

第 2 篇 VLAN 技术

第 4 章 VLAN 的原理

第 5 章 VLAN 的配置

第 6 章 VLAN 扩展技术

第 7 章 VLAN 路由

第4章 VLAN 的原理

交换机可以根据 VLAN 信息在不同的范围内进行帧转发从而隔离广播帧的转发范围。在本章中首先会学习 VLAN 的帧格式，以及交换机是如何对 VLAN 帧转发的；其次还会介绍划分 VLAN 的四种方法以及它们的转发原理，最后介绍了适应于大规模网络的动态 VLAN 注册协议 MVRP。

4.1 本章目标

课程目标

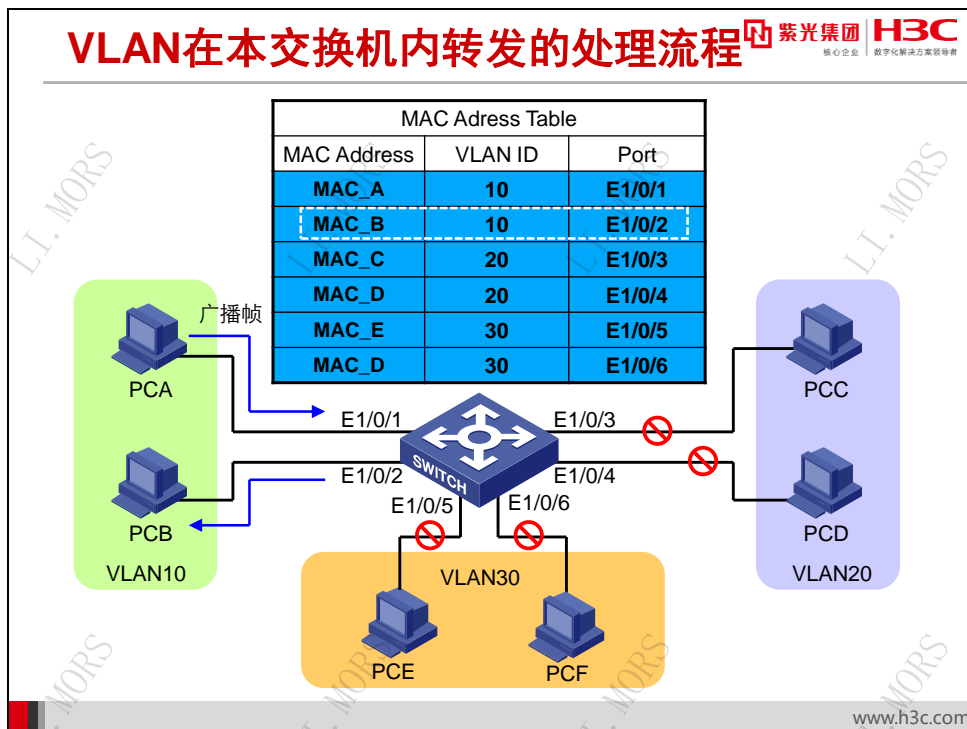
● 学习完本课程，您应该能够：

- 掌握交换机的VLAN实现基础，802.1Q Tag
- 熟悉VLAN的基本工作原理
- 熟悉交换机的三种链路类型
- 熟悉VLAN的四种划分方法
- 熟悉交换机划分VLAN的具体流程
- 熟悉VLAN注册协议MVRP的工作原理



www.h3c.com

4.2 VLAN的技术原理

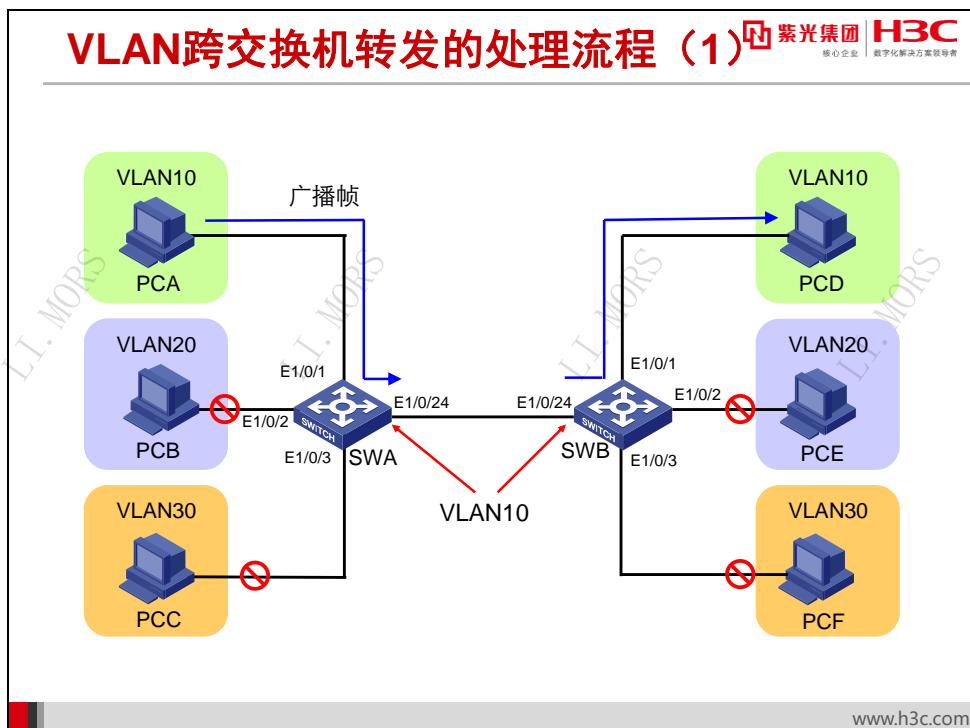


MAC 地址表的表项中包含了与本交换机相连的终端主机的 MAC 地址、本交换机连接主机的端口等信息，交换机是依据 MAC 地址表来进行数据帧的转发的。如果交换机能增加一个判断信息来决定应该从哪些端口转发广播帧，而不是从除源端口之外的所有端口都转发广播帧，这样就减少了广播帧的传播范围，实现了广播域的隔离。这个判断信息就是 VLAN，这就是 VLAN 隔离技术的思想。

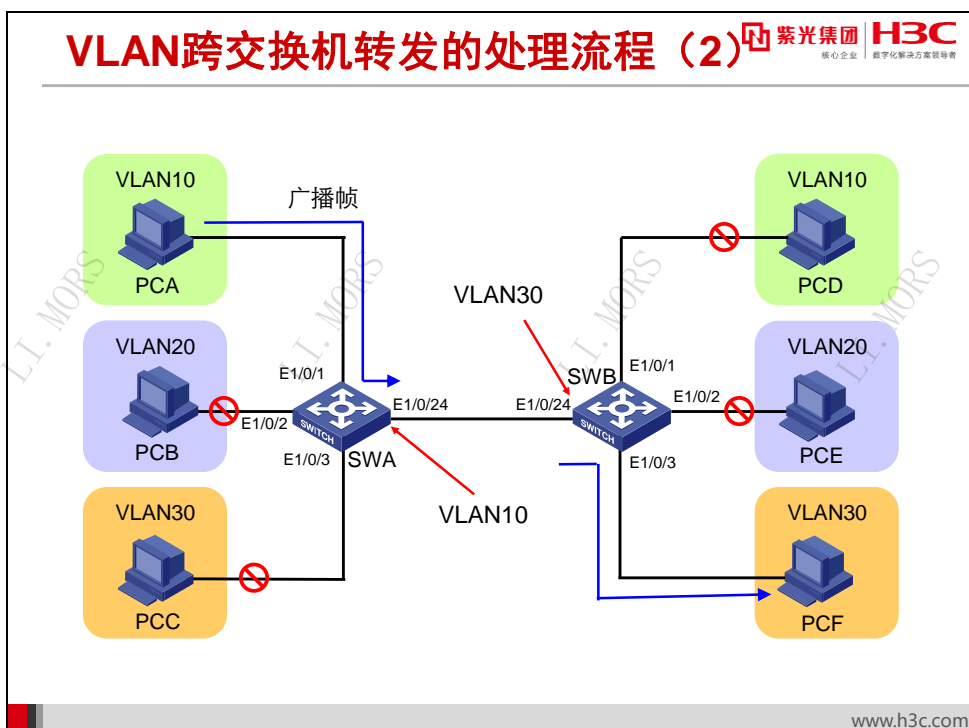
在交换机刚启动时，它的 MAC 地址表项中没有表项。交换机按照端口划分 VLAN 后，当网络中某台 PC 发出数据帧时，交换机记录其中的源 MAC 地址，与接收到数据帧的端口和此端口所属的 VLAN 关联起来，形成带 VLAN ID 的 MAC 地址表项。

MAC 地址表学习完成后，交换机根据 MAC 地址表项进行数据帧转发时，只会在源端口所对应的 VLAN 内查找目的 MAC 地址，以确定数据帧的目的端口。这样相当于用 VLAN 信息把 MAC 地址表里的表项区分开来，只有相同 VLAN 信息的端口之间能够互相转发数据帧。

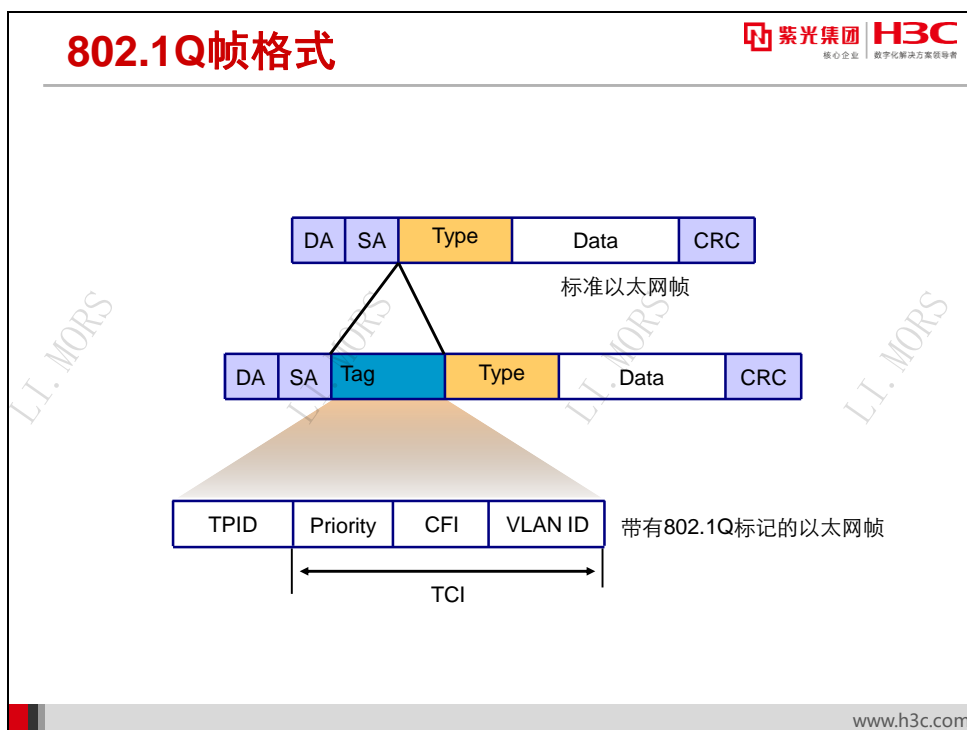
上图中，交换机端口 E1/0/1 和 E1/0/2 被划分到 VLAN10 中，端口 E1/0/3 和 E1/0/4 被划分到 VLAN20 中，端口 E1/0/5 和 E1/0/6 被划分到 VLAN30 中。PCA 发出广播帧时，交换机会把此广播帧向 VLAN10 内除源端口之外的所有端口转发出去。因为只有 PCA 和 PCB 属于 VLAN10，所以只有 PCB 能收到 PCA 发的广播帧，而其他 PC 都收不到 PCA 发出的广播帧。



上图中，SWA 和 SWB 各端口 VLAN 划分如图所示，PCA 发出广播帧，SWA 会把此广播帧向 VLAN10 内的所有端口转发出去（除了 E1/0/1 端口），因为在 SWA 上只有 E1/0/1 和 E1/0/24 属于 VLAN10，所以此广播帧从 SWA 的 E1/0/24 端口转发出去。SWB 的 E1/0/24 端口接收到 SWA 转发过来的广播帧后，因 E1/0/24 也属于 VLAN10，所以，SWB 也会向 VLAN10 内的所有端口广播（除了 E1/0/24 端口），同样道理，在 SWB 上只有属于 VLAN10 的 PCD 才能收到此广播帧。



上图中，把 SWB 的 E1/0/24 端口划分为 VLAN30 后，则 SWA 上 VLAN10 内的 PCA 发出的广播帧，会被 SWB 在 VLAN30 内广播，结果 VLAN30 内的 PCF 接收到了广播帧，而 SWB 上 VLAN10 内的 PCD 接收不到广播帧。这就引出一个问题，VLAN 隔离如何保证跨越交换机生效。



要允许所有 VLAN 成员不用局限在一个物理范围之内,VLAN 的划分可以跨越多个交换机,就必然涉及到 VLAN 流量识别的问题。

要使网络设备能够分辨不同 VLAN 的帧,需要在帧中添加标识 VLAN 的字段。由于普通交换机工作在 OSI 模型的数据链路层,只能对帧的数据链路层封装进行识别。因此,如果添加识别字段,也需要添加到数据链路层封装中。

IEEE 802.1Q 定义了一个新的字段,用于标识以太网帧所属的 VLAN。这个字段添加在以太网帧的源 MAC 之后,类型字段之前,封装具体内容如上图所示。

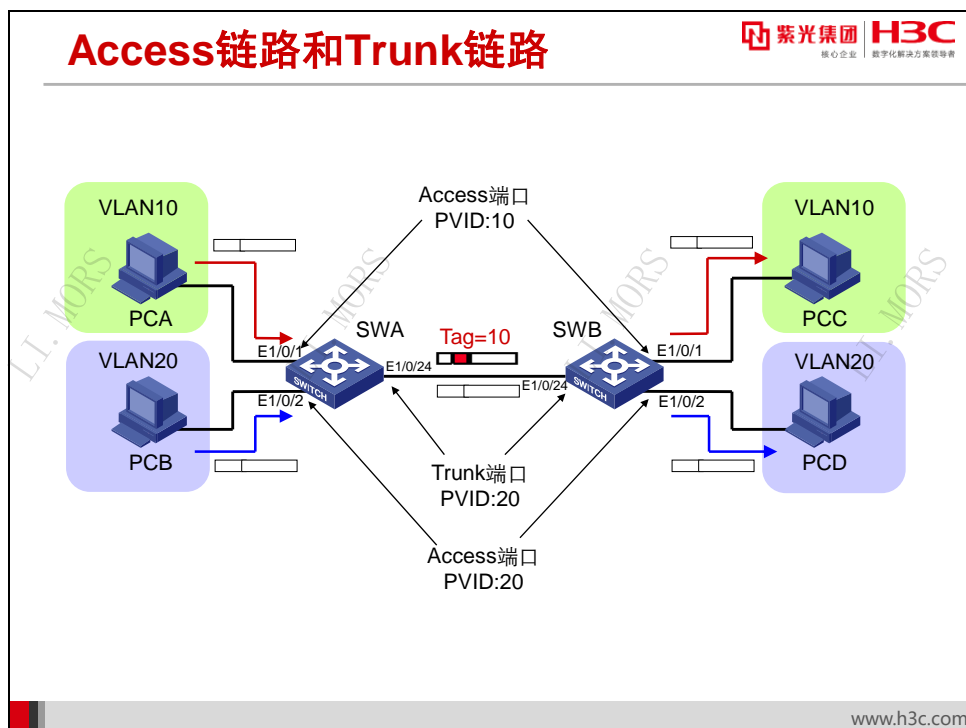
传统的以太网帧中添加了 4 个字节的 802.1Q 标签后,成为带有 VLAN 标签的帧 (Tagged Frame)。而传统的不携带 802.1Q 标签的数据帧称为未打标签的帧 (Untagged Frame)。

802.1Q 标签头包含了 2 个字节的标签协议标识 (TPID) 和 2 个字节的标签控制信息 (TCI)。

TPID (Tag Protocol Identifier) 是 IEEE 定义的新的类型,表明这是一个封装了 802.1Q 标签的帧。TPID 包含了一个固定的值 0x8100。

TCI (Tag Control Information) 包含的是帧的控制信息,它包含了下列元素:

- **Priority:** 这 3 位指明数据帧的优先级。一共有 0~7 共 8 种优先级。在交换机的出端口发生拥塞时,交换机通过识别该优先级,优先发送优先级高的数据帧。
- **CFI (Canonical Format Indicator):** CFI 值为 0 说明是规范格式,为 1 说明是非规范格式。它被用在令牌环/源路由 FDDI 介质访问方法中来指示封装帧中所带地址的比特次序信息。
- **VLAN ID (VLAN Identifier):** 共 12 比特,指明 VLAN 的编号。每个支持 802.1Q 协议的交换机发送出来的数据帧都会包含这个字段,以指明自己属于哪一个 VLAN。在 4096 个可能的 VLAN ID 中,VLAN ID=0 用于识别帧优先级,VLAN ID=4095 (FFF) 作为预留值,所以 VLAN 配置的最大可能值为 4094。



交换机内部的数据帧一律都带有 VLAN 标签，以便以统一方式处理。因为交换机很有可能会配置多个 VLAN，不同 VLAN 流量区分只有依靠标签（Tag）。

端口所属的 VLAN 称为端口缺省 VLAN，又称为 PVID（Port VLAN ID）。除了可以设置端口允许通过的 VLAN，还可以设置端口的缺省 VLAN。在缺省情况下，所有端口的缺省 VLAN 均为 VLAN1，但用户可以根据需要进行配置。Access 端口的缺省 VLAN 就是它所在的 VLAN，不能配置；Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置缺省 VLAN。

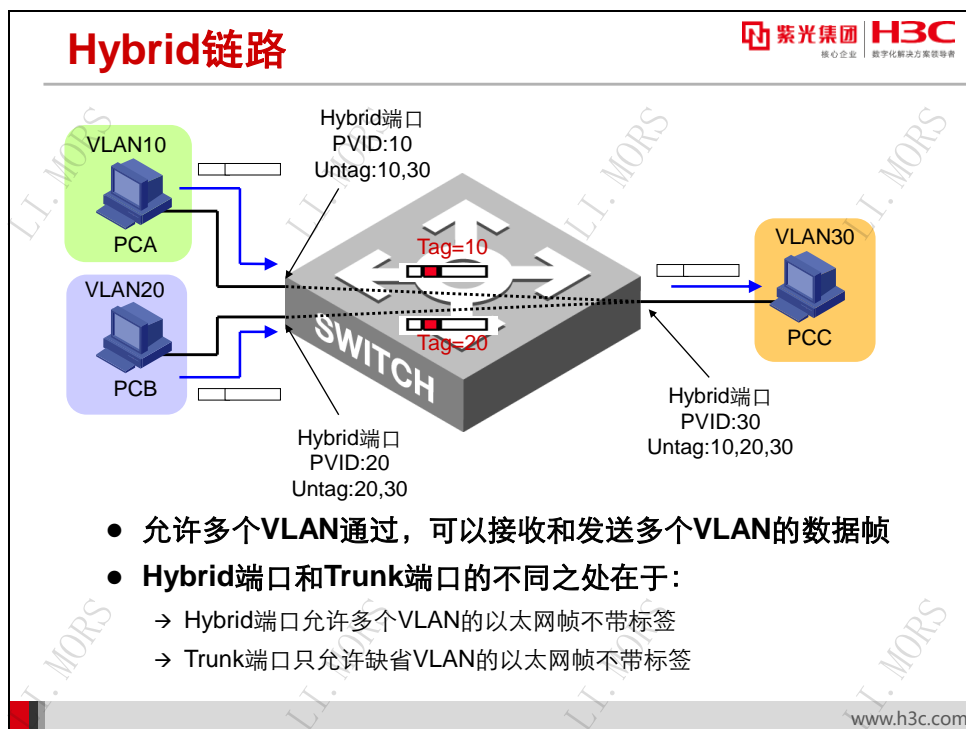
目前，大部分计算机的网卡都不支持带有 VLAN 标签的以太网数据帧，只能发送和接收标准的以太网数据帧，而认为带有 VLAN 标签的数据帧为非法数据帧。所以，支持 VLAN 的交换机在将数据帧发送给主机时，必须检查该数据帧，并剥离 VLAN 标签。

这种只允许缺省 VLAN 的以太网帧通过的端口称为 Access 端口。Access 端口在收到以太网帧后打上 VLAN 标签，转发出端口时剥离 VLAN 标签，对终端主机透明，所以通常用来连接不需要识别 802.1Q 协议的设备，如终端主机、路由器等。

允许多个 VLAN 帧通过的端口称为 Trunk 端口。Trunk 端口可以接收和发送多个 VLAN 的数据帧，且在接收和发送过程中不对帧中的标签进行任何操作，不过缺省 VLAN 帧是一个例外。在发送缺省 VLAN 帧时，Trunk 端口要剥离帧中的标签；同样，交换机从 Trunk 端口接收到不带标签的帧时，要打上缺省 VLAN 标签。Trunk 端口一般用于交换机之间互连。

图示为 PCA 至 PCC、PCB 至 PCD 的标签操作流程。PCA 发出以太网帧，到达 SWA 的 E1/0/1 端口，端口的缺省 VLAN 是 10，所以以太网帧被打上 VLAN10 标签；E1/0/24 端口是 Trunk 端口，VLAN10 标签的帧从端口转发至 SWB；SWB 从帧中的标签得知它属于 VLAN10，于是转发至端口 E1/0/1，经剥离标签后到达 PCC。

PCB 发出的帧在 E1/0/2 端口被打上 VLAN20 的标签；E1/0/24 端口是 Trunk 端口且缺省 VLAN 是 20，所以数据帧被剥离标签后转发；当未带标签的数据帧到达 SWB 的 E1/0/24 端口后，端口给它打上 VLAN20 的标签再转发到端口 E1/0/2，端口 E1/0/2 剥离标签后转发至 PCD。



除了 Access 链路类型和 Trunk 链路类型端口外，交换机还支持第三种类型的端口，称为 Hybrid 端口。Hybrid 端口可以接收和发送多个 VLAN 的数据帧，同时还能够指定对任何 VLAN 帧进行剥离标签操作。Hybrid 端口同样具有缺省 VLAN。在接收到一个不带 VLAN 标签的帧时，Hybrid 端口认为其属于入端口的缺省 VLAN，并对其打上缺省 VLAN 的标签进行转发。在需要发出一个帧时，Hybrid 端口根据其出端口上对每个 VLAN 的标签操作的具体设定，选择是否对此帧剥离 VLAN 标签。

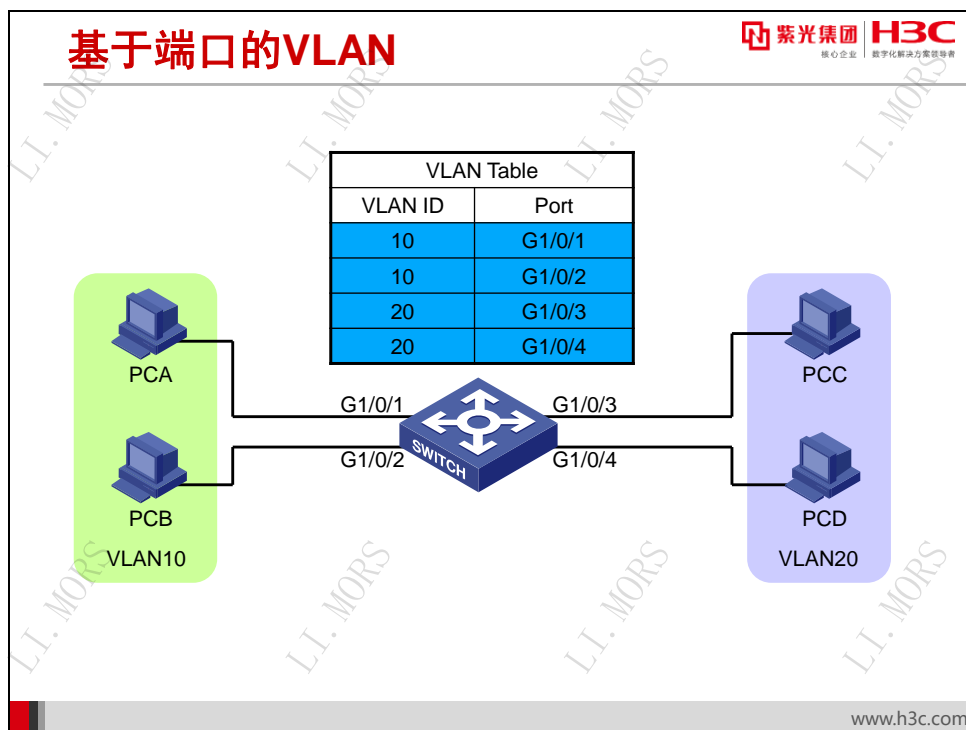
在上图中，PCA 发出的以太网帧进入端口时打上 VLAN10 的标签，在到达连接 PCC 的端口时，端口根据设定（Untag: 10, 20, 30）将数据帧中的标签剥离后发送给 PCC，所以 PCA 与 PCC 能够通信；同理，PCB 也能够与 PCC 通信。但 PCA 发出的以太网帧到达连接 PCB 的端口时，端口上的设定（Untag: 20, 30）表明只对 VLAN20、VLAN30 的数据帧转发且剥离标签，而不允许 VLAN10 的帧通过，所以 PCA 与 PCB 不能互通。

