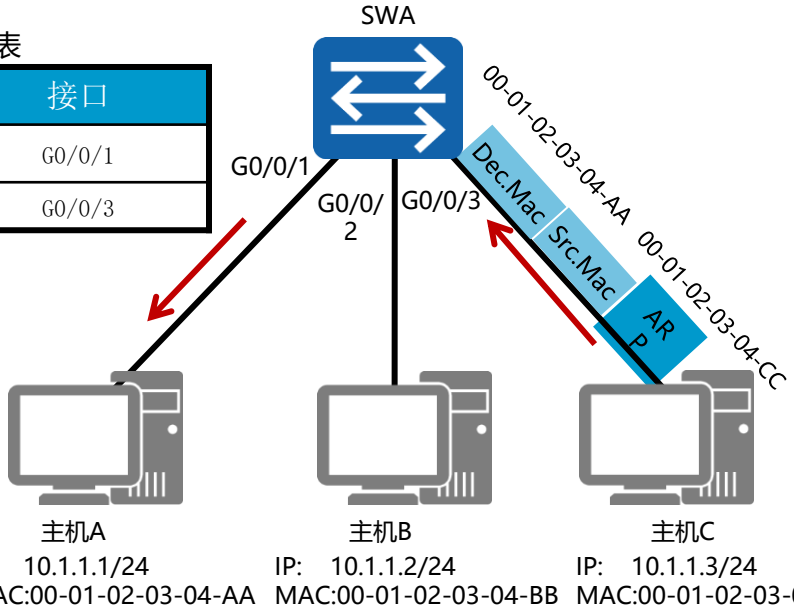


- 当数据帧的目的MAC地址不在MAC表中，或者目的MAC地址为广播地址时，交换机会泛洪该帧。

目标主机回复

MAC地址表

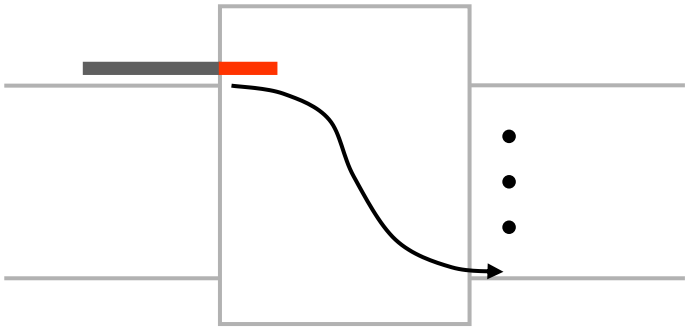
MAC	接口
00-01-02-03-04-AA	G0/0/1
00-01-02-03-04-CC	G0/0/3



- 交换机根据MAC地址表将目标主机的回复信息单播转发给源主机。

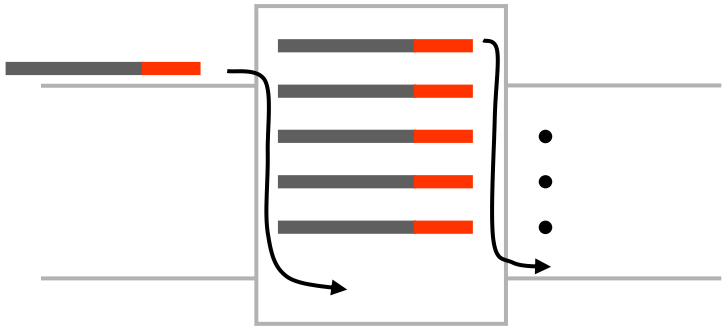
帧转发方式

- 直通转发：交换机收到帧头（通常只检查14个字节）后立刻察看目的MAC地址并进行转发



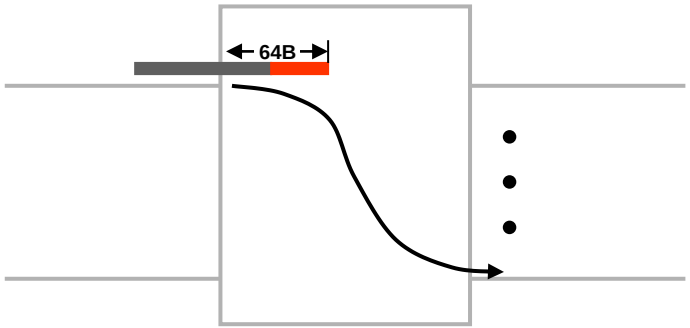
帧转发方式

- 存储转发：接收完整的帧，执行完校验后，转发正确的帧而丢弃错误的帧



帧转发方式

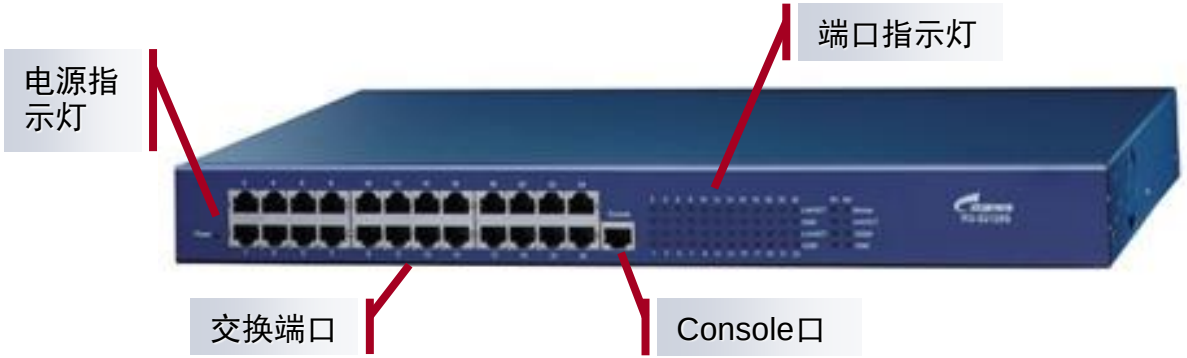
- 无碎片直通转发：交换机读取前64个字节后开始转发



帧转发方式

- 因为芯片技术的不断发展，存储与校验整个数据帧的延迟已经可以忽略，所以当今交换机均使用存储转发的方式。直通转发与无碎片直通转发已不被使用。

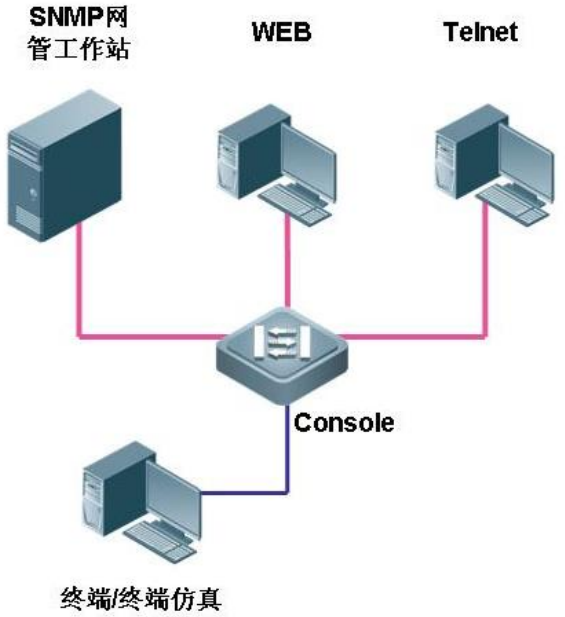
交换机的端口和指示灯



交换机

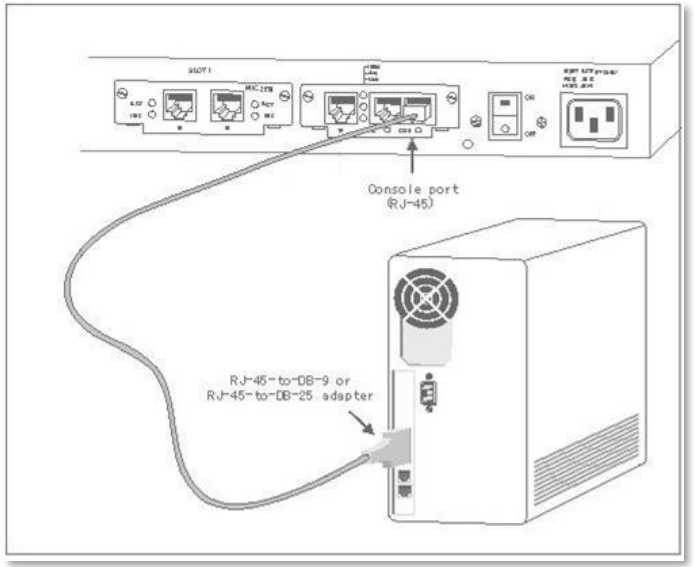
交换机的访问方式

- 通过带外方式对交换机进行管理
- 通过Telnet对交换机进行远程管理
- 通过Web对交换机进行远程管理
- 通过SNMP管理工作站对交换机进行远程管理



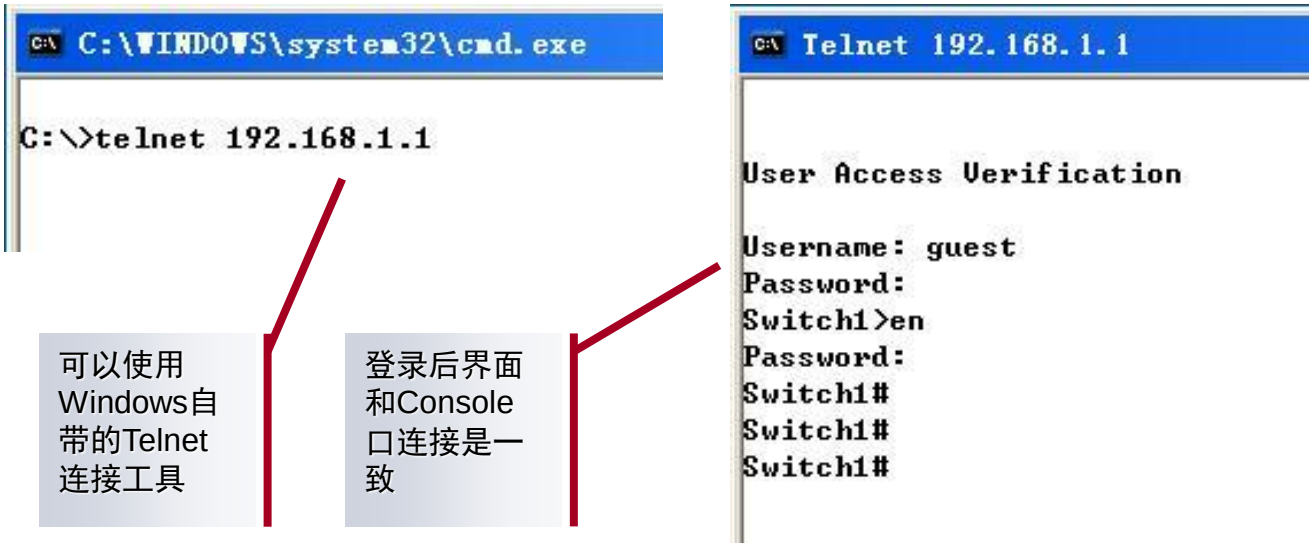
通过带外方式管理交换机

- 通过交换机的Console口，使用超级终端工具



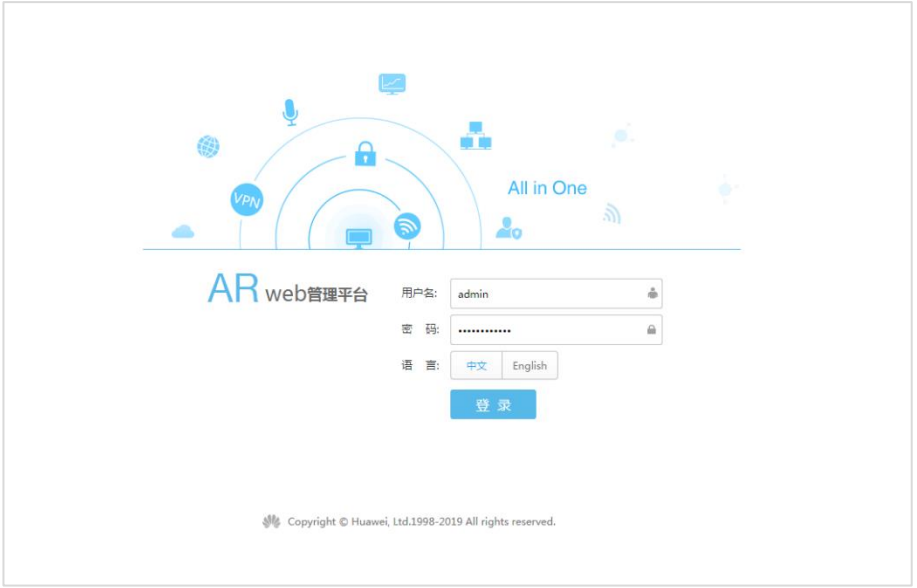
通过Telnet方式管理交换机

- 交换机必须已经配置了管理IP地址、密码等，并开启Telnet



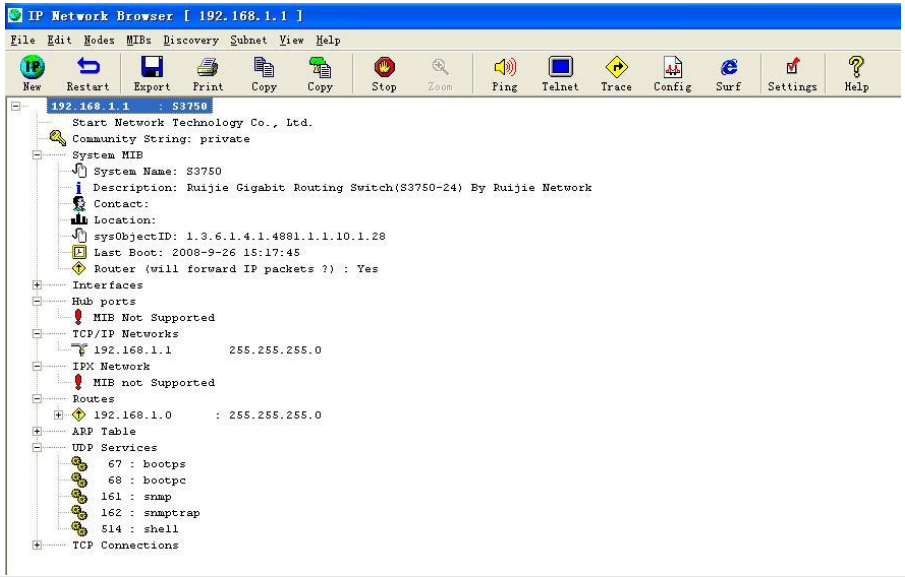
WEB网管方式登录

以华为AR系列路由器为例，PC终端打开浏览器软件，在地址栏中输入“https://192.168.1.1”，按下回车键，显示AR Web管理平台登录界面。



通过SNMP方式管理交换机

- 交换机必须已经配置了管理IP地址等，并设置了SNMP
- 需要网络管理软件配合使用



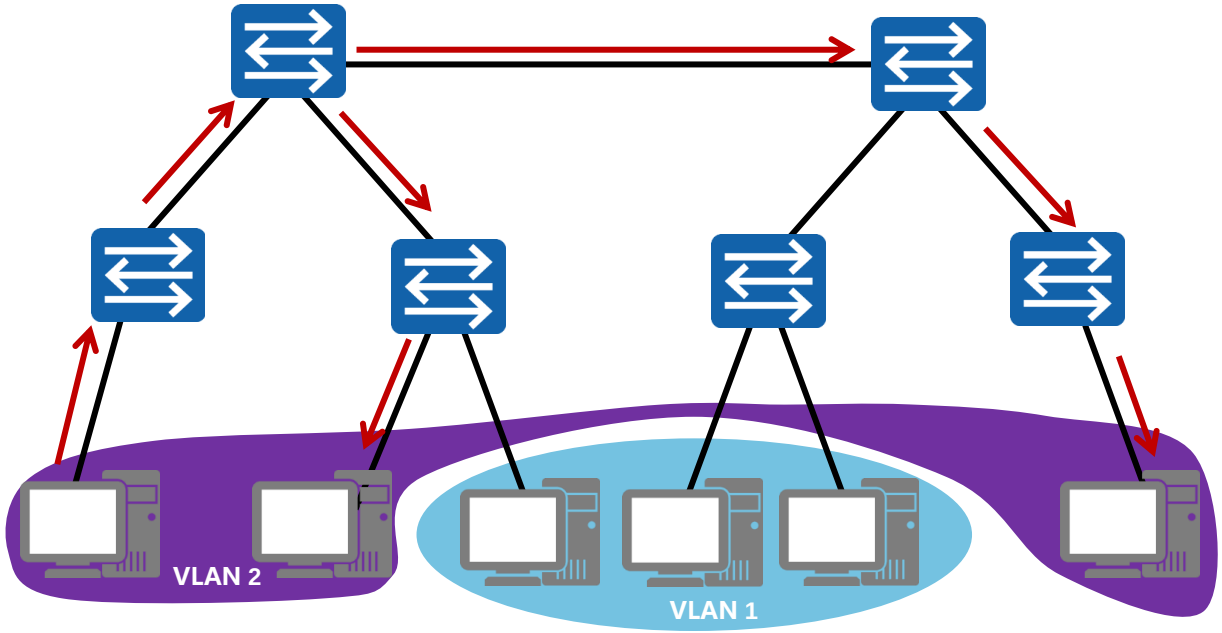
局域网技术

1. 以太网协议介绍
2. 局域网交换机的通讯原理?
3. VLAN-TRUNK
4. Vlan间通信
5. 局域网环路避免技术

VLAN产生的原因

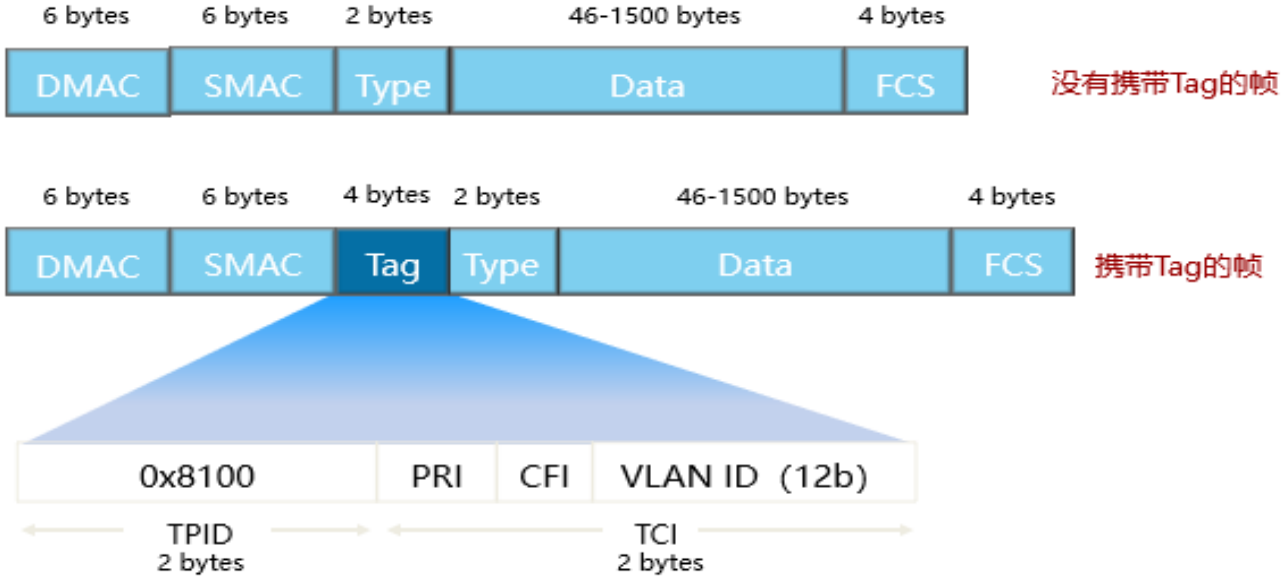
- 随着网络中计算机的数量越来越多，传统的以太网络开始面临冲突严重、广播泛滥以及安全性无法保障等各种问题。
- VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的局域网在逻辑上划分成多个广播域的技术。通过在交换机上配置VLAN，可以实现在同一个VLAN内的用户可以进行二层互访，而不同VLAN间的用户被二层隔离。这样既能够隔离广播域，又能够提升网络的安全性。

