项目 3　可靠型交换网络构建

项目介绍

互联网应用的飞速发展使许多传统的业务都被互联网＋的方式取代，而企业各种信息和商机的获取也对互联网有着很强的依赖性，即使网络发生故障，也希望能马上启用备用链路或备用设备，使用户对网络故障几乎无感知，不影响正常业务。所以，网络可靠性越来越受到企业的重视。作为网络工程设计与部署人员或者网络运维人员，一定要有灾备意识，组建科学可靠的网络架构，避免单点故障或单链路故障等导致企事业单位利益受损。常用的局域网冗余方案有 MSTP＋VRRP＋Eth-Trunk（多生成树＋网关冗余＋链路聚合）和 iStack/CSS＋Eth-Trunk（堆叠/集群＋链路聚合）。本项目通过 MSTP＋VRRP＋Eth-Trunk＋DHCP 的典型综合应用案例，以“总—分—总”的思路介绍可靠型交换网络的构建。

拓扑设计

根据该项目的可靠性等需求设计如图 3-1 所示的拓扑。该案例中 5 个业务部门分别对

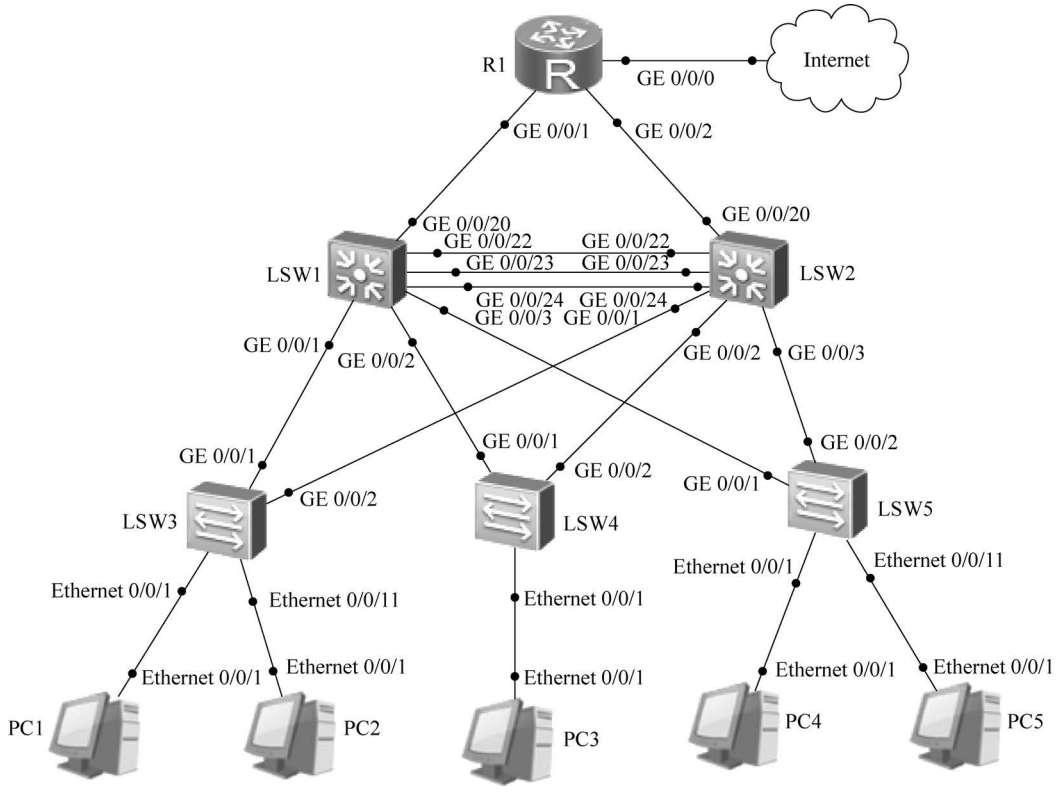

图 3-1　可靠型交换网络实例拓扑

应 VLAN 10、VLAN 20、VLAN 30、VLAN 40、VLAN 50，管理 VLAN 为 VLAN 1。PC1 属于 VLAN 10，PC2 属于 VLAN 20，PC3 属于 VLAN 30，PC4 属于 VLAN 40，PC5 属于 VLAN 50，5 台 PC 分别接入接入层交换机 LSW3、LSW4、LSW5，3 台核心交换机又以双链路分别接入核心交换机 LSW1 和 LSW2，形成双链路备份的部署方式，两台汇聚层交换机 LSW1、LSW2 通过 3 条链路相连并将这 3 条链路聚合成一条链路，以增加网络的带宽和可靠性，LSW1、LSW2 向上连接边界路由器 R1，最终通向外网。