当网络中大部分主机之间需要隔离，但这些隔离的主机又需要与另一台主机互通时，可以使用 Hybrid 端口。

Hybrid 端口既可以用于在交换机之间互连，也可以用来连接终端主机或路由器等不需要识别 802.1Q 协议的设备。

4.3 VLAN 的划分方式

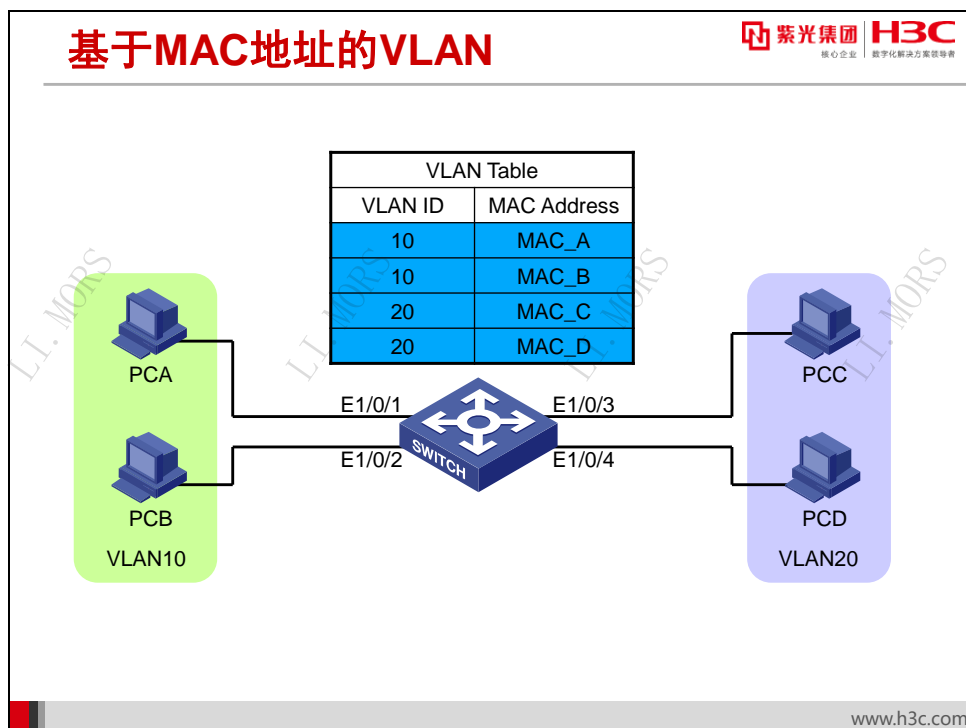
最常见的 VLAN 划分方式包括基于端口的 VLAN、基于 MAC 地址的 VLAN、基于协议的 VLAN 和基于 IP 子网的 VLAN。



基于端口的 VLAN 是最常用的 VLAN 划分方法。它按照设备端口来定义 VLAN 成员。将指定端口加入到指定 VLAN 中之后，该端口就可以转发指定 VLAN 的数据帧。

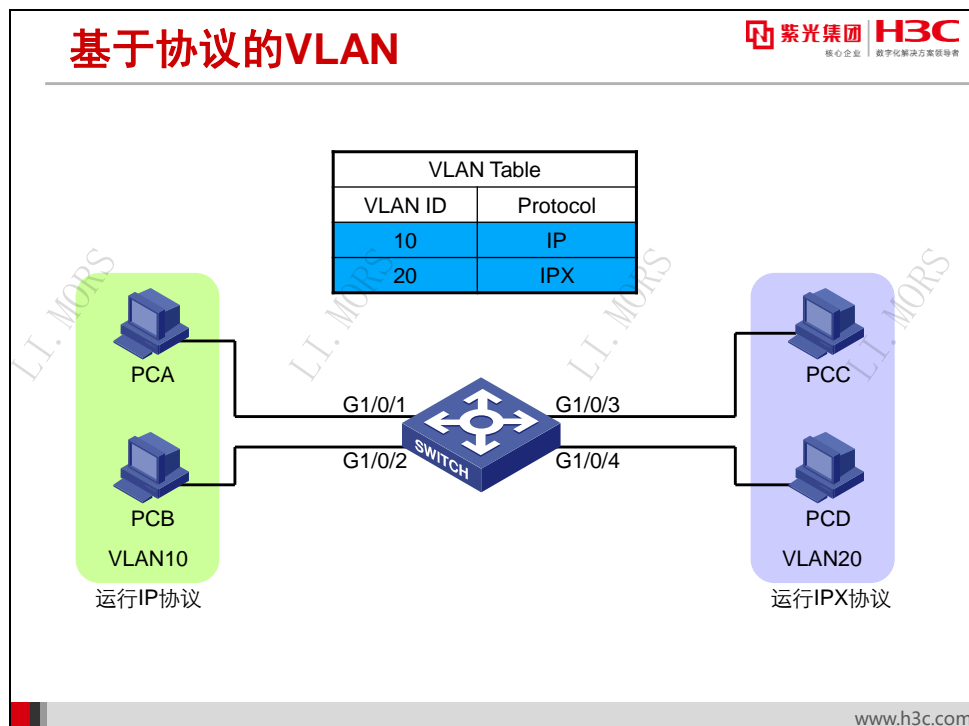
这种划分方法的优点是配置 VLAN 成员时非常简单，只要将端口指定到某个 VLAN 就可以了。它的缺点是当用户物理位置发生变化，例如从一个交换机换到其他的交换机时，就可能需要重新设置端口的 VLAN 属性。

上图中，交换机端口 E1/0/1 和 E1/0/2 被划分到 VLAN10 中，端口 E1/0/3 和 E1/0/4 被划分到 VLAN20 中，则 PCA 和 PCB 处于 VLAN10 中，可以互通；PCC 和 PCD 处于 VLAN20 中，可以互通。但 PCA 和 PCC 处于不同 VLAN，它们之间不能互通。



基于 MAC 地址的 VLAN 根据每个主机的 MAC 地址来划分 VLAN。交换机维护一张 VLAN 映射表，这个 VLAN 表记录了 MAC 地址和 VLAN 的对应关系。这种划分方法的最大优点就是当用户物理位置发生变化，例如从一个交换机换到其他的交换机时，VLAN 不用重新配置。所以这种根据 MAC 地址的划分方法也称为基于用户的 VLAN。

这种划分方法的缺点是，初始配置时，需要收集所有主机的 MAC 地址并逐个配置，如果主机很多，配置的工作量是很大的。此外这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，该端口必须为 Hybrid 端口，以便允许多个 VLAN 的数据帧不打标签通过。这样，某个 VLAN 内的广播帧可能被交换机转发到另外一个 VLAN。



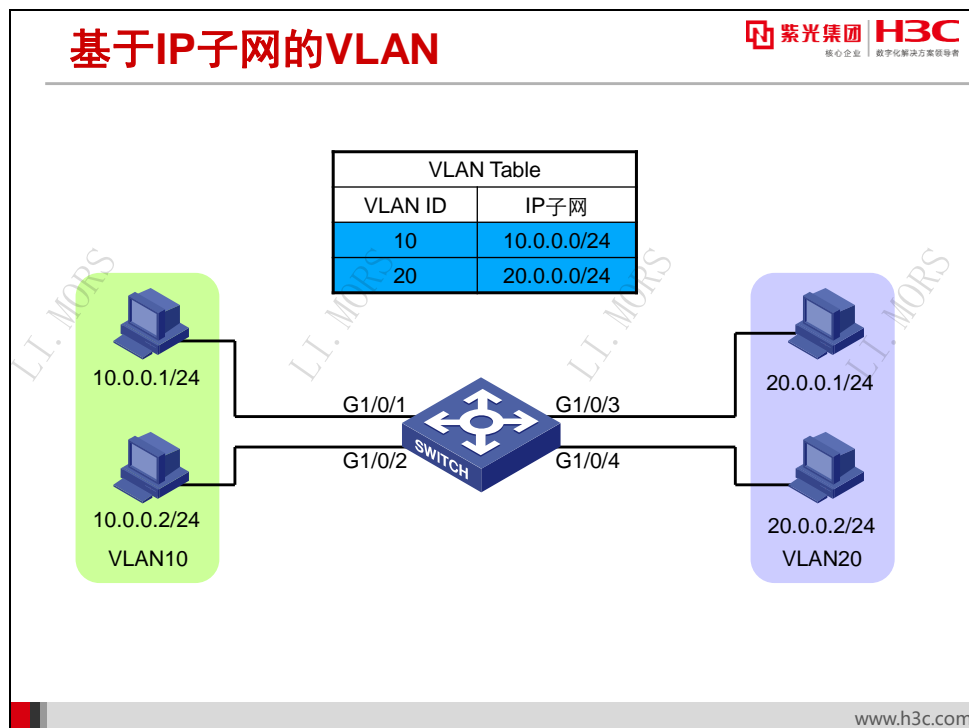
基于协议的 VLAN 是根据端口接收到的帧所属的协议（族）类型及封装格式来给帧分配不同的 VLAN ID。可用来划分 VLAN 的协议族有 IP、IPX、AppleTalk 等，封装格式有 Ethernet II、802.3、802.3/802.2 LLC、802.3/802.2 SNAP 等。

交换机从端口接收到以太网帧后，通过识别帧中的协议类型和封装格式来确定帧所属的 VLAN，然后将数据帧自动划分到指定的 VLAN 中传输。

此特性主要用于将网络中提供的协议类型与 VLAN 相绑定，以方便管理和维护。

这种划分 VLAN 的方法优点是，当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置。

这种划分 VLAN 的方法缺点是效率低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，即该端口为 Hybrid 链路类型端口，允许多个 VLAN 的数据帧不打标签通过，这样，某个 VLAN 内的广播帧可能被交换机转发到另外一个 VLAN。并且，在多数情况下，仅依据协议类型并不能足够细致地划分 VLAN。

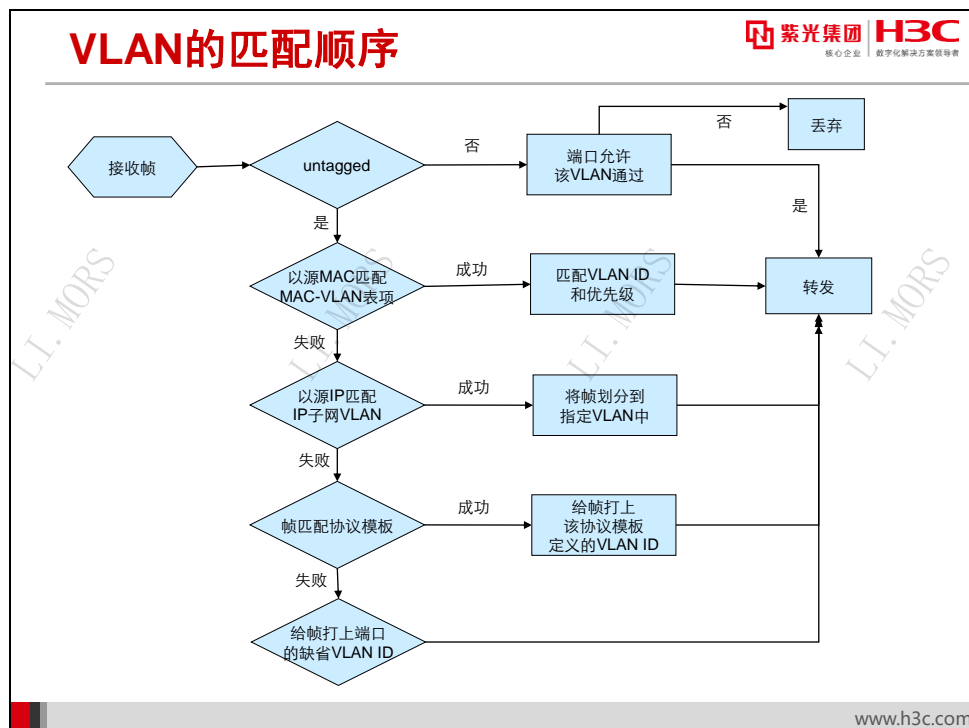


基于 IP 子网的 VLAN 是以帧中 IP 包的源 IP 地址作为依据来进行划分的。设备从端口接收到帧后,根据帧中 IP 包的源 IP 地址,找到与现有 VLAN 的对应关系,然后自动划分到指定 VLAN 中转发。

此特性主要用于将指定网段或 IP 地址发出的数据在指定的 VLAN 中传送。

这种划分 VLAN 的方法优点是当用户物理位置移动时,即从一个交换机换到其他的交换机时, VLAN 不用重新配置。

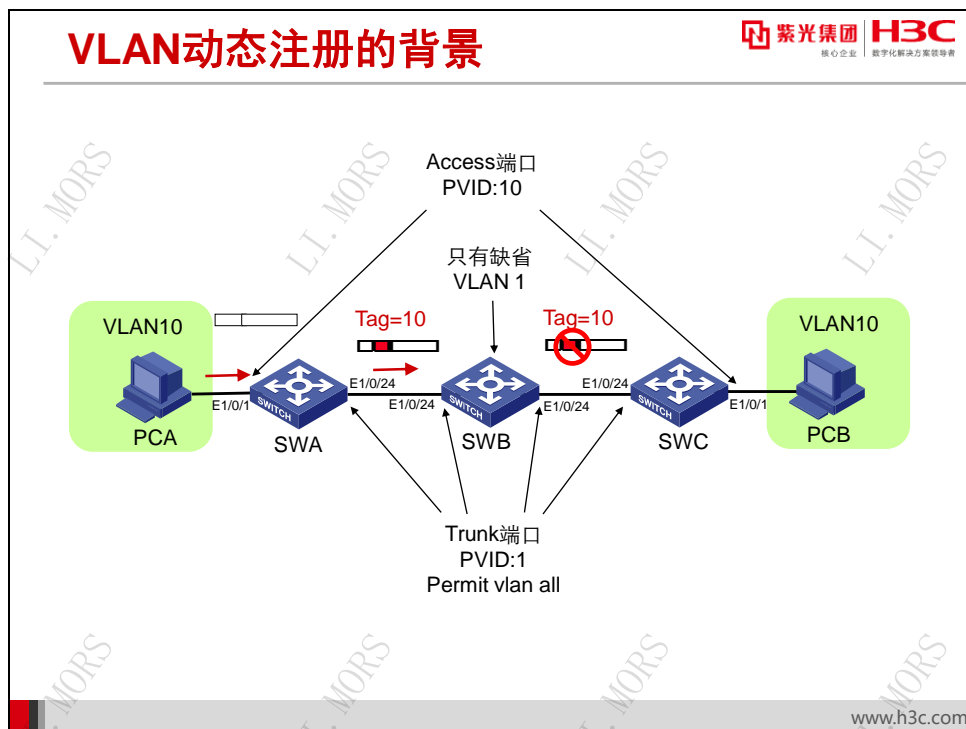
这种划分 VLAN 的方法缺点是效率低,因为检查每一个数据帧的网络层地址是需要消耗处理时间的,一般的交换机芯片都可以自动检查网络上数据帧的头,但要让芯片能检查 IP 头,需要更强的识别和处理能力。



如果交换机的某个端口下同时开启以上四种 VLAN，则缺省情况下，VLAN 将按照基于 MAC 地址的 VLAN、基于 IP 子网的 VLAN、基于协议的 VLAN、基于端口的 VLAN 的先后顺序进行匹配。当交换机的以太网端口收到帧时，将采用以下方法处理：

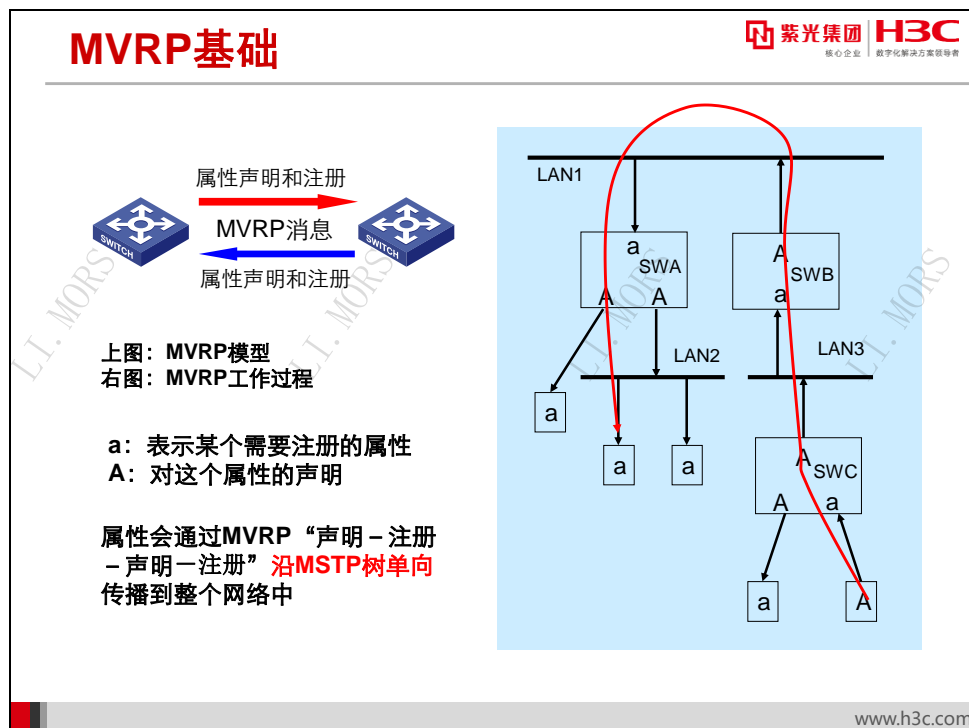
- 1) 当收到的帧为 **Tagged** 帧时，如果端口允许携带该 VLAN 标记的帧通过，则正常转发；如果不允许，则丢弃该帧。
- 2) 当收到的帧为 **Untagged** 帧时，会以帧的源 MAC 地址为依据去匹配 MAC-VLAN 表项。如果匹配成功，则按照匹配到的 VLAN ID 和优先级进行转发；如果匹配失败，则进行下一步处理。
- 3) 按 IP 子网 VLAN 匹配方式进行匹配，依据帧的源地址来确定帧所属的 VLAN，如果匹配成功，将帧自动划分到指定 VLAN 中进行转发；如果匹配失败，则进行下一步处理。
- 4) 按协议 VLAN 匹配方式进行匹配，如果帧匹配协议模板，则给帧打上由该协议模板定义的协议 VLAN 的 VLAN ID 进行转发；如果帧没有匹配协议模板，则给帧打上端口的缺省 VLAN ID 进行转发。

4.4 VLAN信息的传播



交换机只会转发本交换机存在的 VLAN 的数据帧。上图中，交换机的端口属性和 VLAN 划分如图所示。SWA 和 SWC 上都存在 VLAN10，SWB 上只有缺省的 VLAN1，交换机之间的互联端口都为 Trunk 端口，且都允许所有的 VLAN 通过。PCA 访问 PCB 时，SWA 从 E1/0/24 端口转发 PCA 发出的数据帧，并且封装 VLAN10 的标签，SWB 接收到此数据帧检查 VLAN 标签为 10，发现本交换机没有 VLAN10，没法查找到出端口，所以把数据帧丢弃。

如果网络里交换机很多，需要配置的 VLAN 也很多，则需要在每台交换机上配置大量的 VLAN，工作量很大。如果交换机能在一定网络范围内动态学习其他交换机的 VLAN 信息，动态配置 VLAN，并把相关端口加入动态 VLAN 中，保证 VLAN 在该网络中的连通性，则会大大简化 VLAN 配置管理，为网络的管理带来很大便利。



MRP（Multiple Registration Protocol，多属性注册协议）作为一个属性注册协议的载体，可以用来传递属性信息。MVRP（Multiple VLAN Registration Protocol，多 VLAN 注册协议）是 MRP 的一种应用，用于在设备间发布并学习 VLAN 配置信息。

配置了 MVRP 的设备启动后，设备将本地的 VLAN 配置信息向其他设备发送，同时还能够接收来自其他设备的 VLAN 配置信息，并动态更新本地的 VLAN 配置信息，从而使所有设备的 VLAN 信息都达成一致，极大减少了网络管理员的 VLAN 配置工作。在网络拓扑发生变化后，MVRP 还能根据新的拓扑重新发布及学习 VLAN 配置信息，做到 VLAN 配置信息实时与网络拓扑同步更新。

当端口接收到一个属性声明时，该端口将注册该属性，如果端口接收到撤销属性的声明，该端口将注销该属性。很明显，MVRP 协议的属性注册和注销仅仅是对于接收到 MVRP BPDU 的端口而言的，另外一点就是，属性的声明注册过程是沿着 MSTP 树单向传播的。

MRP 支持在 MSTI（Multiple Spanning Tree Instance，多生成树实例）的基础上，协助同一局域网内各成员之间传递属性信息。设备上每一个参与协议的端口都可以视为一个应用实体。当 MRP 应用（如 MVRP）在端口上启动之后，该端口就可视为一个 MRP 应用实体（以下简称 MRP 实体，同样的，MVRP 应用实体简称 MVRP 实体）。

MRP 实体通过发送声明类或回收声明类消息（以下简称声明和回收声明），来通知其他 MRP 实体注册或注销自己的属性信息，并根据其他 MRP 实体发来的声明或回收声明来注册或注销对方的属性信息。通过 MRP 机制，一个 MRP 实体上的配置信息会迅速传遍整个局域网。

所有支持 MVRP 特性的交换机能够接收来自其它交换机的 MVRP VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个端口到

达等。而且所有支持 MVRP 特性的交换机能够将本地的 VLAN 注册信息向其他交换机传播，以便使同一交换网内所有支持 MVRP 特性的设备的 VLAN 信息达成一致。MVRP 传播的 VLAN 注册信息即包括本地手工配置的静态 VLAN 信息，也包括来自其它交换机的动态 VLAN 注册信息。

MVRP消息

● 为了高效控制属性的声明和注册，MVRP提供了五种类型的消息：

- Join
 - JoinEmpty
 - JoinIn
- New
- Leave
- LeaveAll

www.h3c.com

MVRP 应用实体之间的信息交换借助于各种消息的传递来完成，其中主要如下五类消息起作用：

- **Join:** MRP 实体配置了某些属性，需要对端实体来注册自己的属性信息时，它会向对端实体发送 Join 消息。MRP 实体收到来自对端实体的 Join 消息时，它会注册该 Join 消息中的属性，并向本设备的其他实体传播该 Join 消息，其他实体收到传播的 Join 消息后，根据该 Join 消息中的属性在该实体的注册状态，向其对端实体发送 Join 消息。
- **JoinEmpty:** 用于声明 MRP 实体的非注册属性。比如一个 MRP 实体加入了某静态 VLAN（我们将本地手工创建的 VLAN 称为静态 VLAN，通过 MRP 消息学习并创建的 VLAN 称为动态 VLAN），此时若该实体还没有通过 MRP 消息注册该 VLAN，这时该实体向对端实体发送的 Join 消息就为 JoinEmpty 消息。
- **JoinIn:** 用于声明 MRP 实体的注册属性。比如 MRP 实体加入了某静态 VLAN 且通过 MRP 消息注册了该 VLAN，或该实体收到本设备其他实体传播的某 VLAN 的 Join 信息且通过 MRP 消息注册了该 VLAN，这时该实体向对端实体发送的 Join 消息就为 JoinIn 消息。

- **New:** 用于 MSTP (Multiple Spanning Tree Protocol, 多生成树协议) 拓扑变化的情况。当 MSTP 拓扑变化时, MRP 实体需要向对端实体发送 New 消息声明拓扑变化。MRP 实体收到来自对端实体的 New 消息时, 它会注册该 New 消息中的属性, 并向本设备的其他实体传播该 New 消息, 其他实体收到传播的 New 消息后, 向其对端实体发送该 New 消息。
- **Leave:** 用于 MRP 实体注销了某些属性, 需要对端实体进行同步注销时, 它会向对端实体发送 Leave 消息。当一个 MRP 实体收到来自对端实体的 Leave 消息时, 它会注销该 Leave 消息中的属性, 并向本设备的其他实体传播该 Leave 消息, 其他实体收到传播的 Leave 消息后, 根据该 Leave 消息中的属性在本设备上的状态, 决定是否向其对端实体发送该 Leave 消息 (比如该 Leave 消息中的属性为某 VLAN, 若该 VLAN 为动态 VLAN, 且本设备上无实体注册该 VLAN, 则在设备上删除该 VLAN, 并向对端实体发送该 Leave 消息; 若该 VLAN 为静态 VLAN, 则不向对端实体发送该 Leave 消息)。
- **LeaveAll:** 用于 MRP 实体启动时都会启动各自的 LeaveAll 定时器, 当该定时器超时后, MRP 实体就会向对端实体发送 LeaveAll 消息。当一个 MRP 实体收发 LeaveAll 消息时, 它会启动 Leave 定时器, 同时根据自身的属性状态决定是否发送 Join 消息要求对端实体重新注册某属性。该实体在 Leave 定时器超时前, 重新注册收到的来自对端实体的 Join 消息中的属性; 在 Leave 定时器超时后, 注销所有未重新注册的属性信息, 从而周期性地清除网络中的垃圾属性。

MVRP端口注册模式



- **Normal模式**

→ MVRP实体允许进行动态VLAN的注册或注销

- **Fixed模式**

→ MVRP实体禁止进行动态VLAN的注销, 收到的MVRP报文会被丢弃。

- **Forbidden模式**

→ MVRP实体禁止进行动态VLAN的注册, 收到的MVRP报文会被丢弃。

设备开启 MVRP 功能后，能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可通过哪个端口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以便使同一局域网内所有设备的 VLAN 信息达成一致。

MVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。MVRP 的端口注册模式有以下三种：

- **Normal 模式：**该模式下的 MVRP 实体允许进行动态 VLAN 的注册或注销。
- **Fixed 模式：**该模式下的 MVRP 实体禁止进行动态 VLAN 的注销，收到的 MVRP 报文会被丢弃。也就是说，在该模式下，实体已经注册的动态 VLAN 是不会被注销的，同时也不会注册新的动态 VLAN。
- **Forbidden 模式：**该模式下的 MVRP 实体禁止进行动态 VLAN 的注册，收到的 MVRP 报文会被丢弃。也就是说，在该模式下，实体不会注册新的动态 VLAN，一旦在配置该模式前注册的动态 VLAN 被注销后，不会重新进行注册。

MRP定时器

- Periodic定时器
- Join定时器
- Leave定时器
- LeaveAll定时器

紫光集团 H3C
核心企业 数字化转型领导者

www.h3c.com

MRP 的定时器也就是 MVRP 的定时器。MRP 消息发送的时间间隔是通过定时器来实现的，MRP 定义了下列四种定时器，用于控制各 MRP 消息的发送周期：

- **Periodic 定时器：**每个 MRP 实体启动时都会启动各自的 Periodic 定时器，来控制 MRP 消息的周期发送。该定时器超时前，实体收集需要发送的 MRP 消息，在该定时器超时后，将所有待发送的 MRP 消息封装成尽可能少的报文发送出去，这样减少了报文发送数量。随后再重新启动 Periodic 定时器，开始新一轮的循环。

- **Join 定时器：**Join 定时器用来控制 Join 消息的发送。为了保证消息能够可靠地发送到对端实体，MRP 实体在发送 Join 消息时，将启动 Join 定时器。如果在该定时器超时前收到了来自对端实体的 JoinIn 消息，且该 JoinIn 消息中的属性与发出的 Join 消息中的属性一致，便不再重发该 Join 消息，否则在该定时器超时后，当 Periodic 定时器也超时，它将重发一次该 Join 消息。
- **Leave 定时器：**Leave 定时器用来控制属性的注销。当 MRP 实体收到来自对端实体的 Leave 消息（或收发 LeaveAll 消息）时，将启动 Leave 定时器。如果在该定时器超时前，收到来自对端实体的 Join 消息，且该 Join 消息中的属性与收到的 Leave 消息中的属性一致（或与收发的 LeaveAll 消息中的某些属性一致），则这些属性不会在本实体被注销，其他属性则会在该定时器超时后被注销。
- **LeaveAll 定时器：**每个 MRP 实体启动时都会启动各自的 LeaveAll 定时器，当该定时器超时后，该实体就会向对端实体发送 LeaveAll 消息，随后再重新启动 LeaveAll 定时器，开始新一轮的循环，对端实体在收到 LeaveAll 消息后也重新启动 LeaveAll 定时器。

