

项目 3 虚拟局域网

主编：钟祥睿等

上海交通大学出版社

目录

项目三



项目描述



项目分析



相关知识点



项目实施

单元学习目标

知识目标



1. 了解 VLAN 技术的产生背景
2. 理解 VLAN 的工作原理
3. 理解 VLAN 的标识及划分
4. 区分交换机 VLAN 三种端口的异同
5. 理解 VLAN 的数据交互过程
6. 熟知 VLAN 的应用场景

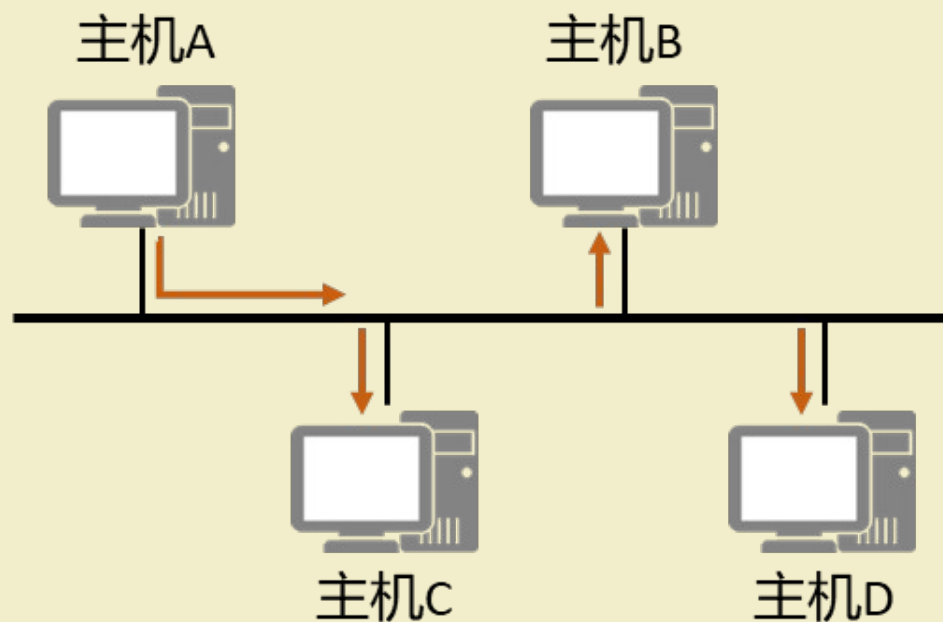
技能目标



1. 能熟练对基于端口的 VLAN 进行配置管理
2. 掌握园区网 VLAN 的基本配置方法
3. 掌握 VLAN 的 TRUNK 口两个属性的配置方法

项目描述

早期的以太网是一种基于 CSMA/CD 的数据网络通信技术，其特征是共享通信介质，且这种网络的结构基本上都是总线型结构的，这种结构存在以下主要问题：



4
图 3-1 传统以太网



项目描述

1. 若某时刻有多个节点同时试图发送消息，那么它们将产生冲突。
2. 从任意节点发出的消息都会被发送到其他节点，形成广播。
3. 所有主机共享一条传输通道，无法控制网络中的信息安全。

这种网络构成了一个冲突域，网络中计算机数量越多，冲突越严重，网络效率越低。同时，该网络也是一个广播域，当网络中发送信息的计算机数量变多时，广播流量将会耗费大量带宽。

因此，传统局域网不仅面临冲突域太大和广播域太大两大难题，而且无法保障传输信息的安全。

项目描述

为了扩展传统 LAN，以接入更多计算机，同时避免冲突的恶化，出现了网桥和二层交换机，它们能有效隔离冲突域。网桥和交换机采用交换方式将来自入端口的信息转发到出端口上，克服了共享网络中的冲突问题。但是，采用交换机进行组网时，广播域和信息安全问题依旧存在。