项目整体规划

为方便项目实施和配置，对如图 3-1 所示的网络拓扑中各设备的端口（即接口）类型、VLAN 及 IP 地址规划如表 3-1 所示。

表 3-1　项目 3 接口类型、VLAN 及 IP 地址规划

设备	接口		接口类型/IP 地址	备注
R1（AR2220）	GE 0/0/1		172.16.1.1/24	连接 LSW1
	GE 0/0/2		172.16.2.1/24	连接 LSW2
核心交换机 LSW1（S5700）	二层接口	GE 0/0/1	Trunk	连接 LSW3
		GE 0/0/2	Trunk	连接 LSW4
		GE 0/0/3	Trunk	连接 LSW5
		GE 0/0/20	Access	连接路由器 R1
		GE 0/0/22 GE 0/0/23 GE 0/0/24	Eth-Trunk 1	聚合端口，连接 LSW2，允许通过所有 VLAN
	三层接口	vlanif 1	192.168.1.1	LSW1 的管理 IP 地址
		vlanif 10	192.168.10.254/24	VLAN 10 网关
		vlanif 20	192.168.20.254/24	VLAN 20 网关
		vlanif 30	192.168.30.254/24	VLAN 30 网关
		vlanif 40	192.168.40.254/24	VLAN 40 网关
		vlanif 50	192.168.50.254/24	VLAN 50 网关
		vlanif 666	172.16.1.2/24	GE 0/0/20 对应逻辑接口
核心交换机 LSW2（S5700）	二层接口	GE 0/0/1	Trunk	连接 LSW3
		GE 0/0/2	Trunk	连接 LSW4
		GE 0/0/3	Trunk	连接 LSW5
		GE 0/0/20	Access	连接路由器 R1
		GE 0/0/22 GE 0/0/23 GE 0/0/24	Eth-Trunk 1	聚合端口，连接 LSW1，允许通过所有 VLAN
	三层接口	vlanif 1	192.168.1.2	LSW2 的管理 IP 地址
		vlanif 10	192.168.10.253/24	VLAN 10 备用网关
		vlanif 20	192.168.20.253/24	VLAN 20 备用网关
		vlanif 30	192.168.30.253/24	VLAN 30 备用网关
		vlanif 40	192.168.40.253/24	VLAN 40 备用网关
		vlanif 50	192.168.50.253/24	VLAN 50 备用网关
		vlanif 666	172.16.2.2/24	GE 0/0/20 对应逻辑接口

续表

设备	接　口	接口类型/IP 地址	备　注
LSW3（S3700）	GE 0/0/1	Trunk	连接 LSW1
	GE 0/0/2	Trunk	连接 LSW2
	Ethernet 0/0/1	Access	连接 VLAN 10 的终端 PC1
	Ethernet 0/0/11	Access	连接 VLAN 20 的终端 PC2
	vlanif 1	192.168.1.3	LSW3 的管理 IP 地址
LSW4（S3700）	GE 0/0/1	Trunk	连接 LSW1
	GE 0/0/2	Trunk	连接 LSW2
	Ethernet 0/0/1	Access	连接 VLAN 30 的终端 PC3
	vlanif 1	192.168.1.4	LSW4 的管理 IP 地址
LSW5	GE 0/0/1	Trunk	连接 LSW1
	GE 0/0/2	Trunk	连接 LSW2
	Ethernet 0/0/1	Access	连接 VLAN 40 的终端 PC4
	Ethernet 0/0/11	Access	连接 VLAN 50 的终端 PC5
	vlanif 1	192.168.1.5	LSW5 的管理 IP 地址
PC1	Ethernet 0/0/1	192.168.10.1/24(网关：192.168.10.252/24)	VLAN 10 的终端
PC2	Ethernet 0/0/1	192.168.20.1/24(网关：192.168.20.252/24)	VLAN 20 的终端
PC3	Ethernet 0/0/1	192.168.30.1/24(网关：192.168.30.252/24)	VLAN 30 的终端
PC4	Ethernet 0/0/1	192.168.40.1/24 网关：192.168.40.252/24	VLAN 40 的终端
PC5	Ethernet 0/0/1	192.168.50.1/24 网关：192.168.50.252/24	VLAN 50 的终端