MVRP定时器取值			
定时器	可配范围	缺省值	推荐值
Periodic	两个取值可选：0或100厘秒	100厘秒	100厘秒
Join	上限：小于1/2 Leave定时器的取值 下限：20厘秒	20厘秒	600厘秒
Leave	上限：小于LeaveAll定时器的值 下限：大于2倍Join定时器的值	60厘秒	3000厘秒
LeaveAll	上限：32760厘秒 下限：大于Leave定时器的取值	1000厘秒	12000厘秒

各个定时器的取值范围之间的关系如上图所示，各定时器的取值范围会由于与它相关的定时器取值的改变而改变。如果用户想要设置的定时器的值不在当前可以设置的取值范围内，可以通过改变相关定时器的取值实现。

在实际组网中，建议用户将 MVRP 定时器配置为上图中的推荐值。

4.5 本章总结

本章总结

- 交换机通过识别带有**802.1Q Tag**的数据帧实现**VLAN跨交换机转发**
- **MVRP**传播的**VLAN**注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息，可以实现**VLAN**的动态配置
- **MVRP**的端口注册模式有**Normal**模式、**Fixed**模式和**Forbidden**模式

www.h3c.com

4.6 习题和解答

4.6.1 习题

- 802.1Q 定义了一个新的以太网帧字段,这个字段添加在以太网帧的哪个位置? ()
A. 源 MAC 地址之前 B. 源 MAC 地址之后
C. 目的 MAC 地址之前 D. 目的 MAC 地址之后
- TCI (Tag Control Information) 包含的是帧的控制信息,它包含了下面的哪些元素?
()
A. TPID B. Priority C. CFI D. VLAN ID
- 关于 MVRP 下面描述正确的是 ()
A. MVRP (Multiple VLAN Registration Protocol, 多 VLAN 注册协议) 为处于同一个交换网内的交换成员之间提供了动态分发、传播、注册某种信息的一种手段
B. MVRP 作为实体存在于设备中
C. MVRP 有 4 种定时器, 分别为 Periodic 定时器、Join 定时器、Leave 定时器和 LeaveAll 定时器
D. MVRP (Multiple VLAN Registration Protocol, 多 VLAN 注册协议) 是 MRP 的一种应用, 用于在设备间发布并学习 VLAN 配置信息。
- MVRP 端口注册模式有 Normal、Fixed 和 Forbidden 三种模式, 这三种模式能在交换机的什么链路类型端口上配置? ()
A. Access 端口 B. Hybrid 端口 C. Trunk 端口 D. 以上三种端口都可以
- 以太网数据帧中包含下面哪个固定的值, 表明这是一个封装了 802.1Q 标签的帧?
()
A. 0x8000 B. 0x8100 C. 0x8200 D. 0x8300

4.6.2 习题答案

1. B 2. BCD 3. ACD 4. C 5. B

第5章 VLAN 的配置

在了解了 VLAN 交换机的转发处理机制后，还需要掌握各种 VLAN 划分方式的基本配置，才能组建基本的局域网。

本章首先介绍各种 VLAN 的基本配置命令，再通过介绍一些详细的配置示例，来进一步讲解各种 VLAN 划分方式的配置和组网应用，最后介绍对 MVRP 中各参数的配置和灵活应用。

5.1 本章目标

课程目标

○ 学习完本课程，您应该能够：


- 应用VLAN交换机组建基本的局域网
- 配置各种VLAN划分方式的交换机
- 在大型网络中配置MVRP动态传输VLAN信息



www.h3c.com

5.2 基于端口的VLAN基本配置

VLAN基本配置命令



紫光集团 H3C
核心企业 数字化转型先锋

- 批量创建VLAN

```
[Switch] vlan { vlan-id1 [ to vlan-id2 ] | all }
```
- 进入VLAN视图

```
[Switch] vlan vlan-id
```
- 向当前VLAN添加端口

```
[Switch-vlan10] port interface-list
```

www.h3c.com

缺省情况下，交换机只有 VLAN1，所有的端口都属于 VLAN1 且是 Access 链路类型端口。Access 端口只能属于 1 个 VLAN，在将 Access 端口加入到指定 VLAN 之前，要加入的 VLAN 必须已经存在。进行 VLAN 配置的基本步骤如下。

第1步：在系统视图下创建 VLAN 并进入 VLAN 视图。配置命令为：

vlan *vlan-id*

第2步：在 VLAN 视图下将指定端口加入到 VLAN 中。配置命令为：

port *interface-list*

Trunk端口配置命令



- 配置端口的链路类型为Trunk类型

```
[Switch-Ethernet1/0/1] port link-type trunk
```

- 允许指定的VLAN通过当前Trunk端口

```
[Switch-Ethernet1/0/1] port trunk permit vlan { vlan-id-list | all }
```

- 设置Trunk端口的缺省VLAN

```
[Switch-Ethernet1/0/1] port trunk pvid vlan vlan-id
```

www.h3c.com

Trunk 端口能够允许多个 VLAN 的数据帧通过，通常用于交换机之间的互连。配置某个端口成为 Trunk 端口的步骤如下。

第1步：在以太网端口视图下指定端口链路类型为 Trunk。配置命令为：

```
port link-type trunk
```

第2步：缺省情况下，Trunk 端口只允许缺省 VLAN 即 VLAN1 的数据帧通过。所以，需要在以太网端口视图下指定哪些 VLAN 帧能够通过当前 Trunk 端口。配置命令为：

```
port trunk permit vlan { vlan-id-list | all }
```

第3步：必要时，可以在以太网端口视图下设定 Trunk 端口的缺省 VLAN。配置命令为：

```
port trunk pvid vlan vlan-id
```

除了可以设置端口允许通过的 VLAN，还可以设置端口的缺省 VLAN。在缺省情况下，所有端口的缺省 VLAN 均为 VLAN1，但用户可以根据需要进行配置：

- Access 端口的缺省 VLAN 就是它所在的 VLAN，不能配置。
- Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，所以需要设置端口的缺省 VLAN ID。
- 当执行 undo vlan 命令删除的 VLAN 是某个端口的缺省 VLAN 时，对 Access 端口，端口的缺省 VLAN 会恢复到 VLAN1；对 Trunk 或 Hybrid 端口，端口的缺省 VLAN 配置不会改变，即它们可以使用已经不存在的 VLAN 作为缺省 VLAN。

注意：

缺省情况下,Trunk 端口的缺省 VLAN 是 VLAN1。可以根据实际情况进行修改缺省 VLAN,以保证两端交换机的缺省 VLAN 相同为原则,否则会发生同一 VLAN 内的主机跨交换机不能够通信的情况。

Hybrid端口配置命令

- 配置端口的链路类型为Hybrid类型
`[Switch-Ethernet1/0/1] port link-type hybrid`
- 允许指定的VLAN通过当前Hybrid端口
`[Switch-Ethernet1/0/1] port hybrid vlan vlan-id-list { tagged | untagged }`
- 设置Hybrid端口的缺省VLAN
`[Switch-Ethernet1/0/1] port hybrid pvid vlan vlan-id`

紫光集团 H3C
核心企业 数字化转型方案领导者
www.h3c.com

在某些情况下,需要用到 Hybrid 端口。Hybrid 端口也能够允许多个 VLAN 帧通过,并且还可以指定哪些 VLAN 数据帧被剥离标签。在设置允许指定的 VLAN 通过 Hybrid 端口之前,允许通过的 VLAN 必须已经存在。配置某个端口成为 Hybrid 端口的步骤如下。

第1步: 在以太网端口视图下指定端口链路类型为 Hybrid。配置命令为:

port link-type hybrid

第2步: 缺省情况下,所有 Hybrid 端口只允许 VLAN1 通过。所以,需要在以太网端口视图下指定哪些 VLAN 数据帧能够通过 Hybrid 端口,并指定是否剥离标签。配置命令为:

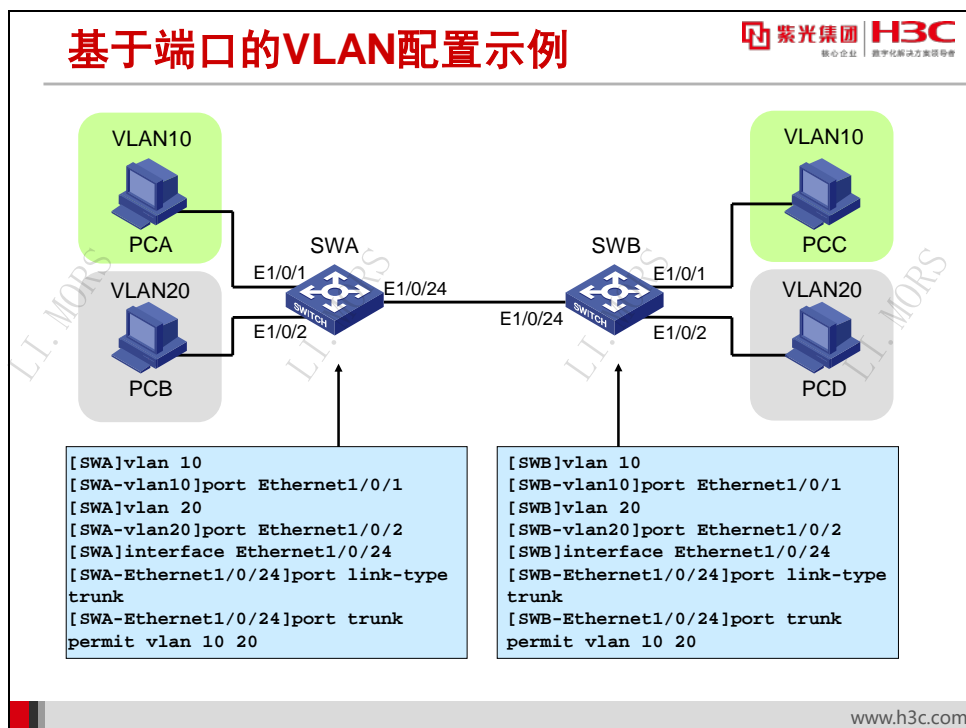
port hybrid vlan *vlan-id-list* { tagged | untagged }

第3步: 在以太网端口视图下设定 Hybrid 端口的缺省 VLAN。配置命令为:

port hybrid pvid vlan *vlan-id*

注意:

Trunk 端口和 Hybrid 端口不能直接切换,只能先设为 Access 端口,再设置为其他类型端口。



上图是基于端口的 VLAN 基本配置示例。图中 PCA 与 PCC 属于 VLAN10，PCB 与 PCD 属于 VLAN20，交换机之间使用 Trunk 端口相连，端口的缺省 VLAN 是 VLAN1。

图示配置完成后，PCA 与 PCC 能够互通，PCB 与 PCD 能够互通；但 PCA 与 PCB 不能够互通，PCC 与 PCD 也不能够互通。

5.3 于协议的VLAN基本配置

基于协议的VLAN配置命令



- 配置基于协议的VLAN，并指定协议模板

```
[Switch-vlan10] protocol-vlan [ protocol-index ] { at |
ipv4 | ipv6 | ipx { ethernetii / llc | snap } | mode
{ ethernetii etype etype-id | llc { dsap dsap-id [ ssap
ssap-id ] | ssap ssap-id } | snap etype etype-id } }
```

- 配置Hybrid端口与基于协议的VLAN关联

```
[Switch-Ethernet1/0/1] port hybrid protocol-vlan
vlan vlan-id { protocol-index [ to protocol-end ] | all }
```

www.h3c.com

可用来划分 VLAN 的协议有 IP、IPX、AppleTalk(AT)，封装格式有 Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP 等。

协议 VLAN 由协议模板定义，在一个端口上，可以同时关联多个协议模板。协议模板是用来匹配报文所属协议类型的标准，协议模板由“封装格式+协议类型”组成，分为如下两种模板：

- **标准模板：**指以 RFC 标准规定的协议封装格式和类型字段取值作为匹配条件的模板。
- **自定义模板：**指以用户在命令中指定的封装格式和标识类型字段的取值作为匹配条件的模板。

基于协议的 VLAN 只对 Hybrid 端口配置才有效。基于协议的 VLAN 主要配置命令如下：

第1步：缺省情况下，没有配置任何协议模板。所以，首先在 VLAN 视图下配置基于协议的 VLAN，并指定协议模板。配置命令为：

```
protocol-vlan [ protocol-index ] { at | ipv4 | ipv6 | ipx { ethernetii | llc | snap } |
mode { ethernetii etype etype-id | llc { dsap dsap-id [ ssap ssap-id ] | ssap
ssap-id } | snap etype etype-id } }
```

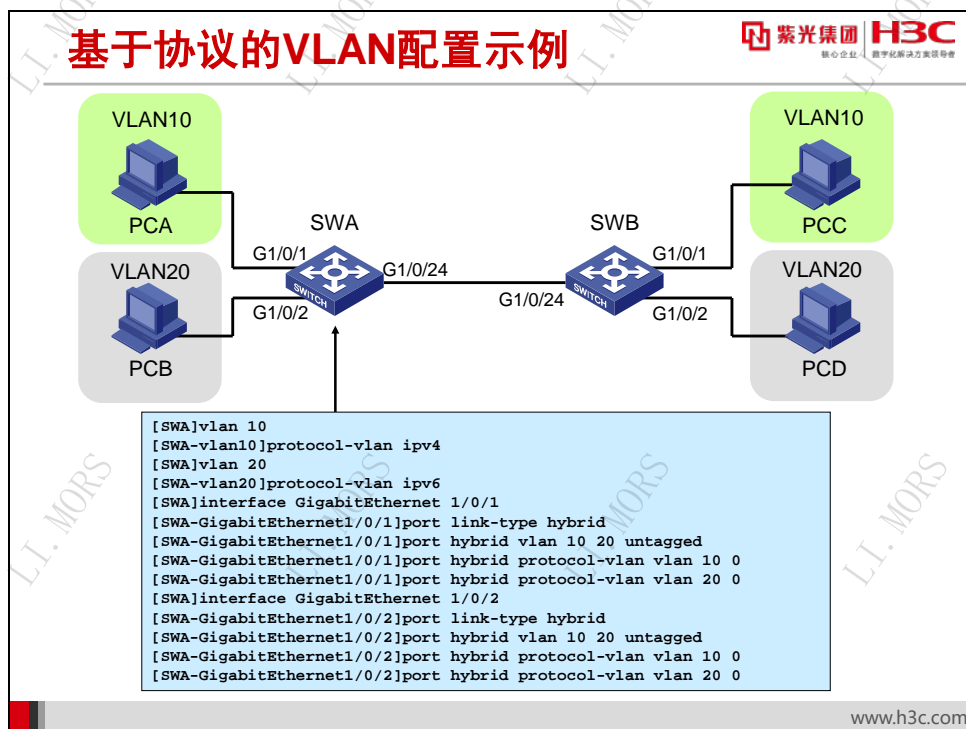
其中主要参数含义如下：

- **at：**基于 AT（AppleTalk）协议的 VLAN。
- **ipv4：**基于 IPv4 协议的 VLAN。

- **ipv6**: 基于 IPv6 协议的 VLAN。
- **ipx**: 基于 IPX 协议的 VLAN。其中的 Ethernet II、LLC、和 SNAP 为 IPX 的三种封装类型。
- **mode**: 配置自定义协议模板。可包括 ethernetii、llc 和 snap 三种封装类型。
- **ethernetii etype etype-id**: 匹配 Ethernet II 封装格式及相应的协议类型值。etype-id 表示入报文的协议类型值,取值范围为 0x0600~0xffff(除 0x0800、0x809b、0x8137、0x86dd 以外的值)。
- **llc**: 以太网报文封装格式为 llc。
- **dsap dsap-id**: 目的服务接入点,取值范围为 00~0xff。
- **ssap ssap-id**: 源服务接入点,取值范围为 00~0xff。
- **snap etype etype-id**: 匹配 SNAP 封装格式及相应的协议类型值。etype-id 表示入报文的以太网类型,取值范围为 0x0600~0xffff,但不能是 snap 封装下的 ipx snap 类型。

第2步: 配置协议模板完成后, 需要为协议 VLAN 添加端口并建立该端口与协议模板的关联, 在端口视图下, 配置 Hybrid 端口与基于协议的 VLAN 的关联。配置命令为:

port hybrid protocol-vlan vlan vlan-id { protocol-index [to protocol-end] | all }



上图是基于协议的 VLAN 基本配置示例。PCA 与 PCC 协议为 IPV4, 与 VLAN10 关联, PCB 与 PCD 的协议为 IPV6, 与 VLAN20 关联, 交换机之间使用 Trunk 端口相连, 端口的缺省 VLAN 是 VLAN1。

配置 SWA:

```
[SWA]vlan 10
[SWA-vlan10]protocol-vlan ipv4
[SWA-vlan10]quit
[SWA]vlan 20
[SWA-vlan20]protocol-vlan ipv6
[SWA-vlan20]quit
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port link-type hybrid
[SWA-Ethernet1/0/1]port hybrid vlan 10 20 untagged
[SWA-Ethernet1/0/1]port hybrid protocol-vlan vlan 10 0
[SWA-Ethernet1/0/1]port hybrid protocol-vlan vlan 20 0
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]port link-type hybrid
[SWA-Ethernet1/0/2]port hybrid vlan 10 20 untagged
[SWA-Ethernet1/0/2]port hybrid protocol-vlan vlan 10 0
[SWA-Ethernet1/0/2]port hybrid protocol-vlan vlan 20 0
[SWA-Ethernet1/0/2]quit
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-type trunk
[SWA-Ethernet1/0/24]port trunk permit vlan 10 20
```


配置 SWB:

```
[SWB]vlan 10
[SWB-vlan10]protocol-vlan ipv4
[SWB-vlan10]quit
[SWB]vlan 20
[SWB-vlan20]protocol-vlan ipv6
[SWB-vlan20]quit
[SWB]interface Ethernet 1/0/1
[SWB-Ethernet1/0/1]port link-type hybrid
[SWB-Ethernet1/0/1]port hybrid vlan 10 20 untagged
[SWB-Ethernet1/0/1]port hybrid protocol-vlan vlan 10 0
[SWB-Ethernet1/0/1]port hybrid protocol-vlan vlan 20 0
[SWB-Ethernet1/0/1]quit
[SWB]interface Ethernet 1/0/2
[SWB-Ethernet1/0/2]port link-type hybrid
[SWB-Ethernet1/0/2]port hybrid vlan 10 20 untagged
[SWB-Ethernet1/0/2]port hybrid protocol-vlan vlan 10 0
[SWB-Ethernet1/0/2]port hybrid protocol-vlan vlan 20 0
[SWB-Ethernet1/0/2]quit
[SWB]interface Ethernet 1/0/24
[SWB-Ethernet1/0/24]port link-type trunk
[SWB-Ethernet1/0/24]port trunk permit vlan 10 20
```

配置完成后，交换机会把 IPv4 协议的数据帧划分为 VLAN10，把 IPv6 协议的数据帧划分为 VLAN20，PCA 与 PCC 都被划分到 VLAN10 中且能够互通，把 PCB 与 PCD 都被划分到 VLAN20 中且能够互通。

5.4 基于IP子网的VLAN基本配置

基于IP子网的VLAN配置命令



紫光集团 H3C
核心企业 数字化转型方案领导者

- 配置当前VLAN与指定的IP子网关联

```
[Switch-vlan10] ip-subnet-vlan [ ip-subnet-index ] ip  
ip-address [ mask ]
```

- 配置当前端口与基于IP子网的VLAN关联

```
[Switch-Ethernet1/0/1] port hybrid ip-subnet-vlan  
vlan vlan-id
```

www.h3c.com

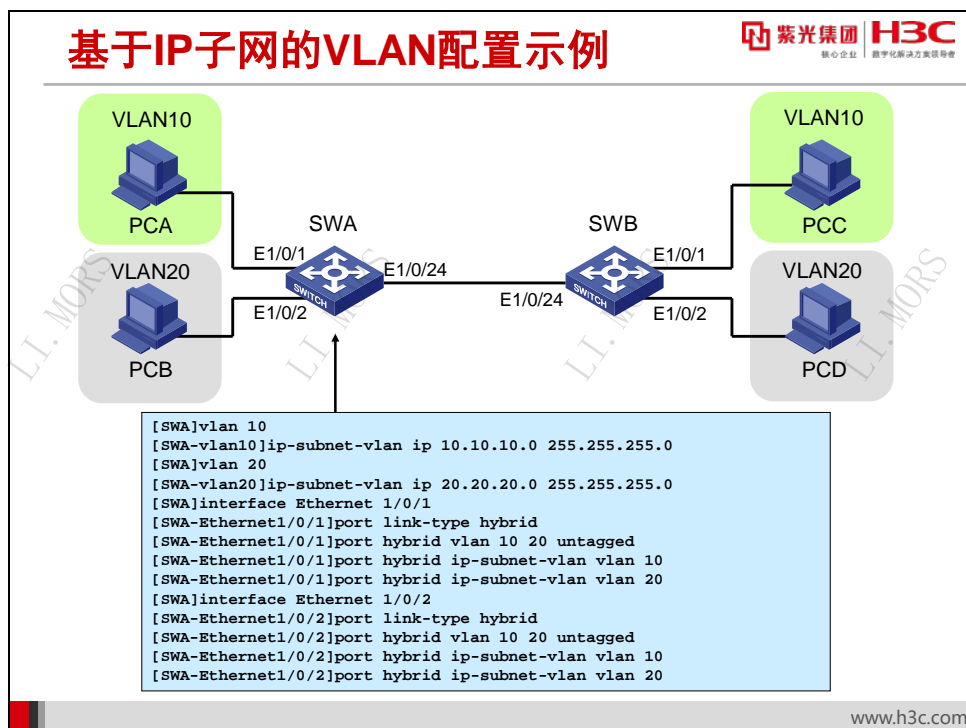
基于 IP 子网的 VLAN 只对 Hybrid 端口配置有效，其主要配置命令如下。

第1步：在 VLAN 视图下配置当前 VLAN 与指定的 IP 子网关联。配置命令为：

```
ip-subnet-vlan [ ip-subnet-index ] ip ip-address [ mask ]
```

第2步：在以太网端口视图下，设置好当前端口为 Hybrid 类型且已经允许该 VLAN 通过后，还需要设定当前端口与基于 IP 子网的 VLAN 关联。配置命令为：

```
port hybrid ip-subnet-vlan vlan vlan-id
```



上图是基于 IP 子网的 VLAN 基本配置示例。图中 PCA 与 PCC 的网段为 10.10.10.0/24，与 VLAN10 关联，PCB 与 PCD 的 IP 网段为 20.20.20.0/24，与 VLAN20 关联，交换机之间使用 Trunk 端口相连，端口的缺省 VLAN 是 VLAN1。

配置 SWA:

```

[SWA]vlan 10
[SWA-vlan10]ip-subnet-vlan ip 10.10.10.0 255.255.255.0
[SWA-vlan10]quit
[SWA]vlan 20
[SWA-vlan20]ip-subnet-vlan ip 20.20.20.0 255.255.255.0
[SWA-vlan20]quit
[SWA]interface Ethernet 1/0/1
[SWA-Ethernet1/0/1]port link-type hybrid
[SWA-Ethernet1/0/1]port hybrid vlan 10 20 untagged
[SWA-Ethernet1/0/1]port hybrid ip-subnet-vlan vlan 10
[SWA-Ethernet1/0/1]port hybrid ip-subnet-vlan vlan 20
[SWA-Ethernet1/0/1]quit
[SWA]interface Ethernet 1/0/2
[SWA-Ethernet1/0/2]port link-type hybrid
[SWA-Ethernet1/0/2]port hybrid vlan 10 20 untagged
[SWA-Ethernet1/0/2]port hybrid ip-subnet-vlan vlan 10
[SWA-Ethernet1/0/2]port hybrid ip-subnet-vlan vlan 20
[SWA-Ethernet1/0/2]quit
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-type trunk
[SWA-Ethernet1/0/24]port trunk permit vlan 10 20
  
```

配置 SWB:


```

[SWB]vlan 10
[SWB-vlan10]ip-subnet-vlan ip 10.10.10.0 255.255.255.0
[SWB-vlan10]quit
[SWB]vlan 20
  
```

```
[SWB-vlan20]ip-subnet-vlan ip 20.20.20.0 255.255.255.0
[SWB-vlan20]quit
[SWB]interface Ethernet 1/0/1
[SWB-Ethernet1/0/1]port link-type hybrid
[SWB-Ethernet1/0/1]port hybrid vlan 10 20 untagged
[SWB-Ethernet1/0/1]port hybrid ip-subnet-vlan vlan 10
[SWB-Ethernet1/0/1]port hybrid ip-subnet-vlan vlan 20
[SWB-Ethernet1/0/1]quit
[SWB]interface Ethernet 1/0/2
[SWB-Ethernet1/0/2]port link-type hybrid
[SWB-Ethernet1/0/2]port hybrid vlan 10 20 untagged
[SWB-Ethernet1/0/2]port hybrid ip-subnet-vlan vlan 10
[SWB-Ethernet1/0/2]port hybrid ip-subnet-vlan vlan 20
[SWB-Ethernet1/0/2]quit
[SWB]interface Ethernet 1/0/24
[SWB-Ethernet1/0/24]port link-type trunk
[SWB-Ethernet1/0/24]port trunk permit vlan 10 20
```

配置完成后，交换机会把 10.10.10.0/24 网段的数据帧划分为 VLAN10，把 20.20.20.0/24 网段的数据帧划分为 VLAN20，PCA 与 PCC 都被划分到 VLAN10 中且能够互通，把 PCB 与 PCD 都被划分到 VLAN20 中且能够互通。

