

项目 1

交换机选用与配置

任务 1.1 交换机选用与基本操作

一、教学目标



- (1) 能够根据用户需求选择合适的交换机;
- (2) 能够查验各种交换机的系统功能、系统信息、性能指标和配置参数;
- (3) 能够用命令行界面进行基本配置;
- (4) 能够描述二层交换机和三层交换机的基本工作原理及性能指标;
- (5) 能够描述二层交换机和三层交换机在局域网中的应用;
- (6) 具有自学能力，能够搜集资料及阅读英语文献。

二、工作任务

某公司的网络工程师负责公司局域网的运行、维护和管理。现在因业务发展，公司需要新增网络节点。公司需要新购若干台交换机，你负责采购，需要写一份交换机选型报告。

采购的交换机收到后，你负责对交换机验收。你必须能查验交换机的系统功能、系统信息、性能指标和配置参数，并能用命令行界面进行基本配置。

三、操作步骤

1. 撰写交换机选型报告

撰写交换机选型报告前，网络工程师必须进行用户需求分析，确定所选用的交换机是接入交换机、汇聚交换机还是核心交换机，有哪些性能指标要求，交换机是否需要支持简单网络管理协议（SNMP），必须选用二层交换机还是三层交换机。

做完用户需求分析后，可以联系本地的网络设备销售商，索取交换机产品资料和报价，主要的网络产品制造商有思科系统公司（Cisco Systems, Inc.）、华为技术有限公司、中兴通信股份有限公司、杭州华三通信技术有限公司（简称 H3C）、锐捷网络有限公司等。也可以通过网络搜集交换机产品资料和报价，对各款符合需求的交换机进行比较，主要比较产品的特点、性能、价格、服务和市场占有率等，最后提出选型建议。

2. 交换机的基本操作

交换机基本配置的网络拓扑图如图 1-1 所示。



图 1-1 交换机基本配置的网络拓扑图

在 Packet Tracer 模拟器中，使用 Console 配置线将计算机串行口连接至交换机 Console 端口，通过计算机超级终端软件向交换机发送命令。

在模拟器网络拓扑图中，单击计算机图标，单击“Desktop”，单击“Terminal”进入终端配置模式，出现“Terminal Configuration”终端参数配置页面，这里选用默认配置参数，单击“OK”按钮，进入终端配置模式，通过计算机 RS232 串行口向交换机发送配置命令。

步骤 1 交换机各个操作模式之间的切换。

```

Switch>enable
Switch#
! 使用 enable 命令从用户模式进入特权模式;
Switch#configure terminal
Switch(config)#
Enter configuration commands , one per line. End with CNTL/Z.
! 使用 configure terminal 命令从特权模式进入全局配置模式;
Switch(config)#interface fastethernet 0/1
Switch(config-if)#
! 使用 interface 命令从全局配置模式进入端口配置模式;
Switch(config-if)#exit
Switch(config)#
! 使用 exit 命令退回上一级操作模式;
Switch(config-if)#end
Switch#
! 使用 end 命令直接退回特权模式。

```

步骤 2 交换机命令行界面基本功能。

```

Switch>?
Exec commands:
<1-99>          Session number to resume
Connect           Open a terminal connection
Disable           Turn off privileged commands
Disconnect        Disconnect an existing network connection
Enable            Turn on privileged commands
exit              Exit from the EXEC
logout            Exit from the EXEC
ping              Send echo messages
resume            Resume an active network connection
show               Show running system information
telnet             Open a telnet connection
terminal          Set terminal line parameters
traceroute        Trace route to destination
! 显示当前模式下所有可执行的命令;
Switch>en <tab>
Switch>enable
! 使用 Tab 键补齐命令;
Switch#co?
configure connect copy
Switch#co

```

```

! 使用? 显示当前模式下所有以 "co" 开头的命令;
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
! 使用命令的简写;
Switch(config)#int ?
    Ethernet      IEEE 802.3
    FastEthernet   FastEthernet IEEE 802.3
    GigabitEthernet GigabitEthernet IEEE 802.3z
    Port-channel   Ethernet Channel of interfaces
    Vlan          Catalyst Vlans
    range         interface range command
Switch(config)#int
! 显示 interface 命令后可以执行的参数;
Switch(config)#int f0/1
Switch(config-if)# <Ctrl>+Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
! 使用组合键"Ctrl+Z"可以直接退回到特权模式;
Switch(config-if)# <Ctrl>+C
%SYS-5-CONFIG_I: Configured from console by console
Switch#
! 使用组合键 Ctrl+C 可以直接退回到特权模式。

```

步骤3 配置交换机的名称和每日提示信息。

```

Switch(config)#hostname Students
Students(config)#
! 使用 hostname 命令将交换机名称 Switch 更改为 Students;
Students(config)#banner motd &
Enter TEXT message. End with the character '&'.
Welcome to switch Students! This switch is used to access internet for
students.
If you are administrator, you should configure this switch carefully!
&
Students(config)#
! 使用 banner 命令设置交换机的每日提示信息，保留字 motd 后面的参数"&"指定以该字符为信息
的结束符号，motd 后面的参数不能使用提示信息中用到的字符，一般使用特殊的 ASCII 字符，如@、#、
$、&等。提示信息输入完成后，以此字符作为信息结束符号。

```

交换机按上述命令配置后，当用户登录该交换机时，将显示如下提示信息：

```

Students con0 is now available
Press RETURN to get started.

```

```

Welcome to switch Students! This switch is used to access internet for students.
If you are administrator, you should configure this switch carefully!