项目模块分析与配置

为剖析 Eth-Trunk、MSTP 和 VRRP 三大技术在项目中的作用及功能实现，从而掌握 MSTP＋VRRP＋Eth-Trunk 的典型部署方案，这里按照“总—分—总”思路对本项目如图 3-1 所示的拓扑进行分析。首先将整个项目分解为 Eth-Trunk、MSTP 和 VRRP 这 3 大功能模块分别介绍，最后将各模块整合起来对项目整体进行实施部署。下面分别介绍各模块相关知识及配置与调试方法。

3.1　模块 1：链路聚合

【教学目标】

知识目标：

- 了解链路聚合的意义。
- 掌握链路聚合的模式。
- 理解 LACP 模式的链路聚合协商过程。
- 掌握链路聚合手工模式和 LACP 模式的配置方法。

➢ 了解 iStack 和 CSS 的原理与优点。

➢ 了解链路聚合与堆叠技术常见应用场景与组网方式。

技能目标：能够正确配置链路聚合，运用链路聚合技术解决单链路故障和带宽不足的问题。

思政目标：

➢ 明确单链路面临的风险，树立维护网络安全的责任意识，保障企事业单位利益。

➢ 培养学生溯本求源的探究精神及一丝不苟的工匠精神。

3.1.1 模块拓扑

为了避免单链路故障或带宽不足给企业带来网络故障或丢包等风险，往往会在交换机之间增加备份链路。如图 3-1 在 LSW1 与 LSW2 之间连接了 3 条链路，并将 3 条链路捆绑为一条链路，使得链路带宽得到扩展，实现负载分担，而且其中某条链路故障时仍能由其他链路进行数据转发。那么链路聚合如何实现呢？

这里将 LSW1 和 LSW2 组成的链路聚合模块独立出来，介绍链路聚合的相关知识及部署。在 eNSP 中构建如图 3-2 所示的拓扑并保存。

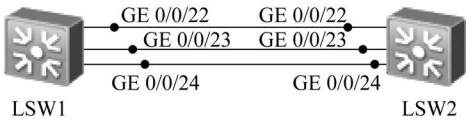

图 3-2 链路聚合拓扑

3.1.2 知识准备

1. 链路聚合的意义

链路聚合即端口聚合，通过将多个物理端口捆绑成一个逻辑端口 Eth-Trunk，以达到增加链路带宽、提高链路可靠性的目的。如图 3-2 所示，假设 LSW1 的 3 个端口都是 GE 端口，每个端口带宽是 1000Mb/s，3 个端口捆绑在一起就是 3000Mb/s，而且 3 条链路可以实现负载均衡，即使其中的一条或多条链路故障了，剩下的链路会继续转发数据，从而增强了网络的可靠性。

2. 链路聚合相关概念

(1) Eth-Trunk 端口及成员端口。将多条链路捆绑在一起形成一条逻辑链路是通过将交换机的多个物理端口加入同一个逻辑接口 Eth-Trunk 实现的，这个逻辑端口又称为聚合端口或 Eth-Trunk 端口。加入 Eth-Trunk 端口的每个物理端口被称为成员端口，每个成员端口对应的每一条链路称为成员链路。如图 3-2 所示，LSW1 和 LSW2 都把 GE 0/0/22～GE 0/0/24 加入 Eth-Trunk 1 端口，则 Eth-Trunk 1 端口为聚合端口(Eth-Trunk 端口)，GE 0/0/22、GE 0/0/23 和 GE 0/0/24 称为成员端口，3 个端口对应的 3 条链路称为成员链路。

(2) 活动端口和活动链路。执行数据转发的成员端口称为活动端口，每个活动端口对应的链路被称为活动链路。相对地，不执行数据转发的端口就称为非活动端口，非活动端口对应的链路就称为非活动链路。

(3) 聚合模式。链路聚合有两种模式：一种为纯手工配置模式，这种模式下聚合链路两端均需要手工配置，无主备协商功能；另一种为根据链路聚合控制协议，(Link Aggregation Control Protocol，LACP)进行主备协商的一种配置模式，这种模式下可以通过