VLAN技术



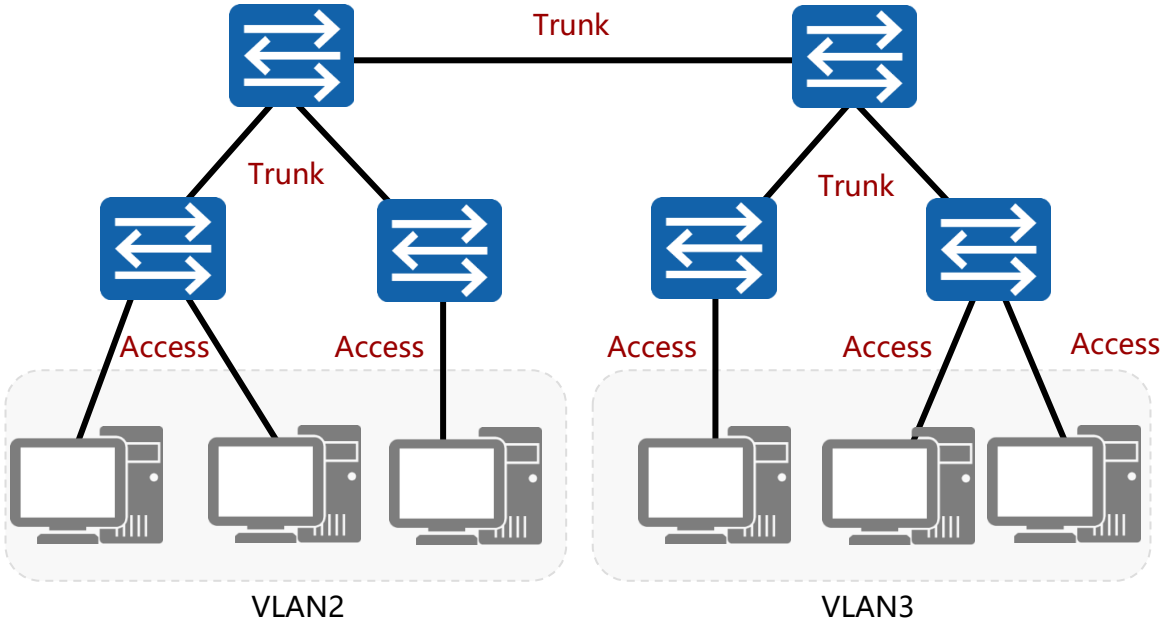
- VLAN能够隔离广播域。

VLAN帧格式



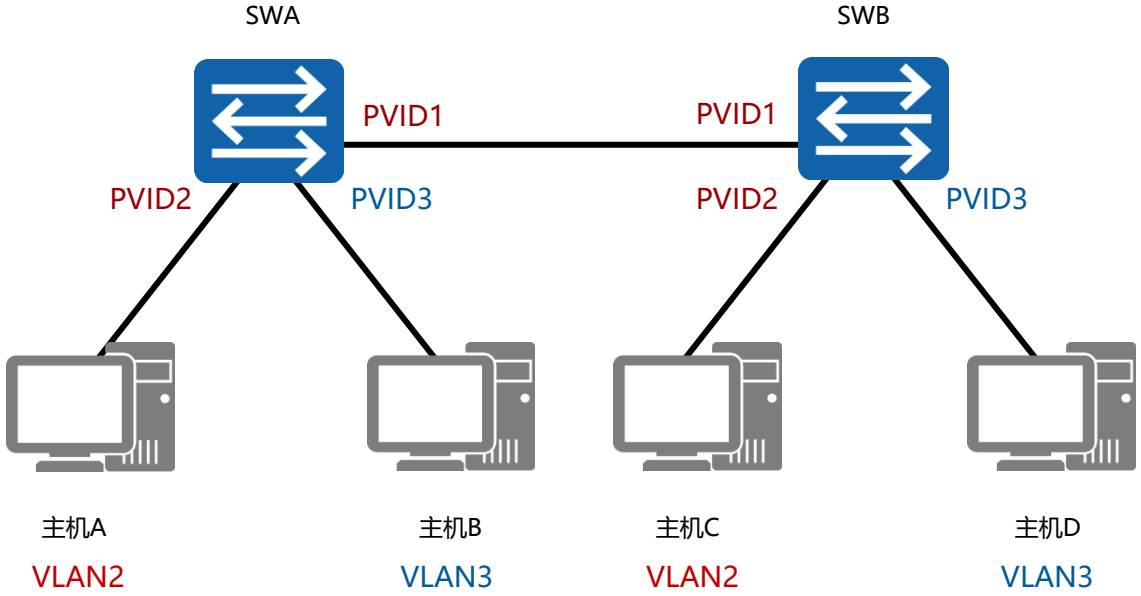
- 通过Tag区分不同VLAN。

链路类型



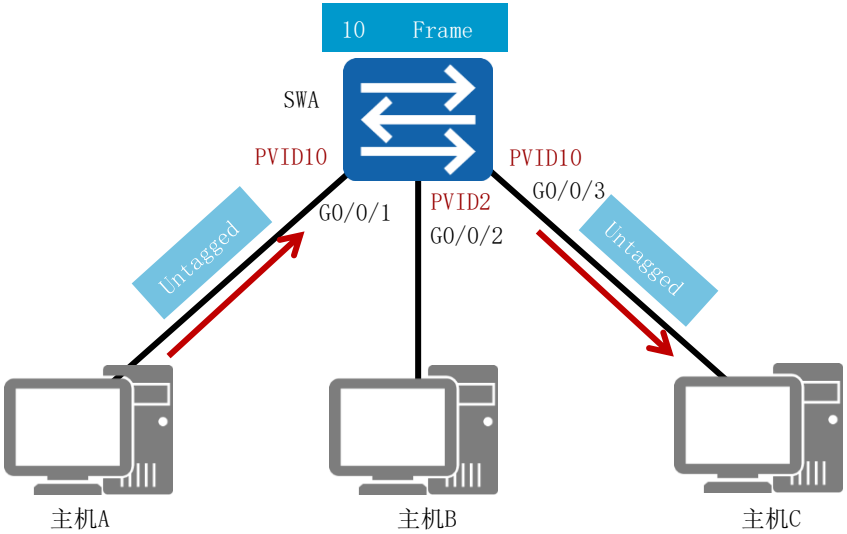
- 用户主机和交换机之间的链路为接入链路，交换机与交换机之间的链路为干道链路。

PVID



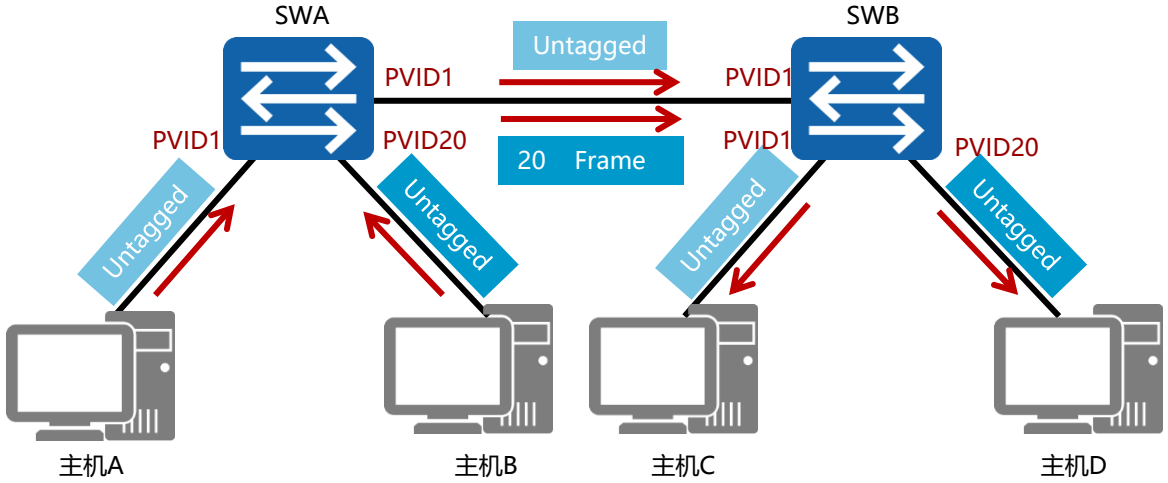
- PVID表示端口在缺省情况下所属的VLAN。

端口类型-Access



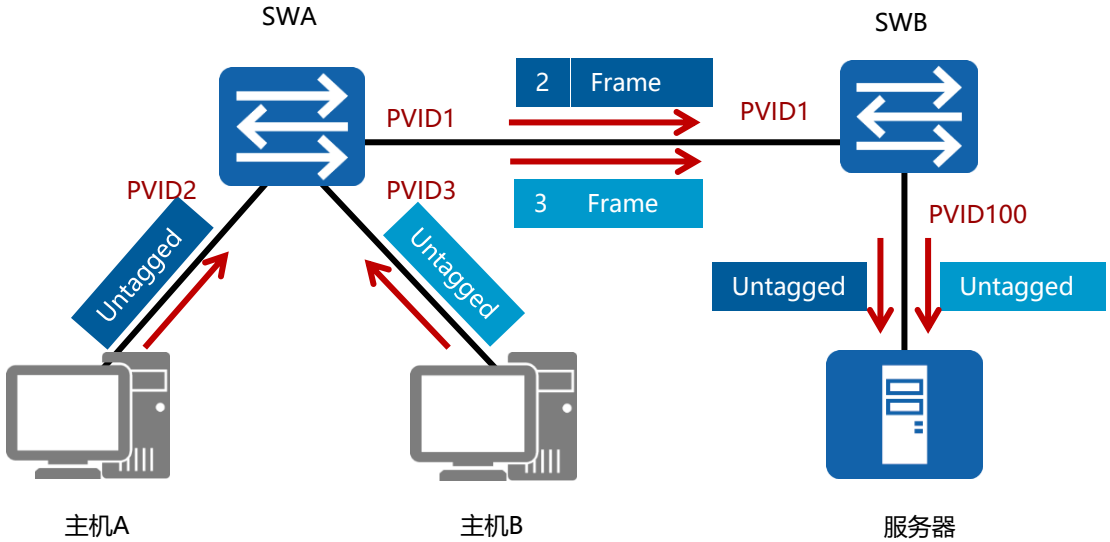
- Access端口在收到数据后会添加VLAN Tag，VLAN ID和端口的PVID相同。
- Access端口在转发数据前会移除VLAN Tag。

端口类型-Trunk



- 当Trunk端口收到帧时，如果该帧不包含Tag，将添加上端口的PVID；如果该帧包含Tag，则不改变。
- 当Trunk端口发送帧时，该帧的VLAN ID在Trunk的允许发送列表中：若与端口的PVID相同时，则剥离Tag发送；若与端口的PVID不同时，则直接发送。

端口类型-Hybrid

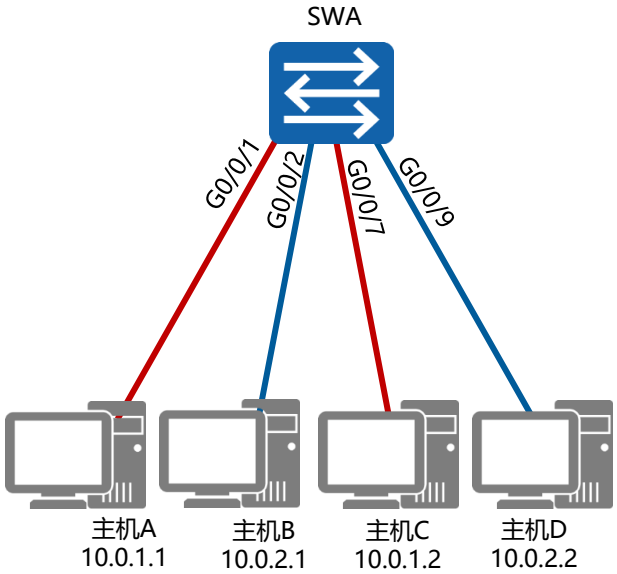


- Hybrid端口既可以连接主机，又可以连接交换机。
- Hybrid端口可以以Tagged 或Untagged方式加入VLAN 。

小结

Access接口	Trunk接口	Hybrid接口
接收数据帧 ▫ Untagged数据帧，打上PVID，接收。 ▫ Tagged数据帧，与PVID比较，相同则接收；不同则丢弃。	接收数据帧 ▫ Untagged数据帧，打上PVID，且VID在允许列表中，则接收；VID不在允许列表，则丢弃。 ▫ Tagged数据帧，查看VID是否在允许列表中，在允许列表中，则接收；VID不在允许列表，则丢弃。	接收数据帧 ▫ Untagged数据帧，打上PVID，且VID在允许列表中，则接收；VID不在允许列表中，则丢弃。 ▫ Tagged数据帧，查看VID是否在允许列表中，在允许列表中，则接收；VID不在允许列表，则丢弃。
发送数据帧 ▫ VID与PVID比较，相同则剥离标签发送；不同则丢弃。	发送数据帧 ▫ VID在允许列表中，且VID与PVID一致，则剥离标签发送。 ▫ VID在允许列表，但VID与PVID不一致，则直接带标签发送。 ▫ 不在允许列表中，则直接丢弃。	发送数据帧 ▫ VID不在允许列表中，直接丢弃。 ▫ VID在Untagged列表中，剥离标签发送。 ▫ VID在Tagged列表中，带标签直接发送。

VLAN划分方法



	VLAN 5	VLAN 10
基于端口	G0/0/1, G0/0/7	G0/0/2 G0/0/9
基于MAC地址	00-01-02-03-04-AA 00-01-02-03-04-CC	00-01-02-03-04-BB 00-01-02-03-04-DD
基于IP子网划分	10.0.1.*	10.0.2.*
基于协议划分	IP	IPX
基于策略	10.0.1.* + G0/0/1+ 00-01-02-03-04-AA	10.0.2.* + G0/0/2 + 00-01-02-03-04-BB

- 基于端口的VLAN划分方法在实际中最为常见。

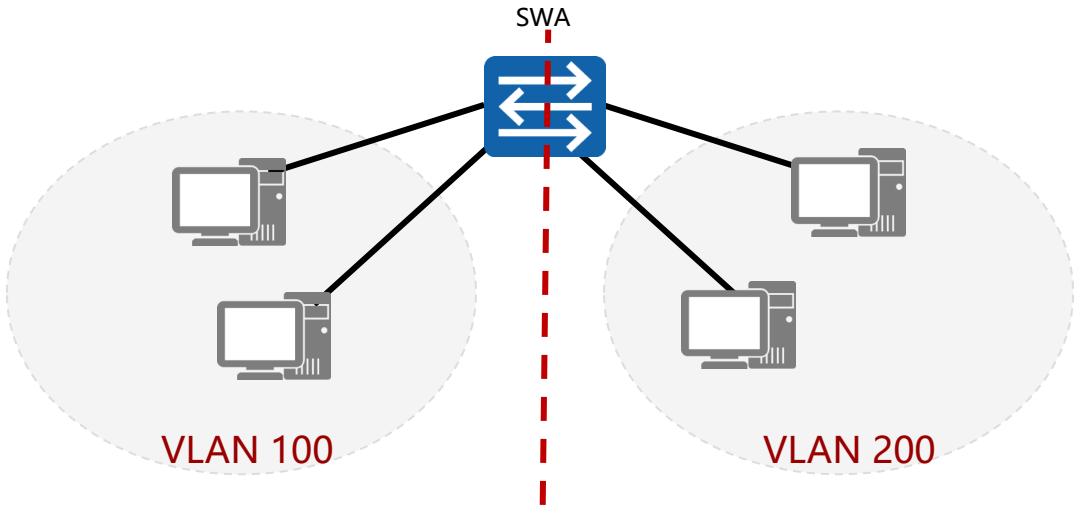
思考题？

1. 如果一个Trunk链路PVID是5，且端口下配置port trunk allow-pass vlan 2 3，那么哪些VLAN的流量可以通过该Trunk链路进行传输？
2. PVID为2的Access端口收到一个不带标记的帧会采取什么样的动作？