```

步骤4 配置交换机端口参数。

交换机快速以太网端口一般情况下的默认设置是 10Mbps/100Mbps 自适应端口，双工模式也是自适应模式，并且交换机端口一般默认设置为开启，当用网线接入交换机以太网端口后，一般不经端口配置便可正常工作。交换机端口参数可以通过以下命令进行配置。

```

Students(config)#int f0/1
! 进入端口 F0/1 的配置模式;
Students(config-if)#speed 10
! 设置端口速率为 10Mbps;
Students(config-if)#duplex half

```

```
! 设置端口的双工模式为半双工;
Students(config-if)#no shutdown
! 开启端口，使端口转发数据;
Students(config-if)#description "This port is used to access internet for student."
! 配置端口的描述信息，可以作为端口提示信息;
Students(config-if)#end
! 回到交换机特权模式;
Students#show int f0/1
! 显示端口 F0/1 的端口状态及配置信息;
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Lance, address is 0002.162b.8801 (bia 0002.162b.8801)
Description: "This port is used to access internet for student."
BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 10Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

步骤 5 查看交换机的系统和配置信息。

```
Students#show version
! 查看交换机的系统信息;
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fcl)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000
ROM: Bootstrap program is C2950 boot loader
Switch uptime is 1 hours, 41 minutes, 15 seconds
System returned to ROM by power-on
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of
memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
```

```
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0090.0C54.97D4
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF
Students#show running-config
! 查看交换机的配置信息;
Building configuration...
Current configuration : 1213 bytes
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Students
interface FastEthernet0/1
  description "This port is used to access internet for student."
  duplex half
  speed 10
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface vlan1
  no ip address
  shutdown
banner motd ^C
  Welcome to switch Students!This switch is used to access internet for
students.
  If you are an administrator, please you should configure this switch
carefully!
^C
```

```
line con 0
line vty 0 4
login
line vty 5 15
login
end
```

步骤 6 保存配置参数。

交换机上述配置完成后，运行参数驻留在系统内存，交换机掉电后，配置参数将丢失。以下3条命令都可以将配置参数保存至NVRAM（非易失存储器），交换机重启后，配置参数不会丢失。

```
Students#copy running-config startup-config
Students#write memory
Students#write
```

四、操作要领

(1) 命令模式。思科和锐捷设备的命令行配置界面分成若干不同的命令模式，用户当前所处的命令模式决定了可以使用的命令。交换机在不同命令模式下支持不同的命令，不可以跨模式执行命令。初学者必须掌握每条命令的模式。当进入一个命令模式后，在命令提示符下输入问号键(?)，可以列出该命令模式下支持使用的命令。

根据配置管理功能不同，思科和锐捷设备可以分为4种命令模式，即用户模式、特权模式、全局模式、接口模式（物理接口模式、VLAN接口模式、虚拟终端接口模式、路由接口模式等）。

当用户和设备管理界面建立一个会话连接时，用户首先进入用户模式（User模式），此时可以使用用户模式的命令。在用户模式下，只可以使用少量命令，并且命令的功能也受到限制，如show命令等。在用户模式下，命令的操作结果不会被保存。

若要使用所有命令，首先必须进入特权模式（Privileged模式）。通常，在进入特权模式时必须输入特权模式口令。在特权模式下，用户可以使用所有的特权模式命令，并且能够由此进入全局配置模式。

在全局模式和接口模式，命令操作将对当前运行的配置参数产生影响。如果用户保存这些配置信息，则这些配置参数将被保存下来，并在系统重启时被操作执行。全局模式下的操作命令一般对设备产生全局性影响。从全局模式出发，可以进入各种接口配置模式。

在接口模式下的操作命令一般只对该接口配置参数起作用。

表1-1列出了4种命令模式、各种模式的提示符及进入每种模式的命令。这里，交换机的名字为默认的Switch。

表1-1 命令模式

命令模式	提示符	进入命令
用户模式	Switch>	开机自动进入
特权模式	Switch#	Switch>enable
全局模式	Switch(config)#	Switch#configure terminal
接口模式	物理接口模式	Switch(config-if)#
	VLAN接口模式	Switch(config-vlan)#
	虚拟终端接口模式	Switch(config-line)#
		Switch(config)#line vty 0 15

下面对每种命令模式进行说明。

① 用户模式 Switch>: 访问交换机时，首先进入用户模式，输入 exit 命令退出该模式。在用户模式可以进行基本测试，显示系统信息。

② 特权模式 Switch#: 在用户模式，使用 enable 命令进入特权模式。输入 exit 或者 disable 命令返回用户模式。在特权模式可以执行系统文件操作，显示系统信息和配置信息，以及各种测试命令等操作。

③ 全局模式 Switch(config)#: 在特权模式，使用 configure terminal 命令进入全局模式。输入 exit 或者 end 命令，或者按 Ctrl+Z 组合键，或者按 Ctrl+C 组合键，返回特权模式。在全局模式可以执行对交换机起全局影响的操作命令。

④ 接口模式 Switch(config-if)#: 在全局模式，使用 interface 命令进入物理接口模式，使用 vlan 命令进入 VLAN 接口模式，使用 line 命令进入虚拟终端接口模式。在接口模式只能对进入的接口配置参数。输入 exit 命令，返回全局模式。输入 end 命令，或者按 Ctrl+Z 组合键，或者按 Ctrl+C 组合键，直接返回特权模式。

(2) 获得帮助。用户可以在命令提示符下输入问号键 (?) 列出各个命令模式支持的所有命令。用户也可以使用问号键列出相同开头的命令关键字或者命令的参数信息。用户也可以使用 Tab 键，自动补齐剩余命令字符。帮助命令的使用方法见表 1-2。

(3) 命令简写。为了提高输入速度，一般使用命令简写进行配置，即只输入命令字符的前面一部分，只要确保这部分字符足够识别唯一的命令关键字。

例如，Switch#show running-config 命令可以简写成：

Switch#sh run

如果输入的命令字符不足以让系统唯一地识别命令关键字，则系统将给出“% Ambiguous command:”提示符。

例如，输入

Switch#co

系统提示：

%Ambiguous command: "co"

说明命令简写“co”不足以让系统识别命令关键字。

表 1-2 帮助命令的使用方法

命 令	说 明
命令字符+?	获得相同开头字符的命令关键字字符 例如： Switch#co? configure connect copy
命令字符+<Tab>	补齐命令关键字全部字符 例如： Switch#show run<Tab> Switch#show running-config

续表

命 令	说 明
命令字符 ?	<p>获得该命令的后续关键字或参数 例如: Switch(config-if)#switchport mode ? access Set trunking mode to ACCESS unconditionally dynamic Set trunking mode to dynamically negotiate access or trunk mode trunk Set trunking mode to TRUNK unconditionally</p>

(4) no 命令的使用。几乎所有命令都有 no 选项。通常，使用 no 命令来禁止某个特性或功能，或者执行与命令本身相反的操作。例如：

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
! 在全局模式创建 VLAN10。
Switch(config-vlan)#exit
Switch(config)#no vlan 10
! 在全局模式删除 VLAN10。
Switch(config)#int f0/1
! 进入物理接口 F0/1。
Switch(config-if)#shutdown
! 使用 shutdown 命令关闭 F0/1 接口。
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
Switch(config-if)#no shutdown
! 使用 no shutdown 命令打开 F0/1 接口。
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