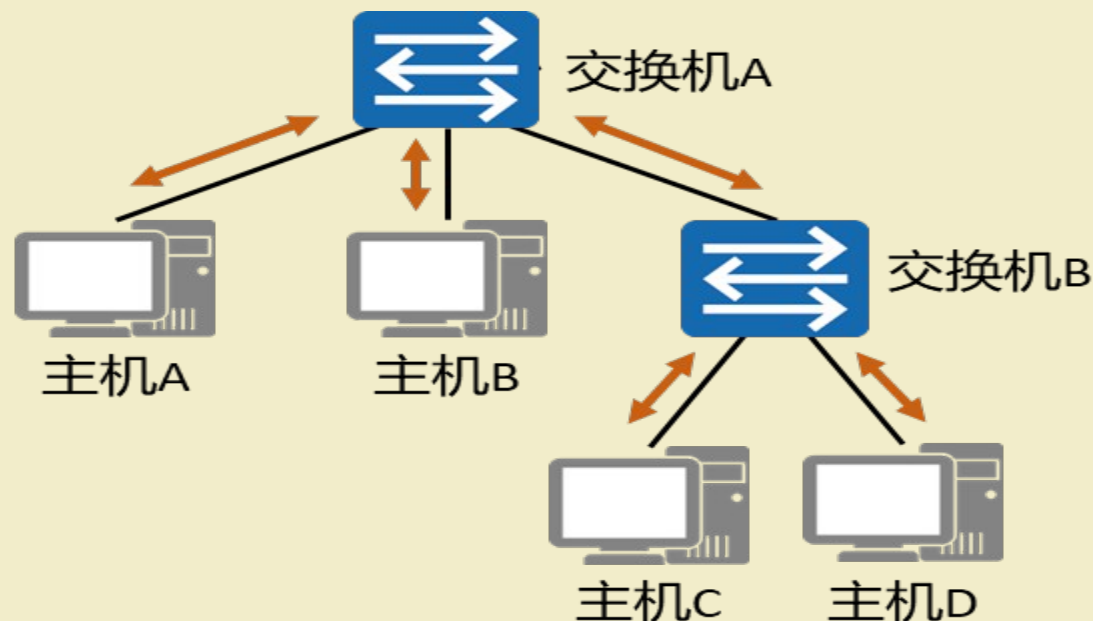


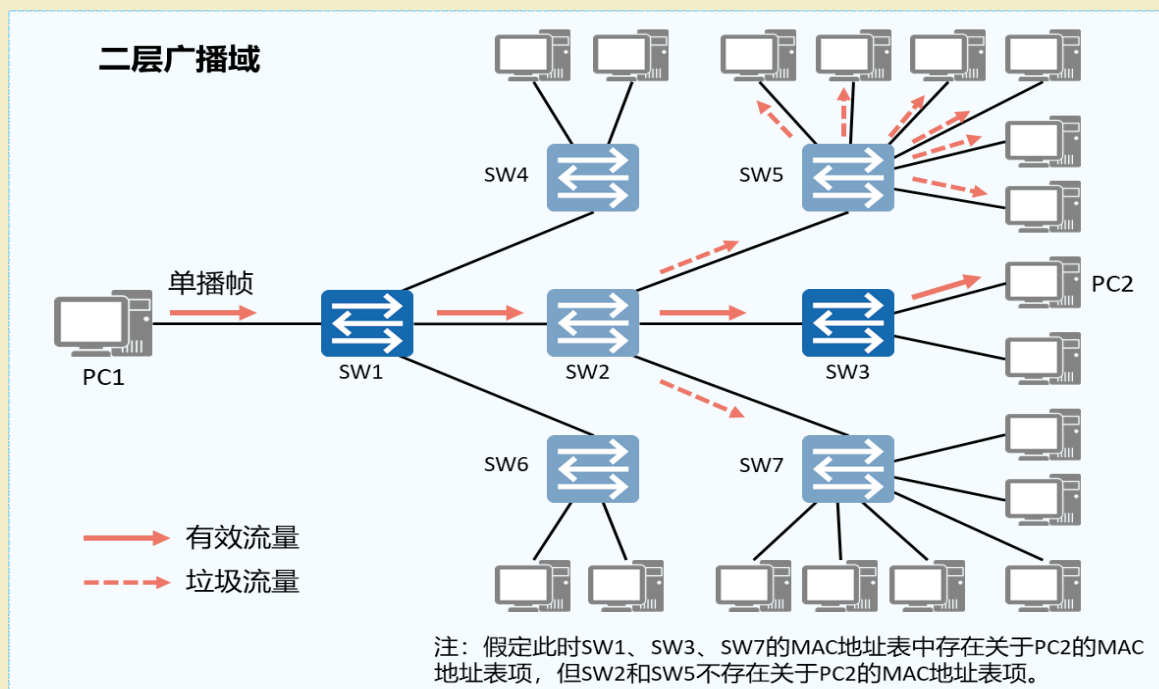
图 3-2 交换式以太网

项目描述

交换机的基础工作原理是根据历史的通信记录，把终端的 **MAC** 地址与交换机的物理接口使用一张表进行一一映射，但是当终端的 **MAC** 地址不在表格内的时候，交换机会发送一个广播数据包进行广播寻找。所以交换机的工作过程中，会出现大量的广播数据包，这些广播数据包对大部分终端来说都是无效数据，从而会降低网络的效率。如何定义一个合适的广播域范围就成为了一个新的议题，如同我们在商场中时常会接收到寻人广播一样，这些寻人广播对绝大部分人和范围来说都是无效的，甚至是干扰的；如果我们能够准确定位到寻找目的范围作精准广播的话，那么将可以大大减少能源损耗甚至减少大量的人力。

交换机的出现，解决了冲突域过于庞大造成的网络带宽紧缺问题，但是也出现了新的问题，就是广播域的问题。默认情况下，一个交换机或者多个直接互联交换机之间都属于一个相同的广播域。当交换机不了解目的 **MAC** 地址所对应的物理接口的时候，会发送一个广播数据包到整个广播域内的所有终端，当该终端的 **MAC** 地址与其不符的时候，会丢弃该数据，若相符则会回应这个广播数据包；这种情况有利于交换机寻找到目的 **MAC** 地址对应的接口，让网络保持正常的通信，但是也会导致网络中存在大量无效的垃圾数据。

为了解决广播范围过于庞大导致的网络效率下降，计算机网络出现了一个新的技术来解决这一问题，它就是虚拟局域网（VLAN，Virtual Local Area Network）。VLAN能够根据网络管理的需求，自定义广播域的范围，每个VLAN一个广播域；VLAN的定义又不受制于网络终端的物理位置，数量等基础信息，是解决局域网通信效率一个非常好用的技术。



图

3.1 VLAN 的基本概念

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。

3.2 VLAN 的应用

在相同的 VLAN 下，即使终端处于不同的交换机中，它们之间通信仍旧类似处于相同的交换机中。当某一个终端发送广播信息的时候，这个信息只会在相同的 VLAN 中进行传播。