5.5 MVRP的基本配置

配置MVRP
核心企业 | 数字化转型方案领导者

- 开启全局MVRP功能
`[Switch] mvrp global enable`
- 开启端口的MVRP功能
`[Switch-Ethernet1/0/1] mvrp enable`
- 配置MVRP注册模式
`[Switch-Ethernet1/0/1] mvrp registration { fixed | forbidden | normal }`

www.h3c.com

必须先开启全局 MVRP 功能，才能开启端口 MVRP 功能。

缺省情况下，全局的 MVRP 功能处于关闭状态。首先，在系统视图下开启全局 MVRP 功能。配置命令为：

mvrp global enable

当开启了全局的 MVRP 功能后，端口上的 MVRP 功能并不会被自动开启，只能在 Trunk 端口上开启 MVRP 功能。配置命令为：

mvrp enable

可以通过配置 Trunk 端口的 MVRP 注册模式来控制 VLAN 信息的传播，缺省情况下，MVRP 端口的注册模式为 Normal 模式。配置命令为：

mvrp registration { fixed | forbidden | normal }

配置MRP定时器

 紫光集团 H3C
核心企业 数字化转型先锋

- 配置Periodic定时器、Join定时器、Leave定时器和Leaveall定时器

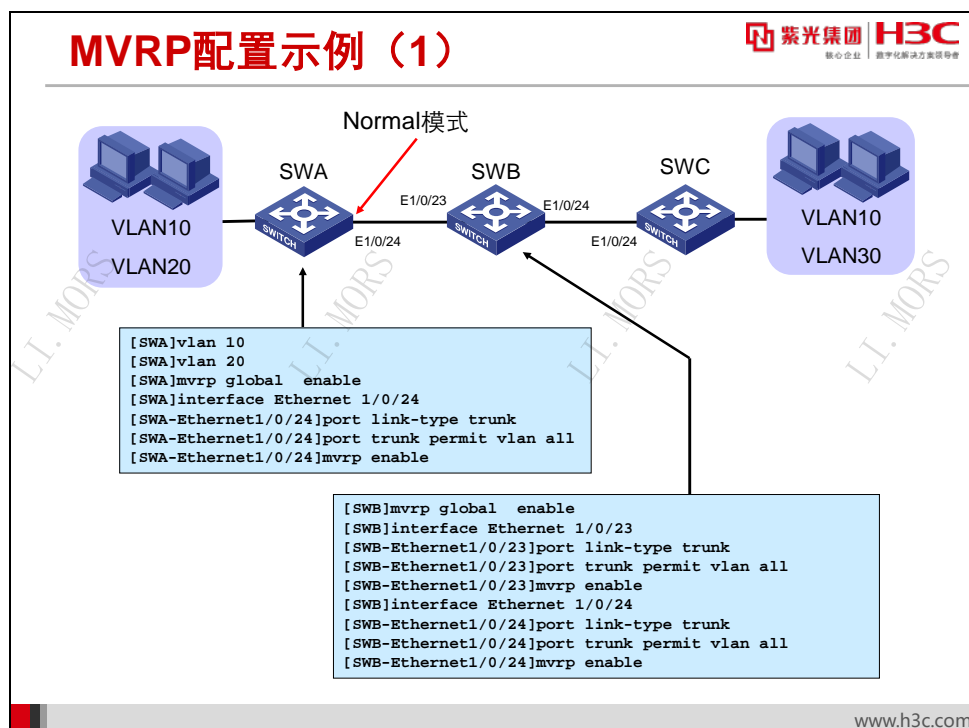
```
[Switch-Ethernet1/0/1] mrp timer {periodic | join |  
leave | leaveall} timer-value
```

www.h3c.com

MRP 定义了四种定时器，用于控制各 MRP 消息的发送周期。

缺省情况下，Hold 定时器的值为 10 厘秒；Join 定时器的值为 20 厘秒；Leave 定时器的值为 60 厘秒。这三个值需要在端口视图下配置。配置命令为：

```
mrp timer { periodic | join | leave | leaveall } timer-value
```



上图是 MVRP 的基本配置示例。图中 SWA 上有 VLAN10 和 VLAN20，SWB 上只有缺省 VLAN1，SWC 上有 VLAN10 和 VLAN30。交换机之间使用 Trunk 端口相连，端口的缺省 VLAN 是 VLAN1，Trunk 端口允许所有的 VLAN 通过。在交换机全局和 Trunk 端口开启 MVRP 功能。

配置 SWA:

```

[SWA]vlan 10
[SWA]vlan 20
[SWA]mvrp global enable
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-type trunk
[SWA-Ethernet1/0/24]port trunk permit vlan all
[SWA-Ethernet1/0/24]mvrp enable
  
```

配置 SWB:

```

[SWB]mvrp global enable
[SWB]interface Ethernet 1/0/23
[SWB-Ethernet1/0/23]port link-type trunk
[SWB-Ethernet1/0/23]port trunk permit vlan all
[SWB-Ethernet1/0/23]mvrp enable
[SWB]interface Ethernet 1/0/24
[SWB-Ethernet1/0/24]port link-type trunk
[SWB-Ethernet1/0/24]port trunk permit vlan all
[SWB-Ethernet1/0/24]mvrp enable
  
```

配置 SWC:

```

[SWC]vlan 10
[SWC]vlan 30
[SWC]mvrp global enable
[SWC]interface Ethernet 1/0/24
[SWC-Ethernet1/0/24]port link-type trunk
[SWC-Ethernet1/0/24]port trunk permit vlan all
[SWC-Ethernet1/0/24]mvrp enable
  
```

因缺省情况下，MVRP 端口的注册模式为 Normal 模式，配置完成后，SWA 可以动态学习到 VLAN30，SWB 可以动态学习到 VLAN10、VLAN20 和 VLAN30，SWC 可以动态学习到 VLAN20。

在 SWA 上查看所有 VLAN 和动态 VLAN 相关信息，如下所示：

```
[SWA]display vlan
Total VLANs: 4
The VLANs include:
1(default), 10, 20, 30

[SWA]display vlan dynamic
Dynamic VLANs: 1
The dynamic VLANs include:
30
```

从以上信息可以看出，SWA 上动态学习到了 VLAN30。

在 SWB 上查看所有 VLAN 和动态 VLAN 相关信息，如下所示：

```
[SWB]display vlan
Total VLANs: 4
The VLANs include:
1(default), 10, 20, 30

[SWB]display vlan dynamic
Dynamic VLANs: 3
The dynamic VLANs include:
10, 20, 30
```

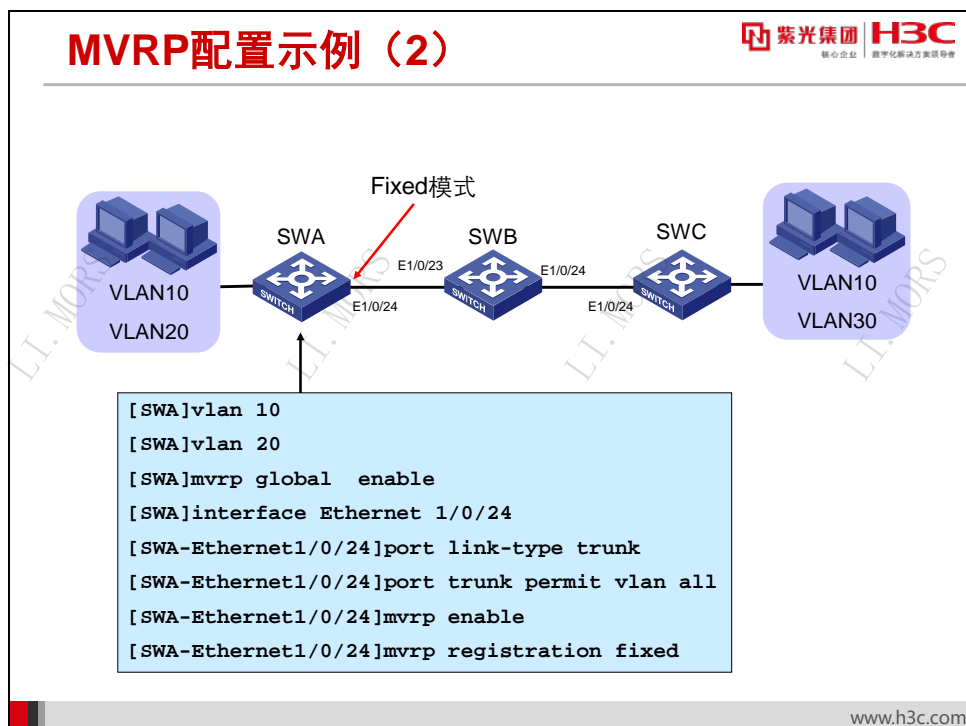
从以上信息可以看出，SWB 上动态学习到了 VLAN10、VLAN20 和 VLAN30。

在 SWC 上查看所有 VLAN 和动态 VLAN 相关信息，如下所示：

```
[SWC]display vlan
Total VLANs: 4
The VLANs include:
1(default), 10, 20, 30

[SWC]display vlan dynamic
Dynamic VLANs: 1
The dynamic VLANs include:
20
```

从以上信息可以看出，SWC 上动态学习到了 VLAN20。



在 MVRP 配置示例一的基础上，把 SWA 的 Trunk 端口 Ethernet1/0/24 的 MVRP 端口注册模式修改为 Fixed，SWB 和 SWC 的配置不变。

配置 SWA:

```

[SWA]vlan 10
[SWA]vlan 20
[SWA]mvrp global enable
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-type trunk
[SWA-Ethernet1/0/24]port trunk permit vlan all
[SWA-Ethernet1/0/24]mvrp enable
[SWA-Ethernet1/0/24]mvrp registration fixed
  
```

配置完成后，在 SWA 上查看所有 VLAN 和动态 VLAN 相关信息，如下所示：

```

[SWA]display vlan
Total VLANs: 3
The VLANs include:
1(default), 10, 20

[SWA]display vlan dynamic
No dynamic VLAN exists.
  
```

从以上信息可以看出，SWA 上没有动态学习到 VLAN30。因为在 SWA 的 Trunk 端口 Ethernet1/0/24 配置了 MVRP 端口注册模式为 Fixed，也就是说 SWA 的 Trunk 端口 Ethernet1/0/24 不会接收从对端来的动态 VLAN 信息。

在 SWA 上查看 Trunk 端口相关信息，如下所示：

```

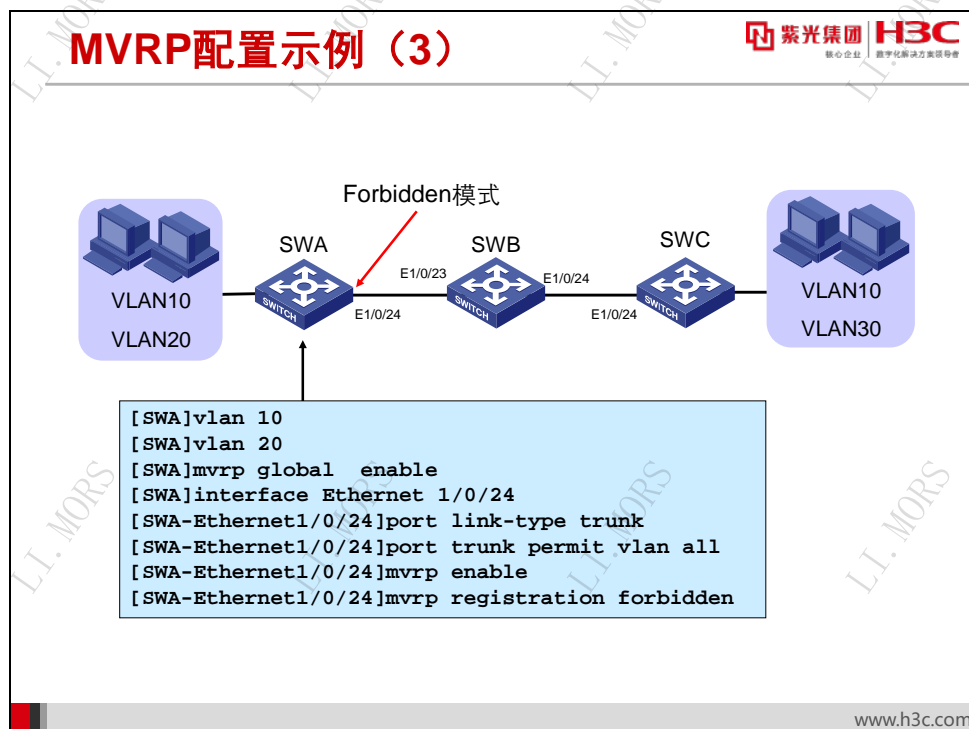
[SWA]display interface Ethernet 1/0/24
.....
PVID: 1
Mdi type: automdix
  
```

```

Port link-type: trunk
VLAN Passing: 1(default vlan), 10, 20
VLAN permitted: 1(default vlan), 2-4094
Trunk port encapsulation: IEEE 802.1q
.....

```

从以上信息可以看出，SWA 的 Trunk 端口 Ethernet1/0/24 被设置为 Fixed 注册模式后，不会注册 VLAN30。即实际通过的 VLAN 也只能是本交换机手动配置的静态 VLAN10 和 VLAN20。



在 MVRP 配置实示例三的基础上，把 SWA 的 Trunk 端口 Ethernet1/0/24 的 MVRP 端口注册模式修改为 Forbidden，SWB 和 SWC 的配置不变。

配置 SWA:

```

[SWA]vlan 10
[SWA]vlan 20
[SWA]mvrp global enable
[SWA]interface Ethernet 1/0/24
[SWA-Ethernet1/0/24]port link-type trunk
[SWA-Ethernet1/0/24]port trunk permit vlan all
[SWA-Ethernet1/0/24]mvrp enable
[SWA-Ethernet1/0/24]mvrp registration forbidden

```

配置完成后，在 SWA 上查看所有 VLAN 和动态 VLAN 相关信息，如下所示：

```

[SWA]display vlan
Total VLANs: 3
The VLANs include:
1(default), 10, 20

[SWA]display vlan dynamic
No dynamic VLAN exists.

```

从以上信息可以看出，SWA 上没有动态学习到 VLAN30。因为在 SWA 的 Trunk 端口 Ethernet1/0/24 配置了 MVRP 端口注册模式为 Forbidden，也就是说 SWA 的 Trunk 端口 Ethernet1/0/24 不会接收从对端来的动态 VLAN 信息。

在 SWA 上查看 Trunk 端口相关信息，如下所示：

```
[SWA]display interface Ethernet 1/0/24
.....
PVID: 1
Mdi type: automdix
Port link-type: trunk
VLAN Passing: 1(default vlan), 10, 20
VLAN permitted: 1(default vlan), 2-4094
Trunk port encapsulation: IEEE 802.1q
.....
```

从以上信息可以看出，SWA 的 Trunk 端口 Ethernet1/0/24 被配置为 Forbidden 注册模式后，不会注册 VLAN30。即实际通过的 VLAN 也只能是本交换机手动配置的静态 VLAN10 和 VLAN20。

5.6 本章总结

本章总结

- 修改Trunk端口或Hybrid端口的缺省VLAN时，以保证两端交换机的缺省VLAN相同为原则
- Trunk端口和Hybrid端口之间不能直接切换，只能先设为Access端口，再设置为其它类型端口
- 基于协议的VLAN和基于IP子网的VLAN只对Hybrid端口配置有效

5.7 习题和解答

5.7.1 习题

1. 下面关于端口缺省 VLAN 描述正确的是（ ）
 - A. Access 端口的缺省 VLAN 就是它所在的 VLAN，不能配置
 - B. Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，可以通过命令设置端口的缺省 VLAN ID
 - C. 当执行 `undo vlan` 命令删除的 VLAN 是某个端口的缺省 VLAN 时，对 Access 端口，端口的缺省 VLAN 会恢复到 VLAN1
 - D. 当执行 `undo vlan` 命令删除的 VLAN 是某个端口的缺省 VLAN 时，对 Trunk 或 Hybrid 端口，端口的缺省 VLAN 配置不会改变
2. 下面关于交换机 Trunk 端口描述正确的是（ ）
 - A. 交换机的 Trunk 端口只能用于交换机之间互联
 - B. 交换机的 Trunk 端口在接收数据帧时，如果数据帧带 VLAN Tag，接收该数据帧并保持 VLAN Tag 不变
 - C. 交换机的 Trunk 端口在发送数据帧时，无论数据帧的 VLAN ID 是否等于 PVID，都会保留原 Tag 不变发送数据帧
 - D. Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 端口
3. 缺省情况下，Hold 定时器的值为（ ）
 - A. 5 厘秒
 - B. 10 厘秒
 - C. 20 厘秒
 - D. 60 厘秒
4. 基于协议的 VLAN 对什么类型的端口配置有效？（ ）
 - A. Access 端口
 - B. Trunk 端口
 - C. Hybrid 端口
 - D. 以上端口都可以
5. VLAN 的划分包含下面哪些方式？（ ）
 - A. 基于端口划分
 - B. 基于协议划分

C. 基于 IP 地址划分

D. 基于 IP 子网划分

5.7.2 习题答案

1. ABCD

2. D

3. B

4. C

5. ABD

第6章 VLAN 扩展技术

VLAN 技术的成熟应用带来了很多的便利，但在实际使用过程中，VLAN 技术还有或多或少的应用场景无法适应。因此针对这些特殊应用，VLAN 也与时俱进，不断地扩展新技术来满足各种应用需求。

本章主要学习的 VLAN 新技术有 Super VLAN 和 Private VLAN。

6.1 本章目标

课程目标

● 学习完本课程，您应该能够：

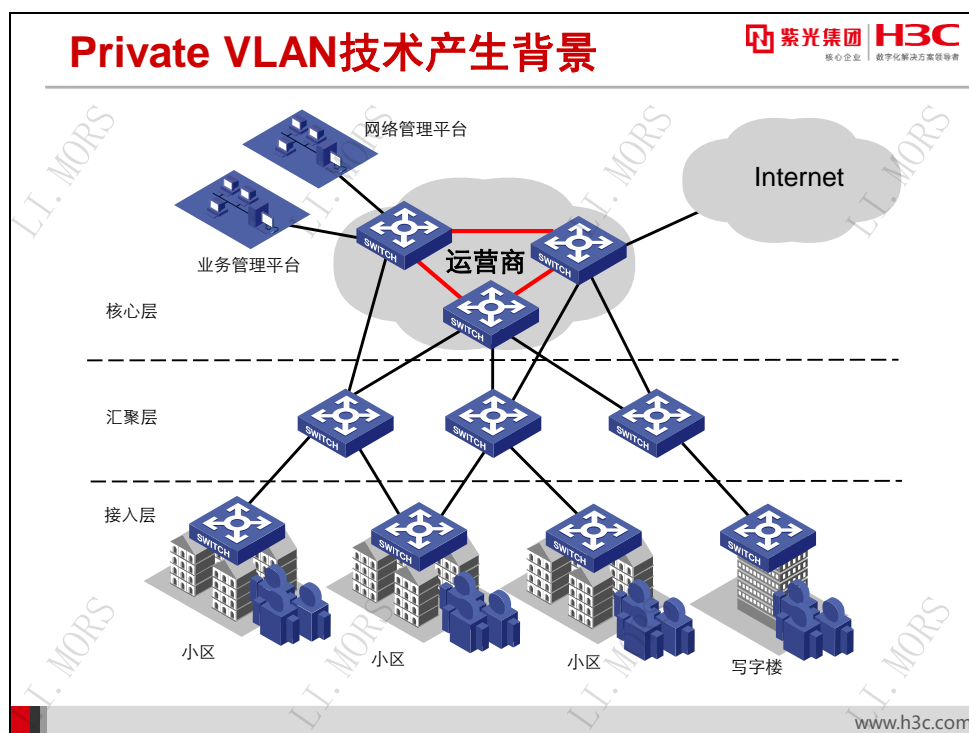
- 熟悉 Private VLAN 的基本原理和配置
- 熟悉 Super VLAN 的基本原理和配置



www.h3c.com

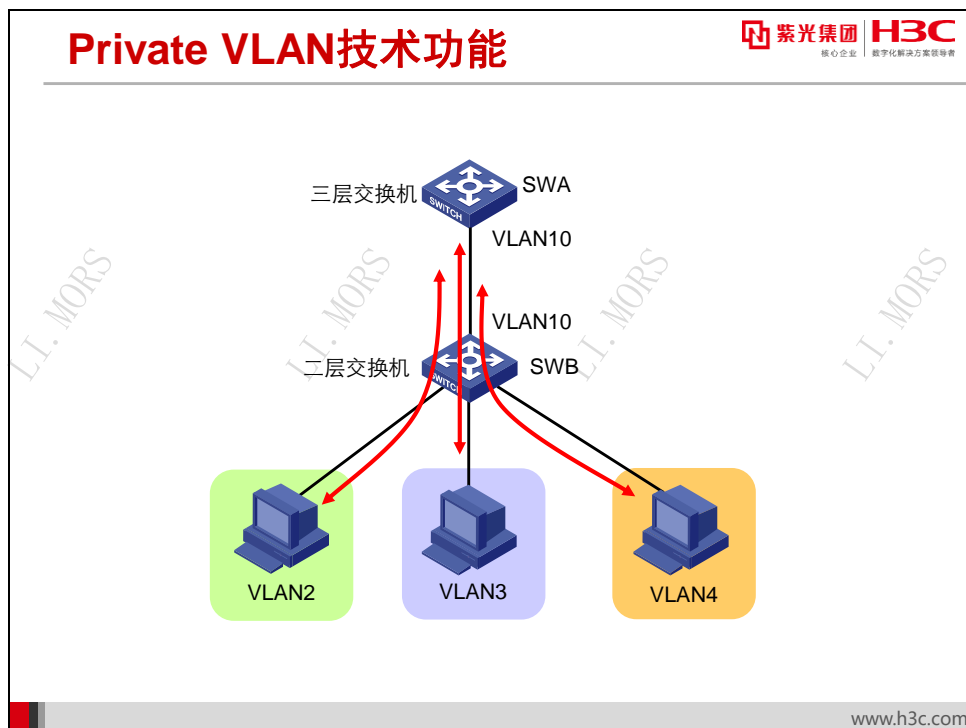
6.2 Private VLAN技术的原理和配置

6.2.1 Private VLAN 技术介绍



随着以太网技术的快速发展，很多运营商采用 LAN 接入小区宽带。基于用户安全和管理计费等方面考虑，运营商一般要求接入用户互相隔离。VLAN 是天然的隔离手段，于是很自然的一个想法是每个用户一个 VLAN。但是，根据 IEEE 802.1Q 协议规定，设备最大可使用的 VLAN 资源为 4094 个。对于运营商的设备来说，如果每个用户一个 VLAN，4094 个 VLAN 远远不够，而且，为每个只包含一个用户的 VLAN 配置第三层接口，将耗费大量的 IP 地址和部署成本。

采用 LAN 接入的小区宽带用户主要应用是上互联网，用户之间相互隔离。VLAN ID 主要消耗在接入层，对于运营商来说，如果即能够保证接入层用户之间相互隔离，又能将接入层的 VLAN ID 屏蔽掉，只可见汇聚层的 VLAN ID，则 4094 个 VLAN 是够用的。为了解决上述问题，Private VLAN 技术应用而生。



Private VLAN 采用二层 VLAN 结构，它在一台设备上设置 Primary VLAN 和 Secondary VLAN 两类 VLAN。功能如下：

- Primary VLAN 用于上行连接，不同的 Secondary VLAN 关联到同一个 Primary VLAN。上行连接的设备只知道 Primary VLAN，而不必关心 Secondary VLAN，简化了网络配置，节省了 VLAN 资源。
- Secondary VLAN 用于连接用户，Secondary VLAN 之间二层帧互相隔离。如果希望实现同一 Primary VLAN 下 Secondary VLAN 用户之间互通，可以通过配置上行设备的本地代理 ARP 功能来实现三层报文的互通。
- 一个 Primary VLAN 可以和多个 Secondary VLAN 相对应，理论上每个 Primary VLAN 可以包含 4094 个 Secondary VLAN，所以相当于提供了 4094×4094 个 VLAN。Primary VLAN 下面的 Secondary VLAN 对上行设备不可见。

如上图所示，SWB 上启动了 Primary VLAN 功能。其中 VLAN10 是 Primary VLAN；VLAN2、VLAN3、VLAN4 是 Secondary VLAN；VLAN2、VLAN3、VLAN4 都映射到 VLAN10；VLAN2、VLAN3、VLAN4 对 SWA 不可见。

Private VLAN技术基本原理

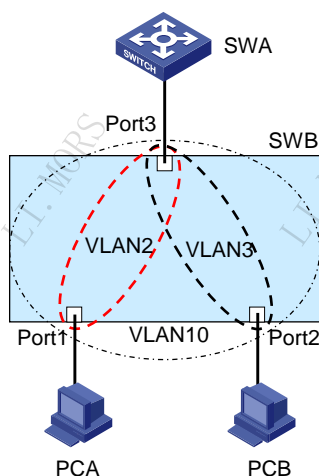
紫光集团 H3C
核心企业 数字化转型领导者

● Hybrid端口技术的应用

- 所有端口都为Hybrid
- 上行端口允许所有VLAN通过
- 下行端口允许Primary VLAN和自己的Secondary VLAN通过

● MAC地址同步技术

- 各Secondary VLAN学习的MAC地址同步到Primary VLAN
- Primary VLAN学习的MAC地址同步到各Secondary VLAN



www.h3c.com

Private VLAN 功能利用 Hybrid 类型端口的灵活性以及 VLAN 间的 MAC 地址同步技术实现。

Hybrid 端口在转发数据时，可以按照需要进行多个 VLAN 数据流量的发送和接收，可以根据需要决定发送数据帧时是否携带 802.1Q 标签。正因为这一灵活性，Hybrid 端口可以用于交换机之间连接，也可用于连接用户计算机。

交换机的端口和所属 VLAN 如上图 SWB 所示，三个端口都设定为 Hybrid 类型，Port1 允许 VLAN2、VLAN10 的数据帧通过，Port2 允许 VLAN3、VLAN10 的数据帧通过，Port3 允许 VLAN2、VLAN3、VLAN10 的数据帧通过，所有发出去的数据帧都不携带 802.1Q 标签。配置完成后，PCA 可以和 SWA 互通，PCB 可以和 SWA 互通，而 PCA 和 PCB 之间隔离。

如果仔细分析不难发现，交换机在转发时会存在一个较为严重的问题。按照需求，如上图所示的三个端口的 PVID 应该分别为 VLAN2、VLAN3 和 VLAN10。一开始 PCA 发送 ARP 请求到 Port1，解析 SWA（网关）的 MAC 地址，PCA 的 MAC 地址被学习到 SWB 的 VLAN2 中，SWB 没能匹配到 SWA 的 MAC 地址表项，只能在 VLAN2 的广播域内广播。

当 SWA 返回的 ARP 响应到达 SWB 的 Port3 时（源 MAC 为 MAC_SWA，目的 MAC 地址为 MAC_PCA），SWA 的 MAC 地址将被学习到 SWB 的 VLAN10 中，SWB 会给报文添加 Tag，VLAN ID 为 10（即端口的缺省 VLAN ID）；然后以“MAC_PCA+VLAN10”为条件去查询 MAC 地址表。由于找不到相应的表项，该报文会在 VLAN10 内广播，并最终从 Port1 和 Port2 发送出去。