```

(5) 理解 CLI 的提示信息。表 1-3 列出了用户在使用 CLI 管理设备时经常遇到的几个错误提示信息，了解这些错误提示信息，能够帮助初学者解决设备配置时经常遇到的问题。

表 1-3 常见 CLI 错误提示信息

错误提示信息	含 义	错误解决方法
% Ambiguous command: "co"	用户没有输入足够字符，系统无法识别唯一的命令关键字	重新输入命令，紧接着在发生歧义的字符后输入问号“？”。可能输入的命令关键字将被显示出来
% Incomplete command.	用户没有输入该命令必需的关键字或变量参数，命令不完整	重新输入命令，输入空格后再输入问号“？”。可能输入的命令关键字或变量参数将被显示出来
% Invalid input detected at '^' marker.	用户输入错误命令字符，符号“^”指明了产生错误字符的位置	在所在命令模式提示符下，输入问号“？”，该模式下允许使用的命令关键字将被显示出来

(6) 使用历史命令。系统提供了用户最近输入命令的历史记录。该特性在输入长而且复杂的命令时非常有用，将帮助用户有效地提高输入速度。调用已经使用过的命令，可以按照表 1-4 所示进行操作。

表 1-4 使用历史命令

操作	结果
Ctrl+P 或上方向键	在历史命令表中浏览前一条命令。从最近一条记录命令开始，重复使用该操作可以查询更早的历史命令记录
Ctrl+N 或下方向键	在使用了 Ctrl+P 或上方向键操作后，使用该操作在历史命令表中返回到更近的一条命令。重复使用该操作可以查询更近的记录

(7) 文件系统管理。常用文件系统管理命令见表 1-5。

表 1-5 常用文件系统管理命令

命 令	作 用
Switch#dir	显示某个文件系统文件列表
Switch#copy running-config startup-config	将当前生效的配置文件复制到系统重启时载入文件
Switch#delete config.text	删除某个文件
Switch#more config.text	显示某个文本文件的内容
Switch#erase startup-config	擦除文件系统某个文件
Switch#write	将当前生效的配置信息写入内存、网络或终端

例如，删除当前配置信息，恢复出厂设置，可以使用命令：

```
Switch#delete config.text
```

也可以使用下面命令：

```
Switch#erase startup-config
```

删除当前所有 VLAN 配置信息，恢复出厂设置，使用命令：

```
Switch#delete vlan.dat
```

(8) 查看配置信息。在特权模式下，可以使用如表 1-6 所示的命令查看配置文件的内容。

表 1-6 查看配置信息

命 令	作 用
Switch#more config.text	查看指定配置文件 config.text 的内容
Switch#show running-config	查看 RAM 里当前生效的配置信息
Switch#show startup-config	查看保存在 Flash 里设备重启时生效的配置信息

(9) 在操作演示中，命令行后以“!”起始的行是对前面命令的说明，帮助理解命令格式、参数、功能和作用。

(10) 初学者在学习交换机操作命令时，不仅要了解完整的执行命令，而且还必须掌握操作命令的简写，以提高操作速度。在本书中为了便于理解命令的含义，不使用简写。

(11) 命令行操作进行自动补齐或命令简写时，要求所简写的字母能够区别该命令。例如，switch#conf 可以代表命令 configure，但 switch#con 无法代表命令 configure，因为以 con 开头的命令有两个 configure 和 connect，设备无法区分。

(12) 配置设备名称，在全局配置模式中使用 hostname 命令时，配置设备名称的字符必须小于 22 个字节，如：

```
Switch(config)#hostname host-name
```

(13) 交换机端口在默认情况下是开启的。AdminStatus 是 UP 状态，如果该端口没有连接其他设备，则 OperStatus 是 Down 状态。

(14) 要重点掌握 show 命令，查看交换机的配置信息及状态。

(15) 用 **show running-config** 命令查看的是当前生效的配置信息，该信息存储在 RAM（随机存储器）里。当交换机重启时，重新生成的交换机配置信息来自交换机 Flash（非易失存储器）Startup-config。必须掌握用 copy 或 write 命令保存配置信息。

五、相关知识

1. 交换机的工作原理

我们通常所说的交换机一般是指二层交换机，二层交换机工作于数据链路层，在数据链路层传输的基本单位为“帧（Frame）”。每一帧包括一定数量的数据和一些必要的控制信息，控制信息主要包括源 MAC 地址、目的 MAC 地址、高层协议标识和差错校验信息。二层交换机可以识别数据帧中的 MAC 地址信息，并根据 MAC 地址进行转发。

数据链路层通过接收物理层提供的比特流服务，在相邻节点之间建立链路，对传输中可能出现的差错进行检错和纠错，向网络层提供无差错的透明传输。

交换机的作用主要有两个：一个是维护 CAM（Context Address Memory）表，该表是交换机端口连接设备的 MAC 地址和交换机端口的映射表；另一个是根据 CAM 表来进行数据帧的转发。