配置优先级使聚合链路两端形成主备关系，然后在主设备做相应配置，备用设备会自动从主设备学习相应配置而无须手工配置。

（4）负载分担模式。Eth-Trunk 负载分担支持基于包的负载分担方式和基于流的负载分担方式。基于包的负载分担可能导致数据帧到达对端时间不一致，从而引起数据乱序，所以对于 Eth-Trunk 推荐采用基于流的负载分担方式，即同一条数据流的所有报文在同一条物理链路转发，而将不同的流分发到不同的物理链路上，这样就实现了流量在聚合组内的各物理链路上的负载分担。基于流的负载分担常见的模式有基于源 IP 地址、源 MAC 地址、目的 IP 地址、目的 MAC 地址、源目 IP 地址、源目 MAC 地址的负载分担，实际业务中用户可以根据业务流量特征选择合适的负载分担方式并做相应配置。

3. 端口聚合模式

（1）手工模式配置。

聚合链路两端 Eth-Trunk 的建立、成员端口的加入等均由手工配置，链路两端之间不使用协议进行协商。这种模式下每条成员链路均为活动链路，参与数据转发，实现负载均衡，如果某条活动链路故障，链路聚合组自动会在剩余活动链路中进行流量的负载均衡。这种方式适用于链路两端设备厂商不同或型号不兼容、不支持 LACP 模式的情况。

（2）LACP 模式。

LACP 模式是通过手工配置优先级确定主动端及主动端活动端口，然后让另一端（被动端）通过 LACP 协商根据主动端的活动端口来选择对应端口作为活动端口的一种模式。

该模式下主动端的活动端口是根据端口优先级（默认为 32 768）在成员端口中进行优选的，优先级越小越优先，端口优先级相同则按照端口编号选择活动端口。由于主动端的选举和主动端活动端口选举都是通过比较优先级竞选的，因此可以通过手工配置优先级的方式指定主动端和主动端的活动端口。活动端口数量可以通过命令配置，与主动端的活动端口相连的被动端端口会被自动确认为被动端的活动端口。活动链路发生故障时非活动链路会自动替换故障的链路，实现数据转发的不间断。LACP 模式下所有活动链路参与负载均衡。

4. 链路聚合使用场景

（1）用于在交换机之间部署多条物理链路并使用 Eth-Trunk 扩充带宽和加强可靠性。

（2）用于将服务器两个或者更多的物理网卡聚合成一个网卡组，然后与接入交换机建立链路聚合，从而扩展接入带宽，加强链路可靠性。

（3）可用于将某交换机的多个端口与堆叠系统中的不同交换机的相应端口进行链路聚合，组建高可靠的无环的网络。

（4）在防火墙双机热备场景中部署 Eth-Trunk 作为状态检测的心跳线，防止单端口、单链路故障导致状态检测错误。

5. 配置命令

（1）创建链路聚合组。

```
[Huawei] interface eth-trunk trunk-id
```

其中，trunk-id 为聚合端口编号，可以是 0～63 的一个整数。

（2）配置链路聚合模式。

```
[Huawei-Eth-Trunk1] mode {lacp-static | manual}
```

其中，lacp-static为LACP模式，manual为手工模式（默认模式，可不申明）。

注意，需要保持两端链路聚合模式一致。

（3）将端口加入链路聚合组中（以太网端口视图）。

```
[Huawei-GigabitEthernet0/0/1] eth-trunk trunk-id
```

（4）将端口加入链路聚合组中（Eth-Trunk视图）。

```
[Huawei-Eth-Trunk1] trunkport interface-type {interface-number}
```

（5）配置系统LACP优先级，用于确定主动端。

```
[Huawei] lacp priority priority
```

（6）配置端口LACP优先级，用于确定主动端的活动端口。

```
[Huawei-GigabitEthernet0/0/1] lacp priority priority
```

（7）配置最大活动端口数。

```
[Huawei-Eth-Trunk1] max active-linknumber {number}
```


视频讲解

3.1.3 配置与测试

目的：扩展LSW1和LSW2两台交换机之间的带宽，并加强链路可靠性，实现负载均衡。

策略：为LSW1和LSW2分别配置管理IP地址192.168.1.1和192.168.1.2，并分别将两台交换机的GE 0/0/22～GE 0/0/24端口加入聚合端口Eth-Trunk 1，使两台交换机能够通过Eth-Trunk 1进行通信。