局域网技术

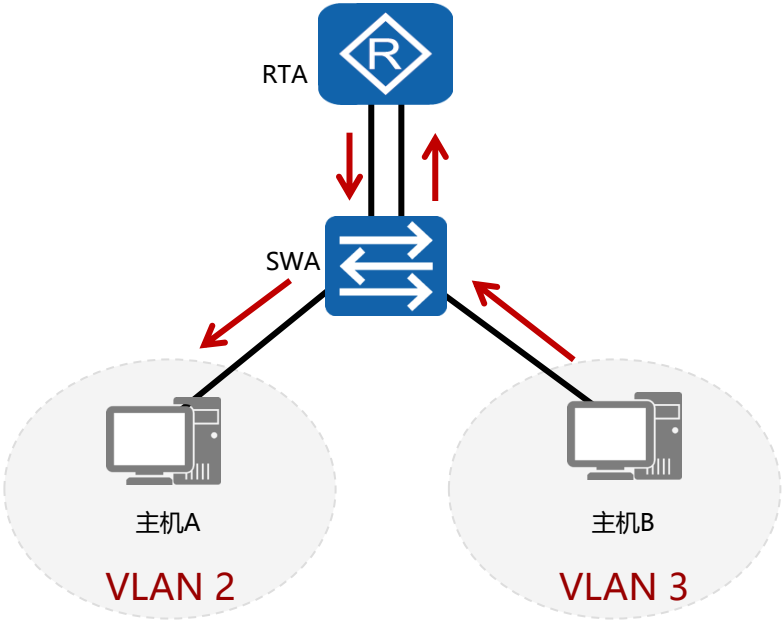
1. 以太网协议介绍
2. 局域网交换机的通讯原理?
3. VLAN-TRUNK
4. Vlan间通信
5. 局域网环路避免技术

VLAN的局限性



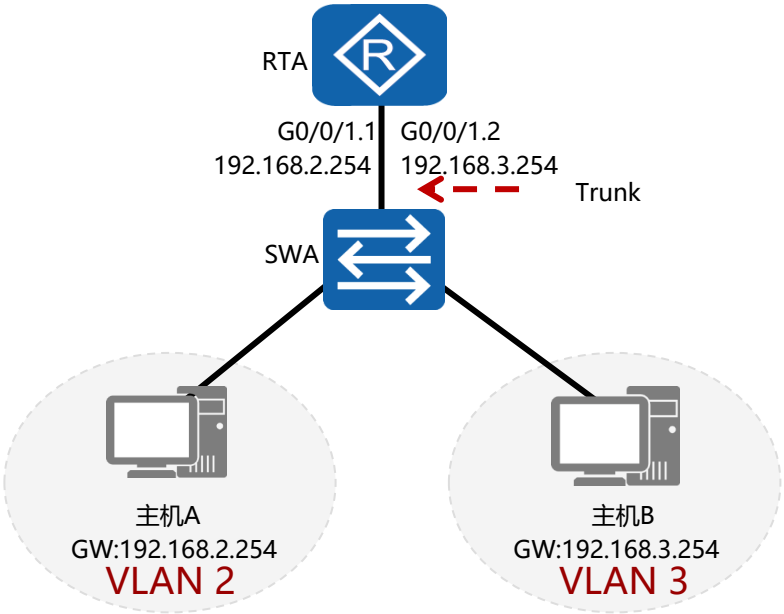
- VLAN在分割广播域的同时也限制了不同VLAN间的主机进行二层通信的能力。

VLAN路由-每个VLAN一个物理连接



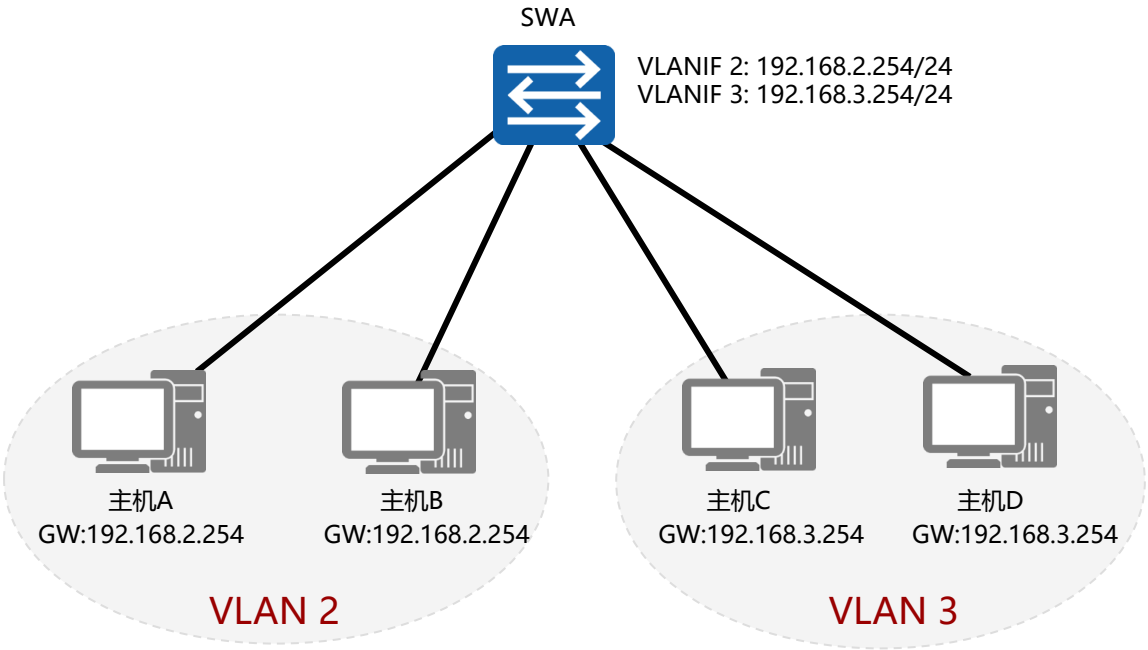
- 在二层交换机上配置VLAN，每一个VLAN使用一条独占的物理链路连接到路由器的一个接口上。

VLAN路由-单臂路由



- 将交换机和路由器之间的链路配置为Trunk链路，并且在路由器上创建子接口以支持VLAN路由。

VLAN路由-三层交换



- 为每个VLAN创建一个VLANIF接口作为网关。

局域网技术

1. 以太网协议介绍
2. 局域网交换机的通讯原理?
3. VLAN-TRUNK
4. Vlan间通信
5. 局域网环路避免技术

局域网环路避免

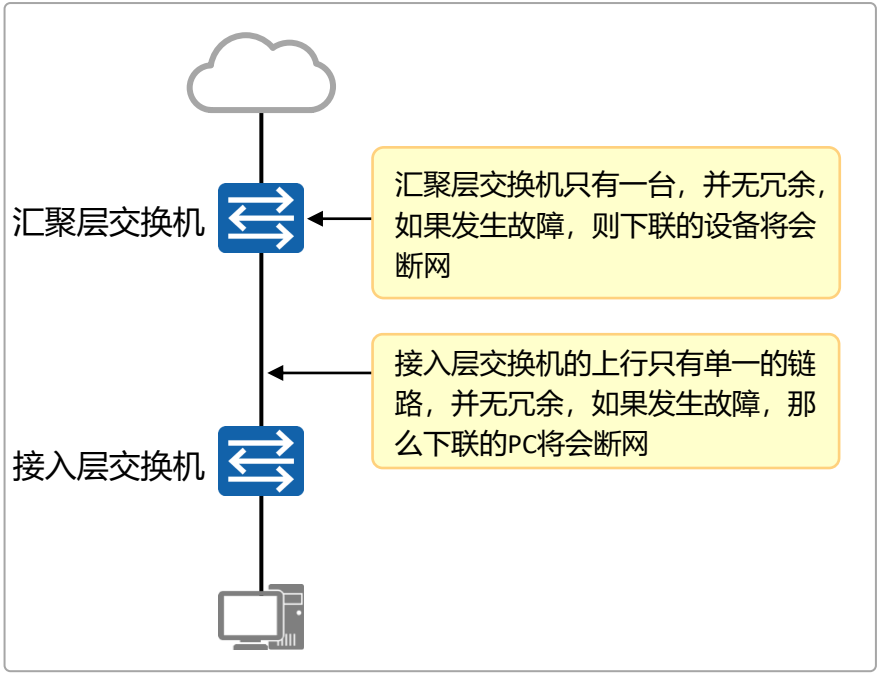
1. 为什么需要冗余？冗余带来的问题？
2. PVST-RPVST-MST，STP-RSTP-MST
3. 生成树优化
4. 生成树安全
5. 以太网链路聚合

生成树

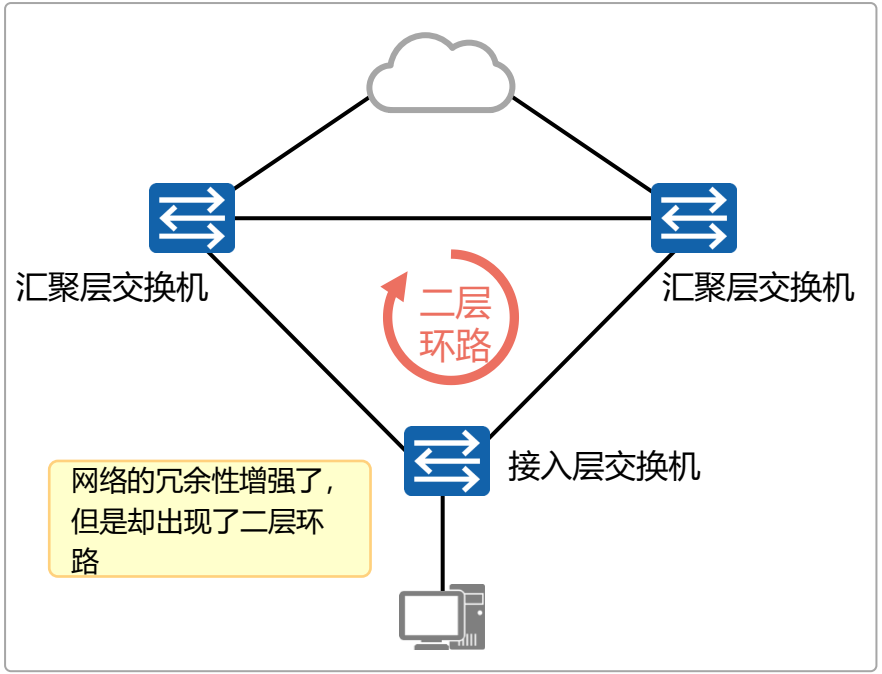
- 以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及MAC地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议STP（Spanning Tree Protocol）。
- 运行STP协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个接口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断循环，避免设备由于重复接收相同的报文造成处理能力下降。
- RSTP（Rapid Spanning Tree Protocol）协议基于STP协议，对原有的STP协议进行了更加细致的修改和补充，实现了网络拓扑快速收敛。

技术背景：二层交换机网络的冗余性与环路

一个缺乏冗余性设计的网络

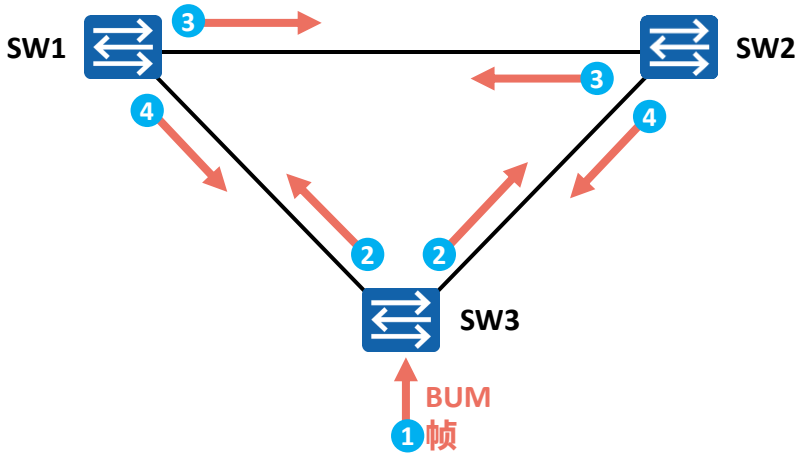


引入冗余性的同时也引入了二层环路



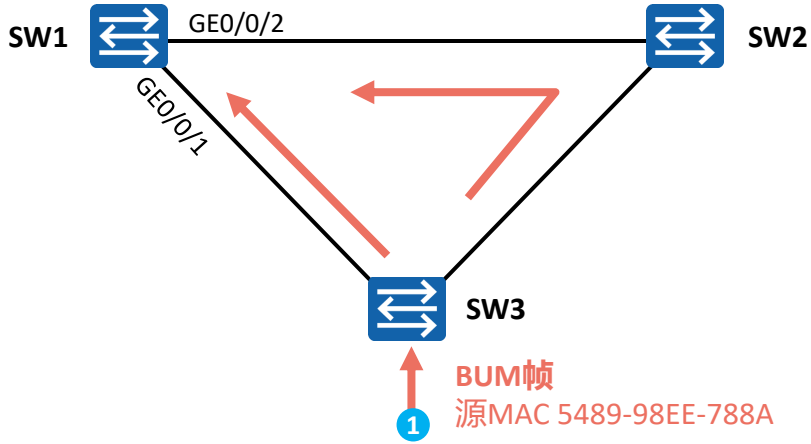
二层环路带来的问题

典型问题1：广播风暴



SW3收到BUM帧后将其进行泛洪，SW1及SW2收到后进一步泛洪，如此反复，最终导致整个网络资源被耗尽，网络瘫痪不可用。

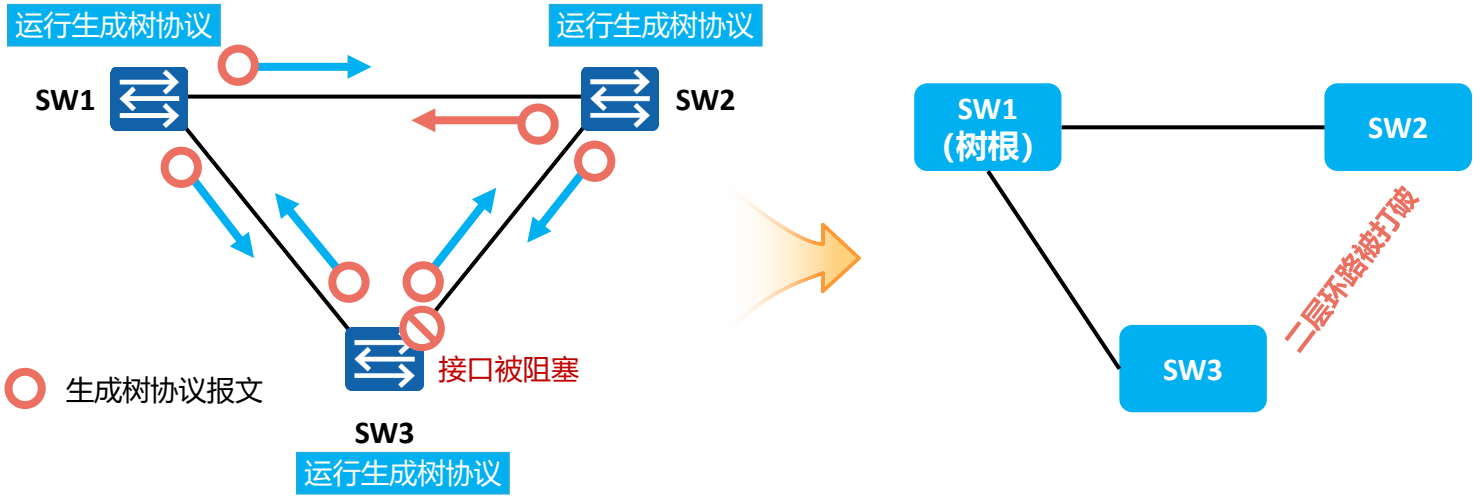
典型问题2：MAC地址漂移



以SW1为例，5489-98EE-788A会不断地在GE0/0/1与GE0/0/2接口之间来回切换，这被称为MAC地址漂移现象。

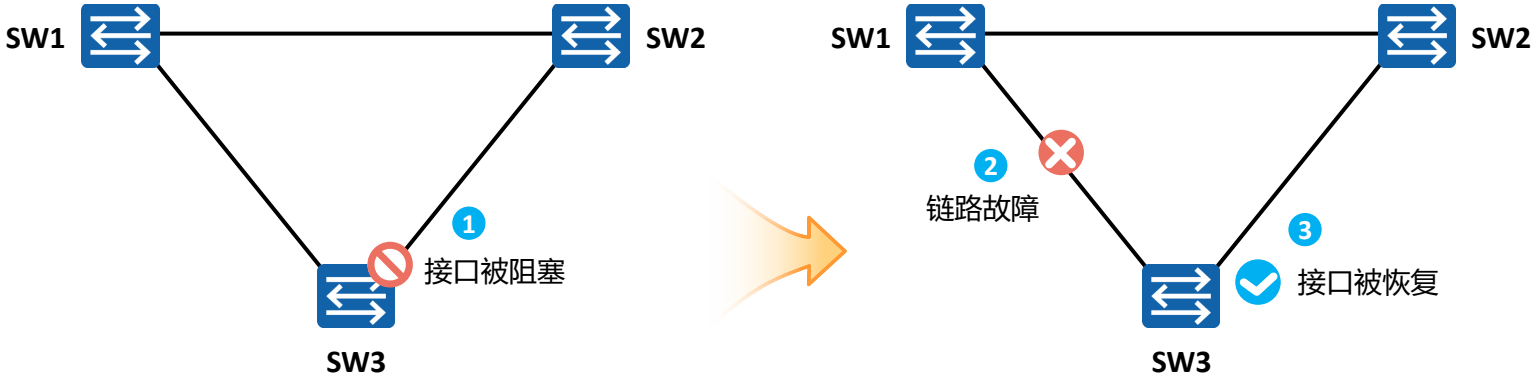
BUM帧（Broadcast，Unknown unicast，Multicast）指定广播、未知单播及组播帧