同理，每次上行和下行的报文都需要广播才能到达目的地。当 Secondary VLAN 和 Primary VLAN 包含的端口较多时，这样的处理方式会占用大量的带宽资源，大大降低了交换机的转发性能，而且不安全（广播报文容易被截获和侦听）。通过 MAC 地址同步机制可以解决这个问题。

Primary VLAN 的 MAC 地址同步机制为：

- Secondary VLAN 到 Primary VLAN 的同步，即下行端口在 Secondary VLAN 内学习到的 MAC 地址都同步到 Primary VLAN 内，而出端口则保持不变。
- Primary VLAN 到 Secondary VLAN 的同步，即上行端口在 Primary VLAN 学习到的 MAC 地址同步到所有的 Secondary VLAN 内，而出端口则保持不变。


如下信息即是交换机 MAC 地址表同步后的结果：

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME
0000-0000-0001	10	Learned	Ethernet0/1	AGING
0000-0000-0001	2	Learned	Ethernet0/1	AGING
0000-0000-0002	10	Learned	Ethernet0/2	AGING
0000-0000-0002	3	Learned	Ethernet0/2	AGING
0000-0000-0005	10	Learned	Ethernet0/10	AGING
0000-0000-0005	2	Learned	Ethernet0/10	AGING
0000-0000-0005	3	Learned	Ethernet0/10	AGING

当 Primary VLAN 下面配置了很多 Secondary VLAN，MAC 地址同步后，将导致 MAC 地址表过于庞大，进而影响设备的转发性能。同时考虑到用户的下行流量要远远大于上行流量，下行流量需要进行单播，上行流量可以进行广播。所以，Secondary VLAN 到 Primary VLAN 的同步所有产品均支持，而 Primary VLAN 到 Secondary VLAN 的同步部分产品不支持。

6.2.2 Private VLAN 技术配置

Private VLAN 技术配置命令



- 设置VLAN的类型为Primary

```
[Switch-vlan10] private-vlan primary
```


- 建立Primary VLAN和Secondary VLAN间的映射关系

```
[Switch-vlan10] private-vlan secondary vlan-id-list
```

www.h3c.com

Private VLAN 配置主要包括如下五个步骤：

- 1) 配置 Primary VLAN。
- 2) 配置 Secondary VLAN。

3) 配置上行/下行端口。

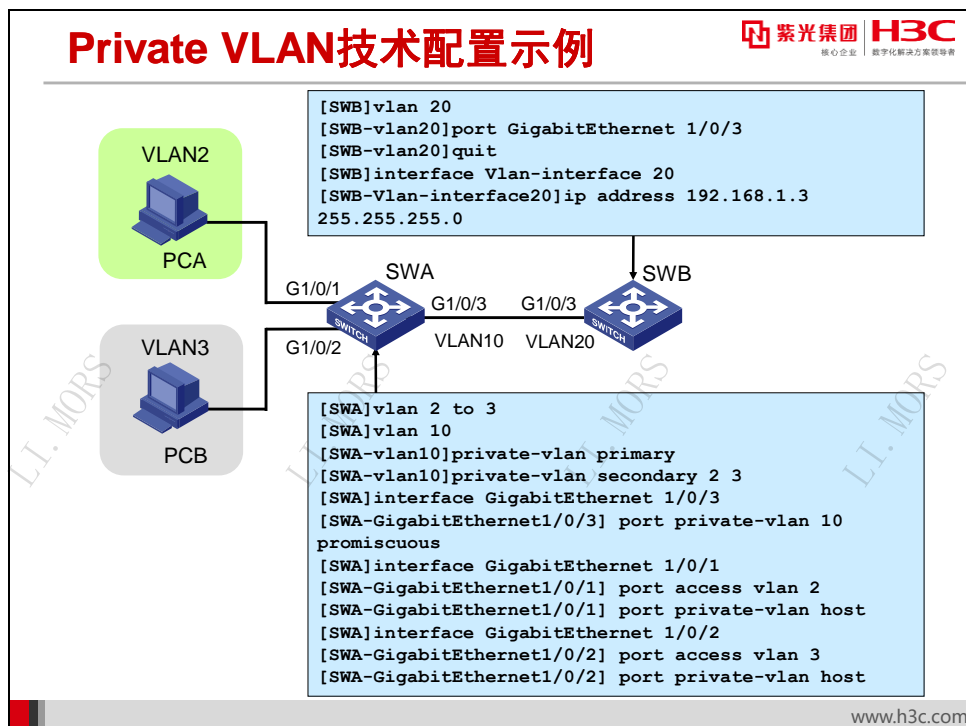
- 当上行端口只对应一个 Primary VLAN，配置该端口工作在 promiscuous 模式，可以实现上行端口加入 Primary VLAN 及同步加入对应的 Secondary VLAN 的功能；当上行端口对应多个 Primary VLAN，配置该端口工作在 trunk promiscuous 模式，可以实现上行端口加入多个 Primary VLAN 及同步加入对应的 Secondary VLAN 的功能。
- 当下行端口只对应一个 Secondary VLAN，配置该端口工作在 host 模式，可以实现下行端口同步加入 Secondary VLAN 对应的 Primary VLAN 的功能；当下行端口对应多个 Secondary VLAN，配置该端口工作在 trunk secondary 模式，可以实现下行端口加入多个 Secondary VLAN 及同步加入对应的 Primary VLAN 的功能。

4) 配置 Primary VLAN 和 Secondary VLAN 间的映射关系。

5) 配置 Primary VLAN 下指定 Secondary VLAN 间三层互通。

配置 Private VLAN 时，需要注意：

- 完成上述五部操作配置后，建议用户作如下配置：对于工作模式为 promiscuous 的端口，确保端口的缺省 VLAN 为 Primary VLAN，端口以 Untagged 方式加入 Primary VLAN 和 Secondary VLAN；对于工作模式为 host 的端口，确保缺省 VLAN 为 Secondary VLAN，端口以 Untagged 方式加入 Primary VLAN 和 Secondary VLAN；对于工作模式为 trunk promiscuous 和 trunk secondary 的端口，确保端口以 Tagged 方式加入 Primary VLAN 和 Secondary VLAN。
- 默认 VLAN（VLAN 1）不支持 Private VLAN 相关配置。



上图是 Private VLAN 技术的基本配置示例。图中 PCA 和 PCB 分别属于 SWA 上 VLAN2 和 VLAN3，是 Secondary VLAN，SWA 上的 VLAN10 为 Primary VLAN。

在 SWA 上创建 VLAN2、VLAN3 和 VLAN10，将 PCA 所连接的端口 GigabitEthernet1/0/1 添加到 VLAN2 中，将 PCB 所连接的端口 GigabitEthernet1/0/2 添加到 VLAN3 中，将 SWA 连接 SWB 的端口 GigabitEthernet1/0/3 添加到 VLAN10 中。设置 VLAN10 为 Primary VLAN，配置 Primary VLAN 和 Secondary VLAN 间的映射关系。

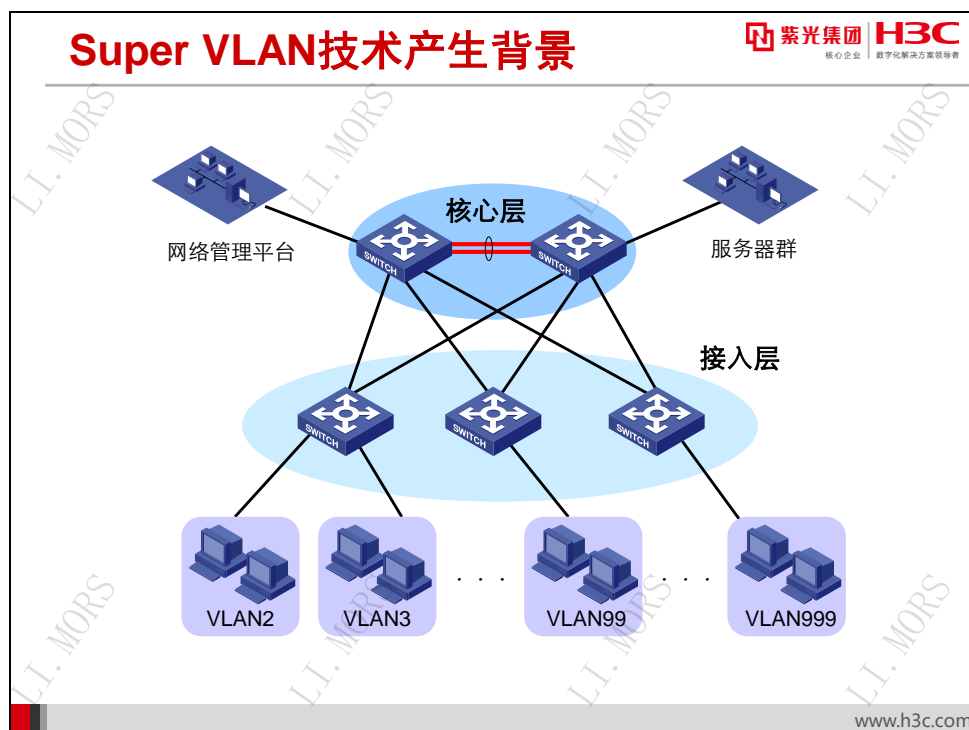
在 SWB 上创建 VLAN20，将连接 SWA 的端口 G1/0/3 添加到 VLAN20 中，给 VLAN20 接口配置 IP 地址 192.168.1.3/24。

SWA 和 SWB 的配置如图所示。

配置完成后，SWB 与 PCA 和 PCB 可以互通，但 PCA 和 PCB 之间不能互通。

6.3 Super VLAN技术的原理和配置

6.3.1 Super VLAN 技术介绍



Private VLAN 成功地解决了降低 VLAN 数量的问题，同时也在一定程度上实现了三层网关的共享。但它也存在 MAC 地址复制而消耗 MAC 地址表项的问题，并且该技术本身属于一个二层 VLAN 技术。

在交换局域网中，VLAN 技术以其对广播域的灵活控制（可跨物理设备）、部署方便而得到了广泛的应用。但是在一般的三层交换机中，通常是采用一个 VLAN 对应一个接口的方式来实现广播域之间的互通的，这在某些情况下导致了 IP 地址的较大浪费。

在某些大型的局域网里，采用接入层和核心层二级结构的组网方式，所有的网关都设在核心层设备上。因为每个 VLAN 都需要一个接口来实现路由的互通，而大部分交换机支持的 VLAN 数量远远多于 VLAN 接口数量。如果因为特殊的需要，网络里划分了成百上千个 VLAN，此时核心层设备会出现 VLAN 接口数量不够的情况。如果有一种技术，可以对 VLAN 进行聚合，从而大幅缩减实际需要的 VLAN 接口数量，则交换机支持的 VLAN 接口少的问题迎刃而解。

为了解决上述问题，Super VLAN 技术应运而生。

Super VLAN技术中的概念



核心企业 数字化解决方案领导者

- **Super VLAN**
 - 只建立三层接口而不包含物理端口
 - 若干Sub VLAN的集合，并为Sub VLAN提供三层转发服务
- **Sub VLAN**
 - 只映射若干物理端口，负责保留各自独立的广播域
 - 不能建立三层VLAN接口
 - 与外部的三层交换是靠Super VLAN的三层接口来实现的

www.h3c.com

Super VLAN 技术中引入了 Super VLAN 和 Sub VLAN 这两个概念。

Super VLAN 和通常意义上的 VLAN 不同，它只建立三层接口，而不包含物理端口。因此，可以把它看作一个逻辑的三层概念——若干 Sub VLAN 的集合。与一般没有物理端口的 VLAN 不同的是，它的接口的 UP 状态不依赖于其自身物理端口的 UP，而是只要它所含 Sub VLAN 中存在 UP 状态的物理端口。

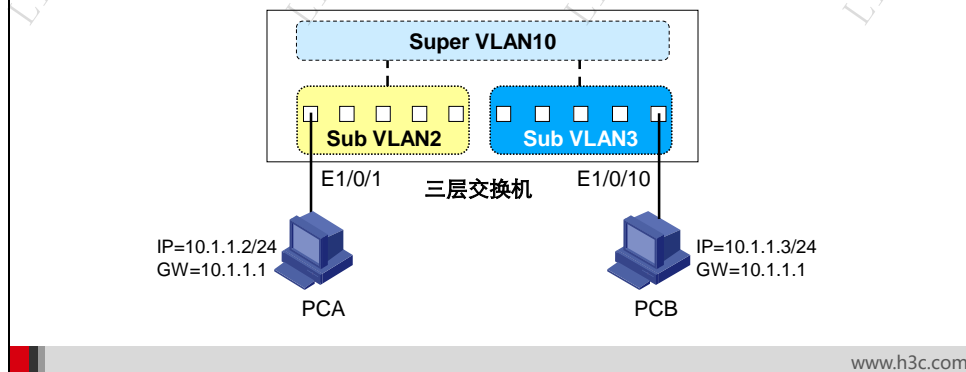
Sub VLAN 则只包含物理端口，但不能建立三层 VLAN 接口。它与外部的三层交换是靠 Super VLAN 的接口来实现的。

Super VLAN技术实现模型

紫光集团 H3C
核心企业 数字化转型方案领导者

● Super VLAN技术的实现

- Super VLAN与Sub VLAN形成映射
- 不同Sub VLAN主机在不同的广播域
- 各Sub VLAN借用Super VLAN的VLAN接口进行三层通信
- Sub VLAN间的通信依靠Super VLAN接口的本地代理ARP完成

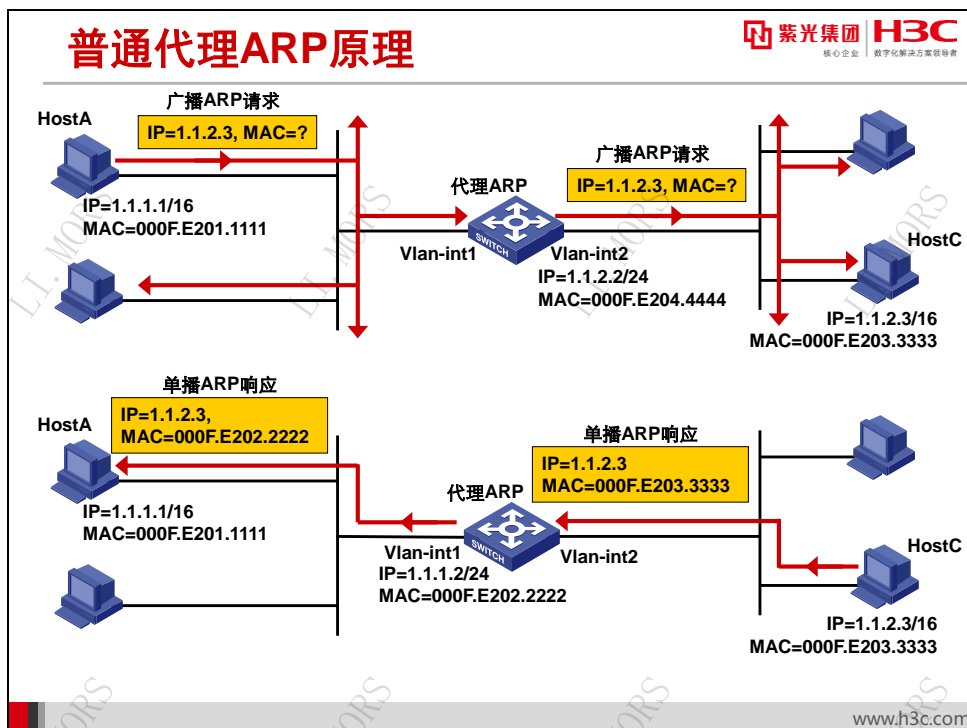


每一个普通 VLAN 都有一个三层逻辑接口和若干物理端口，而 Super VLAN 把这两部分剥离开来。Sub VLAN 只映射若干物理端口，负责保留各自独立的广播域；而用一个 Super VLAN 来实现所有 Sub VLAN 共享同一个接口的需求，使不同 Sub VLAN 内的主机可以共用同一个 Super VLAN 的网关，在 Super VLAN 对应的子网里分配地址；然后再通过建立 Super VLAN 和 Sub VLAN 间的映射关系，把三层逻辑接口和物理端口这两部分有机的结合起来。

这样做既减少了一部分子网号、子网缺省网关地址和子网定向广播地址的消耗，又实现了不同广播域使用同一子网网段地址，消除了子网差异，增加了编址的灵活性，减少了闲置地址浪费。并用本地代理 ARP 来实现 Sub VLAN 间的三层互访，从而在实现普通 VLAN 功能的同时，达到了节省交换机 VLAN 接口的目的。

Super VLAN 的实现模型如上图所示，交换机创建了 Sub VLAN2 和 Sub VLAN3，分别属于不同的广播域，因此有效的隔离了它们之间的广播流量，但是这些 Sub VLAN 都没有自己的 VLAN 接口。而另一个特殊的 VLAN——Super VLAN 则属于另一个独立的广播域，该广播域与前面的 Sub VLAN2 和 Sub VLAN3 建立了映射关系，也可以理解为 Super VLAN10 包含了 Sub VLAN2 和 Sub VLAN3。但是它却没有包含任何端口，仅仅拥有一个 VLAN 接口，并用该接口为所有映射的 Sub VLAN 提供三层通信服务。

6.3.2 代理 ARP



如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP(Proxy ARP)。代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- **普通代理 ARP：**想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- **本地代理 ARP：**想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

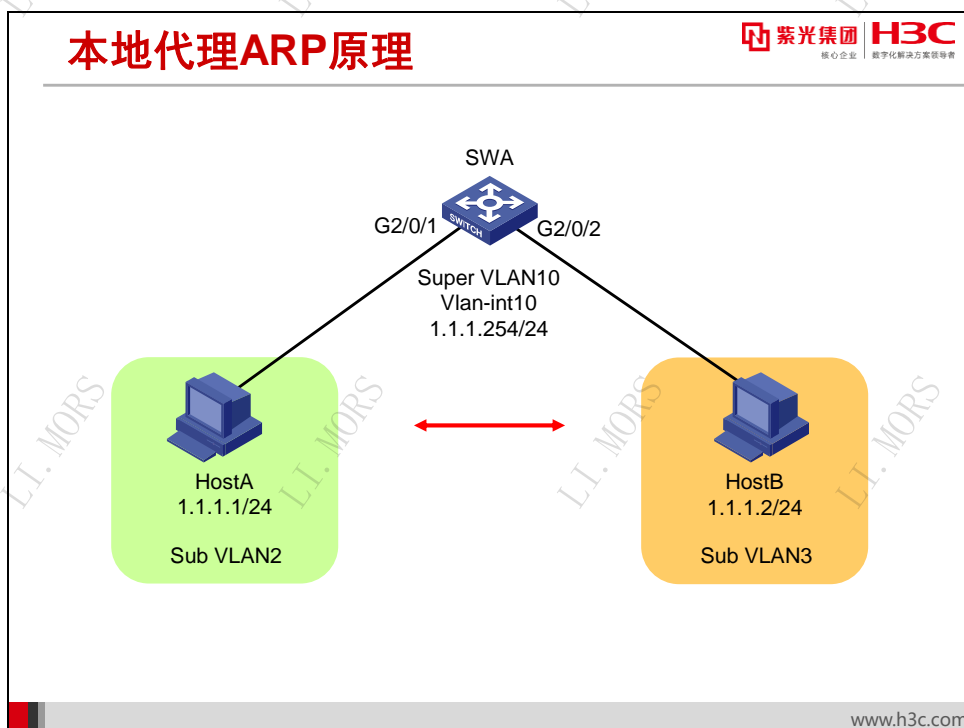
处于同一网段内的主机，当连接到设备的不同三层接口时，可以利用设备的普通代理 ARP 功能，通过三层转发实现互通。

普通代理 ARP 的典型应用环境如上图所示，交换机通过两个 VLAN 接口 Vlan-interface1 和 Vlan-interface2 连接两个网络，两个 VLAN 接口的 IP 地址不在同一个网段，接口地址分别为 1.1.1.2/24、1.1.2.2/24。但是两个网络内的主机 HostA 和 HostC 的地址通过掩码的控制，既与相连设备的接口地址在同一网段，同时二者也处于同一个网段。

在这种组网情况下，当 HostA 需要与 HostC 通信时，由于目的 IP 地址与本机的 IP 地址为同一网段，HostA 直接发送 ARP 请求，解析 HostC 的 MAC 地址。运行了代理 ARP 的交换机收到 ARP 请求后，代理 HostA 在 1.1.2.0 网段发出 ARP 请求，解析 HostC 的 MAC 地址。

HostC 认为交换机向其发出了 ARP 请求，遂回应以 ARP 相应，通告自己的 MAC 地址 000F.E203.3333。交换机收到 ARP 响应后，也向 HostA 发送 ARP 响应，但通告的 MAC 地址是其连接到 1.1.1.0 网络的 VLAN1 接口的 MAC 地址 000F.E202.2222。这样在 HostA 的 ARP 表中会形成 IP 地址 1.1.2.3 与 MAC 地址 000F.E202.2222 的映射项，因此 HostA 实际上会将所有要发给 HostC 的数据包发送到交换机上，再由交换机转发给 HostC。

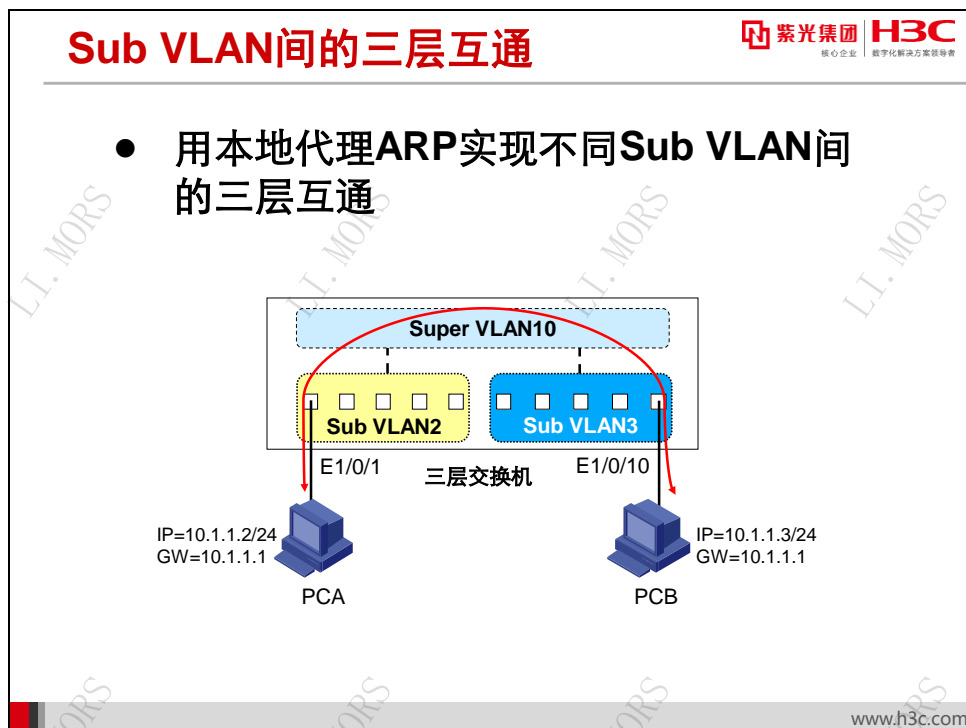
普通代理 ARP 的优点是，它可以只被应用在一个设备上(此时该设备的作用相当于网关)，不会影响到网络中其他设备的路由表。普通代理 ARP 功能可以在 IP 主机没有配置缺省网关或者 IP 主机没有任何路由能力的情况下使用。



为了实现三层互通，在下面三种情况之一需要开启本地代理 ARP 功能：

- 连接到同一个 VLAN 不同二层隔离的端口下的设备要实现三层互通；
- 开启 Super VLAN 功能后，属于不同 Sub VLAN 下的设备要实现三层互通；
- 开启 Private VLAN 功能后，属于不同 Secondary VLAN 下的设备要实现三层互通。

6.3.3 Sub VLAN 的通信



如图所示，假设 PCA 需要发送报文给 PCB，PCA 发现目的 IP 地址和自己在同一网段，所以发送 ARP 请求，而 PCB 在 VLAN3 广播域内，并不能收到这个广播请求，所以，PCA 是不能及时收到 PCB 的 ARP 应答的，但是，Super VLAN10 是可以收到这个 ARP 广播的。

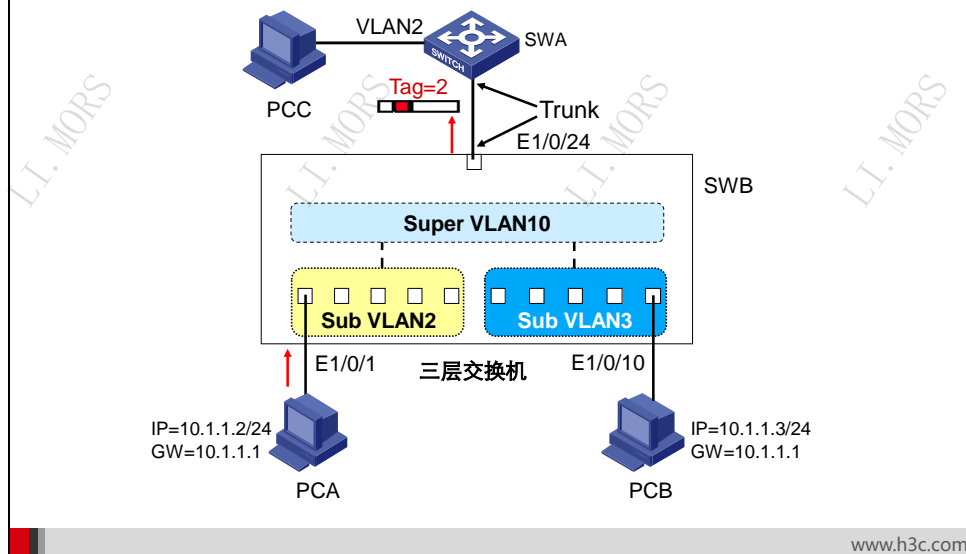
Super VLAN10 的本地代理 ARP 所做的就是：当 PCA 在二层发出的 ARP 请求在其广播域内没有回应时，网关开始在路由表查找，发现下一跳为直连路由接口，则在 Sub VLAN3 内发送新的 ARP 请求 PCB 的 MAC 地址；得到 PCB 的回应后，Super VLAN10 就把自己接口对应的 MAC 地址当作 PCB 的 MAC 地址，在 Sub VLAN2 内给予 PCA 响应。之后，PCA 发送普通 IP 报文给 PCB 时，都通过 Super VLAN 接口进行正常的三层报文转发。

