

VLAN 技术在以太网中的实现

王 硕 (中国人民解放军 92330 部队通信处 266102)

周昕宇 (中国人民解放军第 409 医院 266100)

摘要: 针对网络技术所支持的拓扑结构和实际联网节点的物理分布与现实工作中的行政区划和业务逻辑分工之间存在的分歧,立足现有公开的网络技术规范,分析了 VLAN 技术在实际网络环境中的应用条件、实现机制和配置技术。

关键词: 网络 VLAN 模式 OSI 模型

由于实际工作中的行政管理划分和具体业务分工的原因,有时会要求在同一网段中的节点为了与行政管理模式相对应而分属不同网络组织并实现相互间的信息隔离,有时又会因为实际工作的需要而要求分属不同网段的节点划归同一网络组织,从而允许信息的相互交换,这些对于古典意义上的网络技术而言几乎是不可能实现的。这就需要使用一些新的网络应用技术来适应现实工作中的行政要求,而 VLAN (virtual local area network 虚拟局域网) 技术就是一种为适应上述行政要求而发展并逐渐完善、成熟的解决方案之一。下面就 VLAN 技术在使用古典拓扑模型构造的网络结构中的应用做一个简单分析,仅供参考,为保证拓扑结构的典型性,以古典以太网网络结构为例,设置步骤以命令行形式表述。

1 虚拟局域网技术简介

VLAN 技术是一种正在迅速发展、完善的网络资源分配技术,为越来越多的机构所选用而逐渐成为在少网络地址资源、大物理跨度、大逻辑区划的网络应用环境中资源配置方面实际上的技术解决标准。它可以将存在于不同物理网段、不同拓

扑结构网络的节点组建成一个虚拟局域网,各虚拟局域网之间无法直接相互联络,就如同真的在不同的物理网络中一样。由此可以人为的将同一物理网段中的节点在逻辑上相互隔离,或将不同物理网段中的节点在逻辑上相互联系。

构成 VLAN 的节点可以分布在不同物理位置上的不同网段中却感觉不到彼此间事实上的物理跨度,同一网段中的节点可以按照业务性质关系和行政隶属关系分属不同 VLAN 从而不能直接进行信息传递,同时每个 VLAN 中的节点还可以随时根据需要在网络管理节点上通过系统配置划分到另一个 VLAN 中而不用改变其在物理网段中的实际位置。因此 VLAN 技术大大增加了网络拓扑结构的可扩展性和灵活性。

VLAN 一般采用支持相关功能的交换机和可高速传输信息的主干网络链路连接不同类型的局域网,在这一点上它与古典意义上的网络在数学拓扑结构上是相同的,但不同的是它可以根据网络节点的逻辑隶属关系在交换机上对各端口进行人工配置和划分,构成虚拟工作组即 VLAN,因此在这点上它完成了对整个网络结构在不改变实际物理位置的前提下新

的逻辑拓扑结构扩展。按照划分虚拟网络的实现方法的不同,可以实现在 OSI 层次结构中的第二层虚拟和第三层虚拟。各 VLAN 可以各自独立的在内部传输不同的网络协议报,而相互之间必须使用网桥或路由器来实现彼此通信。因此需要分别对交换机和路由器进行设置。

2 在单个交换机上配 VLAN

通过基于软件的系统配置,交换机上的每个端口都可以分属不同的 VLAN。缺省设置下,交换机的各个端口都从属于同一个 VLAN — Management VLAN, 因此各端口相互之间都是逻辑平等的并且可以相互自由通信,但一旦各端口被设置为分属不同 VLAN, 则分属不同 VLAN 的端口之间不能相互通信而必须经过路由器或网桥进行网络地址解析和转换。在整个网络环境中可以配置处在多个不同的交换机上的端口属于同一个 VLAN, 一个交换机可以设置为拥有多个 VLAN, 但每个交换机拥有且只拥有一个 Management VLAN, 默认设置为 VLAN 1。Management VLAN 唯一标志了交换机在网络中的逻辑位置和逻辑功能, 对交换机的直接逻辑通信也是通过连接由它所拥有

的各端口来实现的。Management VLAN具有如下几个特点:一个交换机只能有一个激活的Management VLAN;除了缺省的VLAN 1,其他Management VLAN都可以被设置或被删除;它不能用于OSI七层模型中的第二层协议如CDP (cisco discovery protocol)、STP (spanning-tree protocol)等,而只能用于第三层IP协议。

