

基于 VLAN 的局域网和基于 VPN 的广域网的互连系统

The System Integration Between Wan And Lan Based On VLAN And VPN

周晓林 (安徽省气象台 合肥 230031)

摘要:本文主要介绍 VLAN 技术在二、三层交换机上的应用以及通过干线将二层交换机和三层交换机之间、三层交换机和三层交换机之间的有机结合以及通过 VPN 技术建立异地通信,最终完成不同网段之间的操作系统通过网关和路由进行局域和广域互连。

关键词:VLAN 交换机 网关 VPN 路由器 系统集成

1 VLAN 技术在二层交换机上的应用

在日常工作中,部门与部门之间的工作性质不同,在组网过程中希望既独立,但又有联系。这样可以使具有很强灵活性和安全性的 VLAN 技术将部门与部门之间的网络分离,VLAN 技术在二层交换机上的具体实现方法如下:如果二层交换机有 12 个端口,希望 1—6 端口为一个 VLAN,7—12 端口为另一个 VLAN,可通过将 1—6 端口设为相同的 ID 号(如 ID 号为 2),将 7—12 端口设为相同的 ID 号(如 ID 号为 3)。然后再在 VLAN2 中将 1—6 端口设为同组成员关系,在 VLAN3 中将 7—12 端口设为同组成员关系,这样 VLAN2 中 1—6 端口同组成员可以相互通信、VLAN3 中 7—12 端口同组成员可以相互通信,VLAN2 中 1—6 端口成员不可以和 VLAN3 中 7—12 端口成员相互通信。此时两个 VLAN 之间要想建立通信,必须使用三层交换机中的路由技术而不是广播方式建立通信。

2 三层交换技术及与二层交换机集成

要解决广播风暴和路由器的低速问题,可使用三层交换机的路由技术和转发技术,三层交换是相对于传统交换概念而提出的。三层交换技术是在网络模型中的第三层实现了数据包的高速转发。是二层交换技术和三层转发技术集成。三层交换技术的出现,解决了传统路由器低速的网络瓶颈问题。它的二层交换的接口模块都是通过高速背板交换数据的,在第三层交换中,路由硬件模块也插接在高速背板上,使得路由模块可以与需要路由的其他模块间高速的交换数据,

从而解决了传统的外接路由器接口速率的问题。实现方法如下:如三层交换机有 12 个端口,使用第 12 端口与前面所述的二层交换机上的 VLAN2 和 VLAN3 通过干线对接,可在三层交换机(CISCO3550-12G)上的配置为:

```
!
! 系统名称
hostname Ahs - qxt
! 特权用户密码
enable password ahqxt
!
ip subnet - zero
ip routing
!
spanning - tree mode pvst
spanning - tree extend system - id
!
! 以太接口配置
interface GigabitEthernet0/1
! 接口工作模式
switchport mode dynamic desirable
no ip address
.....
.....
.....
!
interface GigabitEthernet0/12
```

```

switchport trunk encapsulation dot1q
switchport trunk native vlan 3
switchport trunk allowed vlan 2 ,vlan 3
switchport mode trunk
no ip address
!
interface Vlan1
no ip address
shutdown
!
! Vlan 接口配置
interface Vlan2
ip address 202. 21. 2. 2 255. 255. 255. 0
!
interface Vlan3
ip address 202. 21. 3. 2 255. 255. 255. 0
!
ip http server
!
line con 0
line vty 0 4
password ahqxj_ttt
login
line vty 5 15
login
!

```

此时通过机连线将 VLAN3 连接第 12 端口即可通过 VLAN ip address 202. 21. 2. 2 255. 255. 255. 0 和 ip address 202. 21. 3. 2 255. 255. 255. 0 将 VLAN2 和 VLAN3 中的成员通过第三层 ip 路由技术建立通信。在上述配置中使用了 VLAN 静态干线配置,目的是为了了解决两台交换机之间 VLAN 标识的同步问题(这一点是非常重要的),以上配置解决了二层交换机上的两个 VLAN ,VLAN2 和 VLAN3 通过三层交换机上的一个端口配置加上 VLAN ip 地址配置实现了两个 VLAN 之间通信。同理三层交换机上的不同端口可配置不同的 VLAN,在不同的 VLAN 上配置相应的 ip 地址后,VLAN 之间便可以通信。第三层交换具有以下突出特点:有机的硬件结合使得数据交换加速;优化的路由软件使得路由过程效率提高;除了必要的路由决定过程外,大

部分数据转发过程由第二层交换处理;所以适用于大型局域网。

3 三层交换机与三层交换机之间的集成

对于同一城市的一个单位地处不同的办公大楼,希望使用一个宽带直连网络将两座办公大楼连接起来协同工作,首先,可用一条单模光纤将分别放置在两座办公大楼内的两台三层交换机物理上连接为一体,然后,可分别在三层交换机上进行配置。如上述配置过的三层交换机(CISICO3550-12G)为 A(地处 A 楼),则在 A 交换机上需加上如下配置:

```

...
...
...
interface GigabitEthernet0/10
! 以太接口模式为 Vlan Trunk,使用 802.1Q 协议
switchport trunk encapsulation dot1q
! 以太接口属于 Vlan100
switchport trunk native vlan 100
! 以太接口允许 Vlan100
switchport trunk allowed vlan 100
switchport mode trunk
no ip address
interface Vlan100
ip address 192. 168. 1. 100 255. 255. 255. 248
ip classless
! 静态路由
ip route 202. 21. 85. 0 255. 255. 255. 0 192. 168. 1.