说明：为加强网络安全性、可靠性，该项目中设备远程登录认证均采用AAA认证方式。

1. LSW1配置

（1）初始配置。

```
<huawei>syatem-view
[huawei]sysname LSW1
//设置Telnet远程登录的认证方式(AAA)及认证信息
[LSW1]telnet server enable
[LSW1]user-interface vty 0 4
[LSW1-ui-vty0-4]authentication-mode aaa          //配置远程登录认证模式为AAA认证模式
[LSW1-ui-vty0-4]quit
[LSW1]aaa                                        //进入AAA认证模式配置
[LSW1-aaa]local-user user1 password cipher huawei123  //设置远程登录账号和密码
[LSW1-aaa]local-user user1 service-type telnet   //设置面向远程登录用户提供的服务类型
[LSW1-aaa]local-user user1 privilege level 3     //设置远程登录用户的权限级别
[LSW1-aaa]quit
[LSW1]interface vlanif 1
[LSW1-Vlanif1]ip address 192.168.1.1 24          //配置管理IP地址
[LSW1-Vlanif1]quit
[LSW1]
```

（2）划VLAN，归端口（这里重点研究链路聚合的两种模式及其配置方法，除聚合端口Eth-Trunk外其他端口可暂不配置）。

```
//手工模式的链路聚合配置(默认模式,可不申明)
[LSW1]interface Eth-Trunk 1 //创建聚合端口Eth-Trunk 1并进入其配置视图
[LSW1-Eth-Trunk1]mode manual
```

```
[LSW1 - Eth - Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24 //给 Eth - Trunk 1 添加成员端口
[LSW1 - Eth - Trunk1] port link - type trunk
[LSW1 - Eth - Trunk1] port trunk allow - pass vlan all
[LSW1 - Eth - Trunk1] quit
```

或者

```
//LACP 模式的链路聚合配置(以下是主动端 LSW1 配置,被动端配置见 LSW2)
[LSW1]interface Eth - Trunk 1                    //创建聚合端口 Eth - Trunk 1 并进入其配置视图
[LSW1 - Eth - Trunk1]mode lacp - static          //设置链路聚合模式为 LACP 模式
[LSW1 - Eth - Trunk1]max active - linknumber 2   //配置最大活动端口数为 2
[LSW1 - Eth - Trunk1]lacp preempt enable         //使能主设备抢占功能
[LSW1 - Eth - Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24   //添加成员端口
[LSW1 - Eth - Trunk1]quit
[LSW1]lacp priority 100                          //配置系统 LACP 优先级
[LSW1]interface GigabitEthernet 0/0/22
[LSW1 - GigabitEthernet0/0/22]lacp priority 100  //配置端口 LACP 优先级
[LSW1 - GigabitEthernet0/0/22]quit
[LSW1]interface GigabitEthernet 0/0/23
[LSW1 - GigabitEthernet0/0/23]lacp priority 100  //配置端口 LACP 优先级
[LSW1 - GigabitEthernet0/0/23]quit
[LSW1]interface GigabitEthernet 0/0/24
[LSW1 - GigabitEthernet0/0/24]lacp priority 100  //配置端口 LACP 优先级
[LSW1 - GigabitEthernet0/0/24]quit
```

```
[LSW1]quit
< LSW1 > save
```

2. LSW2 配置

(1) 初始配置。

```
< huawei > syatem - view
[huawei]sysname LSW2
```

```
//设置 Telnet 远程登录的认证方式(AAA)及认证信息
[LSW2]telnet server enable
[LSW2]user - interface vty 0 4
[LSW2 - ui - vty0 - 4]authentication - mode aaa
[LSW2 - ui - vty0 - 4]quit
[LSW2]aaa
[LSW2 - aaa]local - user user1 password cipher huawei123
[LSW2 - aaa]local - user user1 service - type telnet
[LSW2 - aaa]local - user user1 privilege level 3
[LSW2 - aaa]quit
```

```
[LSW2]interface vlanif 1
[LSW2 - Vlanif1]ip address 192.168.1.2 24   //配置管理 IP 地址
[LSW2 - Vlanif1]quit
```