(1) 交换机根据收到数据帧中的源 MAC 地址建立该地址同交换机端口的映射，并将其写入 CAM 表中，这个过程叫作 MAC 地址学习。

(2) 交换机将数据帧中的目的 MAC 地址同交换机内部已建立的 MAC 地址表进行比较，以决定由哪个端口进行转发。

(3) 如数据帧中的目的 MAC 地址不在 CAM 表中，则向除该端口之外的所有端口转发，这一过程称为泛洪（flood）。

(4) 非目的 MAC 地址设备的网卡在接收到广播帧后，如判断出不是自己的 MAC 地址，则将该帧丢弃；拥有该 MAC 地址设备的网卡在接收到该广播帧后，将立即做出应答回复，从而使交换机又学习到一个 MAC 地址与交换机端口的映射，将“端口号—MAC 地址”对照表添加到交换机的 CAM 表中，并将数据从目的 MAC 地址对应的端口进行转发，省去了广播这个过程。

重复上述过程，逐步学习和记忆 MAC 地址。当交换机内 CAM 表成熟稳定之后，再对接收到的数据帧进行转发时，就省略了广播的过程，并直接查找目的 MAC 地址所对应的交换机端口号，直接进行转发。

需要注意的是，CAM 表中的条目是有生命周期的，如果在一定的时间内（锐捷交换机的 CAM 表老化时间为 300s）交换机没有从该端口接收到一个相同源 MAC 地址的帧（用于刷新

CAM 表中的记录), 交换机会认为该主机已经不再连接在这个端口上, 于是这个条目从 CAM 表中删除。

相应地, 如果从该端口收到帧的源 MAC 地址发生了改变, 交换机也会用新的源 MAC 地址去改写 CAM 表中该端口对应的 MAC 地址。这样, 交换机中的 CAM 表就一直能够保持最新, 以提供准确的转发依据。

以太网交换机转发数据帧有以下 3 种方式。

(1) 存储转发 (Store-and-Forward)。存储转发方式是先存储后转发数据帧。首先, 它把从端口接收到的数据帧全部接收并存储起来, 然后进行 CRC (循环冗余码校验) 检查, 并把错误帧丢弃, 最后才取出数据帧目的 MAC 地址, 查找 CAM 表后进行过滤和转发。虽然存储转发方式的生延迟大, 但是它可以对进入交换机的数据帧进行高级别的错误检查。该方式还可以支持不同速度的端口间转发。

(2) 直接转发 (Cut-Through)。当交换机在端口检测到一个数据帧时, 则检查该帧的帧头, 只要获取了帧的目的 MAC 地址, 就开始转发帧。它的优点是开始转发前不需要读取完整的数据帧, 延迟非常小。它的缺点是不能提供差错检测功能。

(3) 无碎片转发 (Fragment-Free)。这是改进后的直接转发方式, 是一种介于前两者之间的解决方法。无碎片转发方式在读取数据帧的前 64 字节后, 就开始转发该帧。这种方式虽然也不提供数据校验, 但是能够避免大多数错误。它的转发速度比直接转发方式慢, 但比存储转发方式快许多。

2. 交换机的主要性能指标

(1) 吞吐量。吞吐量是反映交换机性能的最重要的指标之一。根据 RFC 1242, 吞吐量定义为交换机在不丢失任何一个帧的情况下最大的转发速率。

(2) 延迟。根据 RFC 1242, 存储转发方式下交换机延迟定义为输入帧的最后一一位到达输入端口和输出帧的第一位出现在输出端口的时间间隔, 即 LIFO (Last In First Out) 延迟。直接转发方式下延迟定义为输入帧的第一位已到达输入端口和输出帧的第一位出现在输出端口的时间间隔。对于交换机而言, 延迟是衡量交换机性能的又一重要指标, 延迟越大说明交换机处理帧的速度越慢。另外, 网管型交换机和非网管型交换机由于系统负载不同, 以及处理方式的区别, 在帧转发延迟上会存在较大差异。

(3) 丢帧率。根据 RFC 1242, 丢帧率定义为在稳态负载下由于缺少资源应转发而没有转发的帧所占的比例。该项指标可以用来描述过载状态下交换机的性能。

(4) 背靠背 (Back-to-Back)。根据 RFC 1242, 背靠背定义为对于给定的数据帧, 从空闲状态开始, 以最小合法的时间间隔发送连续的固定长度的帧的时间。此项数值反映了交换机处理突发帧的能力。

(5) CAM 地址表深度。MAC 地址是由 IEEE 分配的, 长度为 6 字节, 又称物理地址。连接到局域网的每个端口或设备都必须至少有一个 MAC 地址。CAM 地址表深度反映了交换机可以学习到的最大 MAC 地址数。如果 CAM 地址表满, 当交换机接收到不明目的 MAC 地址的后续帧时, 交换机将采取在所有端口广播的策略; 当交换机接收到新的源地址后续帧时, 交换机将根据地址更新策略, 或者替换旧地址, 或者丢弃新的源地址。过小的 CAM 地址表将无法适应网络的变化, 造成 CAM 地址表不稳定, 从而最终降低网络性能。因此, CAM 地址表深度越大, 则交换机支持的站点数越大, 对网络的适应能力越好, 避免了因网络变化造成的 CAM 地址表不稳。

(6) 线端阻塞。线端阻塞 (Head-of-Line) 是指外出端口上的拥塞限制了通往非阻塞端口的吞吐量，与过载无关。线端阻塞通常存在于那些采用输入排队的交换机，由于队列头有转发到阻塞端口的帧，造成后继转发到非阻塞端口的帧也必须等待，从而形成线端阻塞。而对于那些采用输出排队的交换机，线端阻塞现象将不存在。对于没有流量控制功能的交换机，由于不存在阻塞现象，所以也不存在线端阻塞现象。

3. 交换机的管理方式

交换机的管理方式可以分为带外管理 (out-of-band) 和带内管理 (in-band) 两种管理模式。带内管理是指网络的管理控制信息与用户网络的承载业务信息通过同一个逻辑信道传送，简而言之，就是占用业务带宽；而在带外管理模式中，网络的管理控制信息与用户网络的承载业务信息在不同的逻辑信道传输，交换机提供专门用于管理的带宽。目前，很多高端的交换机都带有带外网管端口，使网络的管理带宽和业务带宽完全隔离，互不影响，构成单独的网管网。