```

99

```

...
...
...

```

通过 VLAN 静态干线配置将 VLAN ip address 202. 21. 5. 2 255. 255. 255. 0 的 VLAN5 中的成员通过干线和 VLAN ip address 202. 21. 2. 2 255. 255. 255. 0 和 ip address 202. 21. 3. 2 255. 255. 255. 0 的 VLAN2 和 VLAN3 中的成员通过第三层 ip 路由技术建立通信

4 操作系统之间互连的网关配置

在局域网中二层和三层交换机系统集成之后,相同和不同操作系统要想在不同 VLAN 之间相互通信,除了正确配置机器的 ip address 和协议外,还必须正确配置网关。

4.1 基于 VLAN2 的 WIN 和 LINUX 系统的网关配置

net address 202. 21. 2. 0 255. 255. 255. 0, 机器 IP 地址为此网络地址之一。

网关为 202. 21. 2. 2

4.2 基于 VLAN3 的 WIN 和 LINUX 系统的网关配置

net address 202. 21. 3. 0 255. 255. 255. 0, 机器 IP 地址为此网络地址之一。

网关为 202. 21. 3. 2

4.3 基于 VLAN5 的 WIN 和 LINUX 系统的网关配置

net address 202. 21. 5. 0 255. 255. 255. 0, 机器 IP 地址为此网络地址之一。

网关为 202. 21. 5. 2

在相同或不同操作系统上完成了机器 IP 地址和网关配置之后,VLAN2、VLAN3、VLAN5 中的所有成员之间可以实现相互通信,使用同样方法可以建立更多的 VLAN 之间相互通信。

5 基于 VPN 技术广域网的路由协议设置

在完成基于 VLAN 的二、三层交换机和基于 VPN 的路由器系统集成之前,首先完成异地路由器对接以便建立异地通信。下面仅以基于 VPN 技术来实现异地路由器对接。(采用两台华为路由器:R1、R2)其配置要同时支持 GRE 和 IPsec 协议。配置以省气象台:内部网段网号(202. 21. 81. 0);互连网段网号(218. 22. 10. 0);

路由器内部端口 IP 地址(202. 21. 81. 250);路由器 Internet 端口 IP 地址(218. 22. 10. 171);隧道端口 IP 地址(192. 168. 1. 1)与亳州市气象局:内部网段网号(202. 21. 95. 0);互连网段网号(218. 22. 248. 0);路由器内部端口 IP 地址(202. 21. 95. 254);路由器 Internet 端口 IP 地址(218. 22. 248. 82);隧道端口 IP 地址(192. 168. 1. 2)互连为例。配置程序代码略。

6 基于 VLAN 的二、三层交换机和基于 VPN 的路由器系统集成

在上述的完成了基于 VLAN 的二、三层交换机系统集成和基于 VPN 的异地路由器系统集成后,可建立 VLAN2、VLAN3、VLAN5 中的所有成员之间的相互通信,以及它们与异地亳州市气象台之间的通信。静态路由描述略。

7 结束语

可根据网络流量和响应速度要求等具体情况来确定是使用二层交换机,还是使用三层交换机。三层交换机的最重要目的是加快大型局域网内部的数据交换,减小广播风暴的危害。基于这个原因可把大型局域网按功能或组织等因素划成多个小局域网,在本文中也就是多个 VLAN,这样必然导致不同 VLAN 这间存在大量的互访,单纯使用二层交换机没办法实现 VLAN 的互访,所以这种情况下,三层交换机就最为适合,本单位正是根据这一原理划成几个小局域网。以上三层交换机是在 CISICO3550-12G 和 CISICO3550-24EMI 上配置、二层交换机是在 NETGEAR GMS713 上配置和路由器是在华为 NE05 路由器上配置通过。

参考资料

- 1 周晓林、江双五等,《广域网下不同操作系统之间的批文件自动定时互相传输》,成都:计算机应用研究,2005 年增刊。
- 2 陈向阳、谈宏华、巨修练,计算机网络与通信,北京清华大学出版社,2005.11。
- 3 陈明,广域网教程,北京清华大学出版社,2004.2。
- 4 SYNGRESS MEDIA 公司著,Cisco 局域网交换配置技术,机械工业出版社,2000.6。
- 5 蔡皖东,计算机网络技术,西安西安电子科技大学出版社,1998.2。
- 6 黄永峰、阙勇、刘宪军、权进国等,Windows/Unix/Linux 综合组网技术,北京华大学出版社,2002.7。
- 7 华为技术有限公司,《Quidway NetEngine16E/08E/05 路由器用户手册-配置指导二分册》。
- 8 安徽华脉网络有限公司,《VPN 实验系统配置指导手册》。