(2) 划 VLAN,归端口(这里重点研究链路聚合,除 Eth-Trunk 外其他端口可暂不配置)。

(3) 链路聚合配置(两种模式选择一种即可,所选模式要与对端 LSW1 相同)。

```
//手工模式的链路聚合配置(默认模式,不用申明)
[LSW2]interface Eth - Trunk 1 //创建聚合端口 Eth - Trunk 1 并进入其配置视图
[LSW2 - Eth - Trunk1]mode manual
[LSW2 - Eth - Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24 //给 Eth - Trunk 1 添加成员端口
[LSW2 - Eth - Trunk1] port link - type trunk
[LSW2 - Eth - Trunk1] port trunk allow - pass vlan all
[LSW2 - Eth - Trunk1] quit
```

或者

```
//LACP模式的链路聚合被动端配置
[LSW2]interface Eth-Trunk 1                          //创建聚合端口 Eth-Trunk 1并进入其配置视图
[LSW2-Eth-Trunk1]mode lacp-static                    //设置链路聚合模式为LACP模式
[LSW2-Eth-Trunk1]max active-linknumber 2             //配置最大活动端口数为2
[LSW2-Eth-Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24    //添加成员端口
[LSW2-Eth-Trunk1]quit
[LSW2]quit
<LSW2>save
```

3. 测试

用 LSW2 ping LSW1 的管理地址 192.168.1.1，能够 ping 通，说明两端通信正常。

在 LSW1 上用 display eth-trunk 1 命令查看 Eth-Trunk 相关信息，也可以看到该聚合端口当前状态正常(为 Up)，包含 3 个成员：GigabitEthernet 0/0/22～GigabitEthernet 0/0/24，如图 3-3 所示。

在 LSW1 上用 display interface eth-trunk 1 命令查看 Eth-Trunk 相关信息，可以看到该聚合端口当前状态正常为 Up，包含 3 个成员：GigabitEthernet 0/0/22～GigabitEthernet 0/0/24，如图 3-4 所示。

```
<LSW1>display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL          Hash arithmetic: According to
Least Active-linknumber: 1   Max Bandwidth-affected-linknum
Operate status: up           Number Of Up Port In Trunk: 3
--------------------------------------------------------
PortName                     Status      Weight
GigabitEthernet0/0/22        Up          1
GigabitEthernet0/0/23        Up          1
GigabitEthernet0/0/24        Up          1
```

图 3-3　查看 Eth-Trunk 信息

```
<LSW1>display interface eth-trunk  1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According
rent BW: 3G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware
Current system time: 2022-12-24 19:31:24-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------------
PortName                     Status      Weight
--------------------------------------------------------
GigabitEthernet0/0/22        UP          1
GigabitEthernet0/0/23        UP          1
GigabitEthernet0/0/24        UP          1
--------------------------------------------------------
The Number of Ports in Trunk : 3
The Number of UP Ports in Trunk : 3
```

图 3-4　查看 LSW1 的 Eth-Trunk 1 信息

在 LSW2 上用 display interface eth-trunk 1 命令查看 Eth-Trunk 相关信息，也可以看到该聚合端口当前状态正常为 Up，包含 3 个成员：GigabitEthernet 0/0/22～GigabitEthernet 0/0/24，如图 3-5 所示。

```
<LSW2>display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According
rent BW: 3G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware
Current system time: 2022-12-25 08:13:32-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------------
PortName                     Status      Weight
--------------------------------------------------------
GigabitEthernet0/0/22        UP          1
GigabitEthernet0/0/23        UP          1
GigabitEthernet0/0/24        UP          1
--------------------------------------------------------
The Number of Ports in Trunk : 3
The Number of UP Ports in Trunk : 3
```

图 3-5　查看 LSW2 的 Eth-Trunk 1 信息

3.1.4 知识拓展——堆叠/集群

1. 堆叠

堆叠即多台支持堆叠(iStack)特性的盒式交换机通过堆叠线缆连接在一起,从逻辑上变成一台交换设备,作为一个整体参与数据转发的技术,其工作原理如图 3-6 所示。

