

# 交换机高级配置

- 主要内容：
  - 了解VLAN的基本概念与VLAN协议
  - 掌握交换机中VLAN的配置
  - 掌握VTP的配置
  - 了解交换机的端口安全性配置
  - 了解交换机的其他配置

# VLAN的基本概念与VLAN协议介绍

- 为什么要用虚拟局域网（VLAN）
- 虚拟局域网的运作原理

# 为什么要用虚拟局域网（VLAN）

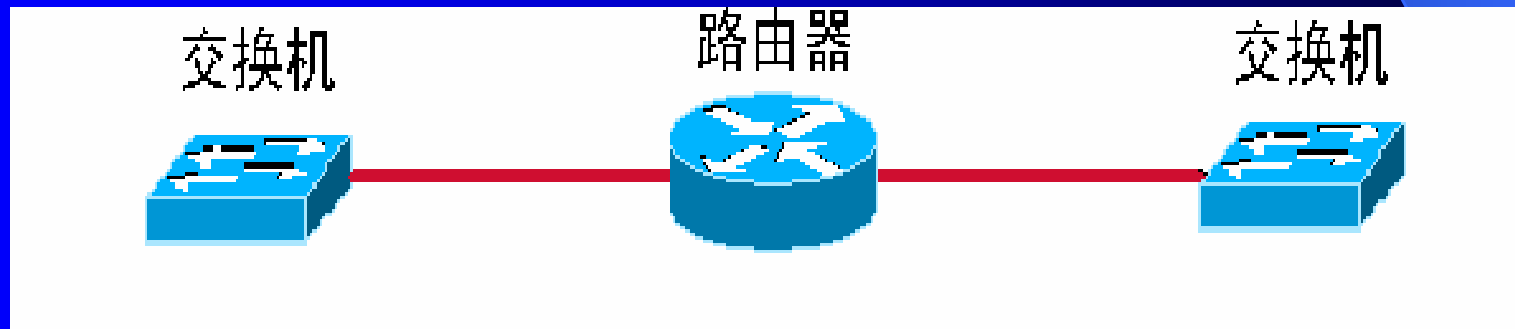
以太网交换物理上把LAN分成单独的冲突域。但是，每个段仍然是一个广播域的一部分。VLAN是网络设备（如交换机）上连接的不受物理限制的用户的一个逻辑组。在一个VLAN上的用户可以按功能、部门、应用等等分类，而不管其物理段位置。VLAN创建了不限于物理段的单一广播域，并像一个子网一样对待。

VLAN可以减轻网络工程师的工作负担。VLAN还可以允许网络管理员取消过去的物理限制，并对用户的第3层网络地址进行控制，而不管其处在网络中的哪个位置。

VLAN的其他优势包括加强网络的安全性能、易于控制广播和能够分布通信量。Cisco Catalyst交换机能够完成很多功能来加强和简化VLAN的实现。中继线（trunking）的使用允许VLAN跨接由小型的或大型区域分开的多个交换机。但实际执行这些操作的还是操作系统。操作系统翻译并执行配置文件中的语句。