这种模式下，网络的管理小组也不会受制于物理位置的限制，对于网络管理人员来说，较少了相当的工作量，也提高了网络管理能力。

通过 VLAN 的划分，网络管理人员可以更好强化网络安全的数据

例如通常各个公司的财务部是不允许其他部门能够访问其终端的数据，从而提高网络的安全性。这样，部门内部可以有一些数据的共享，但是这些数据不会被其他部门的终端侦听截获到。

3.2VLAN 的优点

1. 控制广播风暴

当使用交换机构建一个较大的局域网的时候，局域网内会出现大量的广播数据包，甚至会出现广播风暴现象；一旦出现这类情况，网络的质量效率会极具快速地下降。VLAN 可以把广播数据包控制本VLAN 之内，将很大的广播域划为多个独立地广播域，从而有效地减少广播数据包对网络的影响。

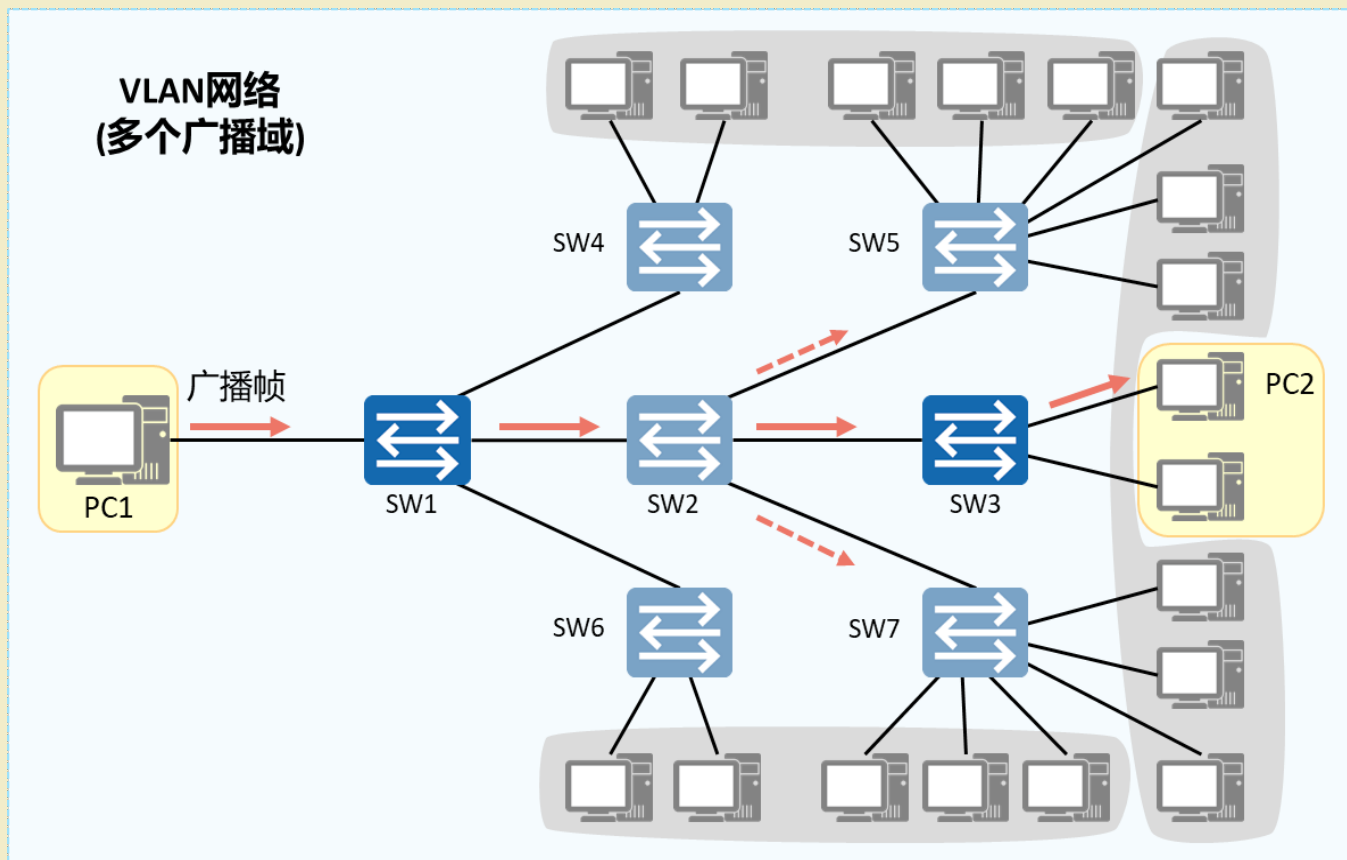


图 3-4 VLAN 网络的广播域

2. 提高网络的安全

VLAN 可以根据交换机的接口，物理地址等方式进行划分。不同的 **VLAN** 之间的主机无法直接通信，计算机网络中某些数据链路层的信息无法直接互通；这种情况会杜绝不同 **VLAN** 之间地设备因为某些漏洞被其他 **VLAN** 的主机控制等情况。例如某些主机的一些默认文件共享或者打印机等外设共享被其他 **VLAN** 的终端所利用。

3. 提高网络管理效能

VLAN 的划分与终端以及其所链接的交换机的物理位置无关，一旦一些终端所属工作小组出现调整，只需要在相关交换机进行配置即可，无需要调整主机位置或者修改终端的系统参数等。