(1) 通过 Console 口管理交换机。通过 Console 口管理是最常用的带外管理方式。通常，用户会在首次配置交换机或者无法进行带内管理时使用带外管理方式。用该方法管理交换机时，必须采用专用的 Console 线将计算机的 Com 口与交换机的 Console 口相连，可以采用操作系统自带的超级终端程序来连接交换机。当然，用户也可以采用自己熟悉的终端程序。

(2) 使用 Telnet 命令管理交换机。交换机启动后，用户可以通过局域网或广域网，使用 Telnet 客户端程序建立与交换机的连接并登录到交换机，然后对交换机进行配置。它一般最多支持 8 个 Telnet 用户同时访问交换机。在使用 Telnet 命令管理交换机时，首先要保证被管理的交换机设置了 IP 地址，并保证交换机与计算机的网络连通性。

(3) 使用 Web 浏览器来管理交换机。使用 Web 浏览器管理交换机时，必须保证以下 3 点：①交换机已经配置了合适的 IP 地址；②交换机已经启用了 Web 配置功能；③配置计算机与交换机能进行网络连通。

(4) 使用支持 SNMP 协议的网络管理软件管理交换机。支持网管功能的交换机可以通过支持 SNMP 协议的网管代理进行交换机的配置和管理。在网管软件能够管理交换机前，交换机也必须配置合适的 IP 地址，启用网管代理，并保证管理机与交换机的网络连通性。

任务 1.2 利用虚拟局域网技术划分网段

一、教学目标



- (1) 能够在交换网络中划分 VLAN；
- (2) 能够利用交换机的 VLAN 技术隔离交换机端口，提高网络的安全性；
- (3) 能够利用 VLAN 技术限制不同工作组之间、用户二层之间的互访；
- (4) 能够描述 VLAN 技术的基本原理及其协议标准；
- (5) 能够描述 VLAN 技术在交换网络中的用途和优点；
- (6) 能够按照网络信息安全操作规程进行操作；
- (7) 能够描述网络管理员的职业道德。

二、工作任务

某贸易公司因业务发展需要进行公司部门调整，原来的业务部拆分为国内业务部和国际业务部。两个部门的计算机仍然使用原来的接入交换机，但由于两个部门的业务范围不同，只允许同一部门内进行工作组用户互访，要求你对接入交换机进行配置，隔离两个部门的工作组之间用户二层互访，确保网络中用户对信息的访问权限。

三、操作步骤

按如图 1-2 所示网络拓扑图，国内业务部和国际业务部的计算机连接在同一台接入交换机上。可以在接入交换机中划分虚拟局域网（VLAN10 和 VLAN20），分别将国内业务部和国际业务部的计算机连接的交换机端口加入 VLAN10 和 VLAN20，利用基于端口的 VLAN 技术（Port Vlan）对交换机端口进行二层隔离，使得属于同一 VLAN 的计算机之间可以进行二层通信，即属于同一子网；属于不同 VLAN 的计算机之间不能进行工作组级的二层访问，确保不同部门用户对网络信息的访问权限不同。

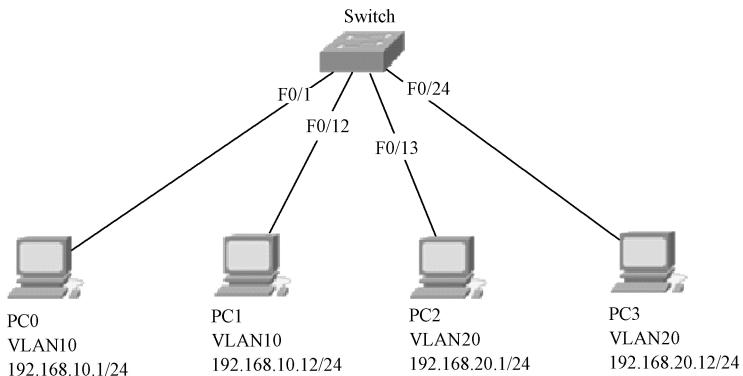


图 1-2 利用 VLAN 隔离交换机端口网络拓扑图

步骤 1 在接入交换机上创建两个 VLAN。

```

Switch>
Switch>en
Switch#conf t
! 进入交换机全局配置模式;
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
! 创建 VLAN 10;
Switch(config-vlan)#name domestic_department
! 将 VLAN 10 命名为 domestic_department;
Switch(config-vlan)#exit
Switch(config)#vlan 20
! 创建 VLAN 20;
Switch(config-vlan)#name international_department
! 将 VLAN 20 命名为 international_department;
Switch(config-vlan)#<Ctrl>+z
! 按组合键 Ctrl+z, 退回到交换机特权模式;
  
```

```

Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan
! 查看交换机上 VLAN 的配置信息;
VLAN Name          Status    Ports
----- 
1    default        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                         Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                         Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                         Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                         Gig1/1, Gig1/2
10   domestic_department  active
20   international_department active
1002 fddi-default       act/unsup
1003 token-ring-default act/unsup
1004 fdnet-default      act/unsup
1005 trnet-default      act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
----- 
1    enet    100001  1500    -     -     -     -     -     0     0
10   enet    100010  1500    -     -     -     -     -     0     0
20   enet    100020  1500    -     -     -     -     -     0     0
1002 fddi    101002  1500    -     -     -     -     -     0     0
1003 tr     101003  1500    -     -     -     -     -     0     0
1004 fd net  101004  1500    -     -     -     ieee  -     0     0
1005 trnet   101005  1500    -     -     -     ibm  -     0     0

Remote SPAN VLANs
----- 

Primary Secondary Type      Ports
----- 