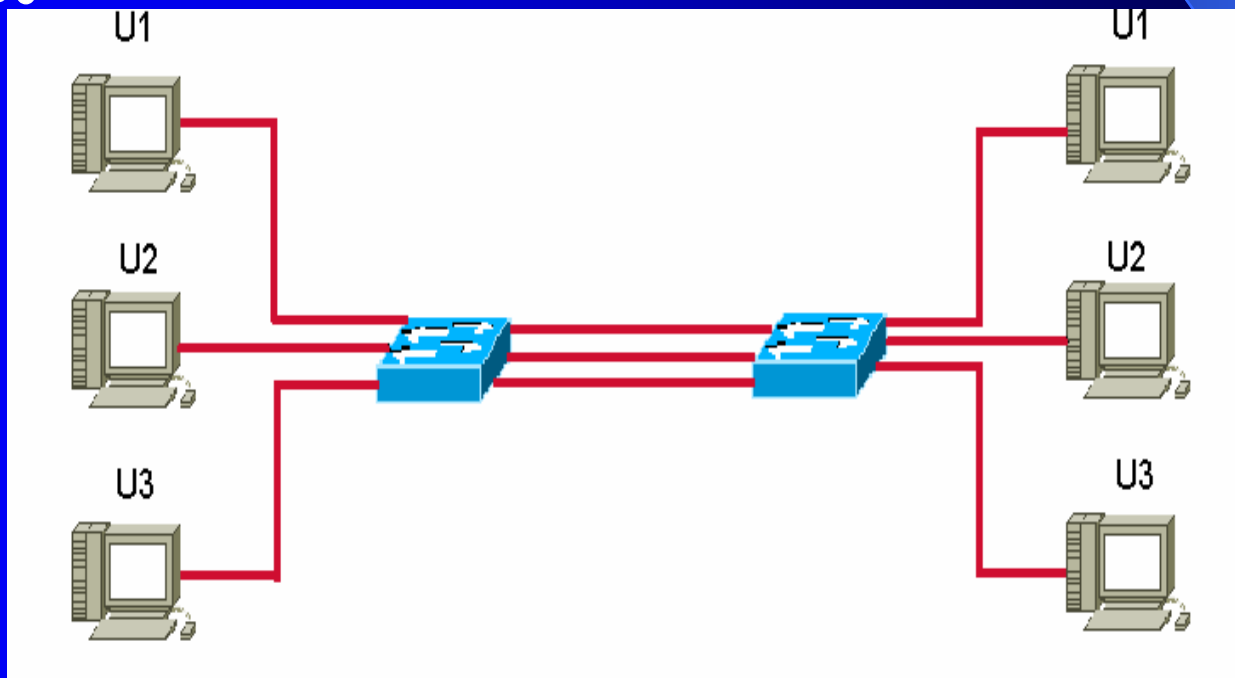
# 虚拟局域网的运作原理

在企业发展初期，为了节约成本，企业采取了通过路由器实现分段的简单结构。在这样的网络下，每一个局域网上的广播数据包都可以被该段上的所有设备收到，而无论这些设备是否需要。



# 虚拟局域网的运作原理

VLAN概念的引入，使交换机承担了网络的分段工作，而不再使用路由器来完成。VLAN具有控制广播、安全性高和灵活性及可扩展性等技术优势。



# 虚拟局域网的运作原理

通过使用VLAN，能够把原来一个物理的局域网划分成很多个逻辑意义上的子网，而不必考虑具体的物理位置，每一个VLAN都可以对应于一个逻辑单位，如部门、车间和项目组等。由于在相同VLAN内的主机间传送的数据不会影响到其他VLAN上的主机，因此减少了数据交互的可能性，极大地增强了网络的安全性。

# 交换机中VLAN的配置

- 动态配置VLAN方式
- 静态配置VLAN方式
- 帧标记

# 动态配置VLAN方式

动态VLAN提供以端用户设备的MAC地址为基础的成员。当一台设备连接到交换机端口的时候，这台交换机必须有效地查询数据库来建立VLAN成员。网络管理者必须把用户MAC地址分配到一个在VLAN成员策略服务器（VMPS）数据库中的VLAN。

对于Cisco交换机，动态VLAN使用网络管理工具来创建和管理，例如Cisco Works 2000。动态VLAN允许端用户具有充分的机动性和灵活性，但是需要更多的管理开销。



# 静态配置VLAN方式

静态VLAN提供基于端口的成员，在那里交换机端口被分配到特殊的VLAN。通过网络管理员的人为干涉，交换机端口被分配到VLAN，因此具有静态的特征。每一个端口接收一个端口VLAN ID（PVID），将它和VLAN号码相关联。在一台单独的交换机上端口可以被分配或者聚集到许多VLAN。