3.3 VLAN 的设置方法

一、基于交换机端口的 VLAN

基于交换机的端口划分的 VLAN 是最简易高效且最常用一种方法。这种方法就是网络管理员根据实际情况将局域网内一个或者多个交换机的某些端口当作某个 VLAN 的集合，而这些端口所连接的设备自然就遵从 VLAN 相关网络原理。这种方法的缺点就是如果终端的位置发生改变，所连接的链路出现变化，而所属的 VLAN 如果不想发生变更的情况，需要手动重新修改设备新链路所连接的交换机端口的配置；但是由于基于交换机端口的 VLAN 相关配置比较简单，所以整体来说还是方便有效的。

二、基于 MAC 地址的 VLAN

这种定义 VLAN 的方式是根据每个终端设备的 MAC 地址来划分的。在交换机上定义某个所属的 VLAN，不在乎终端的位置和所连接的端口号。这种方式的优点是，无论终端设备如何移动，即使物理链路发生变化也不会有影响。这种定义划分 VLAN 的方式的缺点就是得提前收集所有连接上局域网的终端设备 MAC 地址，这个前期工作量相对比较大。

三、基于网络层的 VLAN

这种定义 VLAN 的方式是根据每个终端的 IP 地址或者协议类型来划分的。

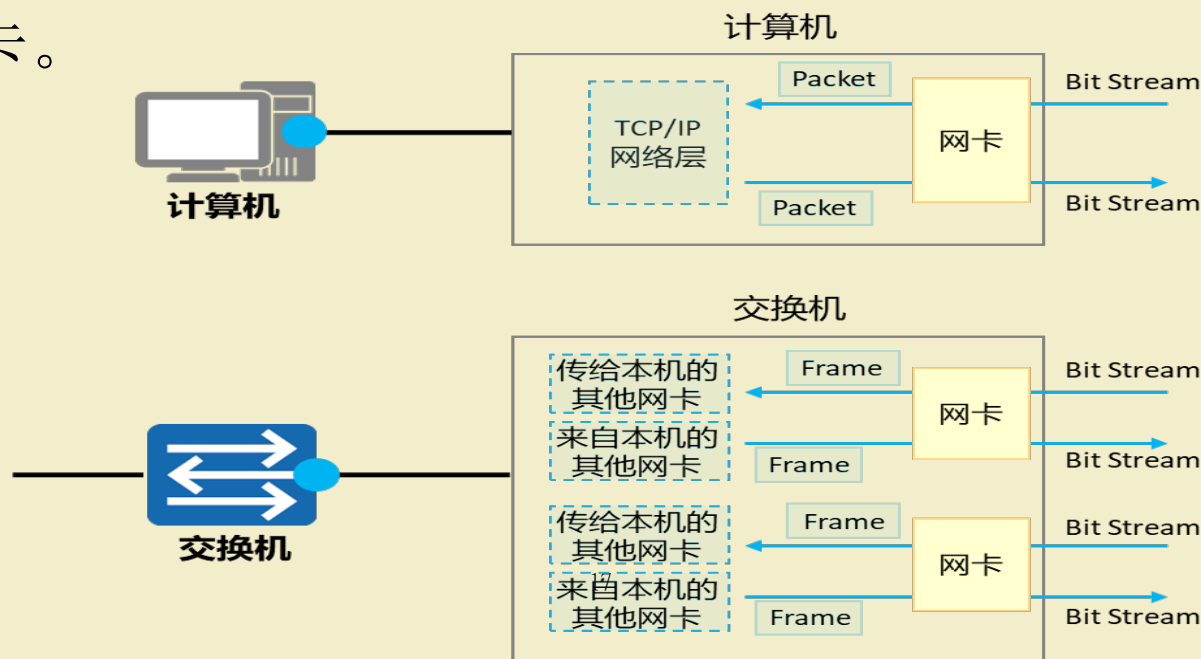
这种划分的方式虽然会检查数据包的 IP 地址，但是由于不是路由，所以并不支持路由相关的协议。这种方式优点和基于 MAC 地址的划分相似，也是不受终端的物理位置和链路所影响。

这种划分 VLAN 的方式的缺点是效率相对低下，因为在交换机中检查数据包的 IP 地址是消耗资源的，也相对需要较多的时间。

三、以太网卡

网络接口卡（ Network Interface Card, NIC ）也称为“网卡”，是计算机、交换机、路由器等网络设备与外部网络世界相连的关键部件。

网卡有很多类型，本教材所提及的均为以太网接口卡，简称以太网卡。所说的交换机也均为以太网交换机，即交换机上每个转发数据的网口所使用的网卡都是以太网卡。



3.4 VLAN 的标准

VLAN 的标准是 IEEE 提出的 802.1Q 协议，只要支持相同的开发标准，就能保证网络的互通。

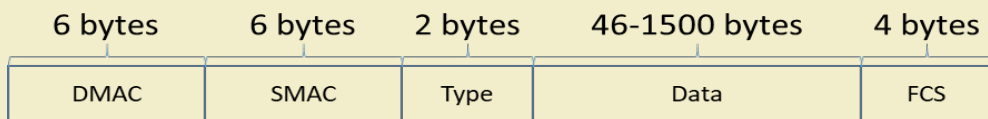
一、802.1Q

IEEE 802.1Q 定义了标识带有 VLAN 成员信息的以太网帧建立了一种标准方法。

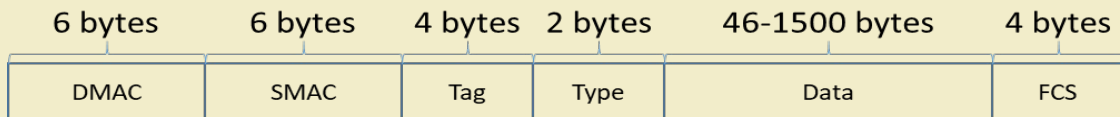
802.1Q 标准定义了 VLAN 网桥操作，解决了大型局域网如何划为多个小网络，从而广播和组播流量不会占据大量带宽的问题。