PCB 回送给 PCA 的报文转发过程和上述的 PCA 到 PCB 的流程类似。

Sub VLAN与外部的二层通信

紫光集团 H3C
核心企业 数字化转型方案领导者

● Trunk链路自动禁止Super VLAN通过



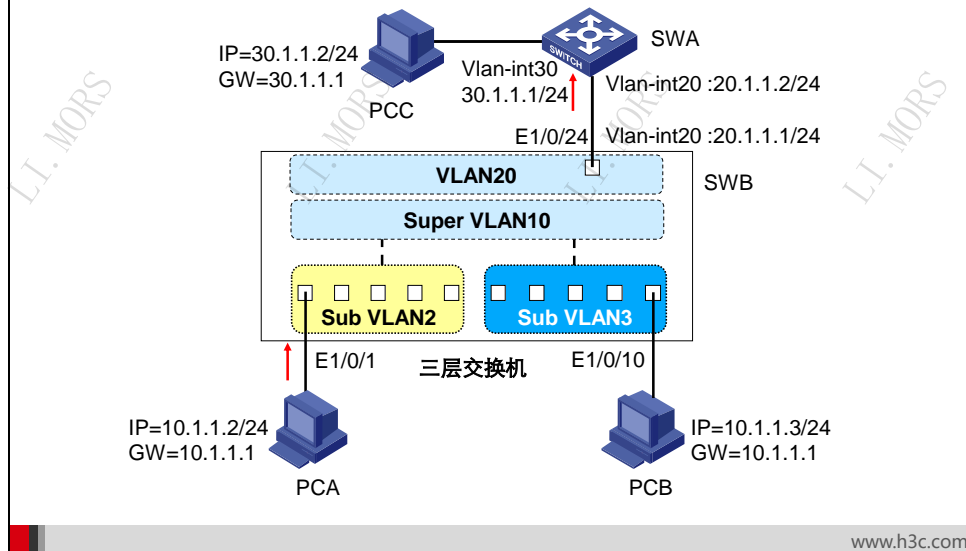
Super VLAN 是个特殊的 VLAN，它并不包含物理端口，不连接任何主机和设备，所以 VLAN10 内根本不可能有携带 VLAN10 标签的数据帧发送到其他交换机，反之如果接收到来自于 Trunk 链路上 VLAN10 的数据帧，交换机也无法转发。所以在开启 Super VLAN 的交换机上，Trunk 链路将自动禁止 Super VLAN 的 VLAN 流量通过，从而避免不必要的处理。

如图所示，在 SWA 上 PCC 属于 VLAN2，PCA 访问 PCC 时，从 SWB 的 E1/0/1 进入的数据帧会打上 VLAN 2 的标签，在 SWB 中这个标签不会变为 VLAN10 的标签。SWB 把此数据帧从 Trunk 端口 E1/0/24 转发出去时，依然是 VLAN 2 的数据帧。对于 SWA 而言，SWB 上有效的 VLAN 只有 VLAN 2 和 VLAN 3，从 PCC 返回的到 SWB 的数据帧可以在 VLAN2 中转发。

Sub VLAN与外部的三层通信

紫光集团 H3C
核心企业 数字化转型方案领导者

● 等同于Super VLAN到外部的三层通信



SWA 和 SWB 上 VLAN 划分和各 PC 的 IP 地址如上图所示，假设 PCA 需要和 PCC 互相通信，下面简述一下上下行报文的转发流程。

PCA 需要发送 IP 报文到 PCC，PCA 检查发现 PCC 与自己属于不同的 IP 网段，所以需要将报文发送给自己的网关 Super VLAN10。因此 PCA 检查自己的网关 IP 地址和 MAC 地址信息，发现只有 IP 地址信息而无 MAC 地址信息，所以发送 ARP 报文请求网关的 MAC 地址。该报文在 Sub VLAN2 内发送并被 SWB 接收，SWB 并没有对应的 VLAN2 接口，但是它发现 Sub VLAN2 被映射到了 Super VLAN10，Super VLAN10 是可以提供三层服务的，所以交换机给予 ARP 响应并在 Sub VLAN2 内发送。

自此 PCA 成功学习到了网关的 MAC 地址，接下来，PCA 发送目的 MAC 为 Super VLAN10、目的 IP 为 30.1.1.2 的报文。Sub VLAN2 接收到报文后，检测到目的 MAC，知道应该进行三层转发，于是查找路由表，发现下一跳地址为 20.1.1.2，出接口为 VLAN20，并通过 ARP 表项和 MAC 表项确定出端口，把报文发送给 SWA，SWA 根据正常的转发流程把报文发送给 PCC。

PCC 返回给 PCA 的报文到达 SWB 时，正常 IP 转发检查发现出接口为 Super VLAN10 的三层接口，但是在 Super VLAN10 内没有包含任何物理端口。开启了 Super VLAN 的交换机始终注意到，如果存在 Super VLAN，那么需要从 Super VLAN 转发出去的报文都应该寻找其对应的 Sub VLAN，并在 Sub VLAN 内按照 ARP 和 MAC 表项进行正常转发。所有此处，SWB 在 Sub VLAN2 内发现了之前已经学习到的 PCA 的 ARP 和 MAC 信息，最终报文转发给 PCA，完成双向通信。

Sub VLAN 与外部的三层通信等同于 Super VLAN 到外部的三层通信。

6.3.4 Super VLAN 技术配置

Super VLAN技术配置命令

 紫光集团

 H3C

核心企业 | 数字化转型方案领导者

- 设置当前VLAN的类型为Super VLAN
`[Switch-vlan10] supervlan`
- 建立Super VLAN和Sub VLAN的映射关系
`[Switch-vlan10] subvlan vlan-list`
- 开启本地代理ARP功能
`[Switch-Vlan-interface10] local-proxy-arp enable`

www.h3c.com

Super VLAN 的配置可以按照如下五个步骤来完成：

- 1) 配置 Sub VLAN；
- 2) 配置 Super VLAN；
- 3) 配置 Super VLAN 和 Sub VLAN 的映射；
- 4) 配置 Super VLAN 接口的 IP 地址；
- 5) 开启本地代理 ARP 功能。

缺省情况下，用户创建的 VLAN 不是 Super VLAN 类型的 VLAN。在 VLAN 视图下，设置当前 VLAN 的类型为 Super VLAN，配置命令为：

supervlan

缺省情况下，用户创建的 Super VLAN 和 Sub VLAN 没有任何映射关系，还需要在 VLAN 视图下建立 Super VLAN 和 Sub VLAN 的映射关系。配置命令为：

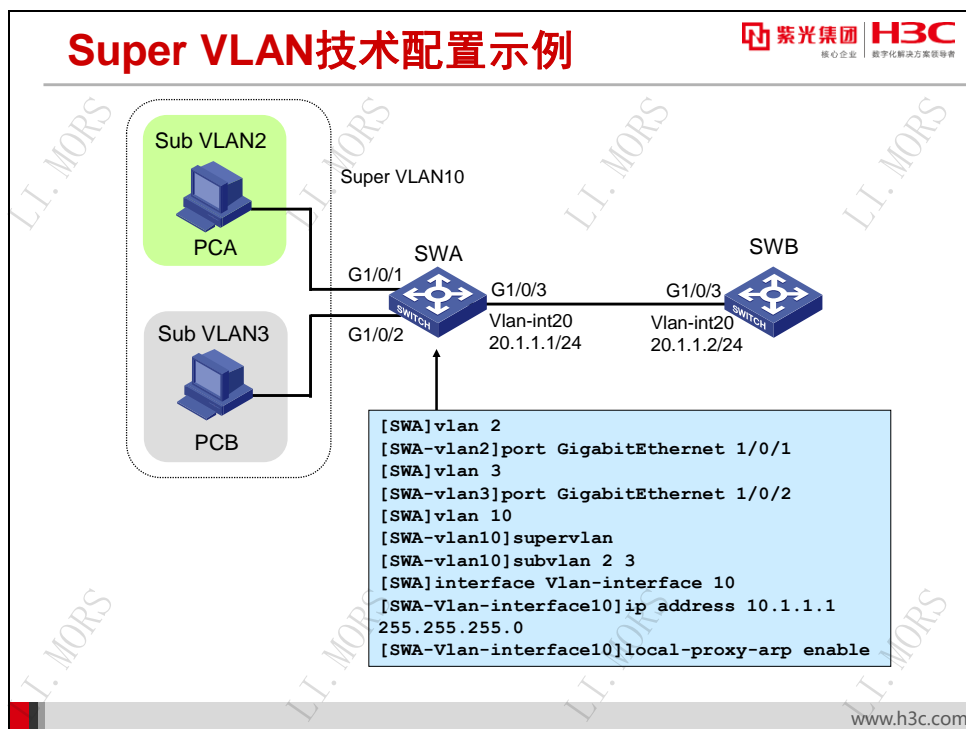
subvlan *vlan-list*

缺省情况下，本地代理 ARP 功能关闭，为了让 Sub VLAN 之间互通，需要在 VLAN 接口视图下开启本地代理 ARP 功能。配置命令为：

local-proxy-arp enable

注意：

- 配置 Super VLAN 中包含的 Sub VLAN 前，Sub VLAN 必须已经创建。
- 在建立了 Sub VLAN 和 Super VLAN 的映射关系后，仍可以向 Sub VLAN 中添加和删除接口。



上图是 Super VLAN 技术的基本配置示例。图中 PCA 和 PCB 分别属于 SWA 上 VLAN2 和 VLAN3，是 Sub VLAN，SWA 上的 VLAN10 为 Super VLAN。

在 SWA 上创建 VLAN2、VLAN3、VLAN10 和 VLAN20，将 PCA 所连接的端口 GigabitEthernet1/0/1 添加到 VLAN2 中，将 PCB 所连接的端口 GigabitEthernet1/0/2 添加到 VLAN3 中，将 SWA 连接 SWB 的端口 GigabitEthernet1/0/3 添加到 VLAN20 中。设置 VLAN10 为 Super VLAN，配置 Super VLAN 和 Sub VLAN 间的映射关系。给 VLAN10 接口配置 IP 地址 10.1.1.1/24，给 VLAN20 接口配置 IP 地址 20.1.1.1/24。

在 SWB 上创建 VLAN20，将连接 SWA 的端口 G1/0/3 添加到 VLAN20 中，给 VLAN20 接口配置 IP 地址 20.1.1.2/24。

配置 SWA:

```

[SWA]vlan 2
[SWA-vlan2]port GigabitEthernet 1/0/1
[SWA-vlan2]quit
[SWA]vlan 3
[SWA-vlan3]port GigabitEthernet 1/0/2
[SWA-vlan3]quit
[SWA]vlan 10
[SWA-vlan10]supervlan
[SWA-vlan10]subvlan 2 3
[SWA-vlan10]quit
[SWA]interface Vlan-interface 10
  
```

```
[SWA-Vlan-interface10]ip address 10.1.1.1 255.255.255.0
[SWA-Vlan-interface10]local-proxy-arp enable
[SWA-Vlan-interface10]quit
[SWA]vlan 20
[SWA-vlan20]port GigabitEthernet 1/0/3
[SWA-vlan20]quit
[SWA]interface Vlan-interface 20
[SWA-Vlan-interface20]ip address 20.1.1.1 255.255.255.0
```

配置 SWB:

```
[SWB]vlan 20
[SWB-vlan20]port GigabitEthernet 0/0/3
[SWB-vlan20]quit
[SWB]interface Vlan-interface 20
[SWB-Vlan-interface20]ip address 20.1.1.2 255.255.255.0
[SWB-Vlan-interface20]quit
[SWB]ip route-static 0.0.0.0 0.0.0.0 20.1.1.1
```

配置完成后，在 SWA 上用命令查看 Super VLAN 和 Sub VLAN 之间的映射关系，如下所示：

```
[SWA]display supervlan
SuperVLAN ID : 10
SubVLAN ID : 2-3

VLAN ID: 10
VLAN Type: static
It is a Super VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0010
Name: VLAN 0010
Tagged Ports: none
Untagged Ports: none

VLAN ID: 2
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports: none
Untagged Ports:
    GigabitEthernet1/0/1

VLAN ID: 3
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports: none
Untagged Ports:
    GigabitEthernet1/0/2
```

从以上信息可知，VLAN10 是 Super VLAN，不包含任何端口；VLAN2 和 VLAN3 是 Sub VLAN，VLAN2 包含物理端口 GigabitEthernet1/0/1，VLAN3 包含物理端口 GigabitEthernet1/0/2；VLAN2 和 VLAN3 都以 VLAN10 接口的 IP 地址 10.1.1.1/24 为路由接口。

因为在 VLAN10 接口视图下开启了本地代理 ARP 功能,所以 PCA 与 PCB 是可以互通的,给 PCA 配置 IP 地址 10.1.1.2/24, 给 PCB 配置 IP 地址 10.1.1.3/24, 网关都配置为 10.1.1.1, 在 PCA 上用 Ping 命令测试与 PCB 互通, 如下所示:

```
C:\Documents and Settings\Administrator>ping 10.1.1.3
```

```
Pinging 10.1.1.3 with 32 bytes of data:
```

```
Reply from 10.1.1.3: bytes=32 time=3ms TTL=127
```

```
Reply from 10.1.1.3: bytes=32 time<1ms TTL=127
```

```
Reply from 10.1.1.3: bytes=32 time<1ms TTL=127
```

```
Reply from 10.1.1.3: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.1.1.3:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

此时, 在 PCA 用 Tracert 命令来查看从 PCA 传到 PCB (IP 地址为 10.1.1.3) 所经过的路径, 如下所示:

```
C:\Documents and Settings\Administrator>tracert 10.1.1.3
```

```
Tracing route to 10.1.1.3 over a maximum of 30 hops:
```

```
  1      1 ms      1 ms      1 ms  10.1.1.1
```

```
  2     <1 ms     <1 ms     <1 ms  10.1.1.3
```

```
Trace complete.
```

从 Tracert 命令的输出信息可知, 虽然 PCA 和 PCB 在同一网段, 但 PCA 访问 PCB 时, 需要经过两跳, 第一跳为 VLAN10 接口 IP 地址, 说明 PCA 和 PCB 三层互通需要 VLAN10 接口做三层转发。

因为 SWB 上配置了缺省路由, PCA 与 SWB 是可以互通的, 在 PCA 上用 Ping 命令测试与 SWB 互通, 如下所示:

```
C:\Documents and Settings\Administrator>ping 20.1.1.2
```

```
Pinging 20.1.1.2 with 32 bytes of data:
```

```
Reply from 20.1.1.2: bytes=32 time=2ms TTL=254
```

```
Reply from 20.1.1.2: bytes=32 time=1ms TTL=254
```

```
Reply from 20.1.1.2: bytes=32 time=1ms TTL=254
```

```
Reply from 20.1.1.2: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 20.1.1.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

6.4 本章总结

本章总结

- **Private VLAN**利用Hybrid端口转发特性和MAC地址同步原理，在节省VLAN资源的基础上实现用户的二层隔离
- **Super VLAN**对VLAN进行聚合，从而大幅缩减三层VLAN接口数量，并利用本地代理ARP技术实现Sub VLAN间三层互通

6.5 习题和解答

6.5.1 习题

1. 下面关于 Private VLAN 技术原理表述正确的是（ ）
 - A. Private VLAN 技术是利用 Hybrid 类型端口的灵活性以及 VLAN 间的 MAC 地址同步技术来实现的
 - B. Secondary VLAN 之间二层帧互相隔离，没法互通
 - C. Secondary VLAN 之间三层报文互相隔离，没法互通
 - D. MAC 地址同步技术仅指当 MAC 地址学习到 Secondary VLAN 时，还需要将该 MAC 地址复制到 Primary VLAN 中，而出端口则保持不变
2. 本地代理 ARP 可以应用在下面哪些情况？（ ）
 - A. 属于同一 VLAN 但做了端口隔离的两台 PC 要实现三层互通
 - B. 处于同一网段的主机，当连接到设备的不同三层接口时，要通过三层转发实现互通
 - C. 开启 Super VLAN 功能后，属于不同 Sub VLAN 下的设备要实现三层互通
 - D. 开启 Private VLAN 功能后，属于不同 Secondary VLAN 下的设备要实现三层互通
3. 在 Super VLAN 技术中，Super VLAN 和 Sub VLAN 的关系是（ ）
 - A. Super VLAN 只建立三层接口，而不包含物理端口
 - B. Super VLAN 是若干 Sub VLAN 的集合，并为 Sub VLAN 提供三层转发服务
 - C. Sub VLAN 只包含物理端口，但不能建立三层 VLAN 接口
 - D. Sub VLAN 与外部的三层交换是靠 Super VLAN 的接口来实现的
 - E. Super VLAN 的接口的 UP 状态不依赖于其自身物理端口的 UP，而是只要它所含 Sub VLAN 中存在 UP 状态的物理端口

6.5.2 习题答案

1. AB
2. ACD
3. ABCDE

第7章 VLAN 路由

用 VLAN 分段，隔离了 VLAN 间的通信，用支持 VLAN 的路由器（三层设备）可以建立 VLAN 间通信的，但使用路由器来互联企业园区网中不同的 VLAN 是不能满足企业内部各部门之间较大业务数据流量通信需求的，因为可以使用三层交换来实现。

传统路由器的路由转发采用 CPU 进行逐包逐跳转发，交换机的三层转发采用专用芯片进行快速转发，效率大大超过路由器，本章将学习交换机的精确匹配和最长匹配转发原理，以及三层转发流程。

熟悉了交换机的三层转发原理，还需进一步掌握交换机 VLAN 路由的配置命令，才能够真正实现网络需求，组建基本的局域网。

交换机常用的 VLAN 路由的配置包括静态路由协议和 RIP、OSPF 等动态路由协议，这些路由协议的配置和路由器一样。

7.1 本章目标

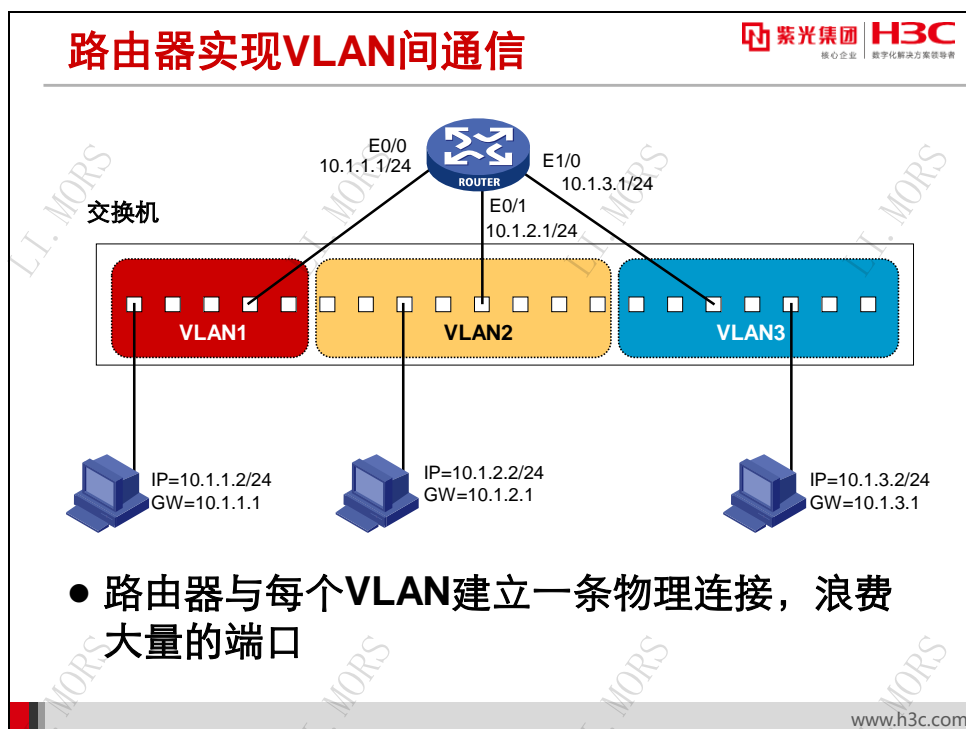
课程目标

● 学习完本课程，您应该能够：

- 了解交换机的精确匹配转发原理
- 掌握交换机的最长匹配转发原理
- 掌握三层交换机的转发处理流程
- 掌握三层交换机的路由配置，组建基本的局域网

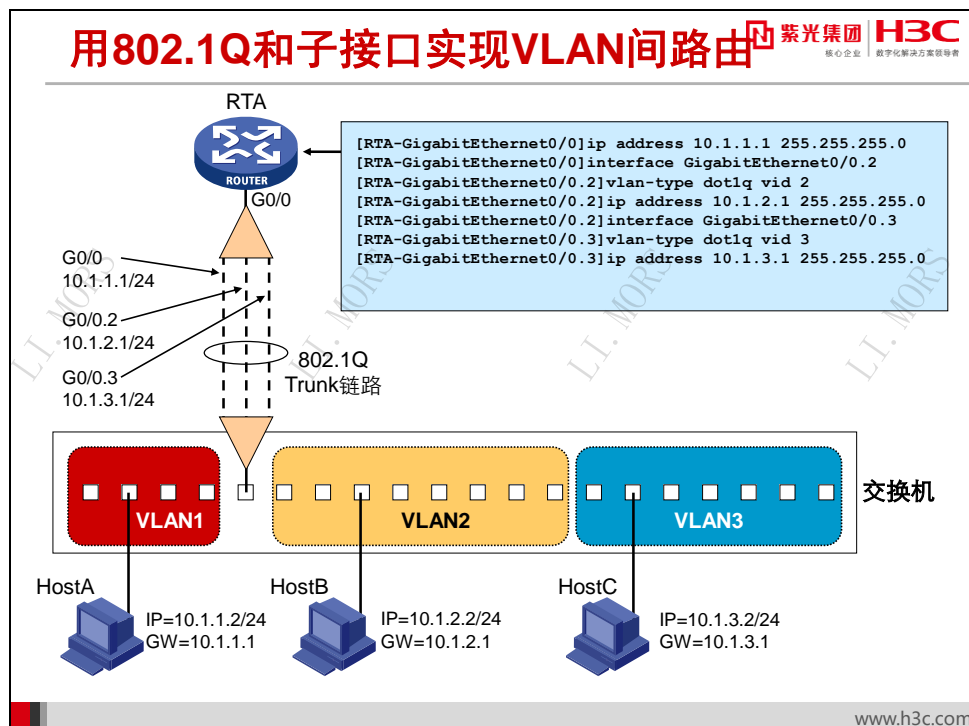


7.2 VLAN路由的实现



引入 VLAN 之后，每个交换机被划分成多个 VLAN，而每个 VLAN 对应一个 IP 网段。为了在 VLAN 之间进行路由，路由器到各个 VLAN 就必须各有一个物理接口和一条物理连接。

如图所示，路由器要为三个 VLAN 提供 VLAN 间路由，就必须用三个以太网口分别连接到交换机的三个 VLAN 的三个物理接口上。显然，在 VLAN 数量较大时，这种方式要求占用路由器和交换机的大量物理接口，并需要大量的物理连线，因而是难以接受的。



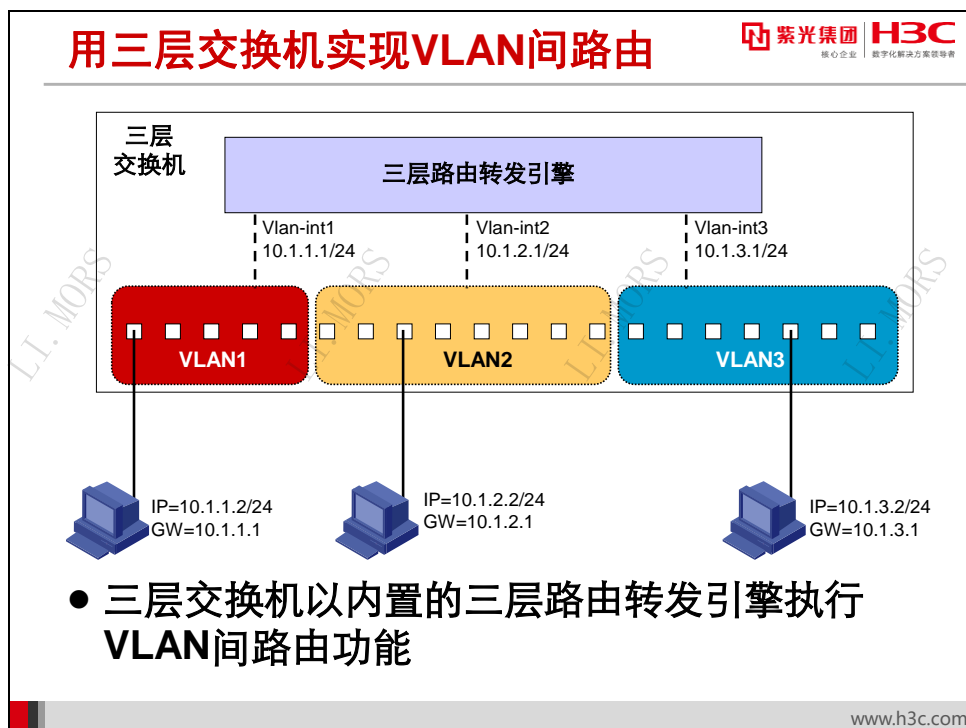
为了避免物理端口和线缆的浪费，简化连接方式，可以使用 802.1Q 封装和子接口，通过一条物理链路实现 VLAN 间路由。这种方式也被形象地称为“单臂路由”。

如上图所示，交换机通过 802.1Q 封装的 Trunk 链路连接到路由器的千兆以太网口 G0/0 上。每一个 VLAN 的数据都可以通过 802.1Q 标记识别出来。在路由器上则为 G0/0 配置了子接口，每个子接口配置了属于相应 VLAN 网段的 IP 地址，并且配置了相应 VLAN 的 802.1Q 标记值。

当 HostB 向 HostA 发送 IP 包时，该 IP 包首先被封装成以太网帧，通过 Trunk 链路发送给路由器，在 Trunk 链路上其 802.1Q VLAN ID 为 2。路由器收到此帧后，根据 VLAN ID 将其交给子接口 G0/0.2 处理。

路由器查找路由表，发现 HostA 处于接口 G0/0 所在网段，因而将此数据包封装成帧从接口 G0/0 发出，发送时不加 802.1Q 标记。由于交换机缺省 PVID 值为 1，此帧到达交换机后，交换机认为此帧为 VLAN1 数据，即可将其转发给 HostA。

这种 VLAN 间路由方式节省了物理端口和线缆的浪费，但应注意 Trunk 链路需承载所有 VLAN 间路由数据，因此通常应选择带宽较高的链路。



二层交换机和路由器在功能上的集成产生了三层交换机，三层交换机在功能上实现了 VLAN 的划分、VLAN 内部的二层交换和 VLAN 间路由的功能。在三层交换机中分别体现为二层 VLAN 转发引擎和三层转发引擎两个部分，二层 VLAN 转发引擎与支持 VLAN 的二层交换机的二层转发引擎是相同的，是用硬件支持 VLAN 内的快速二层转发；三层转发引擎使用硬件 ASIC 技术实现跨网段的三层路由转发。