这种方式有很好的安全性，但灵活性较差。

# 帧标记

当帧在网络中被交换，switches根据类型对其跟踪，加上根据硬件地址来判断如何对他们进行操作。需特别注意的是：在不同类型的连接中，帧被处理的方式也不一样。

# 帧标记

## 交换环境中的2种连接类型：

- access links：指的是只属于一个VLAN，且仅向该VLAN转发数据帧的端口，也叫做native VLAN。switches把帧发送到access-link设备之前，移去任何的VLAN信息。而且access-link设备不能与VLAN外通信，除非access-link设备上数据包被路由。
- trunk links：指的是能够转发多个不同VLAN的通信的端口。trunk link必须使用100Mbps以上的端口来进行点对点连接，一次最多可以携带1005个VLAN信息。trunk link使其单独的1个端口同时成为数个VLAN的端口，这样可以不需要3层设备。当在switches之间使用了trunk link，多个VLAN的信息将从这个连接上通过；如果在switches之间没有使用trunk link而使用一般的连接，那么只有VLAN1的信息通过这个连接被互相传递。VLAN1默认作为管理VLAN。

# 帧标记

VLAN标识符：在交换机的trunk link上，可以通过对数据帧附加VLAN信息，构建跨越多台交换机的VLAN。附加VLAN信息的方法，最具有代表性的有：

- Inter-Switch Link (ISL)：属于Cisco私有，只能在快速和千兆以太网连接中使用，ISL路由可以使用在switch的断端口，router的接口和服务器接口卡等。
- IEEE 802.1Q：俗称dot 1 Q.由IEEE创建，所以在Cisco和非Cisco设备之间，就不能使用ISL必须使用802.1Q.802.1Q所附加的VLAN识别信息，位于数据帧中的源MAC地址与类型字段之间。基于IEEE802.1Q附加的VLAN信息，就像在传递物品时附加的标签当然ISL和802.1Q的主要目的是提供VLAN间通信。

# VTP的配置

- 什么是VTP
- 配置VTP

# 什么是VTP

在交换机或者一个小的交换机机组上的VLAN配置和连接中继（trunking）是相当依靠直觉的。然而，园区网环境通常包括很多互连的交换机，由于配置和管理了大量的交换机。所以，VLAN和VLAN中继线很快就会失去控制。

Cisco公司已经创建了一种用于管理园区网上全部VLAN的方法。VLAN中继线协议（VLAN Trunking Protocol，VTP）使用第2层的中继线帧与一组交换机间的VLAN信息通信。VTP从中央控制点对网络中的全部VLAN的增加，删除和重命名进行管理，任何参与VTP交换的交换机都要意识到，并能够使用VTP所管理的任何VLAN。

# 什么是VTP

## VTP的一些优点：

- 保持VLAN信息的连续性；
- 精确跟踪和监视VLAN；
- 动态报告增加了的VLAN信息给VTP域中所有switch；
- 可以使用即插即用（plug-and-play）的方法增加VLAN；
- 可以在混合型网络中进行trunk link，比如以太网到ATM LANE,FDDI等。

# 什么是VTP

在使用VTP管理VLAN之前，必须先创建个VTP服务器（VTP server），所有要共享VLAN信息的服务器必须使用相同的域名。而且，假如把某个switch和其他的switch配置在1个VTP域里，这个switch就只能和这个VTP域里的switch共享VLAN信息。其实，如果只有1个VLAN，就不需要使用VTP了。VTP信息通过trunk端口进行发送和接收。可以给VTP配置密码，但是要记住的是，所有的switch必须配置相同的密码。

switch通告VTP管理域信息，加上版本号和已知VLAN配置参数信息。还有种叫做透明VTP模式（transparent VTP mode），在这种模式里，可以给switch配置成通过trunk端口转发VTP信息，但是不接受VTP更新信息来更新它自己的VTP数据库。

switch通过VTP通告检测到增加的VLAN，然后把新增加的VLAN和已有的联结在一起共享信息。新的更新信息在之前的版本号上加1。



# 什么是VTP

在VTP域里操作的3种模式：

- 服务器模式（server mode）：所有Catalyst switches的默认设置，1个VTP域里必须至少要有1个服务器用来传播VLAN信息，对VTP信息的改变必须在服务器模式下操作.配置保存在NVRAM里；
- 客户机模式（client mode）：在这种模式下，switches从VTP服务器接受信息，而且它们也发送和接收更新，但是它们不能做任何改变。在VTP服务器通知客户switches说增加了新的VLAN之前，不能在客户switch的端口上增加新的VLAN.配置不保存在NVRAM里；
- 透明模式（transparent mode）：该模式下的switch不能增加和删除VLAN，因为它们保持的有自己的数据库，不和其他的共享配置保存在NVRAM里。