802.1Q 完成以上的功能主要在于标签。支持 802.1Q 的交换机可以用来传输标签帧和无标签帧。当支持 802.1Q 的交换机某接口连接的是支持 802.1Q 的其他交换机的时，那么这些带有 802.1Q 的帧可以在不同交换机之间传送带有 VLAN 成员信息的帧，从而解决了 VLAN 技术在跨交换机中的传输。

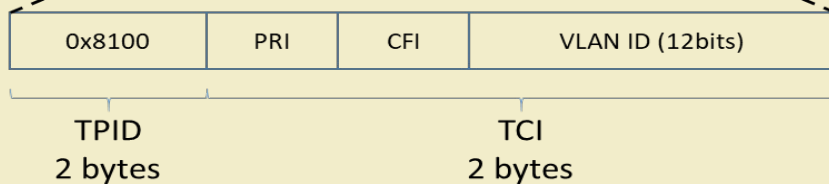
802.1Qtag 字段共占 4 个字节，直接添加在以太网帧头 SMAC 字段和 TYPE 字段中间，IEEE 802.1Q 文档对 VLAN 标签作出了说明，如下图所示。



没有携带Tag的帧



携带Tag的帧



TPID : Tag Protocol Identifier , 2 字节, 固定取值 0x8100 , 是 IEEE 定义的新类型, 表明这是一个携带 802.1Q 标签的帧。如果不支持 802.1Q 的设备收到这样的帧, 会直接将其丢弃。

TCI : Tag Control Information , 2 字节。帧的控制信息, 详细说明如下:

1.Priority : 3 比特, 表示帧的优先级, 取值范围为 0 ~ 7 , 值越大优先级越高。当交换机阻塞时, 优先发送优先级高的数据帧。

2.2. CFI : Canonical Format Indicator , 1 比特。CFI 表示 MAC 地址是否是经典格式。CFI 为 0 说明是经典格式, CFI 为 1 表示为非经典格式。用于区分以太网帧、FDDI (Fiber Distributed Digital Interface) 帧和令牌环网帧。在以太网中, CFI 的值为 0

3. VLAN Identifier : VLAN ID , 12 比特, 指明该数据帧所在的 VLAN 编号。VLAN 的编号共 4096 个, 可配置的 VLAN ID 取值范围为 0 ~ 4095 , 但是 0 和 4095 在协议中规定为保留的 VLAN ID , 不能给用户使用, 所以可用的也就 4094 个, 其中的 VLAN 1 是交换机的默认 VLAN 。

二、默认 VLAN

交换机初始状态下, 只有一个 VLAN , 这个 VLAN 是 VLAN 1 , 交换机的所有端口默认情况下都属于该 VLAN 。交换机是不为默认 VLAN , 即为 VLAN 1 传输的以太网帧添加 802.1Q 标识。所以, 一些不支持 VLAN 标识的交换机也可以与支持 802.1Q 帧交换机互相通信。

3.5 交换机端口分类

基于接口的 VLAN 划分依赖于交换机的接口类型。交换机接口分为三种类型，分别是 access 接口、trunk 接口和 hybrid 接口。

一、Access 接口

Access 接口通常只用于连接计算机终端设备，只能支持特定某一个 VLAN。

终端设备默认是无法识别 VLAN 标识的，所以交换机的 access 接口向终端设备转发数据时候也是不带 802.1Q 帧的信息。

Access 接口接收的数据帧中，只能接收不带有 tag 标识的帧或者带有和该端口相同 VLAN 标识的 tag 标识帧。Access 接口接收和发送帧的过程如下图所示。