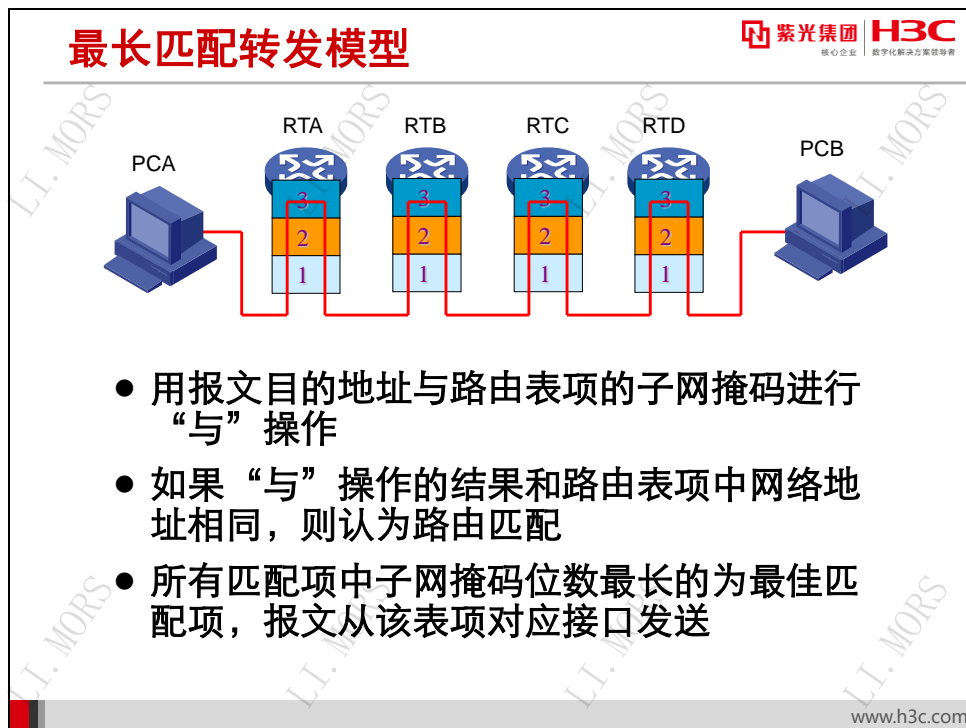
采用“单臂路由”方式进行 VLAN 间路由时，数据在 Trunk 链路上往返发送引入了一定的延迟，VLAN 间路由的大量数据对软件实现的路由器也会造成较大压力。解决的方法是使用三层交换机。

在使用二层交换机和路由器的组网中，每个需要与其它 IP 网段（VLAN）通信的 IP 网段（VLAN）都需要使用一个路由器接口做网关。三层交换机的应用也同样符合 IP 的组网模型，三层转发引擎就相当于传统组网中的路由器的功能，当需要与其他 VLAN 通信的时候，三层交换机为每个 VLAN 创建一个虚拟的三层 VLAN 接口，用来做 VLAN 的网关，这个接口像路由器接口一样工作。只需为 VLAN 接口配置相应的 IP 地址，即可实现 VLAN 间路由功能。

三层交换机通过内置的三层路由转发引擎在 VLAN 间进行路由转发。由于硬件实现的三层路由转发引擎速度快，吞吐量大，而且避免了外部物理连接带来的延迟和不稳定性，因此三层交换机的路由转发性能高于路由器实现的 VLAN 间路由。

7.3 交换机转发机制

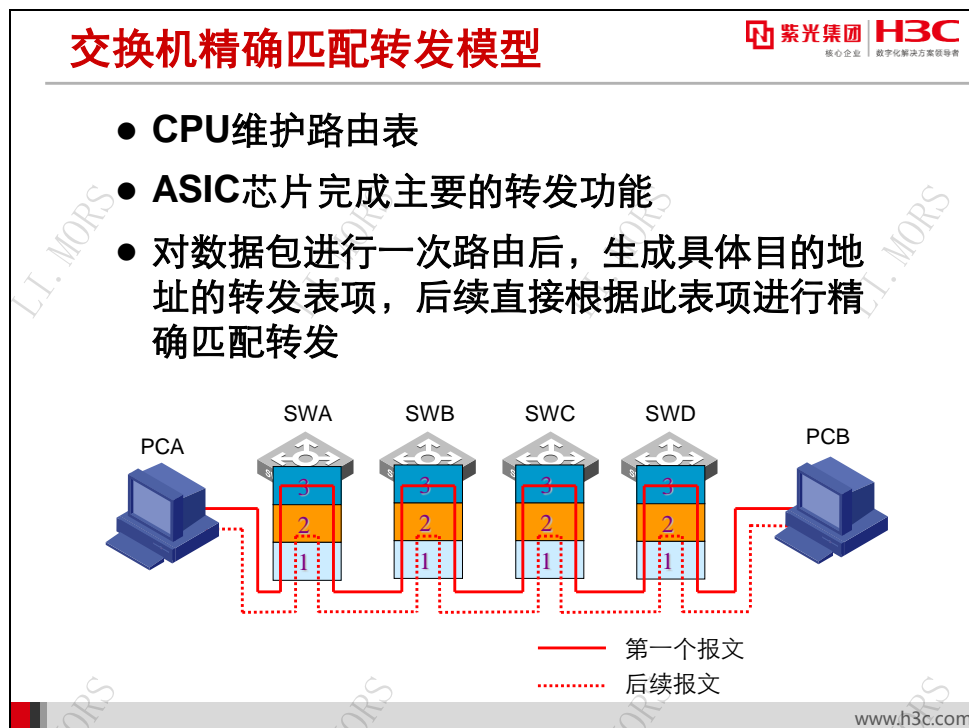
7.3.1 最长匹配转发模型



路由器的路由转发是根据报文的目的地址，与路由表进行匹配操作。匹配的动作是用报文目的地址与路由表项的子网掩码进行“与”操作，如果“与”操作的结果和路由表项中网络地址相同，则认为路由匹配。所有匹配项中子网掩码位数最长的为最佳匹配项，报文从该表项对应接口发送；如果找不到匹配项，则根据缺省路由 0.0.0.0/0 进行转发；如果没有缺省路由则报文被丢弃。

上述这种路由选路过程称之为 LPM（Longest-Prefix Match，最长匹配）。路由表是根据直连、静态配置和动态路由协议生成的。路由器的路由转发主要依靠 CPU 进行，对每个数据包都需要通过 CPU 系统进行路由查找、封装，最后转发，整体处理效率比较低。如上图中的第一个图。

7.3.2 交换机精确匹配转发



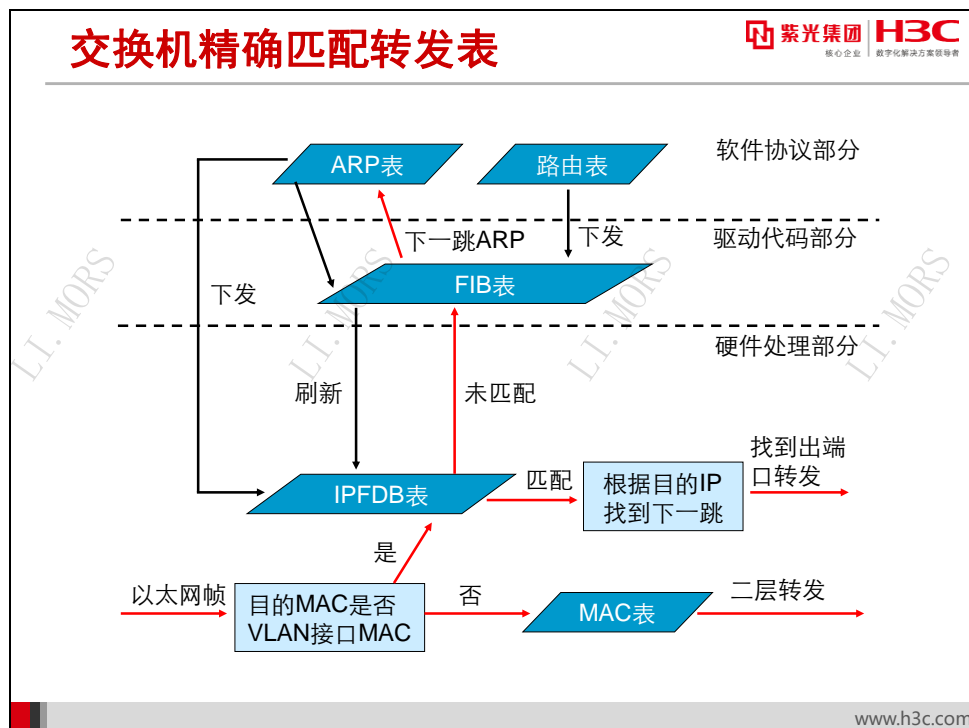
三层交换机内部的两大部分是 ASIC 芯片和 CPU, ASIC 芯片完成主要的二三层转发功能, 内部包含用于二层转发的 MAC 地址表以及用于三层转发的 IPFDB 表; CPU 用于转发的控制, 主要维护一些软件表项, 包括软件路由表、软件 ARP 表等等, 并根据软件表项的转发信息来配置 ASIC 芯片的 IPFDB。

从三层交换机的结构和各部分的作用可以看出, 真正决定高速交换转发的是 ASIC 芯片中的二三层硬件表项, 而 ASIC 芯片的硬件表项来源于 CPU 维护的软件表项。

早期的三层交换机, 其交换芯片多采用精确匹配的方式, 它们的硬件三层表项中只包含具体的目的 IP 地址, 并不带掩码信息。比如在转发目的 IP 地址为 2.1.1.2 的报文时, 通过软件查找匹配了非直连路由 2.1.1.0/24, 那么就将 2.1.1.2 的转发信息添加到 ASIC 芯片的 IPFDB 表。如果继续来了目的 IP 地址为 2.1.1.3 的报文需要转发, 则需要重新进行软件查找, 并在 ASIC 芯片的 IPFDB 表中为 2.1.1.3 增加表项。

因此, 通过多次地址学习, 就可以把表项逐一加进来, 这样后续的流量就可以直接查找 IPFDB 表, 不需要通过 CPU 查找软件路由表。这就是三层交换机所谓的“一次路由, 多次交换”。

从实际应用角度看, 精确匹配转发是有一定的限制的。这样的选路方式和表项结构对交换芯片的硬件资源要求很高, 因为芯片中集成的表项存储空间是很有限的。如果要转发大量目的 IP 地址不同的报文, 那么就需要添加大量的硬件表项。



精确匹配三层交换机整个处理流程中分成了三个大的部分：

- **平台软件协议栈部分**：这部分中关键功能有：运行路由协议，维护路由信息表，IP 协议栈的功能。在整个系统的处理流程中，这部分担负着重要的功能，当硬件不能完成报文转发的时候，这部分可以代替硬件来完成报文的三层转发。
- **硬件处理流程**：主要的表项有：二层 MAC 地址表和三层的 IPFDB（IP Forwarding Database，IP 转发数据库）表，这两个表中用于保存转发信息，在转发信息比较全的情况下，报文的转发和处理全部由硬件来完成处理，不需要软件的干预。
- **驱动代码部分**：其中关键的核心有地址解析任务和地址管理任务。地址解析任务对已经报上来未解析的地址进行学习，以便硬件完成后续的报文的转发而不需软件干预；地址管理任务为了便于软件管理和维护。软件部分保存了一份同硬件中转发表相同的 FIB（Forwarding Information Base，转发信息库）表，这个表的信息来源于软件路由表。

三层交换机精确匹配转发表主要包含表项如上图所示，其中 IPFDB 表来源于地址学习，FIB 表来源于 CPU 维护的软件路由表，如果查找 IPFDB 失败，则继续查找 FIB 表，得到目的网段路由的下一跳和出接口等信息，如果查找 FIB 表失败，则上送 CPU 处理。

精确匹配交换机三层转发主要由 IPFDB 表来完成，IPFDB 表的地址学习过程为：获取目的 IP 地址，用该 IP 去查找 FIB 表，获得下一跳 IP 地址和出接口，并用该下一跳 IP 地址去查找 ARP 表获得其对应的 MAC 地址、出接口，从而将该 IP 地址及相关信息学习到 IPFDB 表中。

对于学习到的目的 IP 地址，交换机以一定数据结构存储在 IPFDB 表中。IPFDB 表项中维护着报文三层转发的 IP 地址、端口号、下一跳对应的 MAC 地址。当交换机学习到转发过程所需的地址表项后，三层报文转发都将由硬件自动完成，无需软件处理。

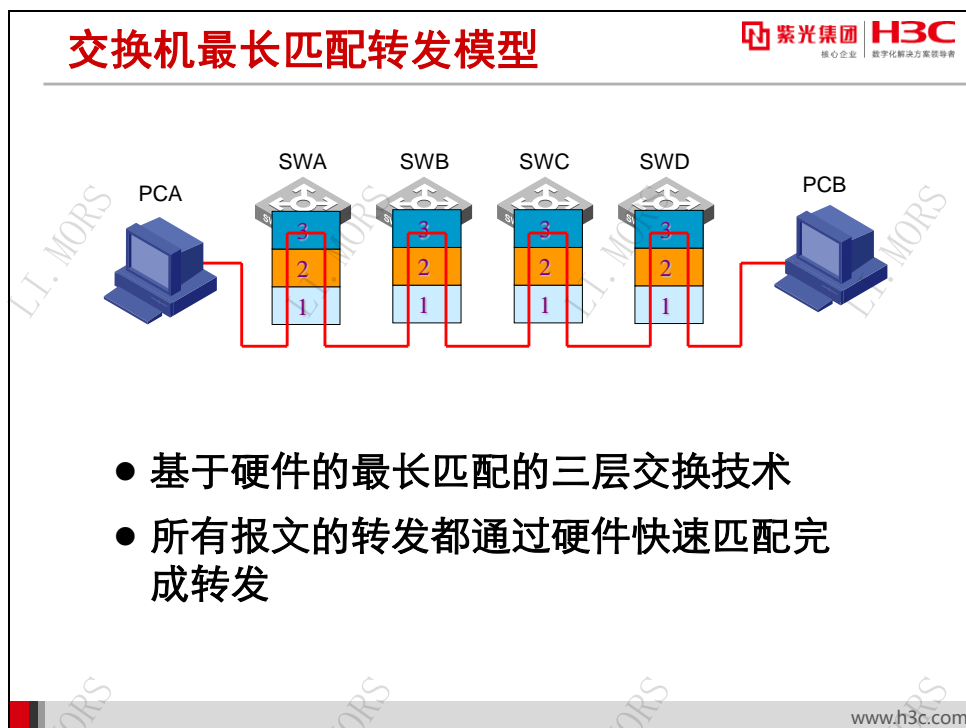
FIB 表支持最长匹配查找，而 IPFDB 表只支持精确匹配查找，可以认为 IPFDB 表项为从 FIB 表查到的下一跳 IP 地址加上下一跳 IP 地址在 ARP 表中对应的 MAC 地址和端口。可以看出 FIB 表中一个网段路由下如果有 100 台主机，就需要在 IPFDB 表中生成 100 条转发表项，这也是为什么在精确匹配交换机受到大量目的 IP 地址变化的报文攻击时，会出现 IPFDB 表满的原因。

交换机收到数据帧，先检查数据帧的 VLAN 属性，然后根据 VLAN 属性查找 MAC 地址表，交换机根据数据帧的目的 MAC 地址来判断是做二层转发还是三层转发。如果数据帧的目的 MAC 地址是本交换机的 VLAN 接口 MAC 地址，交换机查找 IPFDB 做三层转发，否则交换机查找 MAC 地址表做 VLAN 内二层转发。

以下是精确匹配方式交换机进行三层 IP 单播转发的简要步骤：

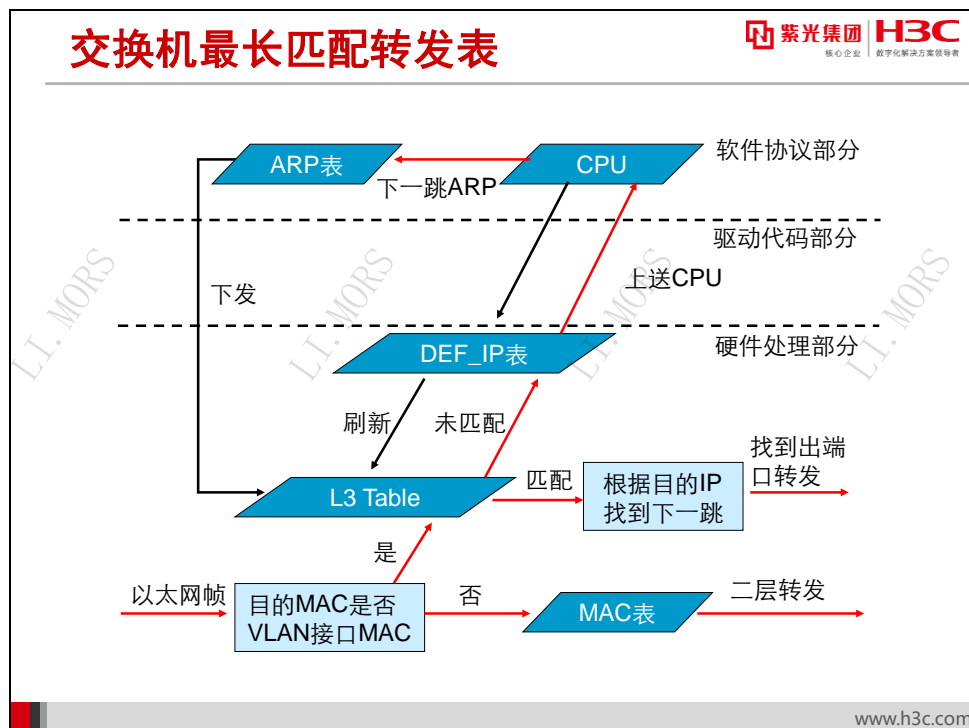
- 1) 在交换机做三层转发时，首先以目的 IP 地址查找 IPFDB 表，如果查找成功，进行下一步处理；否则转步骤 3) 以最长地址匹配查找 FIB 表；
- 2) 然后根据目的 IP 地址找到下一跳，最后根据下一跳找到目的 MAC 地址和出端口进行转发；
- 3) 查找 FIB 表，如果查找成功，再查询 ARP 表，获得下一跳的 MAC 地址和出端口，并刷新 IPFDB 表，进行下一步处理，否则转步骤 5) 上送 CPU 处理；
- 4) 查找 IPFDB 表，然后根据目的 IP 地址找到下一跳，最后根据下一跳找到目的 MAC 地址和出端口进行转发；
- 5) CPU 查找软件路由表，如查找成功并且也查找到下一跳的 ARP 表，刷新 FIB 表，FIB 表再刷新 IPFDB，转步骤 4) 处理，否则丢弃。

7.3.3 交换机最长匹配转发



由于精确匹配方式的三层交换机只能使用在网络比较稳定的情况下，不能像路由器那样很好的适应网络动荡的情况。所以，后期的三层交换机增加了对最长匹配方式的支持，即硬件三层表项中可同时包含 IP 地址和掩码，在查找时遵循最长匹配原则。

三层交换机的三层转发是基于硬件来实现的，最长匹配方式的三层交换机即使在加载大量路由、网络路由频繁波动、网络蠕虫极其严重的情况下，仍然能保证 IP 报文的线速转发，因而可以保障正常业务的运行。



最长匹配三层交换机整个处理流程中也分成了三个大的部分：

- **平台软件协议栈部分**：这部分中关键功能有：运行路由协议，维护路由信息表，IP 协议栈的功能。在整个系统的处理流程中，这部分担负着重要的功能，当硬件不能完成报文转发的时候，这部分可以代替硬件来完成报文的三层转发。
- **硬件处理流程**：主要的表项有：二层 MAC 地址表、L3 Table 和 DEF_IP 表，这三个表中用于保存转发信息，在转发信息比较全的情况下，报文的转发和处理全部由硬件来完成处理，不需要软件的干预。
- **驱动代码部分**：其中关键的核心有 ARP 和路由添加、删除处理，不再赘述。

三层交换机最长匹配转发表主要包含表项如上图所示，其中有别于精确匹配转发的表项为 L3 Table 和 DEF_IP 表。

L3 Table 获取用于跨网段报文下一跳的目的 MAC 地址，来源于 ARP 表和 DEF_IP 表，每个表项包含目的 IP 地址，对应的目的 MAC 地址、路由接口、出端口等信息。

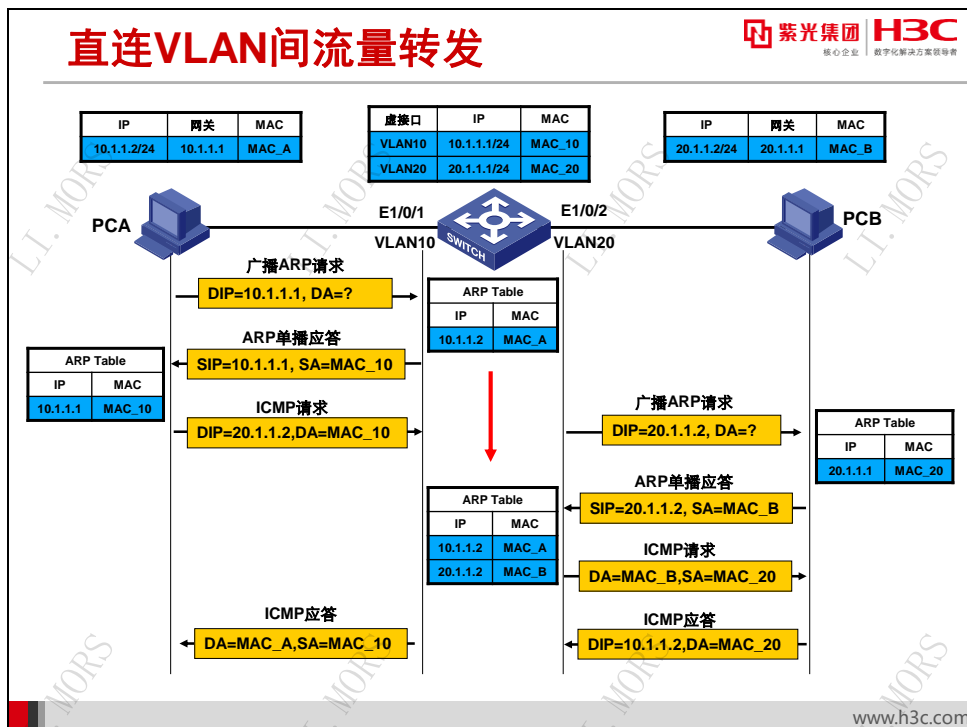
DEF_IP 表即交换机最长地址硬件匹配表，由 CPU 根据软件路由表来维护。如果查找 L3 Table 失败，则继续查找本表，得到目的网段路由的下一跳和出接口等信息，如果查找失败，从 VLAN 表中得到所属 VLAN 的默认路由。

交换机收到数据帧，先检查数据帧的 VLAN 属性，然后根据 VLAN 属性查找 MAC 地址表，交换机根据数据帧的目的 MAC 地址来判断是做二层转发还是三层转发。如果数据帧的目的 MAC 地址是本交换机的 VLAN 接口 MAC 地址，交换机查找 L3 Table 做三层转发，否则交换机查找 MAC 地址表做 VLAN 内二层转发。

以下是最长匹配方式交换机进行三层 IP 单播转发的简要步骤：

- 1) 在交换机做三层转发时，首先以目的 IP 地址查找 L3 Table，如果查找成功，进行下一步处理；否则转步骤 3) 以最长地址匹配查找 DEF_IP 表；
- 2) 然后根据目的 IP 地址找到下一跳，最后根据下一跳找到目的 MAC 地址和出端口进行转发；
- 3) 查找 DEF_IP 表，有芯片保证最长匹配的实现。如果查找成功，通过 CPU 查找 ARP 表，得到下一跳的 MAC 地址和出端口，并刷新 L3 Table，进行下一步处理；
- 4) 查找 L3 Table，然后根据目的 IP 地址找到下一跳，最后根据下一跳找到目的 MAC 地址和出端口进行转发。

7.4 本地三层转发流程介绍

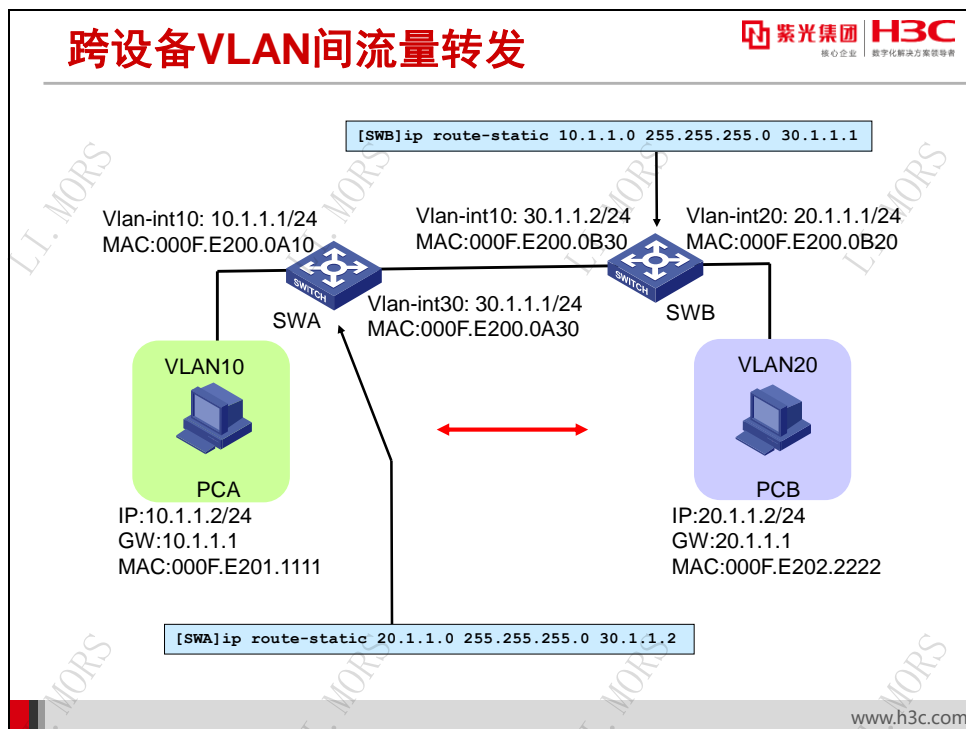


PCA 和 PCB 连接在同一台三层交换机上，但它们位于不同的 VLAN。PC 和交换机的 IP 地址以及 MAC 地址如上图所示，对于三层交换机来说，这两台 PC 都位于它的直连网段内，它们的 IP 对应的路由都是直连路由。假设起初交换机还未建立任何硬件转发表项，PCA 和 PCB 的 MAC 地址表也为空，从 PCA Ping PCB，整个通信过程如下：