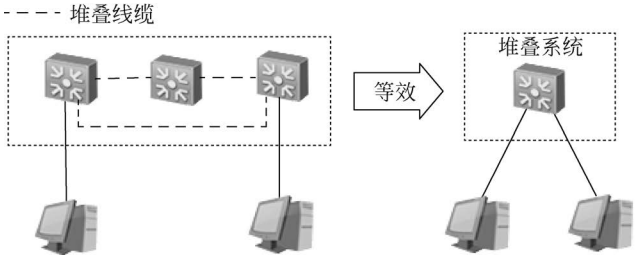

图 3-6 堆叠工作原理

2. 集群

将两台支持集群(Cluster LSWitch System,CSS)特性的框式交换机组合在一起,从逻辑上组合成一台交换设备的技术,其工作原理如图 3-7 所示。

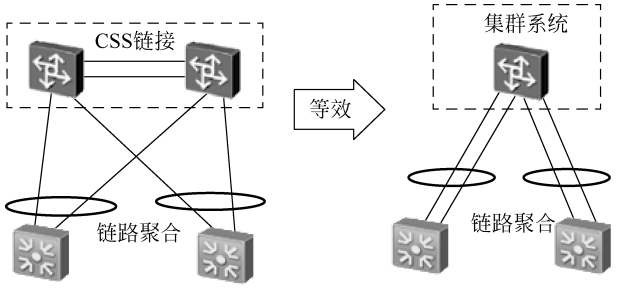

图 3-7 集群工作原理

堆叠和集群将多台或两台交换机逻辑上组合成一台交换机,不仅可以简化运维,方便管理,而且在一台设备发生故障时,其他设备可以接管转发、控制平台,避免了单点故障引发的风险,还可以在接入层设备上使用堆叠扩展端口及带宽。堆叠和集群与 Eth-Trunk 结合使用可以实现跨设备的链路聚合,消除环路,简化配置。在设计网络架构时要仔细分析需求、科学部署网络,使网络效能达到最优,保障企事业单位利益。

3.2 模块 2:生成树与快速生成树

【教学目标】

知识目标:

- 了解二层环路的危害。
- 掌握生成树基本概念。
- 理解生成树的工作原理,了解其应用场景。
- 理解快速生成树对于生成树的改进。
- 掌握生成树与快速生成树的配置方法。

技能目标：能对存在简单物理环路的交换网络部署生成树或快速生成树。

思政目标：

- 明确二层环路面临的风险，明确生成树的稳定性的重要性，树立维护网络安全稳定的责任意识，保障生成树的稳定和可靠，维护企事业单位利益。
- 培养学生溯本求源的探究精神及一丝不苟的工匠精神。

3.2.1 模块拓扑

如图 3-1 所示，每台接入层交换机通过 GE 0/0/1 口上行接入上游设备 LSW1，为了解决单点故障和单链路故障给企业带来网络故障或丢包等风险，增加了备份设备 LSW2，并在每台接入层交换机与 LSW2 之间建立了备份链路，使得下游各终端经接入层交换机如 LSW3 向上游 LSW1 转发的数据可以经 LSW3—LSW2 链路转发。由于设备备份和链路备份后会在 LSW1、LSW2、LSW3 之间形成环路，会导致严重的网络拥塞等问题。为了解决这些问题，应在构成环路的各台交换机部署生成树，从逻辑上消除环路，保证数据的高效转发。这里为了便于生成树工作原理的分析，将 LSW1、LSW2、LSW3 及之间的链路和连接的终端构成的模块独立出来，形成如图 3-8 所示的拓扑。