# 配置VTP

- 配置VTP管理域
- 配置VTP模式
- 配置VTP版本

# 配置VTP管理域

在交换机加入网络中之前，应当确定VTP的管理域。如果这台交换机是该网络中的第一台交换机，那么必须创建管理域。否则，交换机就得加入到已有的管理域（含有其他交换机）中：

使用下列通用的配置命令将交换机分配给某个管理域。其中domain-name是一个32字符厂的文本串：

```
Switch (config)# vtp domain domain-name
```

# 配置VTP模式

使用下面的通用配置命令序列配置  
VTP模式：

```
Switch (config)# vtp mode {server | client |  
transparent }
```

```
Switch (config)# vtp password password
```

# 配置VTP版本

可以使用下列通用配置命令配置VTP版本号：

```
Switch (config)# vtp version {1 | 2 }
```

# 交换机的端口安全性配置

- 什么是端口安全性及其作用
- 端口安全性的配置

# 什么是端口安全性及其作用

在某些情况下，网络能够控制哪些站点能访问自己，从而实现自身的保护。如果用户的工作站是固定不动的，那么往往可以通过MAC地址与相同接入层的交换机端口连接。如果工作站是移动的站点，也可以动态地获得其MAC地址并将该地址加入到一个地址列表中，以实现与交换机端口的连接。

# 控制安全性

该命令定义了一个最大值，即在MAC地址表中与该端口相联系的所允许的最多目的MAC地址。最大计数值范围从1到132，默认情况为132。即最多可有132个目的。MAC地址与该端口对应。

用port secure命令设置端口安全性后，该端口所对应的地址出现在MAC地址表中，不会以动态类型出现。因为，如果该端口对应的静态MAC地址数未达到最大计数值，而且交换机又从端口的帧流量源地址中学到了新的地址，则将该地址自动转变成永久MAC地址存入MAC地址表中。一旦永久或静态MAC地址数达到count值，则不再收受新的地址，这种方式称之为Sticky-Learns（记忆性学习）。该方式解决了未经允许而多人共用一台集线器接入交换机的一个端口所造成的不安全因素。



# 措施

下述两种情况均违反了端口安全性:

- 一个具有安全性的端口所收到帧的源MAC地址已经被赋予另一个具有安全性的端口。
- MAC地址表已满时仍试图学习新地址。

当出现违反端口安全性的情况时，端口有以下几种措施:

- Suspend（挂起）：端口不再工作，直到有数据帧流入并带有合法的地址。
- Disable（禁用）：端口不再工作，除非人工使其再次启用。
- Ignore（忽略）：忽略其违反安全性，端口仍可工作。
- 默认情况是：suspend。

# 端口安全性的配置

Catalyst交换机提供了对端口进行保护的功能，该功能基于MAC地址控制对端口的访问。要在一个接入层的交换机端口配置端口保护，首先用下面的接口配置命令在端口上激活保护功能：

```
Switch (config- if )# switchport port-security
```

# 端口安全性的配置

在各个应用了端口保护的接口，要规定被允许访问的MAC地址的最大数目，可以用下面的接口配置命令：

```
Switch (config- if )# switchport port-security  
maximum max-address
```

默认情况下，各个交换机端口仅允许一个MAC地址对其进行访问。可以设定的地址数目的范围是1到1024。

# 端口安全性的配置

## 端口安全性的配置

在各个应用了端口保护的接口，要规定被允许访问的MAC地址的最大数目，可以用下面的接口配置命令：

```
Switch (config- if )# switchport port-security  
maximum max-address
```