```

从上面显示的 VLAN 信息可以看出，除了交换机出厂设置的默认 VLAN 外，已配置了 VLAN10 和 VLAN 20，其 VLAN 名称分别是 domestic_department 和 international_department，但所有端口属于默认的 VLAN 1。

步骤 2 将接入交换机端口加入新设置的 VLAN。

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range f0/1 - 12
! 用 range 参数同时进入端口 F0/1 到端口 F0/12，下列配置对这 12 个端口都有效;
Switch(config-if-range)#switchport mode access
! 将端口设置为 Access 模式，只有 Access 模式的端口才能加入某一 VLAN;
Switch(config-if-range)#switchport access vlan 10
! 将端口加入 VLAN 10;
Switch(config-if-range)#exit
Switch(config)#int range f0/13 - 24
! 用 range 参数同时进入端口 F0/13 到端口 F0/24;
Switch(config-if-range)#switchport mode access
! 将端口设置为 access 模式;

```

```

Switch(config-if-range)#switchport access vlan 20
! 将端口加入 VLAN20;
Switch(config-if-range)#Ctrl+Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

```

步骤3 查看交换机的 VLAN 信息。

```

Switch#show vlan
! 查看交换机上 VLAN 的配置信息;
VLAN  Name          Status      Ports
----  -----
1    default        active      Gig1/1, Gig1/2
10   domestic_department  active      Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
20   international_department  active      Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                         Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                         Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default      act/unsup
1003 token-ring-default  act/unsup
1004 fdnet-default      act/unsup
1005 trnet-default      act/unsup

VLAN Type     SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
----  -----
1   enet      100001    1500      -       -       -       -       0       0
10  enet      100010    1500      -       -       -       -       0       0
20  enet      100020    1500      -       -       -       -       0       0
1002 fddi     101002    1500      -       -       -       -       0       0
1003 tr       101003    1500      -       -       -       -       0       0
1004 fdnet    101004    1500      -       -       ieee    -       0       0
1005 trnet    101005    1500      -       -       ibm    -       0       0
Remote SPAN VLANs
Primary Secondary Type      Ports
-----  -----  -----

```

从上面显示的 VLAN 信息可以看出，交换机端口 F0/1 到 F0/12 属于 VLAN10，交换机端口 F0/13 到 F0/24 属于 VLAN20，不同业务部门的端口已在不同的 VLAN，已可以隔离不同部门用户之间的二层通信。

步骤4 测试两部门计算机的连通性。

接入交换机配置完成后，必须进行网络的连通性测试，以确保两个部门的二层通信被隔离。由于两个部门被划入不同的 VLAN，其 IP 地址也必须重新分配，每个部门使用不同网络号的 IP 地址。

如图 1-2 所示，PC0 应能 Ping 通 PC1，而不能 Ping 通 PC2 和 PC3；PC1 应能 Ping 通 PC0，而不能 Ping 通 PC2 和 PC3；PC2 应能 Ping 通 PC3，而不能 Ping 通 PC0 和 PC1；PC3 应能 Ping 通 PC2，而不能 Ping 通 PC0 和 PC1。

四、操作要领

(1) 在交换机上创建 VLAN，必须在全局模式，使用下列命令：

```
Switch (config) #vlan vlan-id  
Switch(config-vlan)#name vlan-name
```

这里的 `vlan-id` 是需要创建的 VLAN 识别号，输入创建 VLAN 命令后，系统进入 VLAN 子接口，在该子接口，可以对该 VLAN 命名，这里的 `vlan-name` 就是该 VLAN 名称。

(2) 删除某个 VLAN，可以在全局模式下使用 `no` 命令：

```
Switch (config) #no vlan vlan-id
```

这里的 `vlan-id` 是需要删除的 VLAN 识别号。

例如，`switch(config)#no vlan 10` 命令，可以删除 VLAN10。

(3) VLAN1 属于系统创建的默认 VLAN，不可以被删除。交换机出厂时，默认所有端口属于 VLAN1 成员。

(4) 将交换机某个端口加入某个 VLAN，可以使用下列命令：

```
Switch(config)#interface 端口类型/编号  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan-id
```

这里，端口类型/编号就是需要加入某个 VLAN 的端口，在全局模式，使用 `interface` 命令进入该端口后，首先将该端口设置为 Access 模式，然后再将该端口加入某个 VLAN，这里的 `vlan-id` 就是该端口需要加入的 VLAN 识别号。

(5) 交换机所有的端口在默认情况下属于 Access 端口，只有 Access 端口才能够加入某个 VLAN，TRUNK 端口不能加入某个 VLAN。在接口模式下，利用 `switchport mode access/trunk` 命令可以更改端口的 VLAN 模式。

(6) 在删除某个 VLAN 前，应先将属于该 VLAN 的所有端口加入到其他 VLAN，才能将该 VLAN 删除。

(7) 为了提高配置效率，可以同时进入一批端口，对该批端口进行配置，进入一批端口的命令如下：