初识生成树协议



在网络中部署生成树后，交换机之间会进行生成树协议报文的交互并进行无环拓扑计算，最终将网络中的某个（或某些）接口进行阻塞（Block），从而打破环路。

生成树动态响应网络拓扑变化调整阻塞接口

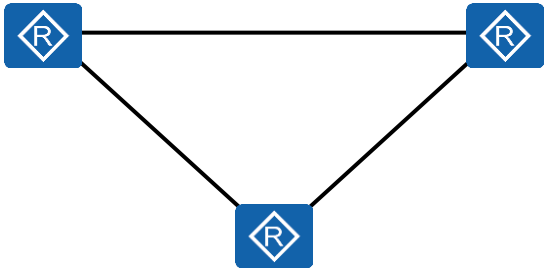


交换机上运行的生成树协议会持续监控网络的拓扑结构，当网络拓扑结构发生变化时，生成树能感知到这些变化，并且自动做出调整。

因此，生成树既能解决二层环路问题，也能为网络的冗余性提供一种方案。

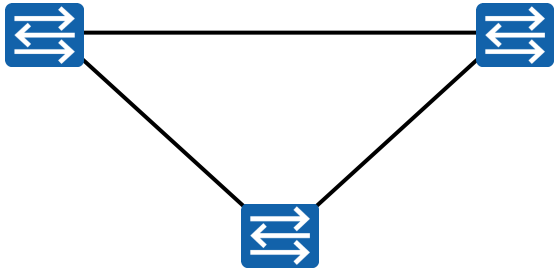
问答：二层及三层环路

三层环路（Layer 3 Loop）



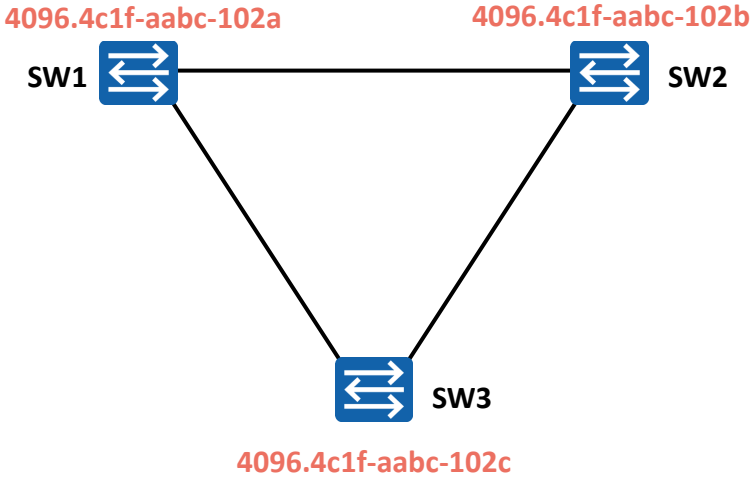
- 常见根因：路由环路；
- 动态路由协议有一定的防环能力；
- IP报文头部中的TTL字段可用于防止报文被无止尽地转发。

二层环路（Layer 2 Loop）



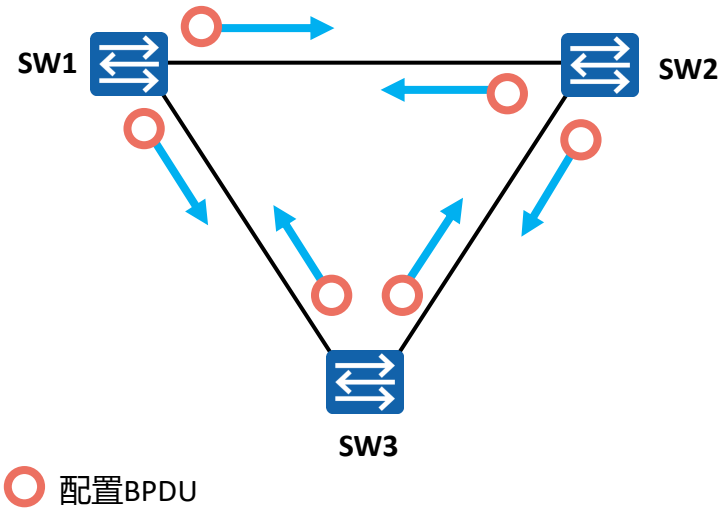
- 常见根因：网络中部署了二层冗余环境，或人为的误接线缆导致；
- 需借助特定的协议或机制实现二层防环；
- 二层帧头中并没有任何信息可用于防止数据帧被无止尽地转发。

STP操作



1. 选举一个根桥。
2. 每个非根交换机选举一个根端口。
3. 每个链路上选举一个指定端口。
4. 阻塞非根、非指定端口。

STP的基本概念：BPDU



BPDU（Bridge Protocol Data Unit，网桥协议数据单元）

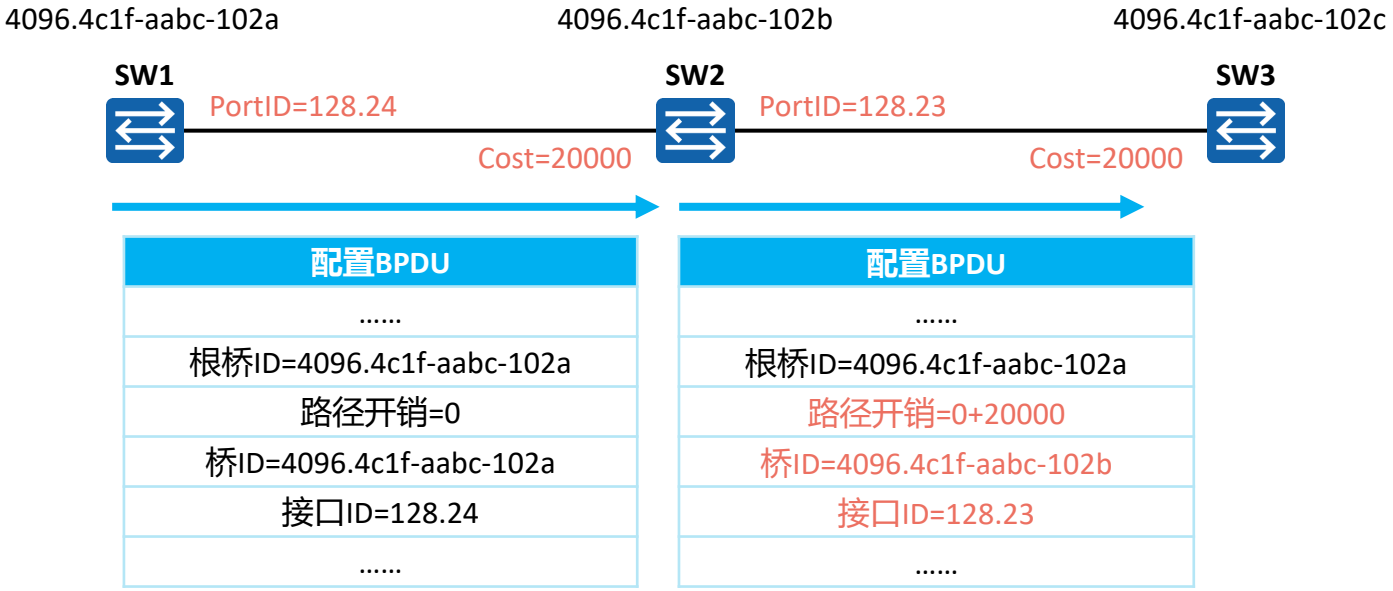
- BPDU是STP能够正常工作的根本。BPDU是STP的协议报文。
- STP交换机之间会交互BPDU报文，这些BPDU报文携带着一些重要信息，正是基于这些信息，STP才能够顺利工作。
- BPDU分为两种类型：
  - 配置BPDU（Configuration BPDU）
  - TCN BPDU（Topology Change Notification BPDU）
- 配置BPDU是STP进行拓扑计算的关键；TCN BPDU只在网络拓扑发生变更时才会被触发。

配置BPDU的报文格式

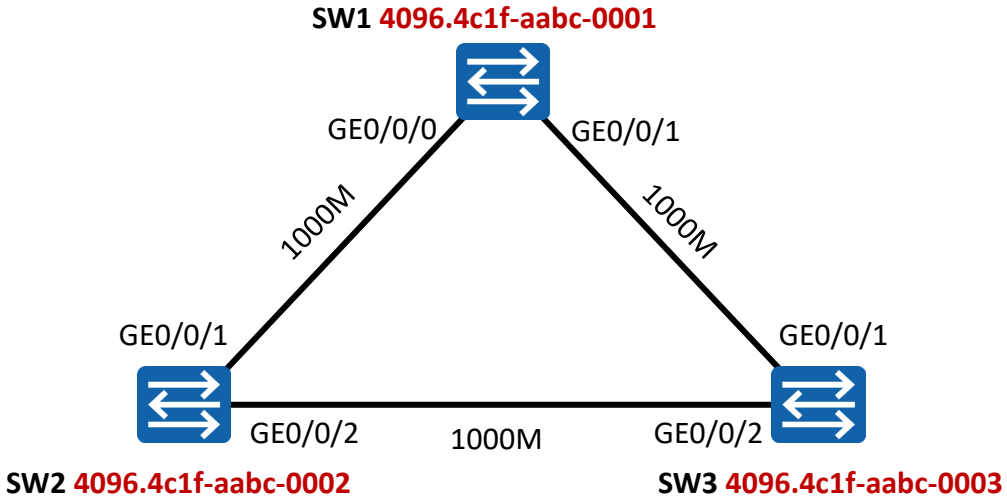
PID	PVI	BPDU Type	Flags	Root ID	RPC	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

字节	字段	描述
2	PID	协议ID，对于STP而言，该字段的值总为0
1	PVI	协议版本ID，对于STP而言，该字段的值总为0
1	BPDU Type	指示本BPDU的类型，若值为0x00，则表示本报文为配置BPDU；若值为0x80，则为TCN BPDU
1	Flags	标志，STP只使用了该字段的最高及最低两个比特位，最低位是TC（Topology Change，拓扑变更）标志，最高位是TCA（Topology Change Acknowledgment，拓扑变更确认）标志
8	Root ID	根网桥的桥ID
4	RPC	根路径开销，到达根桥的STP Cost
8	Bridge ID	BPDU发送桥的ID
2	Port ID	BPDU发送网桥的接口ID（优先级+接口号）
2	Message Age	消息寿命，从根网桥发出BPDU之后的秒数，每经过一个网桥都减1，所以它本质上是到达根桥的跳数
2	Max Age	最大寿命，当一段时间未收到任何BPDU，生存期到达最大寿命时，网桥认为该接口连接的链路发生故障。默认20s
2	Hello Time	根网桥连续发送的BPDU之间的时间间隔，默认2s
2	Forward Delay	转发延迟，在侦听和学习状态所停留的时间间隔，默认15s

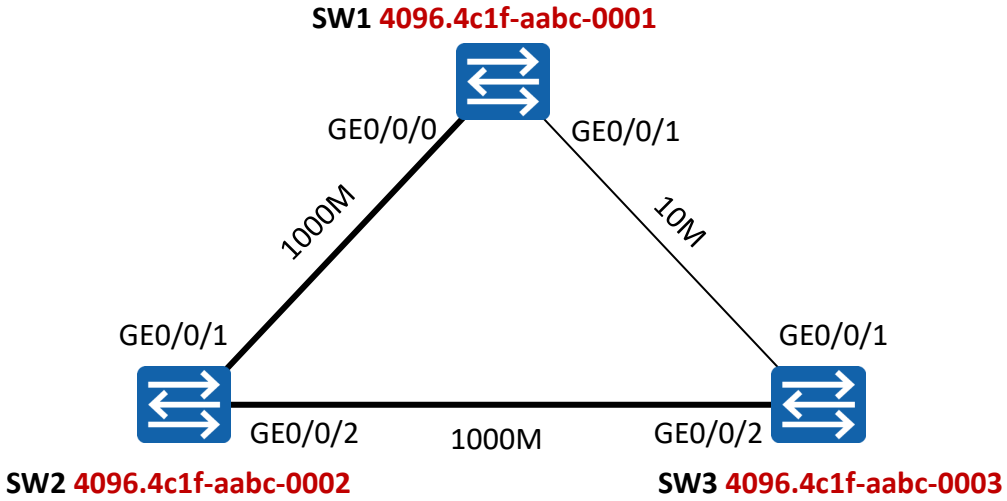
配置BPDU的转发过程



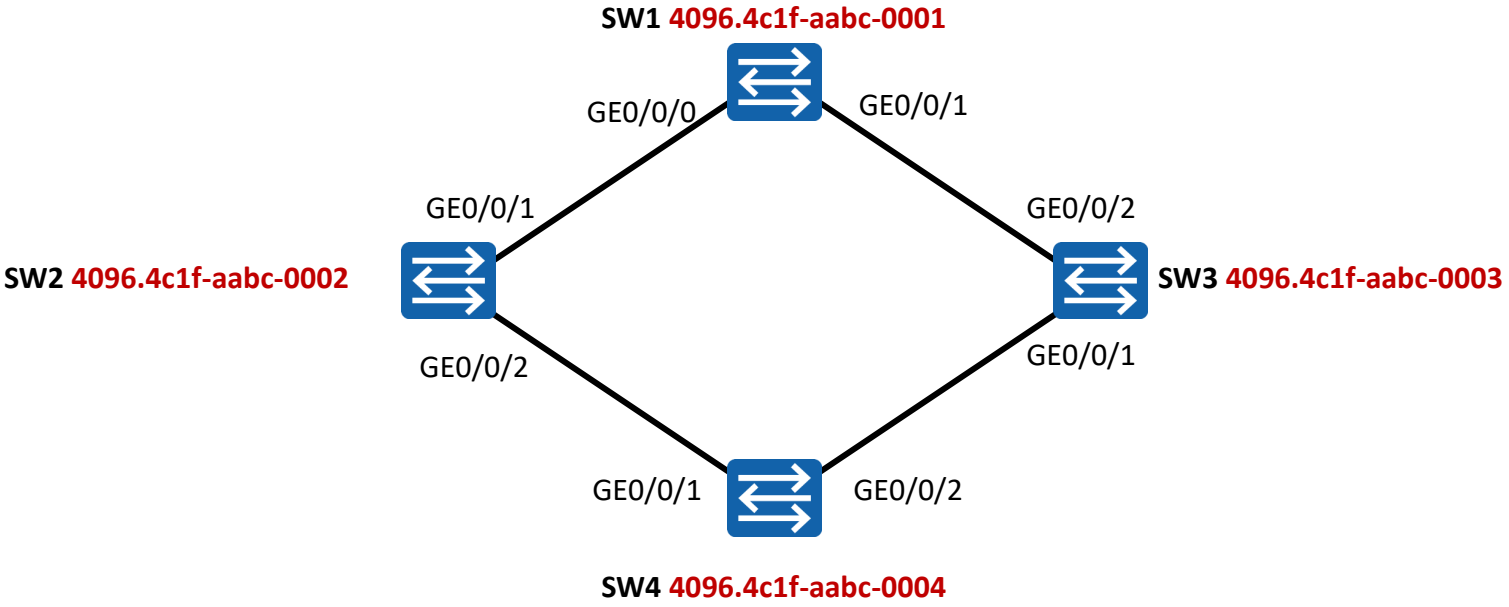
思考题1：识别以下拓扑中的根桥及各种接口角色



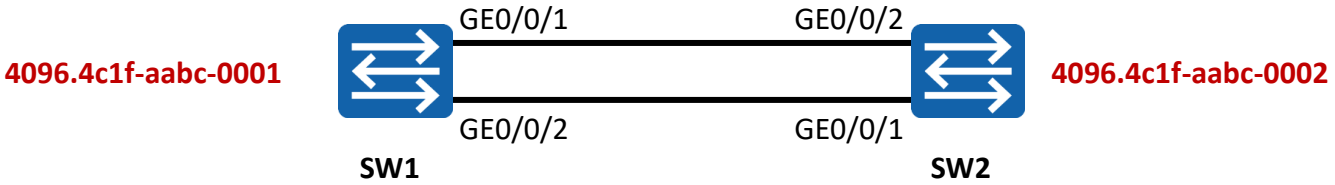
思考题2：识别以下拓扑中的根桥及各种接口角色



思考题3：识别以下拓扑中的根桥及各种接口角色



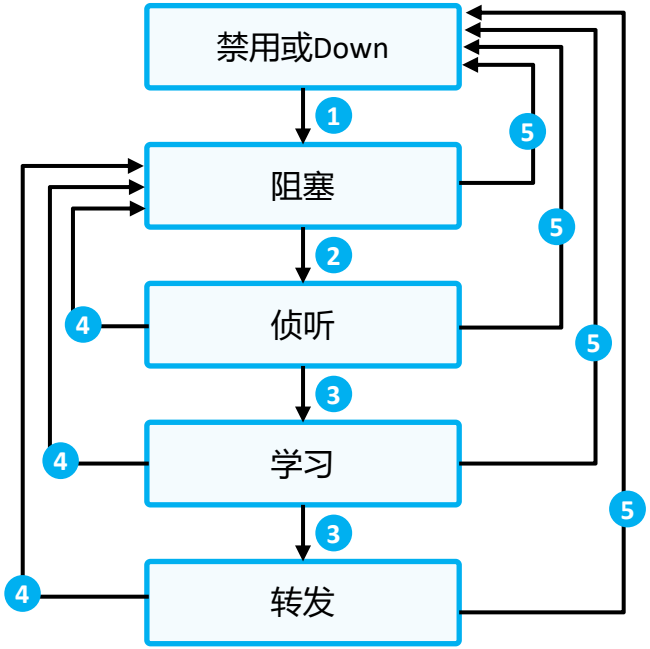
思考题4：识别以下拓扑中的根桥及各种接口角色



STP的接口状态

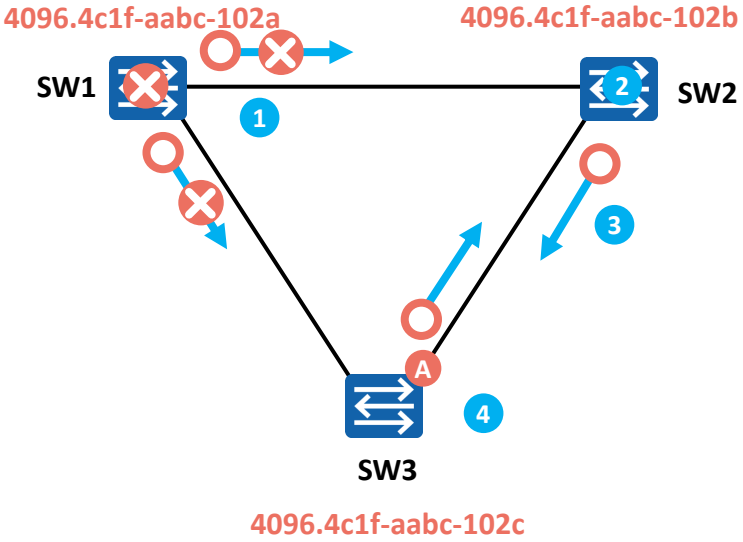
状态名称	状态描述
禁用（Disable）	该接口不能收发BPDU，也不能收发业务数据帧，例如接口为down
阻塞（Blocking）	该接口被STP阻塞。处于阻塞状态的接口不能发送BPDU，但是会持续侦听BPDU，而且不能收发业务数据帧，也不会进行MAC地址学习
侦听（Listening）	当接口处于该状态时，表明STP初步认定该接口为根接口或指定接口，但接口依然处于STP计算的过程中，此时接口可以收发BPDU，但是不能收发业务数据帧，也不会进行MAC地址学习
学习（Learning）	当接口处于该状态时，会侦听业务数据帧（但是不能转发业务数据帧），并且在收到业务数据帧后进行MAC地址学习。可以防止临时环路
转发（Forwarding）	处于该状态的接口可以正常地收发业务数据帧，也会进行BPDU处理。接口的角色需是根接口或指定接口才能进入转发状态

