

交换机端口 untagged、tagged、trunk、access 的区别

首先，将交换机的类型进行划分，交换机分为低端(SOHO级)和高端(企业级)。其两者的重要区别就是低端的交换机，每一个物理端口为一个逻辑端口，而高端交换机则是将多个物理端口捆绑成一个逻辑端口再进行的配置的。

cisco网络中，交换机在局域网中最终稳定状态的接口类型主要有四种：access/ trunk/ multi/ dot1q-tunnel。

- 1、access：主要用来接入终端设备，如PC机、服务器、打印服务器等。
- 2、trunk：主要用在连接其它交换机，以便在线路上承载多个vlan。
- 3、multi：在一个线路中承载多个vlan，但不像trunk，它不对承载的数据打标签。主要用于接入支持多vlan的服务器或者一些网络分析设备。现在基本不使用此类接口，在cisco的网络设备中，也基本不支持此类接口了。
- 4、dot1q-tunnel：用在Q-in-Q隧道配置中。

Cisco网络设备支持动态协商端口的工作状态，这为网络设备的实施提供了一定的方便（但不建议使用动态方式）。cisco动态协商协议从最初的DISL（Cisco私有协议）发展到DTP（公有协议）。根据动态协议的实现方式，Cisco网络设备接口主要分为下面几种模式：

- 1、switchport mode access：强制接口成为access接口，并且可以与对方主动进行协商，诱使对方成为access模式。
- 2、switchport mode dynamic desirable：主动与对方协商成为Trunk接口的可能性，如果邻居接口模式为Trunk/desirable/auto之一，则接口将变成trunk接口工作。如果不能形成trunk模式，则工作在access模式。这种模式是现在交换机的默认模式。
- 3、switchport mode dynamic auto：只有邻居交换机主动与自己协商时才会变成Trunk接口，所以它是一种被动模式，当邻居接口为Trunk / desirable之一时，才会成为Trunk。如果不能形成trunk模式，则工作在access模式。
- 4、switchport mode trunk：强制接口成为Trunk接口，并且主动诱使对方成为Trunk模式，所以当邻居交换机接口为trunk/desirable/auto时会成为Trunk接口。
- 5、switchport nonegotiate：严格的说，这不算是种接口模式，它的作用只是阻止交换机接口发出DTP数据包，它必须与switchport mode trunk或者switchport mode access一起使用。
- 6、switchport mode dot1q-tunnel：配置交换机接口为隧道接口（非Trunk），以便与用户交换机的Trunk接口形成不对称链路。

什么是链路类型？

vlan的链路类型可以分为接入链路和干道链路。

(1) 接入链路(access link)指的交换机到用户设备的链路，即是接入到户，可以理解为由交换机向用户的链路。由于大多数电脑不能发送带vlan tag的帧，所以这段链路可以理解为不带vlan tag的链路。

(2) 干道链路 (trunk link) 指的交换机到上层设备如路由器的链路, 可以理解为向广域网走的链路。这段链路由于要靠 vlan 来区分用户或者服务, 所以一般都带有 vlan tag。

什么是端口类型?

端口类型在以前主要分为两种, 基本上用的也是 access 和 trunk 这两种端口。

(1) access 端口: 它是交换机上用来连接用户电脑的一种端口, 只用于接入链路。例如: 当一个端口属于 vlan 10 时, 那么带着 vlan 10 的数据帧会被发送到交换机这个端口上, 当这个数据帧通过这个端口时, vlan 10 tag 将会被剥掉, 到达用户电脑时, 就是一个以太网的帧。而当用户电脑发送一个以太网的帧时, 通过这个端口向上走, 那么这个端口就会给这个帧加上一个 vlan 10 tag。而其他 vlan tag 的帧则不能从这个端口上下发到电脑上。

(2) trunk 端口: 这个端口是交换机之间或者交换机和上层设备之间的通信端口, 用于干道链路。一个 trunk 端口可以拥有一个主 vlan 和多个副 vlan, 这个概念可以举个例子来理解: 例如: 当一个 trunk 端口有主 vlan 10 和多个副 vlan 11、12、30 时, 带有 vlan 30 的数据帧可以通过这个端口, 通过时 vlan 30 不被剥掉; 当带有 vlan 10 的数据帧通过这个端口时也可以通过。如果一个不带 vlan 的数据帧通过, 那么将会被这个端口打上 vlan 10 tag。这种端口的存在就是为了多个 vlan 的跨越交换机进行传递。