```
Switch(config)#interface range f0/1 - 10 , f0/15 , f0/20  
Switch(config-if-range) #
```

这里 `f0/1-10` 表示连续的 10 个端口号 F0/1 到 F0/10，中间用符号 “-” 连接，`F0/15 , F0/20` 表示离散的 2 个端口号，中间用符号 “,” 分隔，特别注意符号 “-” 和符号 “,” 前后都有一个空格。上述命令表示同时进入一批端口 F0/1 到 F0/10，以及端口 F0/15 和端口 F0/20，进入批量接口模式后，可以同时对一批端口操作，以提高配置效率。

五、相关知识

1. VLAN 的定义和基本原理

以太网是一种基于 CSMA/CD (Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问) 技术的共享通信介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域。当网络中主机数目较多时会导致冲突严重，广播泛滥，性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了虚拟局域网 (Virtual Local Area Network, VLAN) 技术，这种技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN。处于同一

VLAN 的主机能够直接互通，而处于不同 VLAN 的主机则不能直接互通。这样，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域。

VLAN 是一种可以将局域网内的交换设备逻辑地而不是物理地划分成一个个网段的技术，也就是在物理网络上进一步划分出来的逻辑网络。VLAN 和普通局域网相比，不仅具有和普通局域网相同的属性，而且没有物理位置的限制。第二层的单播、多播和广播帧只在相同 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。VLAN 内的用户，即使位于不同的交换机上，也像在同一个局域网内一样可以互相访问，而不是本 VLAN 的用户，即使连接在同一交换机上也无法通过数据链路层的方法访问本 VLAN 内的成员。如果一个 VLAN 内的主机想要同另一个 VLAN 内的主机通信，则必须通过一个三层设备（如路由器）才能实现。

VLAN 的划分不受物理位置的限制：物理位置不在同一范围的主机可以属于同一个 VLAN；一个 VLAN 包含的主机既可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 的实现方法有多种，常见的主要包括基于端口的 VLAN、基于 MAC 地址的 VLAN、基于网络层的 VLAN 和基于 IP 组播的 VLAN，不同的 VLAN 实现方法各有优缺点，适用于不同的应用场合。

(1) 基于端口的 VLAN。基于端口的 VLAN 是划分虚拟局域网最简单也是最常用的方法。这种 VLAN 的实现方法是根据以太网交换机的端口来划分的，每个 VLAN 实际上是交换机上某些端口的集合。网络管理员只需要管理和配置交换机上的端口，使之属于不同的 VLAN，而不用考虑这些端口连接什么设备。这种实现方法的优点是定义 VLAN 成员非常简单。它的缺点是如果某个 VLAN 的成员离开了原来的端口，移动到交换机的新端口时，就必须重新配置交换机端口的 VLAN。

由于基于端口的 VLAN 实现方法，一旦交换机的 VLAN 配置完成，端口属于哪个 VLAN 是固定不变的，所以，这种 VLAN 也称为静态 VLAN。

(2) 基于 MAC 地址的 VLAN。这种 VLAN 的实现方法是根据每个主机网卡的 MAC 地址来划分 VLAN 的，即网络中每个 MAC 地址的主机被配置属于某一个 VLAN。这种 VLAN 的实现方法的最大优点是当用户主机的物理位置移动时，VLAN 不用重新配置。缺点是配置 VLAN 时需要对网络中主机的 MAC 地址进行登记，并根据 MAC 地址配置 VLAN，并且，有些交换机的端口可能存在很多 VLAN 组成员，这样就无法限制广播，导致交换机执行效率下降。

(3) 基于网络层的 VLAN。这种 VLAN 的实现方法是根据每个主机的网络层地址或协议类型进行划分的。交换机虽然查看每个数据包的 IP 地址或协议，并根据 IP 地址或协议决定该数据包属于哪个 VLAN，进而转发，但并不进行路由，只进行第二层转发。这种方法的优点是用户的物理位置改变时，不需要重新配置他所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理很重要。这种方法的缺点是需要对每个数据包的网络层地址或协议进行检查，与数据链路层的帧转发相比，很耗费机器资源和时间，效率较低。

(4) 基于 IP 组播的 VLAN。IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩展到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要缺点是效率不高。

2. VLAN 的优点

在交换网络中划分 VLAN 具有以下几个优点。

(1) 限制广播包。根据交换机的转发原理,如果一个数据帧找不到应该从哪个端口转发出去时,交换机就会将该数据帧向所有的其他端口发送,即数据帧的泛洪。这样的结果极大地浪费了网络带宽资源。如果配置了 VLAN,交换机只会将此数据帧广播到属于该 VLAN 的其他端口,而不是交换机的所有端口,这样,就将数据帧限制在了一个 VLAN 内,提高了网络效率。

(2) 提高网络的安全性。由于在交换网络中配置 VLAN 后,数据帧只能在同一个 VLAN 内转发,不能在不同 VLAN 之间转发,确保了该 VLAN 的信息不会被其他 VLAN 的用户通过数据链路层窃取,提高了网络的安全性。

(3) 网络管理简单。对于交换式以太网,如果对某些用户重新进行网段分配,则需要对网络系统的物理结构进行重新调整,甚至需要增加网络设备,增大网络管理的工作量。而对于采用 VLAN 技术的网络来说,一个 VLAN 可以根据部门职能、对象组或应用将不同地理位置的网络用户划分为一个逻辑分组。在不改动网络物理连接的情况下,可以任意地将工作站在工作组或子网之间移动。