STP的接口状态迁移



1. 接口初始化或激活，自动进入阻塞状态
2. 接口被选举为根接口或指定接口，自动进入侦听状态
3. 转发延迟计时器超时且接口依然为根接口或指定接口
4. 接口不再是根接口或指定接口或指定状态
5. 接口被禁用或者链路失效

拓扑变化 – 根桥故障

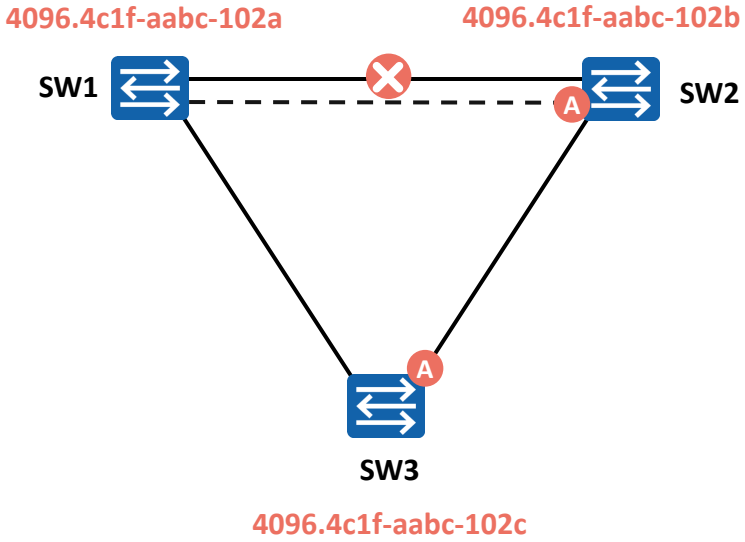


根桥故障恢复过程

1. SW1根桥发生故障，停止发送BPDU报文。
2. SW2等待Max Age计时器（20 s）超时，从而导致已经收到的BPDU报文失效，又接收不到根桥发送的新的BPDU报文，从而得知上游出现故障。
3. 非根桥会互相发送配置BPDU，重新选举新的根桥。
4. 经过重新选举后，SW3的A端口经过两个Forward Delay（15 s）时间恢复转发状态。

- 非根桥会在BPDU老化之后开始根桥的重新选举。
- 根桥故障会导致50 s左右的恢复时间。

拓扑变化 – 直连链路故障



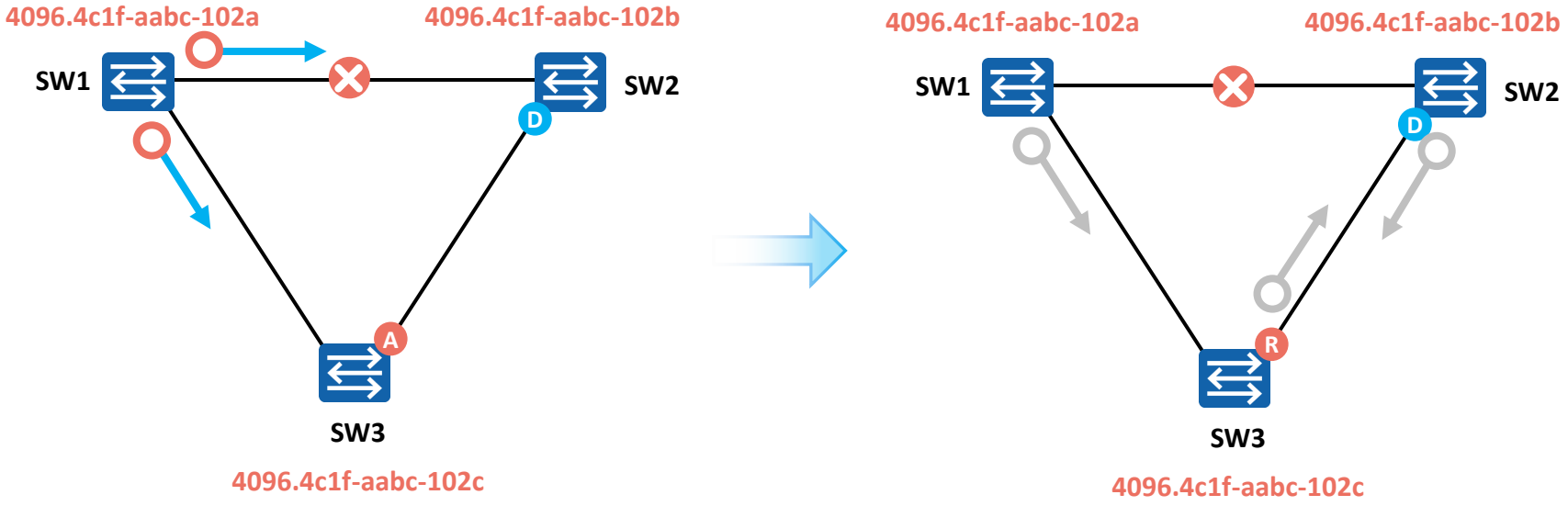
直连链路故障恢复过程

当交换机SW2网络稳定时检测到根端口的链路发生故障，则其备用端口会经过两倍的Forward Delay（15s）时间进入用户流量转发状态。

- SW2检测到直连链路物理故障后，会将预备端口转换为根端口。
- 直连链路故障，备用端口会经过30s后恢复转发状态。

拓扑变化 – 非直连链路故障

- 非直连链路故障后，SW3的备用端口恢复到转发状态，非直连故障会导致50s左右的恢复时间。

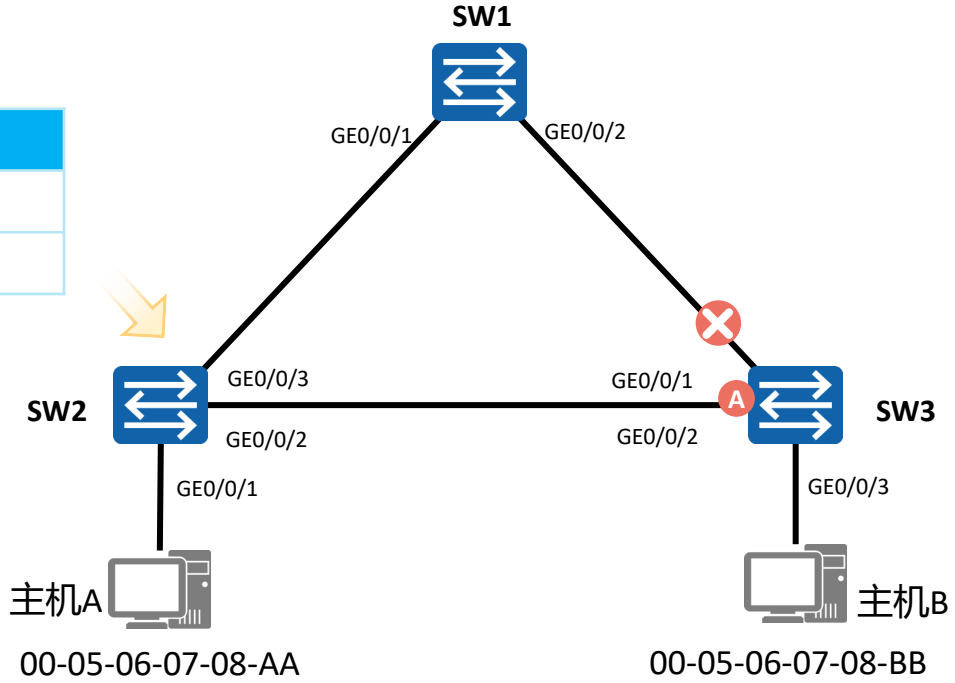


拓扑改变导致MAC地址表错误

MAC地址表

MAC	端口
00-05-06-07-08-AA	GE0/0/1
00-05-06-07-08-BB	GE0/0/3

如图，SW3的根端口发生故障，导致生成树拓扑重新收敛，在生成树拓扑完成收敛之后，从主机A到主机B的帧仍然不能到达目的地。这是因为交换机依赖MAC地址表转发数据帧，缺省情况下，MAC地址表项的老化时间是300秒。那么该怎么快速恢复转发?

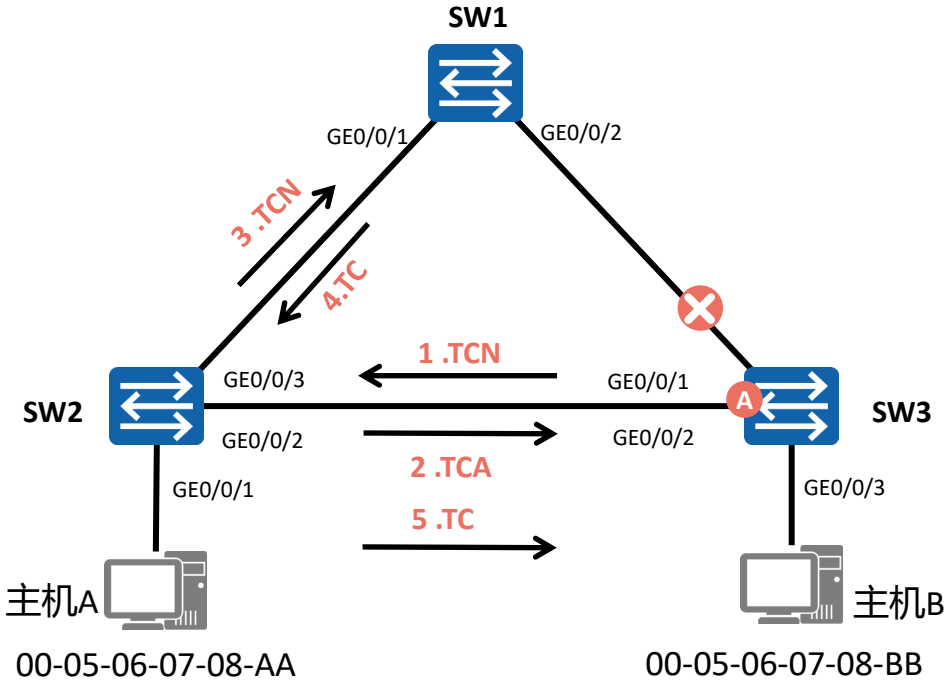


拓扑改变导致MAC地址表错误

MAC地址表

MAC	端口
00-05-06-07-08-AA	GE0/0/3
00-05-06-07-08-BB	GE0/0/1
00-05-06-07-08-BB	GE0/0/2

- TCN BPDU在网络拓扑变化的时候产生。
- 报文格式：协议标识、版本号和类型。
- 拓扑变化：会使用到配置BPDU中Flags的TCA和TC位。



STP的基础配置命令（1）

1. 配置生成树工作模式

```
[Huawei] stp mode { stp | rstp | mstp }
```

交换机支持STP、RSTP和MSTP（Multiple Spanning Tree Protocol）三种生成树工作模式，默认情况工作在MSTP模式。

2. （可选）配置根桥

```
[Huawei] stp root primary
```

配置当前设备为根桥。缺省情况下，交换机不作为任何生成树的根桥。配置后该设备优先级数值自动为0，并且不能更改设备优先级。

3. （可选）备份根桥

```
[Huawei] stp root secondary
```

配置当前交换机为备份根桥。缺省情况下，交换机不作为任何生成树的备份根桥。配置后该设备优先级数值为4096，并且不能更改设备优先级。

STP的基础配置命令（2）

1. （可选）配置交换机的STP优先级

```
[Huawei] stp priority priority
```

缺省情况下，交换机的优先级取值是32768。

2. （可选）配置接口路径开销

```
[Huawei-GigabitEthernet0/0/1] stp cost cost
```

设置当前接口的路径开销值。

STP的基础配置命令（3）

1. （可选）配置接口优先级

```
[Huawei-intf] stp priority priority
```

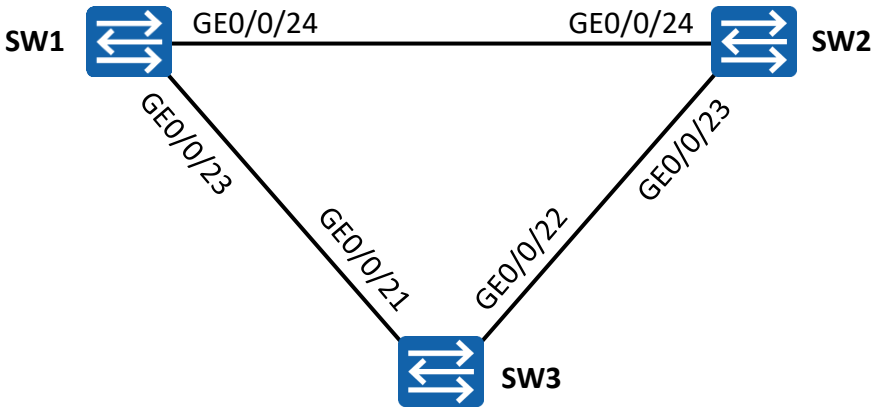
配置接口的优先级。缺省情况下，交换机接口的优先级取值是128。

2. 启用STP/RSTP/MSTP

```
[Huawei] stp enable
```

使能交换机的STP/RSTP/MSTP功能。缺省情况下，设备的STP/RSTP/MSTP功能处于启用状态。

案例1：STP的基础配置



- 在上述三台交换机上部署STP，以便消除网络中的二层环路。
- 通过配置，将SW1指定为根桥，并使SW3的GE0/0/22接口被STP阻塞。

SW1的配置如下：

```
[SW1] stp mode stp
[SW1] stp enable
[SW1] stp priority 0
```

SW2的配置如下：

```
[SW2] stp mode stp
[SW2] stp enable
[SW2] stp priority 4096
```

SW3的配置如下：

```
[SW3] stp mode stp
[SW3] stp enable
[SW3] stp priority 0
```

案例1：STP的基础配置

在SW3上查看STP接口状态摘要：

<SW3> **display stp brief**

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/21	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/22	ALTE	DISCARDING	NONE

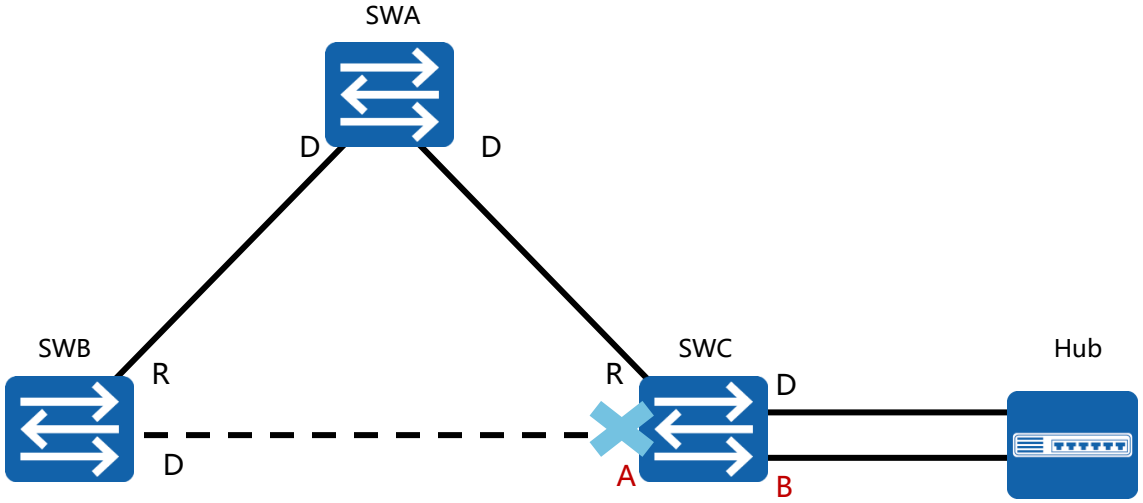
RSTP概述

- IEEE 802.1w中定义的RSTP可以视为STP的改进版本，RSTP在许多方面对STP进行了优化，它的收敛速度更快，而且能够兼容STP。
- RSTP引入了新的接口角色，其中替代接口的引入使得交换机在根接口失效时，能够立即获得新的路径到达根桥。备份端口作为指定端口的备份，帮助链路上的网桥快速获得到根桥的备份路径。RSTP的状态规范根据端口是否转发用户流量和学习MAC地址把原来的5种状态缩减为3种。 另外，RSTP还引入了边缘接口的概念，这使得交换机连接终端设备的接口在初始化之后能够立即进入转发状态，提高了工作效率。