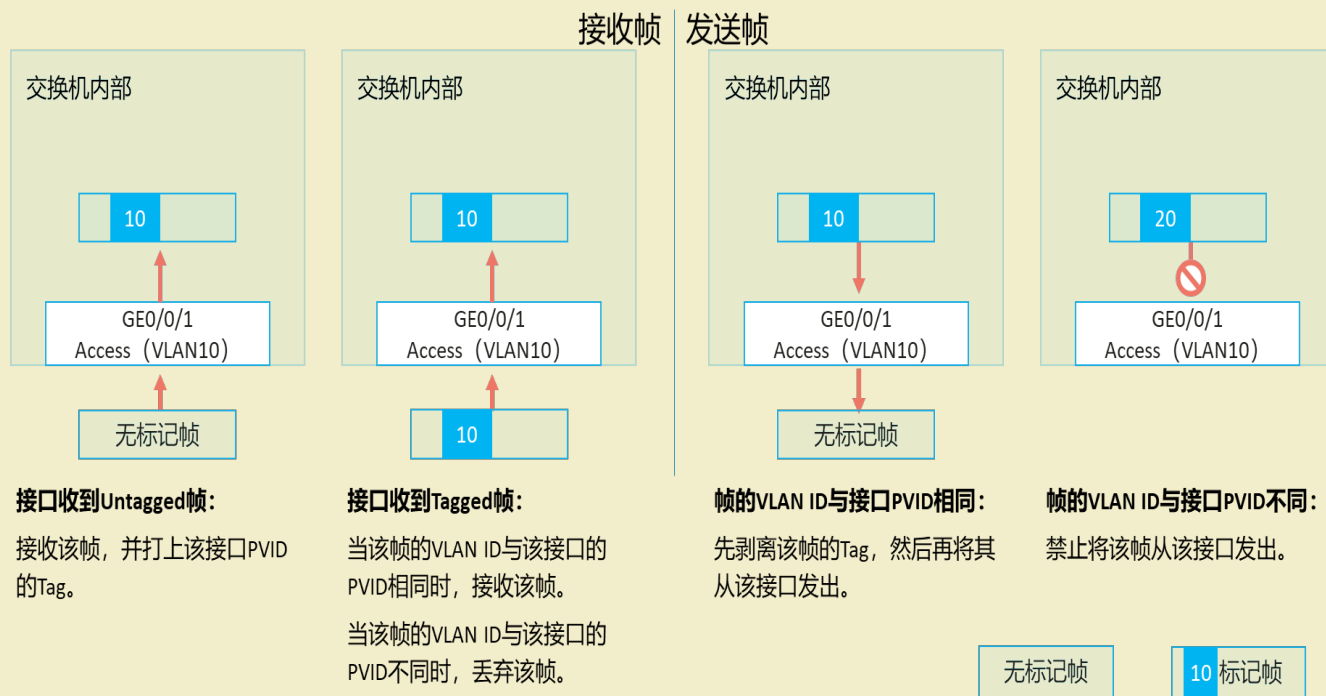


图 3-6 Access 接口接收和发送帧的过程

二、Trunk 接口

Trunk 接口用于连接交换机等网络设备，可以支持多个 VLAN 的以太网数据帧。

Trunk 接口可接收不带 tag 的帧和接口允许的 VLAN 范围的 tag 帧。

Trunk 接口转发数据帧的时候，如果该数据帧非默认 VLAN，就会带着该 VLAN 的 tag 发送；如果该数据帧是默认的 VLAN 帧或者与该 trunk 口所属的 VLAN 相同时候，那么转发的数据帧将不带 tag 标记。Trunk 接口接收和发送帧的过程如下图所示。