按缺省设置,交换机所拥有的IP地址会自动分配给Management VLAN使用,属于Mnanger VLAN的各个端口在逻辑上都平等的共享这个IP地址,网络中各节点设备与交换机Management VLAN所拥有的各端口进行数据包交换时也都是通过这个IP地址,因此连接到Management VLAN所拥有的任一个端口也就相当于直接连接到了交换机本身。而如果将交换机设置为拥有多个VLAN,除了Management VLAN以外的所有VLAN将不拥有独立的IP地址,与这些VLAN所属端口相连接的网络节点设备也只能与连接到同一个VLAN所属端口上的其他网络节点设备进行直接通信,但不能直接连接到交换机本身。

交换机上的每个端口可以只属于一个VLAN,也可以属于多个VLAN。如果一个端口只属于一个VLAN,它只能直接与同处同一个VLAN的端口进行相互间的直接通信,要与属于其他VLAN的端口进行通信,必须经路由器或网桥进行数据包地址转换,此时这个端口可以设置为固定访问端口 (static-access port),也可以设置为多VLAN端口 (multi-VLAN port)。而如果一个端口同时属于多个VLAN,那么它可以与和它同处一个VLAN的任何端口直接通信而不论这些端口之间是否同属一个VLAN,如果端口既属于

Management VLAN又属于其他VLAN,那么该端口将与其他同属Management VLAN的端口共享交换机的IP地址,但此地址不会与其他不属于Management VLAN的交换机端口共享,至于它是否使用这个IP地址,则视传递到它的数据包是否需要连接到交换机本身而定。由于同处一个VLAN的各端口之间是逻辑平等的,因此分属不同VLAN的这个端口同时还可以担负起达成分属不同VLAN的各端口之间传递数据包的任务,在跨VLAN端口传递数据包过程中,其他端口在接到要求发向本VLAN以外的IP数据包时都将数据包传递到该端口,该端口再将数据包传输到路由器或网桥上,路由器或网桥会自动解析数据包IP地址并进行转换,然后将解析后的数据包传递回该端口,该端口再按照解析后的IP地址将数据包传递到交换机相应VLAN所属的特定端口上,由此完成多个VLAN之间的传递数据包达成,要完成这项功能该端口必须设置为多VLAN端口 (multi-VLAN port)。

2.1 设置 Management VLAN

Management VLAN可以设置为是任一个VLAN,但必须是唯一的。如果设置另一个VLAN为Management VLAN,在将其激活后,原有的Management VLAN将降级为普通VLAN,不再拥有交换机所属IP地址,但所拥有的VLAN ID号不变。命令行设置内容为:

```
Switch>enable; 进入应用模式
Switch#>configure terminal; 进入全局设置模式
```

```
Switch config>interface VLAN n;
进入端口设置模式并选择将要进行配置操作的VLAN
```

```
Switch config-if>ip address ip-address subnet-mask; 配置VLAN的
```

IP地址和子网掩码,这个IP地址也就是交换机的IP地址

```
Switch config-if>management;
激活该VLAN为Management VLAN,同时旧的Management VLAN自动降级为普通VLAN,放弃交换机所属IP地址,但其ID号不变。
```

2.2 配置交换机端口属于某个特定VLAN

交换机端口可以配置为属于单一VLAN或多个VLAN,相对应的端口模式也不相同。

(1)设置端口为只属于单一VLAN的命令行设置内容为:

```
Switch>enable; 进入应用模式
Switch#>configure terminal; 进入全局设置模式
```

```
Switch config>interface interface;
进入端口设置模式并选择将要进行配置操作的端口
```

```
Switch config-if>switchport mode access; 设置端口模式为固定访问端口
```

```
Switch config-if>switchport access vlan n; 设置端口属于某个特定的VLAN
```

设置端口为属于多个VLAN的命令行设置内容为:

```
Switch>enable; 进入应用模式
Switch#>configure terminal; 进入全局设置模式
```

```
Switch config>interface interface;
进入端口设置模式并选择将要进行配置操作的端口
```

```
Switch config-if>switchport mode multi; 设置端口为多VLAN端口
```

```
Switch config-if>switchport multi vlan add vlan ID-list; 设置端口属于哪几个VLAN
```