默认情况下，各个交换机端口仅允许一个MAC地址对其进行访问。可以设定的地址数目的范围是1到1024。

# 端口安全性的配置

最后，必须确定使用端口保护的接口，在遇到违法的MAC地址时应该怎样做，可以用下面的接口配置命令进行这项设置：

```
Switch (config- if )# switchport port-security  
violation {shutdown | restrict | protect }
```

违法：是指获得超过最大数目的MAC地址，或者一个未知的（非静态定义的）MAC地址试图访问端口。

# 交换机的其他配置

- 配置MAC地址表及相关信息
- 配置交换机端口

# 配置MAC地址表及相关信息

MAC地址表对于交换机而言如同路由表对于路由器一样。因此，对MAC地址表的配置也尤为重要。

# Switch # show mac-address-table

在show mac-address-table 命令中我们可以看到MAC地址表。

MAC地址表由三种地址组成：

- 永久地址
- 限制性静态地址
- 动态地址



# Switch # show mac-address-table

MAC地址表组成如下：

地址：目的MAC地址；

目的端口：从目的端口转发数据帧，即可以到达符合目的MAC地址的主机；

类型：动态意味着MAC地址表中的地址是通过学习流入该端口的数据帧的帧头中源端MAC地址得来的（即交换机的学习功能）。该表项必须被不断更新（即有流量通过），否则一段时间后该表项被自动删除。

1900交换机最多可在该表中容纳1024个MAC地址。一旦MAC地址表已填满，除非有表项超时被自动删除，否则新地址不能加入。

源端口表：可以向目的端口转发帧的源端口集合。

# 设置永久地址

设置永久地址的目的MAC地址与其转发端口，该地址永久不会超时，所有的端口均可以转发帧给它。

命令如下：

```
Switch(config)#mac-address-table  
permanent [MAC Address] [type slot/port]
```

# 设置限制性静态地址

限制性静态地址不但继承了永久地址的所有特性，更进一步严格限制了源端口，安全性得到进一步增强。

命令如下：

```
Switch(config)#mac-address-table  
restricted static [mac address] [type  
slot/port] [source interface list]
```

# 删除表项

如果不需要某条MAC地址表项，就可以删除它。

命令如下：

```
Switch#clear mac-address-table  
[dynamic|permanent|restricted]
```

# 配置交换机端口

- 认证端口
- 端口速度
- 端口模式

# 认证端口

可以给交换机端口配置增加一个文本描述来帮助认证配置，这个描述仅仅意味着一个注释域，作为端口使用的一条记录或者其他惟一的信息。当显示交换机配置的时候，包括端口描述。

为了给端口分配一个注释或者描述，在接口配置模式下输入如下命令：

```
Switch (config-if)# description description-string
```

使用接口配置命令“**no description**”移除一个描述。

# 端口速度

可以通过交换给配置命令给交换机端口指定一个特殊的速度，快速以太网10/100端口可以为自协商模式，设置速度为10，100或者Auto（默认）。

使用如下接口配置命令，在一个特殊的以太网端口上指定端口速度：

```
Switch (config-if)# speed {10 | 100 | auto}
```

# 端口模式

也能够为一个基于以太网的交换机端口指定一个特殊的连接模式。因此，端口在半双工、全双工或者自协商模式下操作。

在接口配置模式下输入如下命令，在交换机端口上设置连接模式：

```
Switch (config-if)# duplex {auto | full | half }
```



# 删除NVRAM中的内容

1900和2950的配置文件是存储在NVRAM里的，但是，1900里不能查看NVRAM或startup-config的内容，只能查看running-config的内容，在1900里，对配置所进行的修改自动被复制到NVRAM里。所以没有copy run start这样的命令；但是，2950就有startup-config和running-config，使用copy run start来保存配置到NVRAM里，擦除2950里startup-config文件使用“erase startup-config”命令。

# 改变交换机转发类型

- 查看转发类型

查看转发类型的命令如下：

```
Switch # show port system
```

- 改变转发类型

某些情况下，需要改变交换机的转发类型。具体配置命令如下：

```
Switch (config) # switching-mode {fragment-free|store-and-forward}。
```

一旦改变了转发类型，则所有端口都改变。