也可以看出, 这两种链路方式恰好对应两种端口方式, 理解起来也不算困难。原理理解了, 当看到交换机时, 配置几遍就完全明白了。

access 和 truck 主要是区分 VLAN 中交换机的端口类型

truck 端口为与其它交换机端口相连的 VLAN 汇聚口, access 端口为交换机与 VLAN 域中主机相连的端口

trunk 一般是打 tag 标记的, 一般只允许打了该 tag 标记的 vlan 通过, 所以该端口可以允许多个打 tag 标记的 vlan 通过, 而 access 端口一般是 untag 不标记的端口, 而且一个 access vlan 端口只允许一个 access vlan 通过。

access, trunk, hybrid 是三种端口属性;

具有 access 性质的端口只能属于一个 vlan, 且该端口不打 tag;

具有 trunk 性质的端口可以属于多个 vlan, 且该端口都是打 tag 的;

具有 hybrid 性质的端口可以属于多个 vlan, 至于该端口在 vlan 中是否打 tag 由用户根据具体情况而定;

交换机三种端口模式 Access、Hybrid 和 Trunk 的理解

端口有三种模式: access, hybrid, trunk。access 性质的端口只能属于一个 vlan, 且该端口不打 tag, trunk 可以属于多个 vlan, 可以接收和发送多个 vlan 的报文, 一般用于交换机之间的连接; hybrid 也可以属于多个 vlan, 可以接收和发送多个 vlan 的报文, 可以用于交换机之间的连接也可以用于交换机和用户计算机之间的连接。trunk 和 hybrid 的区别主要是, hybrid 端口可以允许多个 vlan 的报文不打标签, 而 trunk 端口只允许缺省 vlan 的报文不打标签, 同一个交换机上不能 hybrid 和 trunk 并存。

Tag, untag 以及交换机的各种端口模式是网络工程技术人员调试交换机时接触最多的概念了，然而笔者发现在实际工作中技术人员往往对这些概念似懂非懂，笔者根据自己的理解再结合一个案例，试图向大家阐明这些概念 untag 就是普通的 ethernet 报文，普通 PC 机的网卡是可以识别这样的报文进行通讯；tag 报文结构的变化是在源 mac 地址和目的 mac 地址之后，加上了 4bytes 的 vlan 信息，也就是 vlan tag 头；一般来说这样的报文普通 PC 机的网卡是不能识别的

带 802.1Q 的帧是在标准以太网帧上插入了 4 个字节的标识。其中包含：

2 个字节的协议标识符（TPID），当前置 0x8100 的固定值，表明该帧带有 802.1Q 的标记信息。

2 个字节的标记控制信息（TCI），包含了三个域。

Priority 域，占 3bits，表示报文的优先级，取值 0 到 7，7 为最高优先级，0 为最低优先级。该域被 802.1p 采用。

规范格式指示符（CFI）域，占 1bit，0 表示规范格式，应用于以太网；1 表示非规范格式，应用于 Token Ring。

VLAN ID 域，占 12bit，用于标示 VLAN 的归属。

以太网端口有三种链路类型：Access、Hybrid 和 Trunk。

Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；

Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口；

Hybrid 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时：Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

在这里先向大家阐明端口的缺省 VLAN 这个概念

Access 端口只属于 1 个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，不用设置；

Hybrid 端口和 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID。缺省情况下，Hybrid 端口和 Trunk 端口的缺省 VLAN 为 VLAN 1

如果设置了端口的缺省 VLAN ID，当端口接收到不带 VLAN Tag 的报文后，则将报文转发到属于缺省 VLAN 的端口；当端口发送带有 VLAN Tag 的报文时，如果该报文的 VLAN ID 与端口缺省的 VLAN ID 相同，则系统将去掉报文的 VLAN Tag，然后再发送该报文。

注：对于华为交换机缺省 VLAN 被称为“Pvid Vlan”，对于思科交换机缺省 VLAN 被称为“Native Vlan”

交换机接口出入数据处理过程如下：

access 端口收报文：

收到一个报文,判断是否有 VLAN 信息：如果没有则打上端口的 PVID, 并进行交换转发, 如果有则直接丢弃（缺省）

access 端口发报文：

将报文的 VLAN 信息剥离, 直接发送出去

trunk 端口收报文：

收到一个报文,判断是否有 VLAN 信息：如果没有则打上端口的 PVID, 并进行交换转发, 如果有判断该 trunk 端口是否允许该 VLAN 的数据进入：如果可以则转发, 否则丢弃