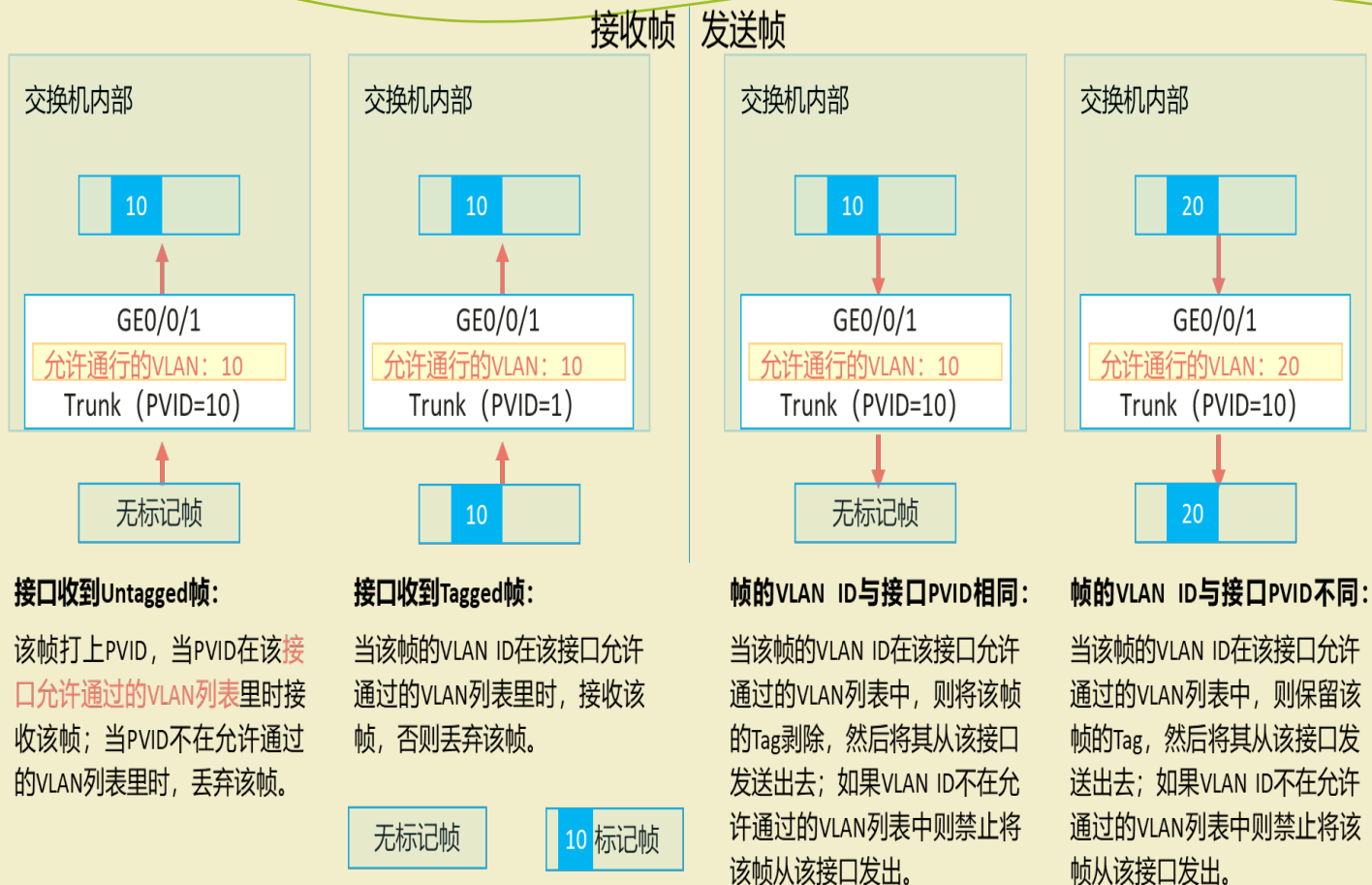
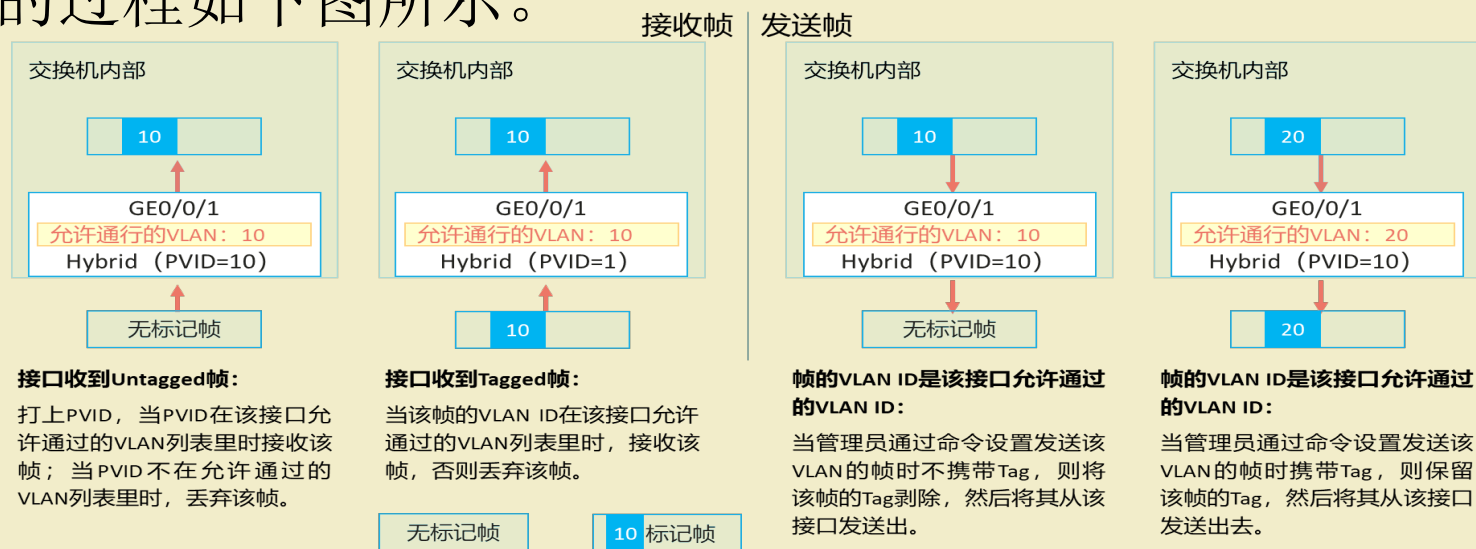


图 3-7Trunk 接口接收和发送帧的过程

三、Hybird 接口

Hybrid 接口是华为系列交换机端口的默认工作模式，它能够接收和发送多个 VLAN 的数据帧，可以用于链接交换机之间的链路，也可以用于连接终端设备。

Hybird 接口同时具备有 access 端口和 trunk 端口的特点，根据网络的需求给予合适的配置即可。Hybird 接口接收和发送帧的过程如下图所示。



各类接口添加或剥除 VLAN 标签的处理过程总结如下表所示。

表 3-1 不同类型接口接收和发送帧的过程总结

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。

3.6 VLAN 配置命令

1. 创建 VLAN

创建 VLAN 并进入 VLAN 视图，如果 VLAN 已存在，直接进入该 VLAN 的视图。vlan-id

是整数形式，取值范围是 1 ~ 4094

[Huawei] vlan vlan-id

批量创建 VLAN 。其中： batch ， 指定批量创建的 VLAN ID ； vlan-id1 ， 表示第一个 VLAN 的编号； vlan-id2 ， 表示最后一个 VLAN 的编号

[Huawei] vlan batch { vlan-id1 [to vlan-id2] }

2. Access 接口的配置命令

在接口视图下配置接口的链路类型为 Access

```
[Huawei-GigabitEthernet0/0/1] port link-type access
```

在接口视图下配置接口的缺省 VLAN 并同时加入这个 VLAN。
vlan-id，配置缺省 VLAN 的编号，整数形式，取值范围是 1 ~ 4094

```
[Huawei-GigabitEthernet0/0/1] port default vlan vlan-id
```

3. Trunk 接口的配置命令

在接口视图下，配置接口的链路类型为 Trunk

```
[Huawei-GigabitEthernet0/0/1] port link-type trunk
```

在接口视图下，配置 Trunk 类型接口加入的 VLAN

```
[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] }  
| all }
```

（可选）在接口视图下，配置 Trunk 类型接口的缺省 VLAN

```
[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan vlan-id
```