3 在交换机群中设置VLAN

交换机集群 (switch cluster) 是一组彼此之间实现相互连接的交换机,

它们一同运行，就象是一个交换机一样，从而实现了交换机端口的逻辑扩展。这些交换机可以同处在网络环境的同一个物理位置上并彼此之间实现端口直接物理连接，也可以分处网络环境中的不同物理位置而通过 OSI 模型中的第二层交换实现端口之间的逻辑连接，与此同时它们可以在网络应用环境中共享使用同一个 IP 地址。每个交换机集群由一个主控交换机 (command switch) 和最多 15 个成员交换机 (member switch) 组成，成员交换机通过主控交换机进行各种配置。通过在交换机集群中配置 VLAN 可以极大的扩展 VLAN 在网络环境中的逻辑分布，有效的实现跨地域、跨网段网络终端的逻辑规划，丰富了网络规划的技术手段和网络管理的层次结构。

要在交换机集群中设置 VLAN，首先必须保证主控交换机和各成员交换机中准备实现集群管理的各端口同处于一个 Manager VLAN 中。然后必须先创建交换机集群并指定管理交换机，然后按照业务需要逐个添加成员交换机到交换机集群中。设置时先连接到将要作为主控管理使用的交换机上，其余交换机通过端口的物理层相连与主控交换机实现逻辑连接。交换机集群创建的命令行设置内容为：

```
switch>enable; 进入应用模式
switch#>configure terminal; 进入全局设置模式
switch config>cluster enable name; 允许创建交换机集群并命名
switch config>end; 退出到应用模式
switch#>show cluster candidates; 显示与管理交换机相连接的其他交换机的列表和 MAC 地址
switch#>show cluster members; 显示已成为交换机集群成员的交换机列表和所分配序号
```

```
switch#>configure terminal; 进入全局设置模式
```

```
switch config>cluster member n mac-address mac address password password; 增加交换机集群中的成员，注意分配的序号不能与已有的序号冲突，同时 MAC 地址必须与新加入的交换机相对应。
```

在配置好交换机集群后，就可以对配置到其中的 VLAN 进行管理，同时也可以按照配置单个交换机端口 VLAN 状况的方法配置交换机集群中各交换机的不同端口的 VLAN 分配状况，而不必理会端口是属于同一个 VLAN (包括 Manager VLAN) 还是属于有别于 Manager VLAN 的其他 VLAN。

4 在路由器上配置端口

各 VLAN 之间是彼此独立的逻辑网段，不可以直接交换数据报的而必须经路由器进行地址路由和数据中转。因此需要在路由器上对端口进行配置。如果各 VLAN 都抽出一个端口分别连接路由器的不同端口，路由器按照一般的顺序针对不同端口配置网络地址，设置路由协议等，但这样需要每个 VLAN 都必须抽出一个交换口并须消耗路由器的多个端口，而且需要明确每个路由端口连接哪各 VLAN。下面以传输 IP 协议为例说明具体配置命令：

```
router>enable; 进入应用模式
router#>configure terminal; 进入全局设置模式
router config>interface ethernet n; 进入端口设置模式
router config-if>ip address net-address netmask; 配置端口所在 IP 网络地址和掩码
router config>router ospf 101; 设置 OSPF 动态路由协议，进程号 101
```

```
router config>network network-number invert-netmask area n; 路由器端口相连接的其他网段地址 (即各 VLAN 的网络地址)、反向掩码。自治域号取 0
```

```
router config>neighbor net-address; 针对其他非广播协议配置与路由器端口相连接的其他路由器端口地址
```

如果各 VLAN 通过一个分属各 VLAN 的配置为多端口模式的交换口连接路由器，则可以节省大量交换口和路由器端口。路由器端口就需要配置子端口。同样的，也需要明确不同子端口对应的 VLAN 地址。下面以传输 IP 协议报，使用 OSPF 动态路由协议为例说明具体配置命令：

```
router>enable; 进入全局设置模式
router#>configure terminal; 进入端口设置模式
router config>interface ethernet n.subnumber; 进入端口设置模式并配置子端口
router config-if>ip address net-address netmask; 配置端口所在 IP 网络地址和掩码
router config>router ospf 101; 设置 OSPF 动态路由协议，进程号 101
router config>network network-number invert-netmask area n; 路由器端口相连接的其他网段地址 (即各 VLAN 的网络地址)、反向掩码。自治域号取 0
router config>neighbor net-address; 针对其他非广播协议配置与路由器端口相连接的其他路由器端口地址
```

参考文献

- 1 《Cisco 网络高级 IP 路由技术》，(美) Terry Slattery & William Burton 著，机械工业出版社，1999 年版。
- 2 《Cisco 网络交换机技术手册》，(美) Cisco 公司著，2000 年版。