- 1) PCA 首先检查出目的 IP 地址 20.1.1.2（PCB）与自己不在同一网段，则进行三层转发，通过网关来转发报文。
- 2) PCA 检查 ARP 表，发现网关不在 ARP 表中。
- 3) PCA 向网关发送 ARP 请求，请求内容为 IP 地址 10.1.1.1 对应的 MAC 地址。
- 4) 交换机收到 PCA 的 ARP 请求后，检查 ARP 请求报文，发现被请求 IP 是自己的 VLAN10 接口的 IP 地址，因此发送 ARP 应答，并将自己 VLAN10 接口的 MAC 地址 MAC_10 包含在其中。同时它还会把 PCA 的 IP 地址与 MAC 地址对应关系记录到自己的 ARP 表项中去，因为 PCA 的 ARP 请求报文中包含了发送者的 IP 和 MAC。
- 5) PCA 收到 ARP 应答报文后，学习到交换机 VLAN10 接口的 MAC 地址 MAC_10。
- 6) PCA 发送 ICMP 请求报文，报文的目的 IP 地址为 20.1.1.2，目的 MAC 地址为 MAC_10。
- 7) 交换机接收到 ICMP 请求报文后，首先根据报文的源 MAC+VLAN ID 更新 MAC 地址表，然后根据报文的目的 MAC+VLAN ID 查找 MAC 地址表，发现匹配了自己 VLAN10 接口的 MAC 地址，判断该报文为三层转发报文。

- 8) 交换机根据报文的目的 IP 地址 20.1.1.2 去查找其三层转发表项, 由于之前未建立任何表项, 因此查找失败, 于是将报文送到 CPU 去进行软件处理。
- 9) CPU 根据报文的目的 IP 地址去查找其软件路由表, 发现匹配了一个直连网段 (PCB 对应的网段), 于是继续查找其软件 ARP 表, 仍然查找失败。然后交换机会在目的网段对应的 VLAN20 的所有端口发送 ARP 请求, 请求报文的源 MAC 地址为 MAC_20, 源 IP 地址为 20.1.1.1, 目的 IP 地址为 20.1.1.2。
- 10) PCB 收到交换机发送的 ARP 请求后, 检查发现被请求 IP 是自己的 IP, 因此发送 ARP 应答, 并将自己的 MAC 地址 MAC_B 包含在其中。同时, 将交换机 VLAN20 接口的 IP 地址与 MAC 地址的对应关系记录到自己的 ARP 表中去。
- 11) 交换机收到 PCB 的 ARP 应答后, 将 PCB 的 IP 地址和 MAC 地址对应关系记录到自己的 ARP 表中去, 并将 PC A 的 ICMP 请求报文发送给 PCB, 报文的目的 MAC 地址修改为 PCB 的 MAC 地址 MAC_B, 源 MAC 修改为自己的 VLAN20 接口的 MAC 地址 MAC_20。同时, 交换机在交换芯片的三层转发表项中根据刚得到的三层转发信息添加表项 (内容包括 IP、MAC、出口 VLAN、出端口), 这样后续的 PC A 发往 PC B 的报文就可以通过该硬件三层表项直接转发了。
- 12) PCB 收到交换机转发过来的 ICMP 请求报文以后, 回应 ICMP 应答给交换机。ICMP 应答报文的转发过程与前面类似, 只是由于交换机在之前已经得到 PCA 的 IP 地址和 MAC 地址对应关系了, 也同时在交换芯片中添加了相关三层转发表项, 因此这个报文直接由交换芯片硬件转发给 PC A。
- 13) 这样, 后续的往返报文都经过查 MAC 表、查三层转发表的过程, 由交换芯片直接进行硬件转发了。这也就是我们经常说的“一次路由, 多次交换”。

7.5 跨设备三层转发流程介绍



PCA 和 PCB 通过两台三层交换机互连，它们位于不同的 VLAN，上图中标明了两台 PC 的 IP 地址、网关和 MAC 地址，以及两台三层交换机不同 VLAN 接口的 MAC 地址和 IP 地址。

假设 SWA 上配置了路由 `ip route-static 20.1.1.0 255.255.255.0 30.1.1.2`；SWB 上配置了路由 `ip route-static 10.1.1.0 255.255.255.0 30.1.1.1`。这种情况下的转发过程与“直连 VLAN 间流量转发”情况是类似的。下面的流程讲解中将省略部分前面已经分析过的细节内容。当 PCA 向 PCB 时发 Ping 包时，整个通信过程如下：

- 1) PCA 首先检查出目的 IP 地址 20.1.1.2 (PCB) 与自己不在同一网段，因此它通过 ARP 解析得到网关地址 10.1.1.1 对应的 MAC 地址 000F.E200.0A10。然后，PCA 封装 ICMP 报文并发送，报文的目的 MAC=000F.E200.0A10、源 MAC=000F.E201.1111、目的 IP=20.1.1.2、源 IP=10.1.1.2。
- 2) SWA 交换机接收到 ICMP 请求报文后，首先根据报文的源 MAC+VLAN ID 更新 MAC 地址表，然后根据报文的目的 MAC+VLAN ID 查找 MAC 地址表，发现匹配了自己 VLAN10 接口的 MAC 地址表项，判断该报文为三层转发报文。
- 3) SWA 根据报文的目的 IP 地址 20.1.1.2 去查找其三层转发表项，由于之前未建立任何表项，因此查找失败，于是将报文送到 CPU 去进行软件处理。
- 4) CPU 根据报文的目的 IP 地址去查找其软件路由表，发现匹配路由 20.1.1.0/24，其下一跳 IP 地址为 30.1.1.2，于是继续查找 30.1.1.2 是否有对应的 ARP，仍然查找失败。

然后 SWA 在下一跳地址对应的 VLAN30 内发起 ARP 请求，并得到 SWB 的回应，从而得到 SWB 的 VLAN30 接口的 IP 地址和 MAC 地址对应关系。

- 5) SWA 将 PCA 发出的 ICMP 请求报文转发给 SWB，报文的目的 MAC 地址修改为 000F.E200.0B30，源 MAC 地址修改为自己的 VLAN30 接口的 MAC 地址 000F.E200.0A30。同时，SWA 将刚刚用的转发信息添加到交换芯片的三层转发表中，包括匹配的网段 20.1.1.0/24、下一跳地址的 MAC 地址、出口 VLAN、出端口。这样后续发往 20.1.1.2 的报文就可以通过该硬件三层表项直接转发了。
- 6) SWB 收到报文后，与“直连 VLAN 间流量转发”中的处理类似，经过查 MAC 表、查三层转发表、送 CPU 匹配直连路由、ARP 解析、转发报文同时添加硬件表项的过程，将报文转发给 PCB，此时报文的目的 MAC 地址修改为 PCB 的 MAC 地址 000F.E202.2222，源 MAC 地址修改为 SWB 的 VLAN20 接口的 MAC 地址 000F.E200.0B20。这样后续发往 20.1.1.2 的报文就可以通过该硬件三层表项直接转发了。
- 7) PCB 收到 SWB 转发的 PCA 的 ICMP 请求报文后进行应答。由于在 ICMP 请求报文转发过程中，每个网段的两端节点都已经通过 ARP 解析得到对方的 IP 和 MAC 对应关系，因此应答报文的转发完全由交换芯片完成。
- 8) 这样，后续的往返报文都经过查 MAC 表、查三层转发表的过程，由交换机芯片直接进行硬件转发。

7.6 VLAN路由的相关配置

创建VLAN接口配置命令

- 创建VLAN接口

```
[Switch] interface vlan-interface vlan-interface-id
```

- 配置VLAN接口的IP地址

```
[Switch-Vlan-interface10] ip address ip-address  
{ mask | mask-length } [ sub ]
```


紫光集团 H3C
核心企业 数字化解决方案领导者

www.h3c.com

由于交换机硬件资源所限，一般交换机支持的 VLAN 数量远远多于 VLAN 接口数量。

在创建 VLAN 接口之前，对应的 VLAN 必须已经存在，否则，将不能创建指定的 VLAN 接口。创建 VLAN 接口的配置命令为：

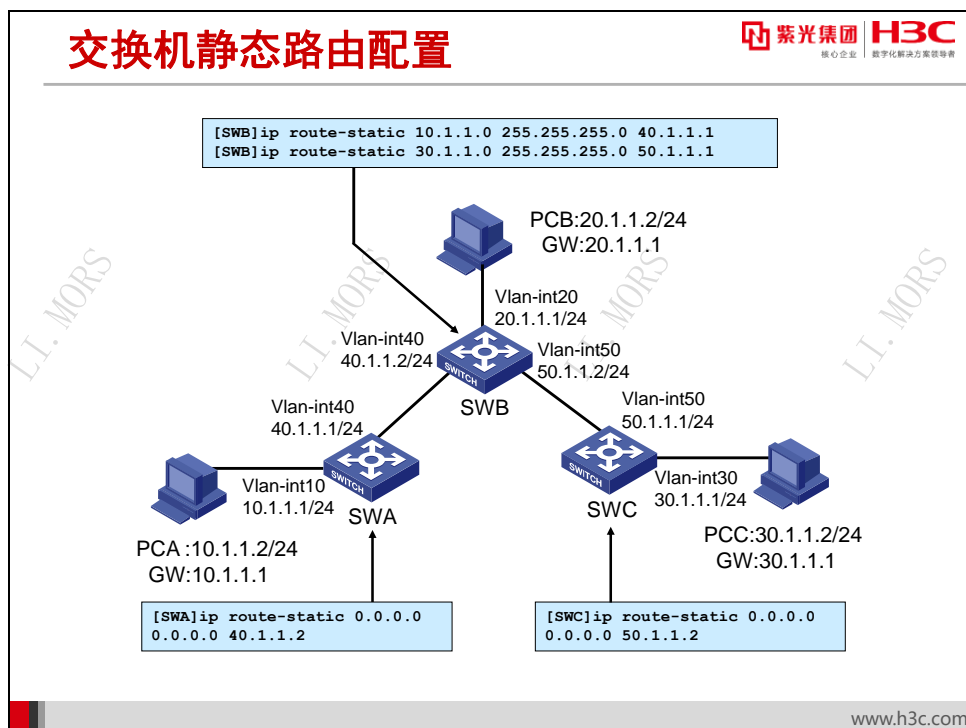
interface vlan-interface *vlan-interface-id*

创建了 VLAN 接口后，需要给 VLAN 接口配置 IP 地址。只有给两个及两个以上的 VLAN 接口配置了 IP 地址，交换机才具有三层路由转发功能。

ip address *ip-address* { *mask* | *mask-length* } [*sub*]

一般情况下，一个接口配置一个 IP 地址即可，但为了使交换机的一个 VLAN 可以与多个子网相连，VLAN 接口可以配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址，可配置九个从 IP 地址。主从地址的配置关系为：

- 当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被新配置的地址取代。
- 在删除主 IP 地址之前必须先删除从 IP 地址。



静态路由是一种特殊的路由，由管理员手工配置；配置静态路由后，去往指定目的地的数据报文将按照管理员指定的路径进行转发。在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。

静态路由的配置在系统视图下进行，配置命令为：

```
ip route-static dest-address { mask | mask-length } { next-hop-address |
interface-type interface-number next-hop-address } [ preference preference-value ]
```

其中各参数的解释如下：

- **dest-address**: 静态路由的目的 IP 地址，点分十进制格式。
- **mask**: IP 地址的掩码，点分十进制格式。
- **mask-length**: 掩码长度，取值范围为 0~32。
- **next-hop-address**: 指定路由的下一跳的 IP 地址，点分十进制格式。
- **interface-type interface-number**: 指定静态路由的出接口类型和接口号。
- **preference preference-value**: 指定静态路由的优先级，取值范围 1~255，缺省值为 60。

在配置静态路由时，建议不要直接指定广播类型接口作出接口（如三层以太网接口、VLAN 接口等）。因为广播类型的接口，会导致出现多个下一跳，无法唯一确定下一跳。在某些特殊应用中，如果必须配置广播接口（如三层以太网接口、VLAN 接口等）为出接口，则必须同时指定其对应的下一跳地址。

通过对静态路由优先级（**Preference**）进行配置，可以灵活应用路由管理策略。如在配置到达相同网络目的地的多条路由时，若指定相同优先级，可实现负载分担；若指定不同优先级，则可实现路由备份。

如果到达某个指定网络的数据报文在交换机的路由表里找不到对应的表项，那么该报文将被交换机丢弃。给当前交换机配置一条缺省路由后，如果报文的目的地址不能与路由表的任何表项相匹配，那么该报文将选取缺省路由；如果没有缺省路由且报文的目的地址不在路由表中，那么该报文将被丢弃，将向源端返回一个 **ICMP** 报文报告该目的地址或网络不可达。

在交换机上合理配置缺省路由能够减少路由表中表项数量，节省路由表空间，加快路由匹配速度。缺省路由可以手工配置，也可以由某些动态路由协议生成，如 **OSPF**、**IS-IS** 和 **RIP**。

缺省路由是静态路由的一个特例，在使用 **ip route-static** 配置静态路由时，如果将目的地址与掩码配置为全零（**0.0.0.0/0.0.0.0**），则表示配置的是缺省路由。

如上图，在 **SWA**、**SWB** 和 **SWC** 上配置静态路由后，**PC** 之间可以互通。

配置 **SWA**:

```
[SWA]ip route-static 0.0.0.0 0.0.0.0 40.1.1.2
```

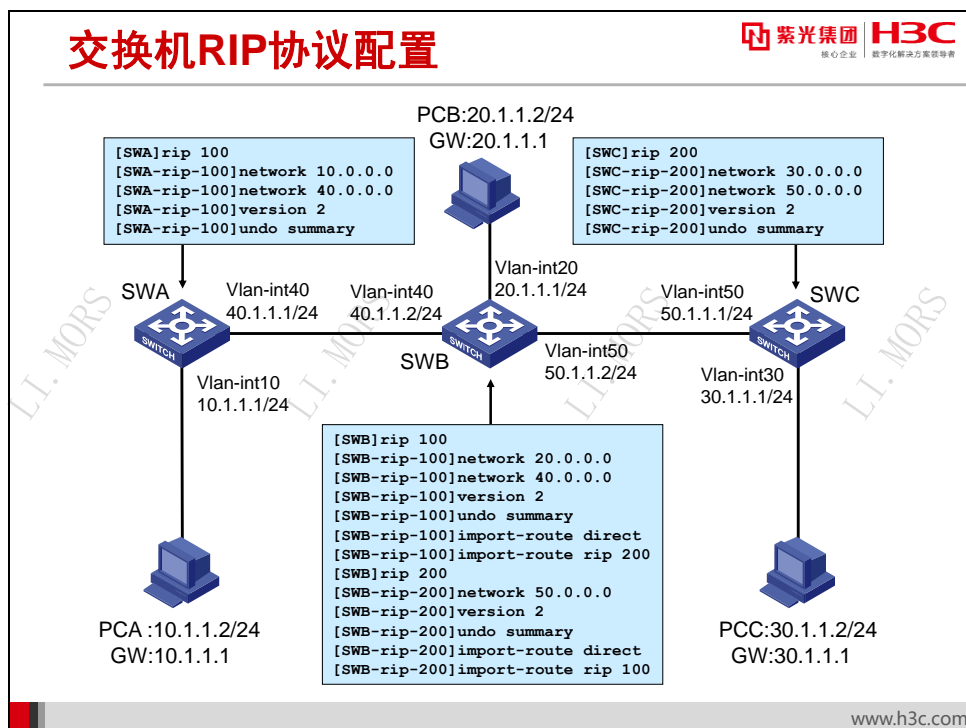
配置 **SWB**:

```
[SWB]ip route-static 10.1.1.0 255.255.255.0 40.1.1.1
[SWB]ip route-static 30.1.1.0 255.255.255.0 50.1.1.1
```

配置 **SWC**:

```
[SWC]ip route-static 0.0.0.0 0.0.0.0 50.1.1.2
```

配置静态路由时，需要注意下一跳地址不能为本地接口 **IP** 地址，否则路由不会生效。



交换机动态路由协议配置和路由器一样，此处以 RIP 协议配置为例来了解一下交换机的动态路由协议配置。

上图是 RIP 协议多进程配置举例，使用 RIPv2，并关闭 RIPv2 自动路由聚合功能。交换机上 VLAN10 接口、VLAN20 接口和 VLAN40 接口在进程 100 中开启 RIP 功能，VLAN30 接口和 VLAN50 接口在进程 200 中开启 RIP 功能。为了能够让 RIP 进程 100 和 RIP 进程 200 之间路由互通，需要配置 RIP 进程 100 引入直连路由和 RIP 进程 200 的路由，同理，RIP 进程 200 引入直连路由和 RIP 进程 100 的路由。

配置 SWA:

```
[SWA]rip 100
[SWA-rip-100]network 10.0.0.0
[SWA-rip-100]network 40.0.0.0
[SWA-rip-100]version 2
[SWA-rip-100]undo summary
```

配置 SWB:

```
[SWB]rip 100
[SWB-rip-100]network 20.0.0.0
[SWB-rip-100]network 40.0.0.0
[SWB-rip-100]version 2
[SWB-rip-100]undo summary
[SWB-rip-100]import-route direct
[SWB-rip-100]import-route rip 200
[SWB]rip 200
[SWB-rip-200]network 50.0.0.0
[SWB-rip-200]version 2
[SWB-rip-200]undo summary
[SWB-rip-200]import-route direct
[SWB-rip-200]import-route rip 100
```

配置 SWC:

```
[SWC]rip 200
[SWC-rip-200]network 30.0.0.0
[SWC-rip-200]network 50.0.0.0
[SWC-rip-200]version 2
[SWC-rip-200]undo summary
```

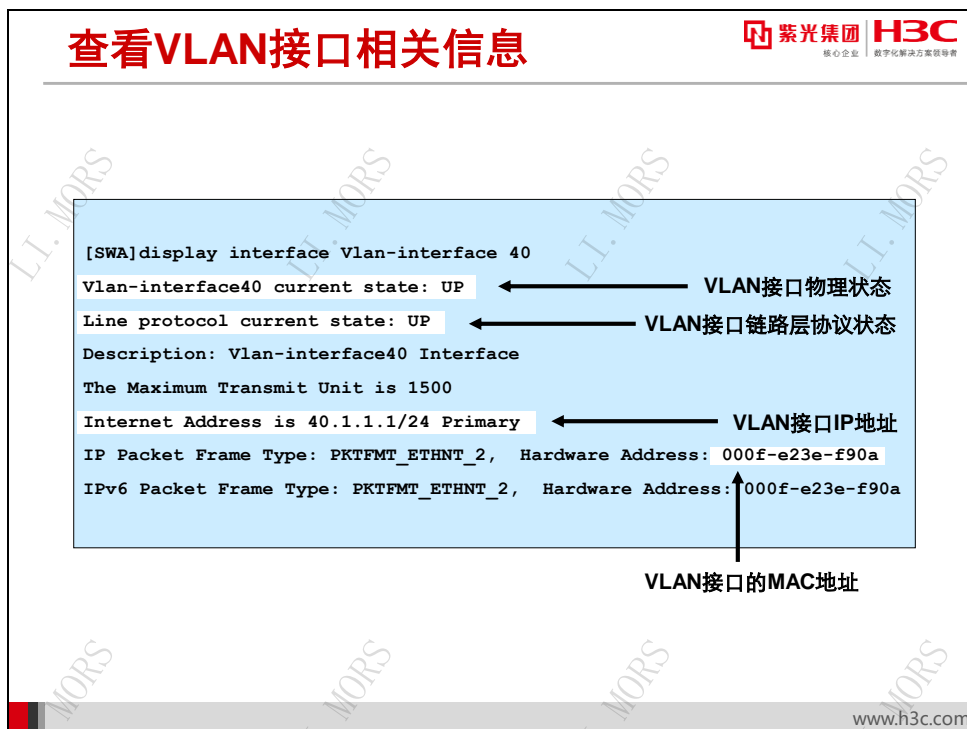
配置完成后，在 SWA 上查看 IP 路由表，如下所示：

```
[SWA]display ip routing-table
Routing Tables: Public
Destinations : 9      Routes : 9
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan10
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	RIP	100	1	40.1.1.2	Vlan40
30.1.1.0/24	RIP	100	1	40.1.1.2	Vlan40
40.1.1.0/24	Direct	0	0	40.1.1.1	Vlan40
40.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
50.1.1.0/24	RIP	100	1	40.1.1.2	Vlan40
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

从以上路由表信息可知，SWA 通过 RIP 协议学习到了路由 20.1.1.0/24 和 30.1.1.0/24。

7.7 VLAN路由的相关维护调试命令



在任意视图下可以使用 **display interface vlan-interface** 命令用来查看 VLAN 接口的相关信息。如果指定了 **vlan-interface-id**，则显示指定 VLAN 接口的信息；如果不指定，将显示已创建的所有 VLAN 接口的信息。

由上图中可以看到，VLAN40 接口的物理状态为 UP，链路层协议状态都为 UP，IP 地址为 40.1.1.124，MAC 地址为 000F.E23E.F90A。

只要属于 VLAN 的任一物理接口 UP，VLAN 接口的物理状态就会 UP；给 VLAN 接口配置 IP 地址后，VLAN 接口的链路层协议状态就会 UP。

查看ARP表相关信息

```
[SWB]display arp all count
Total entry(ies): 3
```

```
[SWB]display arp
```

IP Address	Type: S-Static		D-Dynamic		Aging Type	
	MAC Address	VLAN ID	Interface			
20.1.1.2	00e0-4c90-3bbe	20	Eth1/0/1	20	D	
40.1.1.1	000f-e23e-f90a	40	Eth1/0/23	18	D	
50.1.1.1	000f-e220-0d35	50	Eth1/0/24	20	D	

```
[SWB]display arp vlan 20
```

IP Address	Type: S-Static		D-Dynamic		Aging Type	
	MAC Address	VLAN ID	Interface			
20.1.1.2	00e0-4c90-3bbe	20	Eth1/0/1	15	D	

www.h3c.com

如果想查看交换机当前所有 ARP 表项的数目，可以在任意视图下用如下命令来查看：

display arp all count

由上图中可以看出，交换机当前有 3 条 ARP 表项。

在任意视图下，可以使用如下命令来查看交换机当前 ARP 表项，如果不指定任何参数，则显示所有的 ARP 表项：

display arp

ARP 表项中各列含义如下表所示。

字段	描述
IP Address	ARP表项的IP地址
MAC Address	ARP表项的MAC地址
VLAN ID	ARP表项所属的VLAN ID
Interface	ARP表项所对应的出端口
Aging	动态ARP表项的老化时间，单位为分钟
Type	ARP表项类型：动态，用D表示；静态，用S表示；OpenFlow，用O表示；多端口，用M表示；无效，用I表示

如果想查看指定 VLAN 的 ARP 表项，可以在任意视图下用如下命令来查看：

display arp vlan vlan-id

比如，用命令 **display arp vlan 20** 就可以查看 VLAN20 内的 ARP 表项。由上图中所显示信息可知，VLAN20 内只有 1 条 ARP 表项。

查看路由表相关信息

紫光集团 H3C
核心企业 数字化解决方案领导者

```
[SWA]display ip routing-table
```

Routing Tables: Public

Destinations : 11 Routes : 11

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan10
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan20
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	OSPF	10	2	20.1.1.2	Vlan20
40.1.1.0/24	OSPF	10	3	20.1.1.2	Vlan20
50.1.1.0/24	OSPF	10	4	20.1.1.2	Vlan20
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.1/32	O_ASE	150	1	20.1.1.2	Vlan20
192.168.2.1/32	O_ASE	150	1	20.1.1.2	Vlan20

www.h3c.com

如果想查看路由表中当前激活路由的摘要信息，可以在任意视图下用如下命令来查看：

display ip routing-table

该命令以摘要形式显示最优路由表的信息，每一行代表一条路由，内容包括目的地址/掩码长度、协议、优先级、度量值、下一跳、出接口。使用此命令仅能查看到当前被使用的路由，即最优路由。

路由表中各列含义如下表所示。

字段	描述
Destinations	目的地址个数
Routes	路由条数
Destination/Mask	目的地址/掩码长度
Proto	发现该路由的路由协议
Pre	路由的优先级
Cost	路由的度量值
Nexthop	此路由的下一跳地址
Interface	输出接口，即到该目的网段的数据包将从此接口发出

7.8 本章总结

本章总结

- 二层交换机和路由器在功能上的集成产生了三层交换机，三层交换机可以很好的解决以上两种方案的弊端
- 最长匹配转发模式所有转发都通过硬件的快速匹配完成转发，即使在加载大量路由、网络路由频繁波动，仍然保证 IP 报文的线速转发，比精确匹配转发模式转发性能优
- 给两个及两个以上的 VLAN 接口配置了 IP 地址，交换机才具有三层路由转发功能
- 交换机的路由协议配置和路由器一样

www.h3c.com

7.9 习题和解答

7.9.1 习题

- 下面哪些是三层交换机代替路由器实现 VLAN 间路由的原因？（ ）
 - 路由器采用“单臂路由”方式进行 VLAN 间路由时，数据在 Trunk 链路上往返发送引入了一定的延迟
 - 路由器的价格比交换机要高，使用路由器提高了局域网的部署成本
 - 大部分中低端路由器使用软件转发，转发性能不高，容易在网络中造成性能瓶颈
 - 三层交换机采用硬件实现的三层路由转发引擎速度高，吞吐量大，而且避免了外部物理连接带来的延迟和不稳定性
- 三层交换机整个处理流程中分成以下哪些部分？（ ）
 - 路由协议部分
 - 平台软件协议栈部分
 - 硬件处理流程
 - 驱动代码部分
- 最长匹配三层交换机硬件处理部分主要包含哪些表项？（ ）
 - 二层 MAC 地址表
 - L3 Table
 - ARP 表
 - DEF_IP 表
- 交换机收到数据帧，先检查（ ）
 - 数据帧的 VLAN 属性
 - 数据帧的目的 MAC 地址
 - 数据帧的原 MAC 地址
 - 数据帧的目的 IP 地址
 - 数据帧的原 IP 地址
- 下面关于 H3C 三层交换机 VLAN 接口描述正确的是（ ）
 - 交换机有多少个 VLAN 就可以创建多少个 VLAN 接口
 - VLAN 接口是一种虚拟接口，它不作为物理实体存在于交换机上
 - 每个 VLAN 接口只可以配置一个 IP 地址
 - 每个 VLAN 可以配置一个主 IP 地址，多个从地址

7.9.2 习题答案

1. ABCD 2. BCD 3. ABD 4. A 5. BD