(4) 方便实现虚拟工作组。虚拟工作组的目标是建立一个动态的组织环境。例如,在校园网中,同一系科的工作站就好像在同一个局域网,很容易实现互相访问、交流信息,同时,所有的广播也限制在该 VLAN 内,而不影响其他 VLAN 的用户。如果一个用户从一个办公地点换到了另一个办公地点,而他仍然在该系科,那么,他的网络配置无须改变。而如果一个用户虽然办公地点没有变化,但他换了一个系科,则只需配置相应的 VLAN 参数即可,无须改变网络物理结构。

3. VLAN 的协议标准

有两种常见的 VLAN 标签格式,思科公司的 Inter-Swith Link (ISL) 格式和标准的 IEEE 802.1Q 格式。ISL 技术在原有帧上重新加了一个帧头,并重新生成了帧校验序列 (FCS), ISL 是思科公司特有的技术,不能在非思科交换机上使用。IEEE 802.1Q 技术在原有帧的源 MAC 地址字段后插入标记字段,同时用新的 FCS 字段替代了原有的 FCS 字段,该技术是国际标准,得到了所有交换机厂家的支持。

如图 1-3 所示,每一个支持 IEEE 802.1Q 协议的主机,在发送数据包时,都在原来的以太网帧头中的源 MAC 地址后增加了一个 4 字节的 IEEE 802.1Q 帧头,之后接原来以太网帧的长度或类型域。

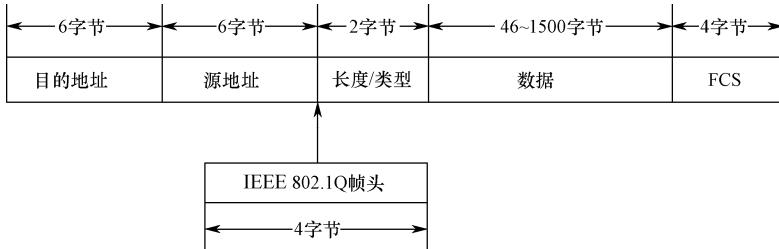


图 1-3 带有 IEEE 802.1Q 协议标签头的以太网帧

这个 4 字节的 IEEE 802.1Q 标签头包含 2 字节的标签协议标识 TPID (Tag Protocol Identifier, 它的值是 0x8100), 和 2 字节的标签控制信息 TCI (Tag Control Information), TPID 是 IEEE 定义的新类型, 表明这是一个加了 IEEE 802.1Q 标签的文本。

TCI 标签控制信息字段包含 3 位用户优先级字段（User Priority）、1 位规范格式指示器（Canonical Format Indicator）和 12 位虚拟局域网识别号（VLAN Identified）。

用户优先级字段（User Priority）用来指定用户帧的优先级，用 3 位表示，一共有 8 种优先级，主要用于当交换机发生拥塞时，指明交换机优先发送哪个数据帧。

规范格式指示器（CFI）用 1 位表示，主要用于总线型的以太网与 FDDI、令牌环网交换数据时的帧格式指示。在以太网交换机中，规范格式指示器总被设置为 0。

虚拟局域网识别号（VLAN ID）是一个 12 位的域，指明 VLAN 的 ID 号，每个支持 IEEE 802.1Q 协议的主机发送出来的数据帧都会包含这个域，以指明自己属于哪个 VLAN。该字段为 12 位，理论上支持 4096 个 VLAN 的识别。不过，在 4096 个 VLAN ID 中，VLAN 号 0 用于识别帧优先级，VLAN 号 4095 作为预留值，所以交换机系统能配置的最大 VLAN 数为 4094。

任务 1.3 跨交换机实现 VLAN



一、教学目标

- (1) 能够跨交换机构建逻辑子网；
- (2) 能够配置跨交换机实现 VLAN；
- (3) 能够正确应用和配置 TAG VLAN；
- (4) 理解 TAG VLAN 的基本原理和工作过程；
- (5) 掌握交换机中 Access 端口和 Trunk 端口的不同作用；
- (6) 培养学生在网络信息安全方面的基本技能。

二、工作任务

某公司因业务发展，财务处需要新增设办公地点，新办公地点有两台计算机需要接入局域网。由于新办公地点与原来财务处相距较远，两个办公地点的计算机分别连接不同的接入交换机。你作为公司的网络管理员，请进行适当配置，使新增办公地点的两台计算机与原财务处的计算机在同一网段，并可以进行工作组互访，但其他部门的计算机与财务处计算机不可以进行二层互访。

三、操作步骤

如图 1-4 所示网络拓扑图，原财务处与其他部门公用一台接入交换机 SwitchA，在该接入交换机 SwitchA 上划分了 VLAN10 和 VLAN20，财务处网络属于 VLAN20，其他部门网络属于 VLAN10，财务处新增办公地点的计算机通过交换机 SwitchB 接入网络，这样，财务处两个办公地点的计算机通过不同的交换机接入网络，实现新增办公地点的两台计算机与原财务处的计算机在同一网段。因此，必须在新接入的交换机 SwitchB 上创建 VLAN20，将财务处新增办公地点的两台计算机加入 VLAN20，并将连接两台交换机的端口设置为 Trunk 模式，就可以跨交换机实现 VLAN，确保同一部门的计算机可以进行工作组互访，其他部门的计算机与财务处计算机不可以进行二层互访。

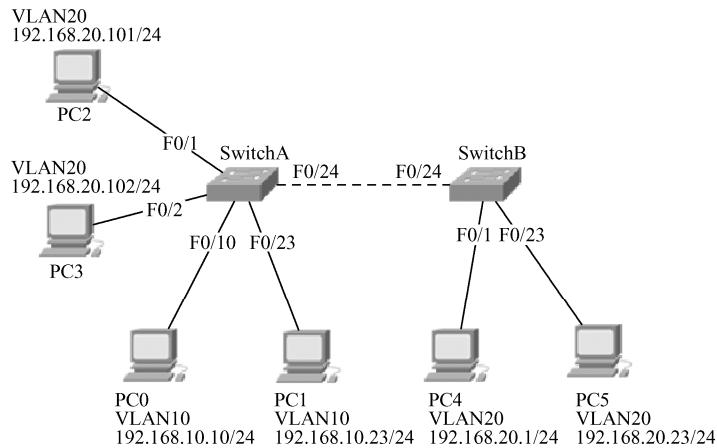


图 1-4 跨交换机实现 VLAN 网络拓扑图

步骤 1 配置两台交换机的主机名。

进入左侧交换机 SwitchA 的命令行：

```

Switch>
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host SwitchA
SwitchA(config)#

```

进入右侧交换机 SwitchB 的命令行：

```

Switch>
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host SwitchB
SwitchB(config)#

```

步骤 2 在原交换机 SwitchA 上划分 VLAN，并将不同端口加入对应 VLAN。

在交换机 SwitchA 上进入命令行：

```

SwitchA(config)#vlan 10
SwitchA(config-vlan)#name qita
! 在原交换机 SwitchA 上创建 VLAN 10，并命名为 qita;
SwitchA(config-vlan)#vlan 20
SwitchA(config-vlan)#name caiwu
! 在原交换机 SwitchA 上创建 VLAN 20，并命名为 caiwu;
SwitchA(config-vlan)#exit
SwitchA(config)#int range f0/1 - 9
! 进入交换机端口 F0/1 至 F0/9;
SwitchA(config-if-range)#switchport mode access
! 将端口 F0/1 至 F0/9 设置为 access 模式;
SwitchA(config-if-range)#switchport access vlan 20
! 将端口 F0/1 至 F0/9 加入 VLAN20;
SwitchA(config-if-range)#exit

```