trunk 端口发报文：

比较端口的 PVID 和将要发送报文的 VLAN 信息, 如果两者相等则剥离 VLAN 信息, 再发送, 如果不相等则直接发送

hybrid 端口收报文：

收到一个报文,判断是否有 VLAN 信息：如果没有则打上端口的 PVID, 并进行交换转发, 如果有则判断该 hybrid 端口是否允许该 VLAN 的数据进入：如果可以则转发, 否则丢弃(此时端口上的 untag 配置是不用考虑的, untag 配置只对发送报文时起作用)

hybrid 端口发报文：

1、判断该 VLAN 在本端口的属性（disp interface 即可看到该端口对哪些 VLAN 是 untag, 哪些 VLAN 是 tag）

2、如果是 untag 则剥离 VLAN 信息, 再发送, 如果是 tag 则直接发送

以下案例可以帮助大家深入理解华为交换机的 hybrid 端口模式：

```
[Switch-Ethernet0/1]int e0/1
[Switch-Ethernet0/1]port link-type hybrid
[Switch-Ethernet0/1]port hybrid pvid vlan 10
[Switch-Ethernet0/1]port hybrid vlan 10 20 untagged
[Switch-Ethernet0/1] int e0/2
[Switch-Ethernet0/2]port link-type hybrid
[Switch-Ethernet0/2]port hybrid pvid vlan 20
[Switch-Ethernet0/2]port hybrid vlan 10 20 untagged
```

此时 inter e0/1 和 inter e0/2 下的所接的 PC 是可以互通的, 但互通时数据所走的往返 vlan 是不同的。

以下以 inter e0/1 下的所接的 pc1 访问 inter e0/2 下的所接的 pc2 为例进行说明 pc1 所发出的数据, 由 inter0/1 所在的 pvid vlan10 封装 vlan10 的标记后送入交换机, 交换机发现 inter e0/2 允许 vlan 10 的数据通过, 于是数据被转发到 inter e0/2 上, 由于 inter e0/2 上 vlan 10 是 untagged 的, 于是交换机此时去除数据包上 vlan10 的标记, 以普通包的形式发给 pc2, 此时 pc1->p2 走的是 vlan10 再来分析 pc2 给 pc1 回包的过程, pc2 所发出的数据, 由 inter0/2 所在的 pvid vlan20 封装 vlan20 的标记后送入交换机, 交换机发现 inter e0/1 允许 vlan 20 的数据通过, 于是数据被转发到

inter e0/1 上, 由于 inter e0/1 上 vlan 20 是 untagged 的, 于是交换机此时去除数据包上 vlan20 的标记, 以普通包的形式发给 pc1, 此时 pc2->pc1 走的是 vlan20

Cisco 交换机设备 access、trunk、hybrid 端口的处理流程为交换机设备上 access、trunk、hybrid 端口的处理流程: 注: 数据帧在交换机内部处理时, 均带有 vlan tag。

a) access 端口

发送 (从交换机内部往外发送):

带有 vlan tag: 删除 tag 后, 发送

不带 vlan tag: 不可能出现

接收:

带有 vlan tag: 若该 tag 等于该 access 端口的 pvid, 则可以接收, 进入交换机内部

不带 vlan tag: 添加该 access 端口的 pvid, 进入交换机内部

b) trunk 端口 (允许发送 native VLAN 数据的时候, 可以不加 tag)

发送 (从交换机内部往外发送):

带有 vlan tag: 若 tag 等于该 trunk 端口的 pvid, 则删除 tag 后发送; 否则保留 tag 直接发送

不带 vlan tag: 不可能出现

接收:

带有 vlan tag: 保留该 tag, 进入交换机内部

不带 vlan tag: 添加该 trunk 端口的 pvid, 进入交换机内部

c) hybrid 端口 (允许发送多个 VLAN 数据的时候, 可以不加 tag)

发送 (从交换机内部往外发送):

带有 vlan tag: 是否带 tag 进行发送, 取决于用户配置 (用户可以配置 tagged list, untagged list)

不带 vlan tag: 不可能出现

接收:

带有 vlan tag: 保留该 tag, 进入交换机内部

不带 vlan tag: 添加该 hybrid 端口的 pvid, 进入交换机内部

在设备上允许 trunk 和 hybrid 端口同时存在, 但是不能将 hybrid 端口直接改为 trunk 端口 (hybrid-->access--->trunk), 反之亦然 (早期是这样, 现在不知道改没改)。id 端口可以允许多个 vlan 的数据不带 tag, 而 802.1q 的 trunk 只能是 native vlan (即 pvid) 对应的 vlan 的数据不带 tag, 应该说 hybrid 可以实现 trunk 端口的特性。实际使用时都可以用 hybrid 端口, 而不用 trunk。