RSTP对STP的其他改进

- 配置BPDU的处理发生变化：
  - 拓扑稳定后，配置BPDU报文的发送方式进行了优化
  - 使用更短的BPDU超时计时
  - 对处理次等BPDU的方式进行了优化
- 配置BPDU格式的改变，充分利用了STP协议报文中的Flag字段，明确了接口角色
- RSTP拓扑变化处理：相比于STP进行了优化，加速针对拓扑变更的反应速度

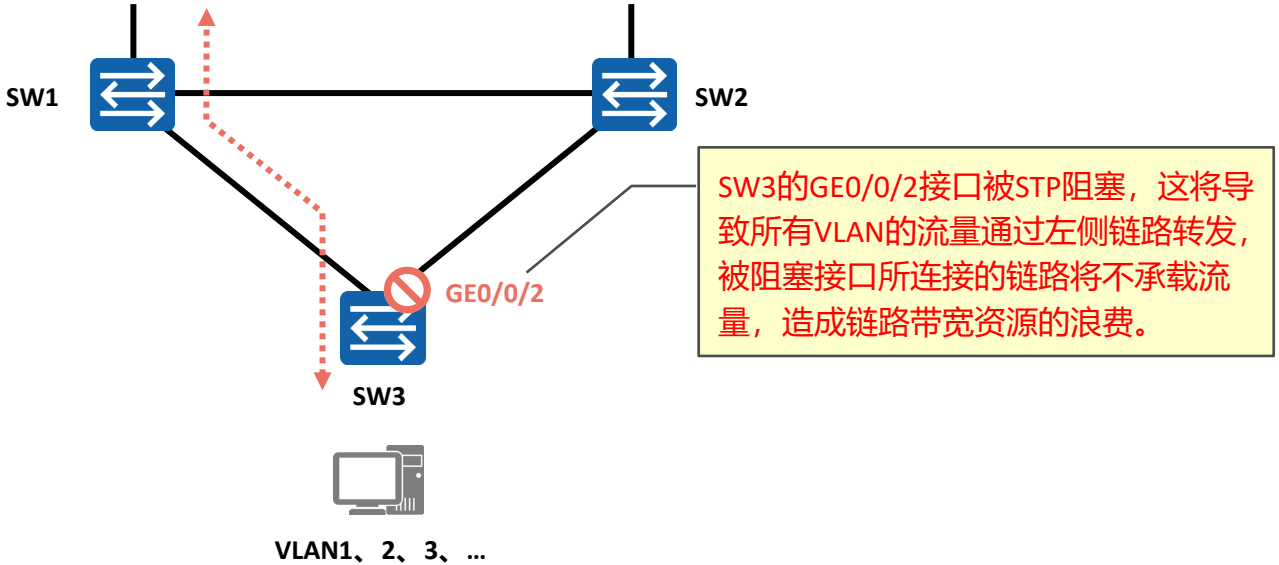
RSTP端口角色



角色	描述
Backup	Backup端口作为指定端口的备份，提供了另外一条从根桥到非根桥的备份链路。
Alternate	Alternate端口作为根端口的备份端口，提供了从指定桥到根桥的另一条备份路径。

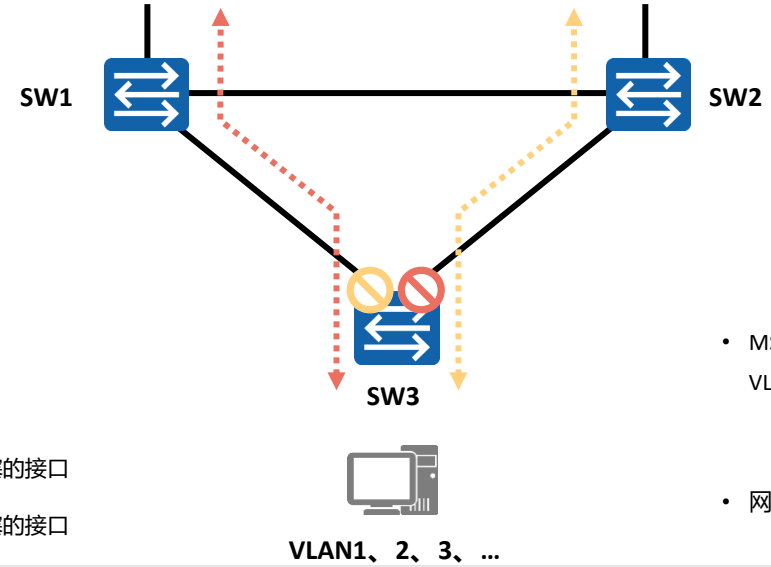
STP/RSTP的缺陷：所有的VLAN共享一棵生成树

- RSTP在STP基础上进行了改进，实现了网络拓扑快速收敛。
- 但RSTP和STP还存在同一个缺陷：由于局域网内所有的VLAN共享一棵生成树，因此无法在VLAN间实现数据流量的负载均衡，链路被阻塞后将不承载任何流量，还有可能造成部分VLAN的报文无法转发。



MSTP：多生成树

- 为了弥补STP和RSTP的缺陷，IEEE于2002年发布的802.1s标准定义了MSTP。
- MSTP兼容STP和RSTP，既可以快速收敛，又提供了数据转发的多个冗余路径，在数据转发过程中实现VLAN数据的负载均衡。



- MSTP将VLAN映射到一个生成树的实例，若干个VLAN可共用一棵生成树。例如：
  - 将偶数VLAN映射到实例1
  - 将基数VLAN映射到实例2
- 网络中将只维护2棵生成树。

MSTP概述

- MSTP把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。
- 每棵生成树叫做一个多生成树实例MSTI（Multiple Spanning Tree Instance）。
- 所谓生成树实例就是多个VLAN的一个集合。
- 通过将多个VLAN捆绑到一个实例，可以节省通信开销和资源占用率。
- MSTP各个实例拓扑的计算相互独立，在这些实例上可以实现负载均衡。
- 可以把多个相同拓扑结构的VLAN映射到一个实例里，这些VLAN在接口上的转发状态取决于接口在对应实例的状态。

生成树协议的比较

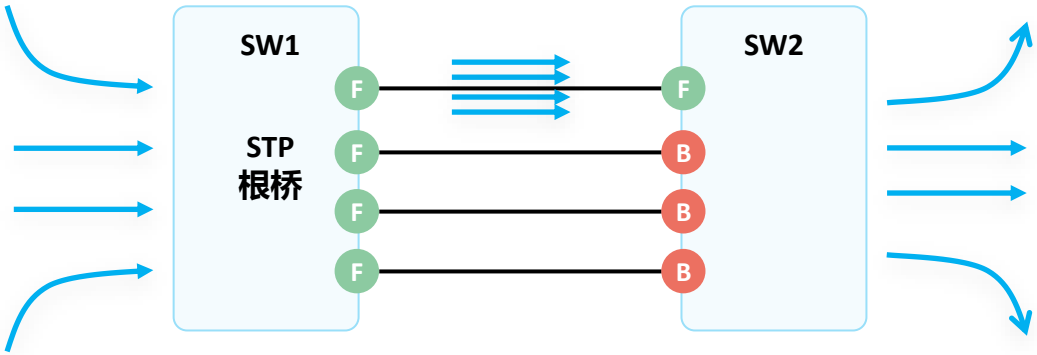
	标准	占用资源	收敛	
CST	802.1D	低	慢	所有VLAN
PVST+	Cisco	高	慢	每VLAN
RSTP	802.1W	中等	快	所有VLAN
PVRST+	Cisco	非常高	快	每VLAN
MSTP	802.1s Cisco	中等或高	快	VLAN列表

提升链路带宽

- 设备之间存在多条链路时，由于STP的存在，实际只会有一条链路转发流量，设备间链路带宽无法得到提升。

F 转发流量的接口

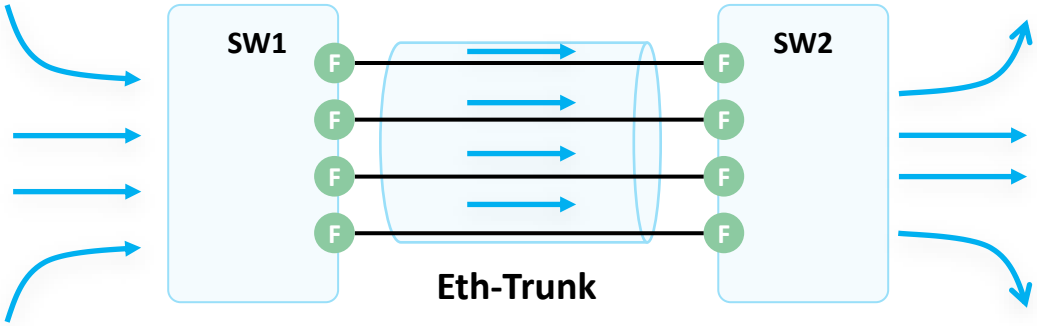
B STP阻塞端口，不转发流量



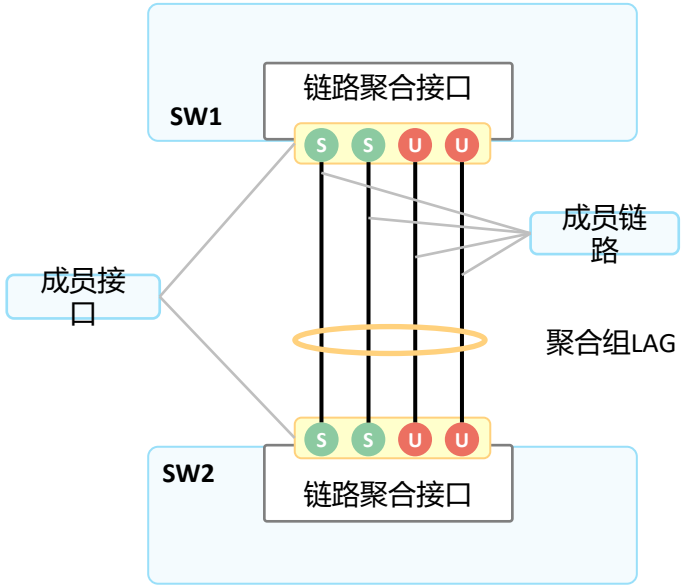
以太网链路聚合

- 以太网链路聚合Eth-Trunk：简称链路聚合，通过将多个物理接口捆绑成为一个逻辑接口，可以在不进行硬件升级的条件下，达到增加链路带宽的目的。

F 转发流量的接口

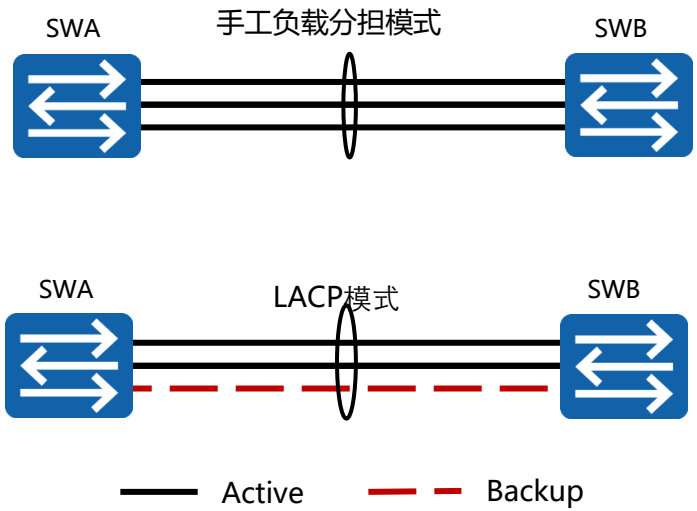


链路聚合基本术语/概念



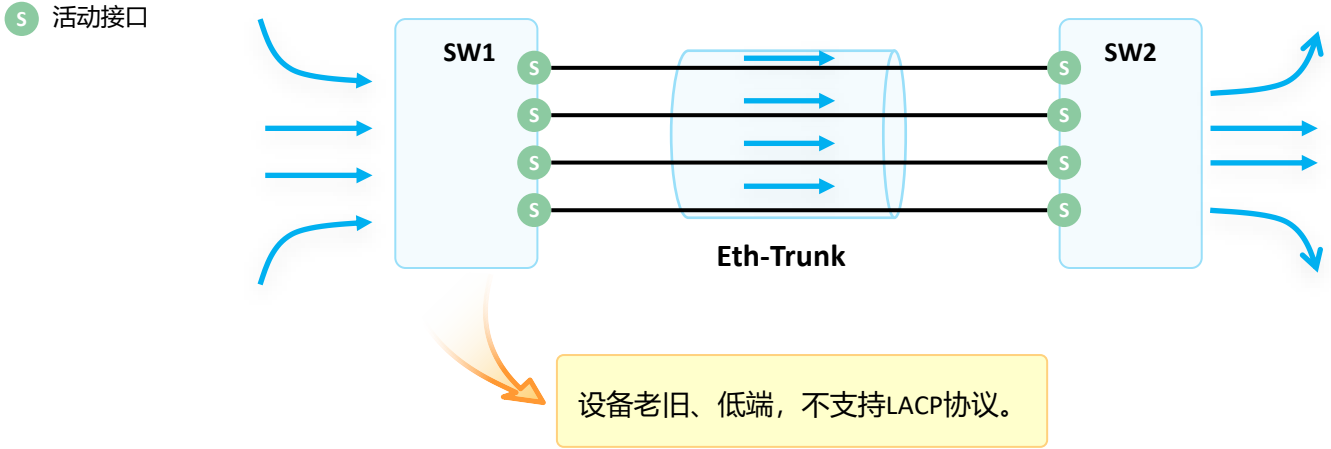
- 聚合组（Link Aggregation Group，LAG）：若干条链路捆绑在一起所形成的的逻辑链路。每个聚合组唯一对应着一个逻辑接口，这个逻辑接口又被称为链路聚合接口或Eth-Trunk接口。
- 成员接口和成员链路：组成Eth-Trunk接口的各个物理接口称为成员接口。成员接口对应的链路称为成员链路。
- 活动接口和活动链路：活动接口又叫选中（Selected）接口，是参与数据转发的成员接口。活动接口对应的链路被称为活动链路（Active link）
- 非活动接口和非活动链路：又叫非选中（Unselected）接口，是不参与转发数据的成员接口。非活动接口对应的链路被称为非活动链路（Inactive link）。
- 聚合模式：根据是否开启LACP（Link Aggregation Control Protocol，链路聚合控制协议），链路聚合可以分为手工模式和LACP模式。
- 其他概念：活动接口上限阈值和活动接口下限阈值。

链路聚合模式



- 手工负载分担模式下所有活动接口都参与数据的转发，分担负载流量。
- LACP模式支持链路备份。

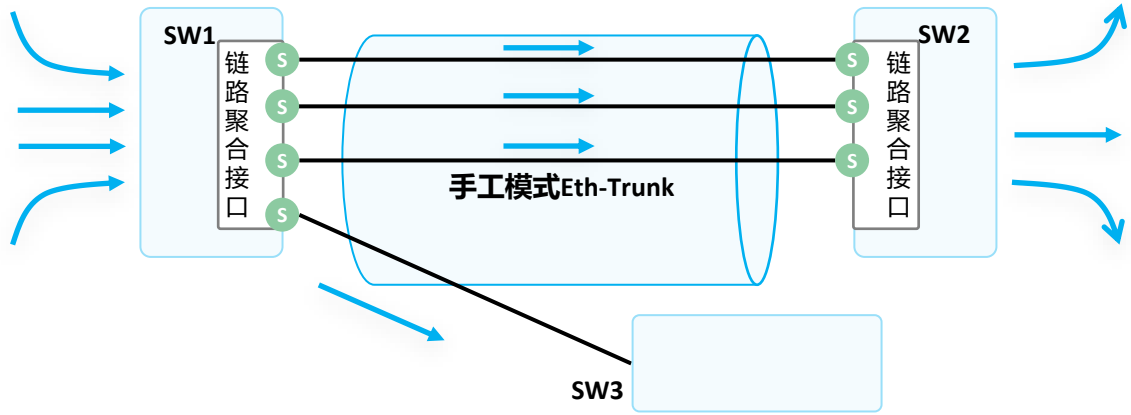
手工模式



- 手工模式： Eth-Trunk的建立、成员接口的加入均由手动配置，双方系统之间不使用LACP进行协商。
- 正常情况下所有链路都是活动链路，该模式下所有活动链路都参与数据的转发，平均分担流量，如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。
- 当聚合的两端设备中存在一个不支持LACP协议时，可以使用手工模式。

手工模式缺陷（1）

S 活动接口

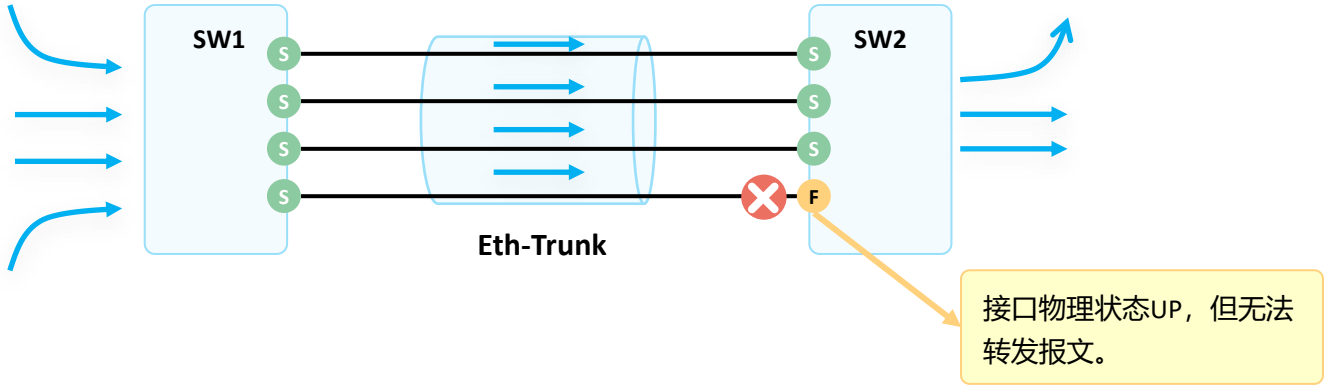


- 为了使链路聚合接口正常工作，必须保证本端链路聚合接口中所有成员接口的对端接口：
  - 属于同一设备
  - 加入同一链路聚合接口
- 手工模式下，设备间没有报文交互，因此只能通过管理员人工确认。