4. Hybrid 接口的配置命令

在接口视图下配置接口的链路类型为 Hybrid

```
[Huawei-GigabitEthernet0/0/1] port link-type hybrid
```

在接口视图下配置 Hybrid 类型接口加入的 VLAN ， 这些 VLAN 的帧以 Untagged 方式通过接口

```
[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan
```

```
{ { vlan-id1 [ to vlan-id2 ]
```

```
} | all }
```

在接口视图下配置 Hybrid 类型接口加入的 VLAN ， 这些 VLAN 的帧以 Tagged 方式通过接口

```
[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan
```

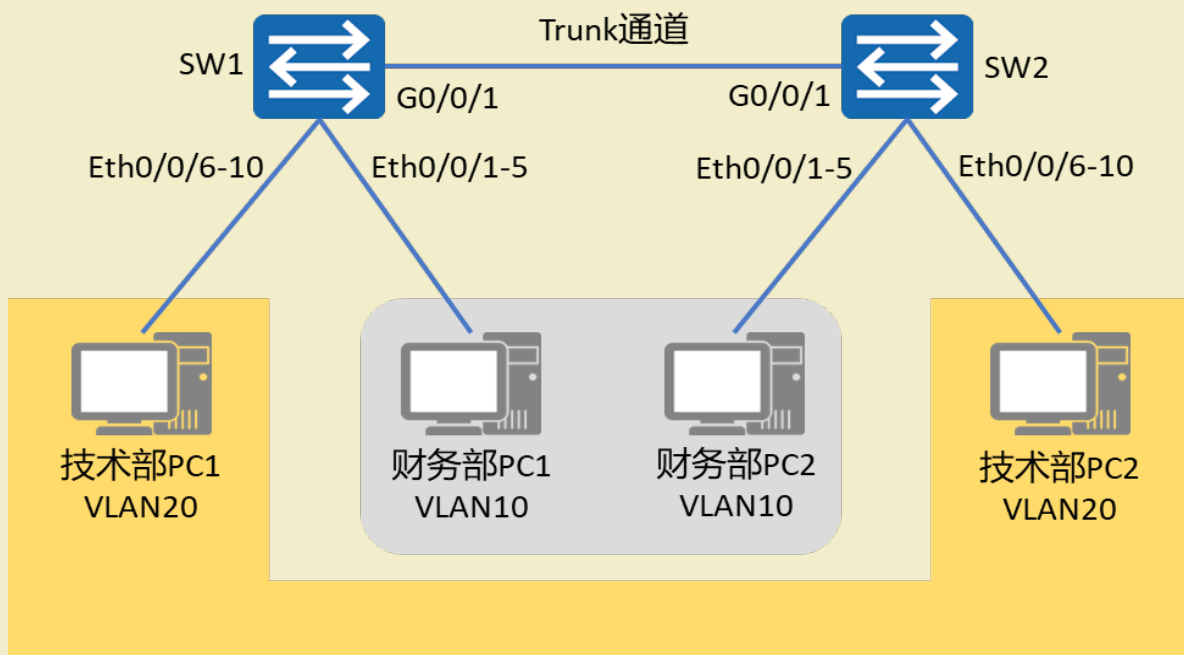
```
{ { vlan-id1 [ to vlan-id2 ] } |
```

```
all }
```

（可选）在接口视图下配置 Hybrid 类型接口的缺省 VLAN

3.7 VLAN 配置案例

以下图为例，详细介绍 VLAN 的配置过程。由于两个交换机配置过程类似，下面只介绍交换机 SW1 的配置。



1. 根据需求新建 VLAN 。

```
[SW1] vlan batch 10 20
```

2. 根据网络拓扑设置终端连接的接口的端口属性，设置接口的 PVID 值。

```
[SW1] interface GigabitEthernet 0/0/1
```

```
[SW1-GigabitEthernet0/0/1] port link-type access
```

```
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

```
[SW1-GigabitEthernet0/0/1] quit
```

```
[SW1] interface GigabitEthernet 0/0/2
```

```
[SW1-GigabitEthernet0/0/2] port link-type access
```

```
[SW1-GigabitEthernet0/0/2] port default vlan 20
```

```
[SW1-GigabitEthernet0/0/2] quit
```

3. 根据网络拓扑设置交换机之间级联端口属性，并设置允许通过的 VLAN ID 。

```
[SW1] interface GigabitEthernet 0/0/24
```

```
[SW1-GigabitEthernet0/0/24] port link-type trunk
```

```
[SW1-GigabitEthernet0/0/24] port trunk allow-pass vlan 10  
20
```

4. SW2 的配置与 SW1 相似，只需要根据拓扑结构图的内容修改命令参数即可。

具体实施过程参考实训报告

【项目总结】

本项目详细介绍了虚拟局域网（VLAN）的相关知识及应用，主要学习了以下知识内容。

1. VLAN 的作用，VLAN 的标识及划分。
2. VLAN 的数据交互，VLAN 的应用。
3. VLAN 的相关配置命令。
4. 通过 VLAN 技术，可以将物理的局域网划分成多个广播域，实现同一 VLAN 内的网络设备可以直接进行二层通信，不同 VLAN 内的设备不可以直接进行二层通信。
5. 基于端口配置的 VLAN 技术配置简单，使用方便，终端设备不需要任何物理位置的移动。

A thin, light green wavy line starts at the top left, has a small peak and dip, and then flows horizontally across the top of the slide.

谢谢！

Two thin, light green wavy lines start from the left edge and flow diagonally downwards across the bottom of the slide.