手工模式缺陷（2）

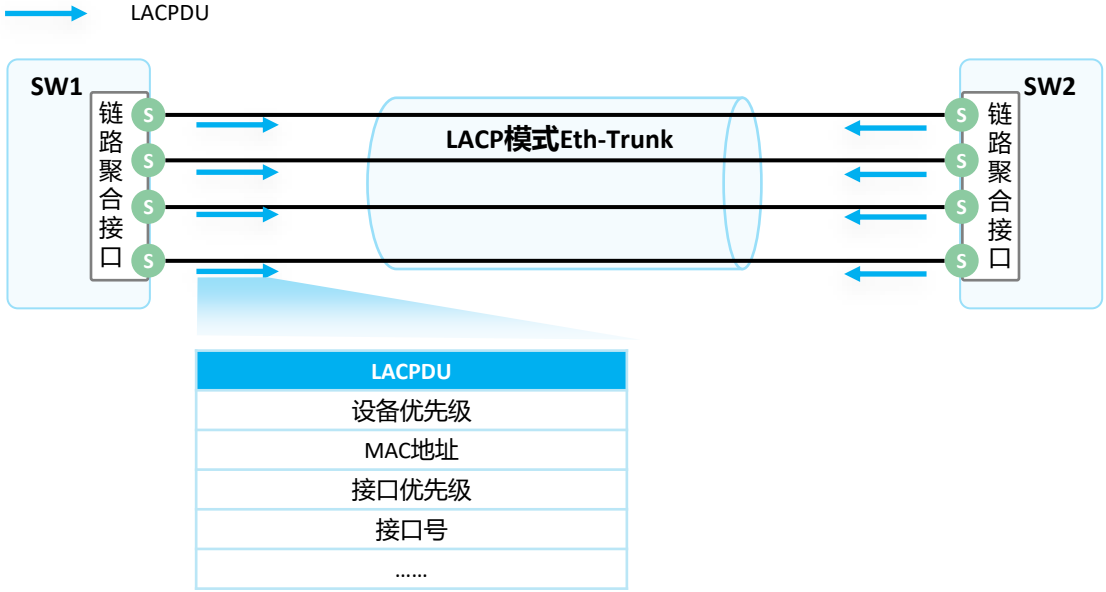
S 活动接口

F 故障接口



- 手动模式下，设备只能通过物理层状态判断对端接口是否正常工作。

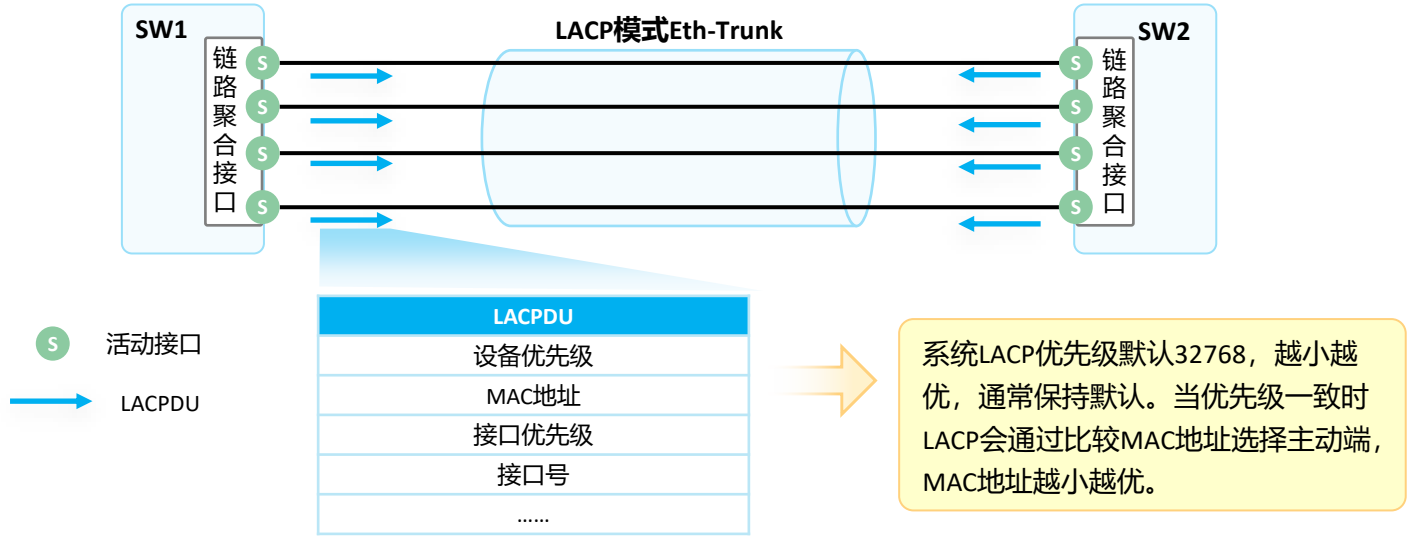
LACPDU



- LACP模式：采用LACP协议的一种链路聚合模式。设备间通过链路聚合控制协议数据单元（Link Aggregation Control Protocol Data Unit，LACPDU）进行交互，通过协议协商确保对端是同一台设备、同一个聚合接口的成员接口。
- LACPDU报文中包含设备优先级、MAC地址、接口优先级、接口号等。

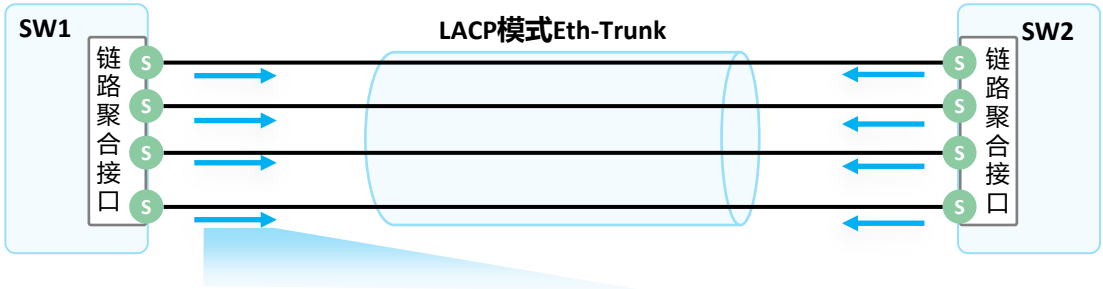
系统优先级

- LACP模式下，两端设备所选择的活动接口数目必须保持一致，否则链路聚合组就无法建立。此时可以使其中一端成为主动端，另一端（被动端）根据主动端选择活动接口。
- 通过系统LACP优先级确定主动端，值越小优先级越高。



接口优先级

- 选出主动端后，两端都会以主动端的接口优先级来选择活动接口，优先级高的接口将优先被选为活动接口。接口LACP优先级值越小，优先级越高。

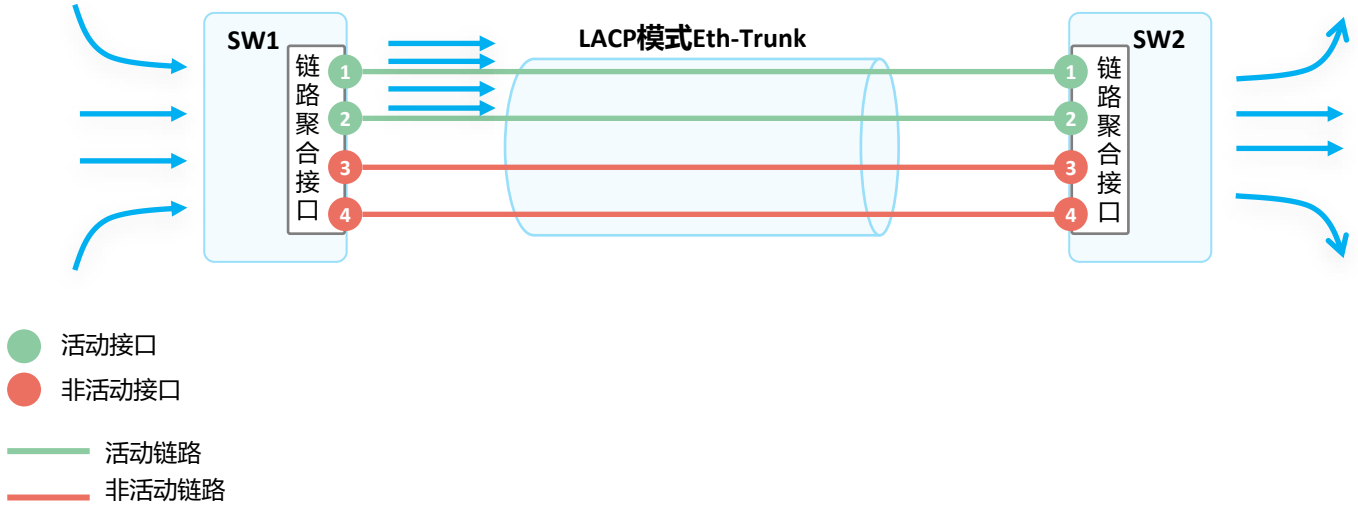


LACPDU
设备优先级
MAC地址
接口优先级
接口号
……

接口LACP优先级默认为32768，越小越优，通常保持默认，当优先级一致时LACP会通过接口编号选择活动接口，越小越优。

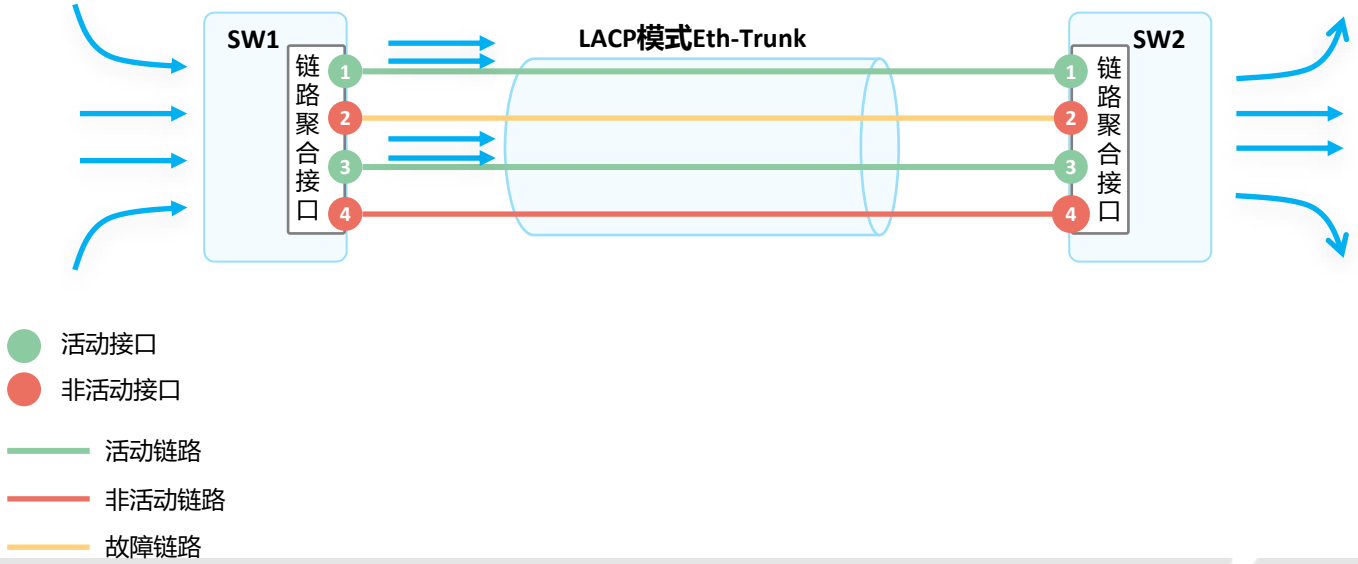
最大活动接口数 (1)

- LACP模式支持配置最大活动接口数目，当成员接口数目超过最大活动接口数目时会通过比较接口优先级、接口号选举出较优的接口成为活动接口，其余的则成为备份端口（非活动接口），同时对应的链路分别成为活动链路、非活动链路。交换机只会从活动接口中发送、接收报文。

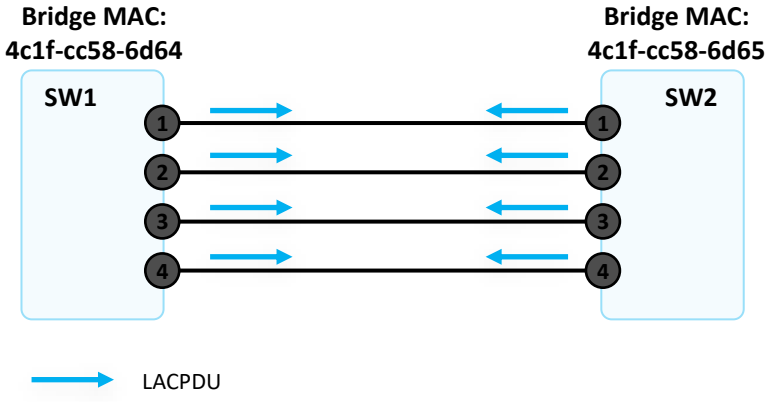


最大活动接口数 (2)

- 当活动链路中出现链路故障时，可以从非活动链路中找出一条优先级最高（接口优先级、接口编号比较）的链路替换故障链路，实现总体带宽不发生变化、业务的不间断转发。

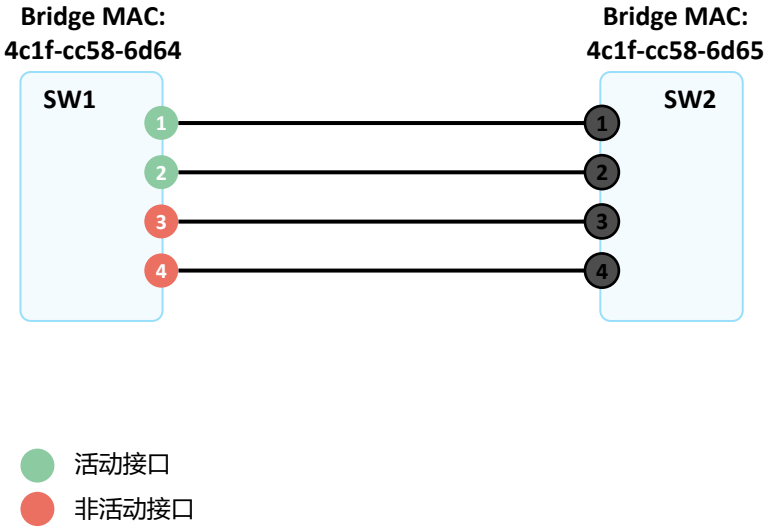


活动链路选举 (1)



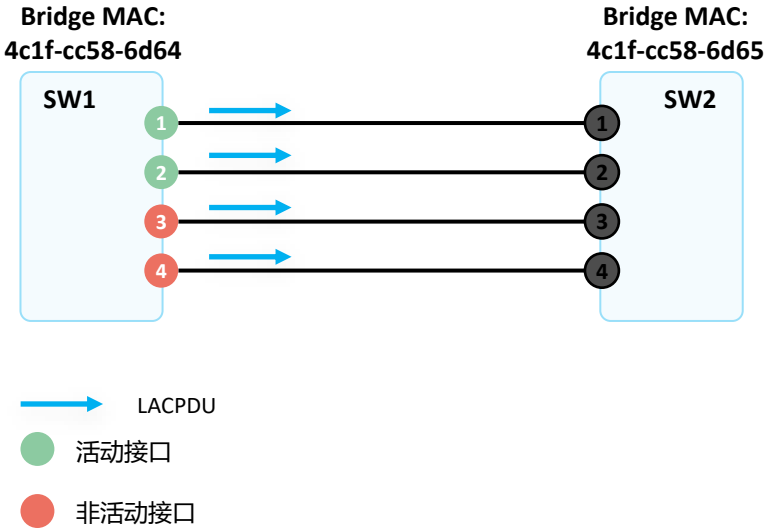
- SW1、SW2配置LACP模式的链路聚合。两端都设置最大活跃接口数为2。
- 通过LACPDU选举出优先级较高的交换机SW1，作为LACP协商过程的主动端。

活动链路选举 (2)



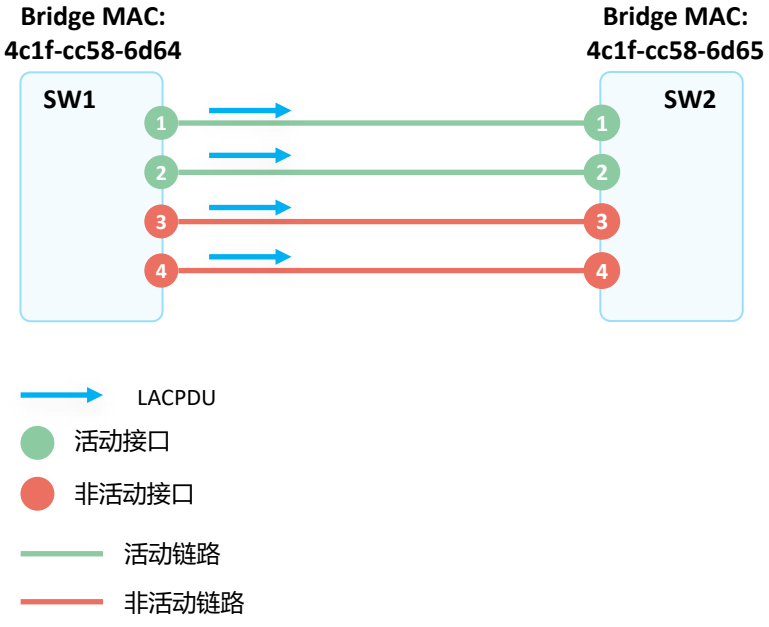
- SW1在本端通过比较接口优先级、接口编号选举出活动接口，其中1、2号接口在相同的接口优先级下拥有更小的接口编号，成为活动接口。

活动链路选举 (3)



- SW1通过LACPDU将本端活动端口选举结果告知对端。

活动链路选举 (4)

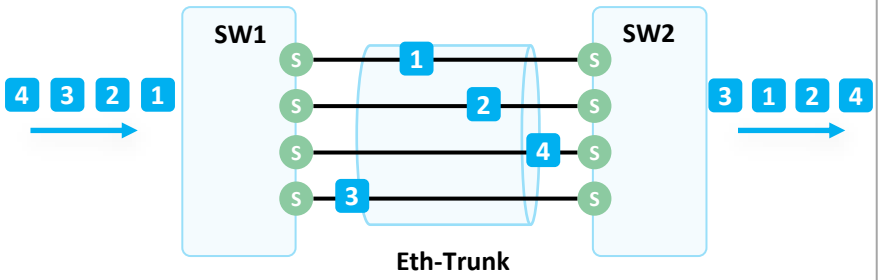


- SW2依据SW1的选举结果，明确本端的活动接口，同时对应的链路成为活动链路。
- 至此，Eth-Trunk的活动链路选举过程完成。

负载分担

基于包的负载分担

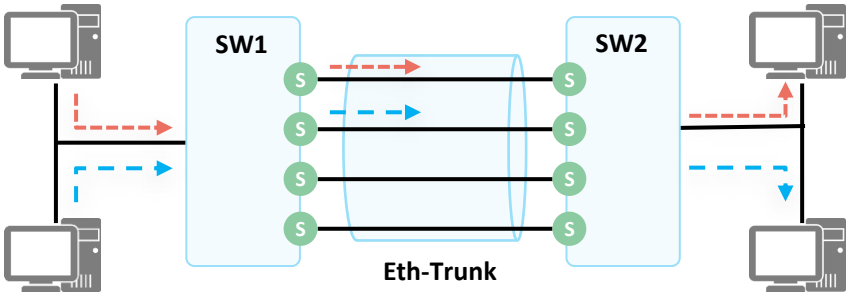
S 活动接口



在使用Eth-Trunk转发数据时，由于聚合组两端设备之间有多条物理链路，如果每个数据帧在不同的链路上转发，则有可能导致数据帧到达对端时间不一致，从而引起数据乱序。

基于流的负载分担

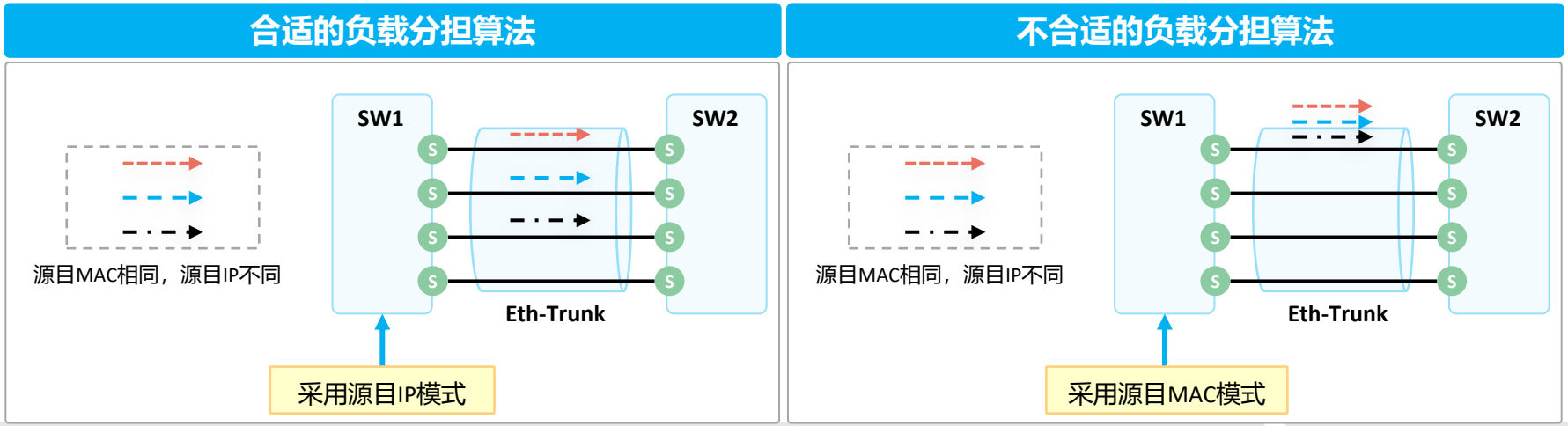
S 活动接口



Eth-Trunk推荐采用逐流负载分担的方式，即一条相同的流负载到一条链路，这样既保证了同一数据流的数据帧在同一条物理链路转发，又实现了流量在聚合组内各物理链路上的负载分担。

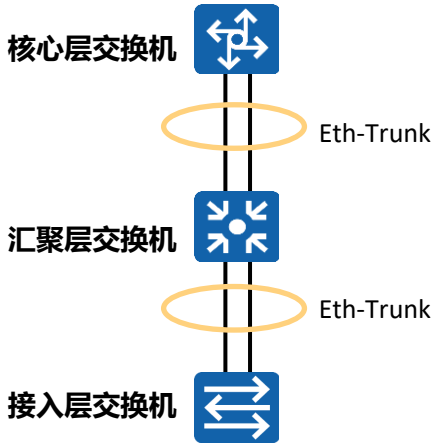
负载分担模式

- Eth-trunk支持基于报文的IP地址或MAC地址来进行负载分担，可以配置不同的模式（本地有效，对出方向报文生效）将数据流分担到不同的成员接口上。
- 常见的模式有：源IP、源MAC、目的IP、目的MAC、源目IP、源目MAC。
- 实际业务中用户需要根据业务流量特征选择配置合适的负载分担方式。业务流量中某种参数变化越频繁，选择与此参数相关的负载分担方式就越容易实现负载均衡。



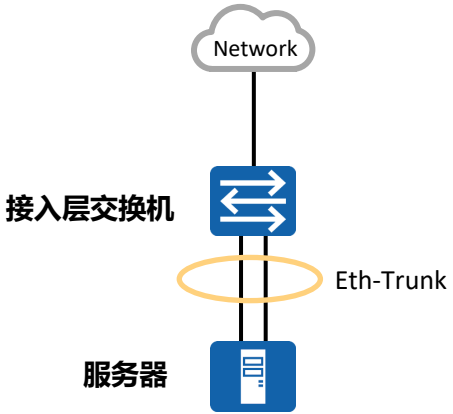
典型使用场景

交换机之间



为保证交换机之间的链路带宽以及可靠性，可以在交换机之间部署多条物理链路并使用Eth-Trunk。

交换机与服务器之间



为了提高服务器的接入带宽和可靠性，将两个或者更多的物理网卡聚合成一个网卡组，与交换机建立链路聚合。

配置命令介绍 (1)

1. 创建链路聚合组

```
[Huawei] interface eth-trunk trunk-id
```

创建Eth-Trunk接口，并进入Eth-Trunk接口视图。

2. 配置链路聚合模式

```
[Huawei-Eth-Trunk1] mode {lacp | manual load-balance }
```

Mode lacp配置链路聚合模式为lacp模式，mode manual load-balance配置链路聚合模式为手工模式。
注意：需要保持两端链路聚合模式一致。

3. 将接口加入链路聚合组中（以太网接口视图）

```
[Huawei-GigabitEthernet0/0/1] eth-trunk trunk-id
```

在接口视图下，把接口加入到Eth-Trunk中。

配置命令介绍 (2)

4. 将接口加入链路聚合组中（Eth-Trunk视图）

```
[Huawei-Eth-Trunk1] trunkport interface-type { interface-number}
```

在Eth-Trunk视图中将接口加入到链路聚合组中。3、4两种方式都可以将接口加入到链路聚合组中。

5. 使能允许不同速率端口加入同一Eth-Trunk接口的功能

```
[Huawei-Eth-Trunk1] mixed-rate link enable
```

缺省情况下，设备未使能允许不同速率端口加入同一Eth-Trunk接口的功能，只能相同速率的接口加入到同一个Eth-Trunk接口中。

6. 配置系统LACP优先级

```
[Huawei] lacp priority priority
```

系统LACP优先级值越小优先级越高，缺省情况下，系统LACP优先级为32768。

配置命令介绍 (3)

7. 配置接口LACP优先级

[Huawei-GigabitEthernet0/0/1] **lacp priority** *priority*

在接口视图下配置接口LACP优先级。缺省情况下，接口的LACP优先级是32768。接口优先级取值越小，接口的LACP优先级越高。
只有在接口已经加入到链路聚合中才可以配置该命令。

8. 配置最大活动接口数

[Huawei-Eth-Trunk1] **max active-linknumber** *{number}*

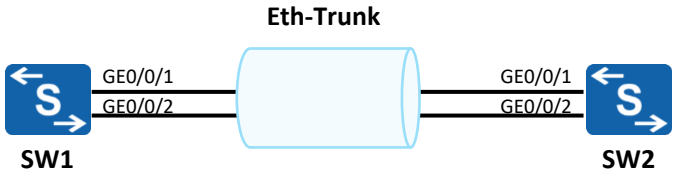
配置时需注意保持本端和对端的最大活动接口数一致，只有LACP模式支持配置最大活动接口数。

9. 配置最小活动接口数

[Huawei-Eth-Trunk1] **least active-linknumber** *{number}*

本端和对端设备的活动接口数下限阈值可以不同，手动模式、LACP模式都支持配置最小活动接口数。
配置最小活动接口数目的是为了保证最小带宽，当前活动链路数目小于下限阈值时，Eth-Trunk接口的状态转为Down。

手工模式链路聚合配置举例



- 案例需求描述：
  - SW1、SW2都连接着VLAN10、VLAN20的网络。
  - SW1和SW2之间通过两根以太网链路互联，为了提供链路冗余以及保证传输可靠性，在SW1、SW2之间配置手工模式的链路聚合。

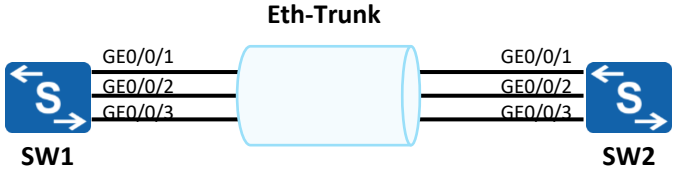
SW1的配置如下：

```
[SW1] interface eth-trunk 1
[SW1-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/2
[SW1-Eth-Trunk1] port link-type trunk
[SW1-Eth-Trunk1] port trunk allow-pass vlan 10 20
```

SW2的配置如下：

```
[SW2] interface eth-trunk 1
[SW2-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/2
[SW2-Eth-Trunk1] port link-type trunk
[SW2-Eth-Trunk1] port trunk allow-pass vlan 10 20
```

LACP模式链路聚合配置举例 (1)

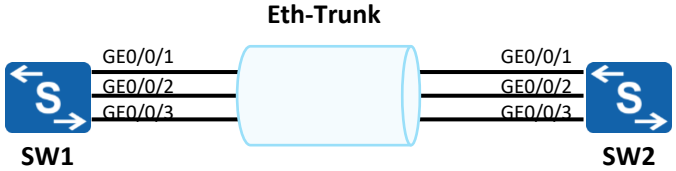


- 案例需求描述：
  - SW1、SW2都连接着VLAN10、VLAN20的网络。
  - SW1和SW2之间通过三根以太网链路互联，为了提供链路冗余以及保证传输可靠性，在SW1、SW2之间配置LACP模式的链路聚合，并且手动调整优先级让SW1成为主动端，并配置最大活跃端口为2，另外一条链路作为备份。

SW1的配置如下：

```
[SW1] interface eth-trunk 1
[SW1-Eth-Trunk1] mode lacp
[SW1-Eth-Trunk1] max active-linknumber 2
[SW1-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3
[SW1-Eth-Trunk1] port link-type trunk
[SW1-Eth-Trunk1] port trunk allow-pass vlan 10 20
[SW1-Eth-Trunk1] quit
[SW1] lacp priority 30000
```

LACP模式链路聚合配置举例（2）

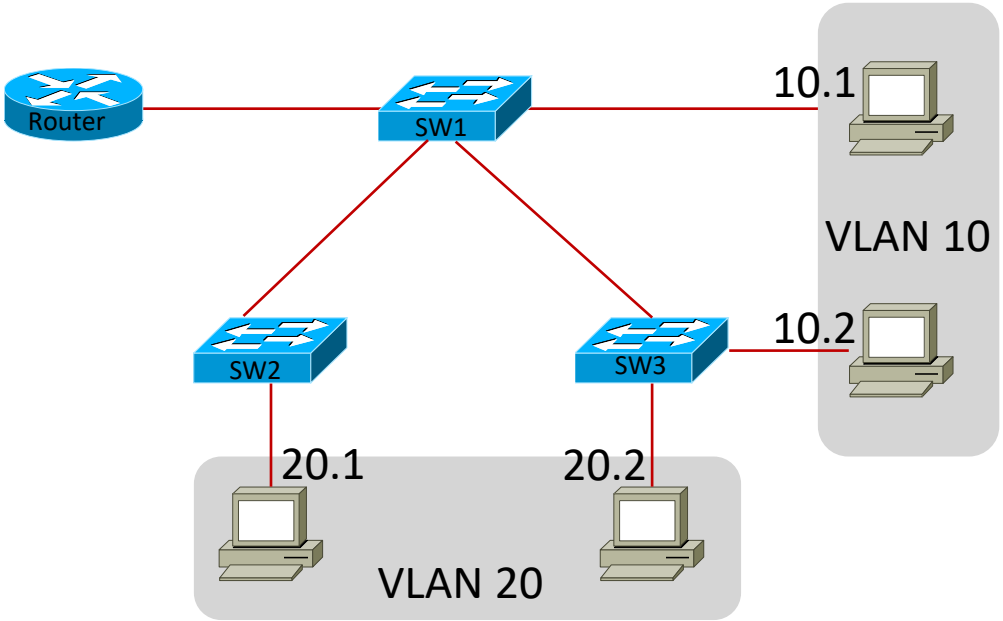


- 案例需求描述：
  - SW1、SW2都连接着VLAN10、VLAN20的网络。
  - SW1和SW2之间通过三根以太网链路互联，为了提供链路冗余以及保证传输可靠性，在SW1、SW2之间配置LACP模式的链路聚合，并且手动调整优先级让SW1成为主动端，并配置最大活跃端口为2，另外一条链路作为备份。

SW2的配置如下：

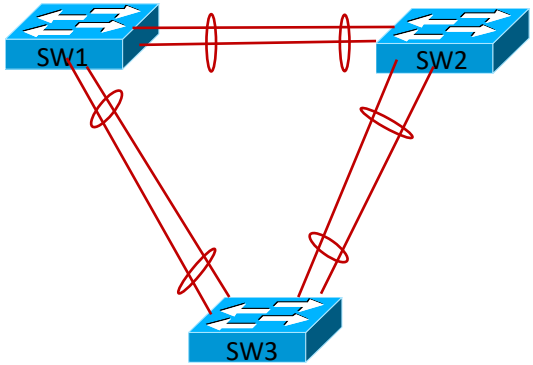
```
[SW2] interface eth-trunk 1
[SW2-Eth-Trunk1] mode lacp
[SW2-Eth-Trunk1] max active-linknumber 2
[SW2-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3
[SW2-Eth-Trunk1] port link-type trunk
[SW2-Eth-Trunk1] port trunk allow-pass vlan 10 20
[SW2-Eth-Trunk1] quit
```

课后实验二



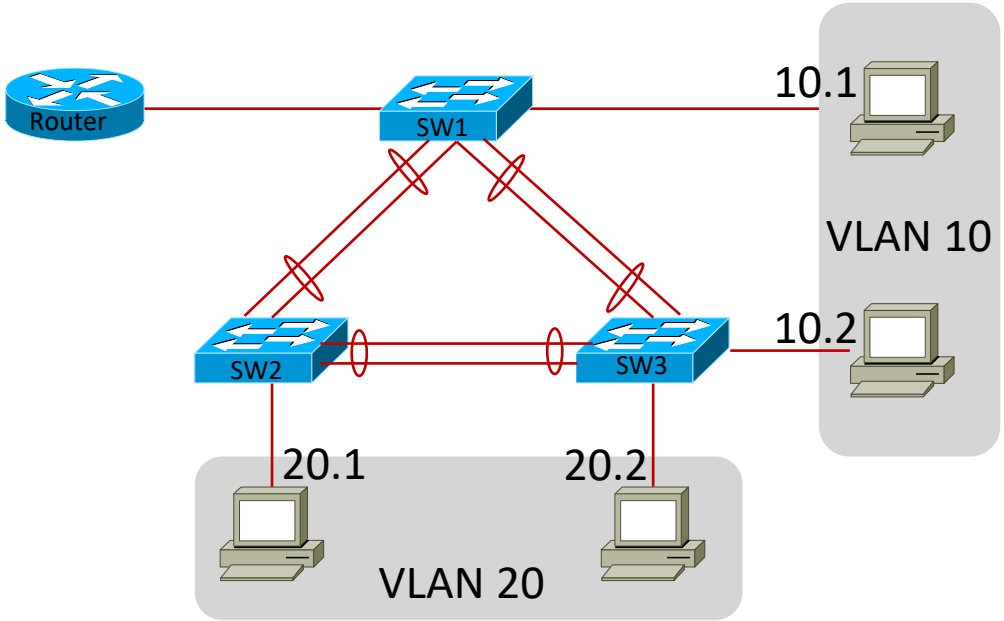
实验需求：
1.全网有vlan10，vlan20，vlan30
2.vlan10/20/30，192.168.10/20/30.0/24
3.配置Trunk（或者Hybrid），Access接口
4.所有vlan的网关在Router
5.单臂路由来实现所有的通讯
6.vlan30是所有网络设备的管理vlan
7.配置三个交换机的Telnet
测试：
1.所有主机都可以互相ping通
2。主机都能远程登陆管理交换机

课后实验三



实验需求：
1.完成L2的链路聚合实验
2.运行生成树实现核心之间的负载分担
3.完成L3的链路聚合实验

实验可以整合



THANK YOU

Ping 通您的梦想～

腾讯课堂交流群：17942636

ADD：苏州市干将东路666号和基广场401-402；Tel：0512-8188 8288；

课程咨询QQ：2853771087 ； 官网 :www.51glab.com