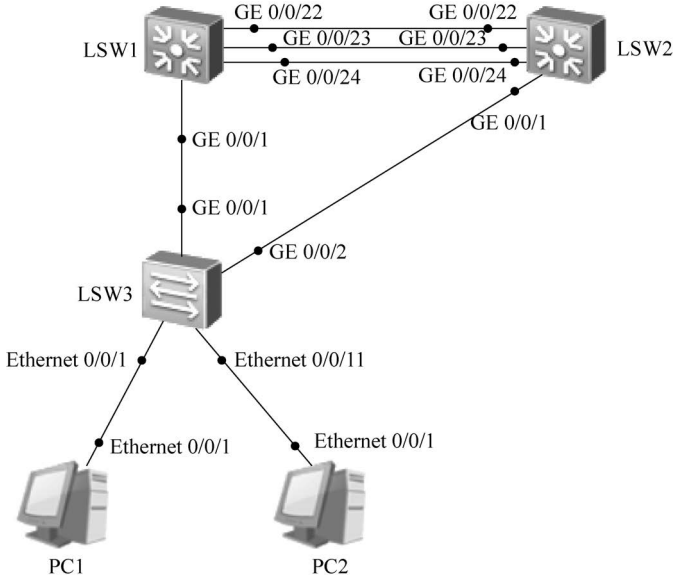

图 3-8　生成树＋Eth-Trunk 拓扑

注意，该拓扑中 LSW1 和 LSW2 之间有 3 条链路，所以该模块的配置应在模块 1 链路聚合的基础上进行，把 LSW1 和 LSW2 之间看成用 Eth-Trunk 端口连接的单链路，再来研究生成树的应用与配置。通过该模块可以学习链路聚合和生成树的综合应用，在实践中这两种技术也往往是结合使用的。如果仅仅是研究生成树工作原理，也可以在 LSW1 和 LSW2 之间仅保留一条链路。

3.2.2 知识准备

1. 广播风暴

在传统的交换网络中，网络设备之间通过单条链路进行连接，当某个节点或某条链路发

生故障时将导致严重的网络故障，解决单点故障或单链路故障的方法是在网络中提供冗余链路及冗余设备，但是交换网络中的冗余链路容易引发广播风暴、数据帧重复、MAC 地址表振荡等问题，消耗大量 CPU、内存及带宽资源，使网络性能严重下降，甚至导致网络瘫痪。

如图 3-9 所示，PC1 将一个广播帧发送到交换机 LSW1，LSW1 收到广播帧后会向除接收端口之外的所有端口如 GE 0/0/23 和 GE 0/0/24 转发，这样交换机 LSW2 就会分别从 GE 0/0/23 和 GE 0/0/24 收到 LSW1 转发的广播帧，于是它将从 GE 0/0/23 收到的广播帧再广播给 GE 0/0/24 和 PC2，同时还将从 GE 0/0/24 收到的广播帧再广播给 GE 0/0/23 和 PC2，这时 PC2 会重复收到同样的帧，而 LSW1 又会收到 LSW2 广播回来的广播帧，然后对每个广播帧继续从除接收端口之外的所有端口广播出去，这样就会导致广播帧在 LSW1 和 LSW2 之间不停地转发，就会形成可怕的广播风暴，引发 MAC 地址表振荡。

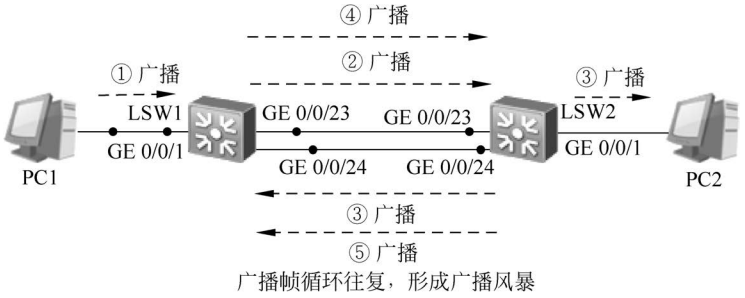

图 3-9　广播风暴示意

提示：可用两三台交换机构建有环路的网络并关闭生成树协议，然后用所连接的终端进行 ping 测试，抓取环路上的报文（发现数量庞大，也可能不久后链路被拥塞），体验广播风暴的危害。

2. 生成树概述

生成树协议（Spanning Tree Protocol，STP）可以在物理上存在环路的网络上使用生成树算法计算出逻辑上无环路的树型结构网络，并使树型结构网络之外的链路处于备用状态（暂时通过阻塞该链路上某个端口阻止数据经过该链路），这样网络上任何两个节点之间不论物理上有几条链路相通，但在逻辑上都只保留一条链路，从而可以避免物理环路引发的广播风暴等问题。

生成树协议的计算及阻塞相应端口等处理过程结束后，网络中的环路被消除，网络会趋于稳定状态，这个过程称为收敛。网络拓扑发生变更或网络局部故障时，会重新引发生成树计算和收敛过程，原来阻塞的端口可能被启用，原来备份的链路或设备可能成为工作链路或工作设备。

3. 生成树协议的工作过程

生成树的计算收敛过程主要经历了 4 步：第 1 步，选举根桥；第 2 步，在每个非根桥上选举一个根端口；第 3 步，在每条链路上选举一个指定端口；第 4 步，阻塞非根、非指定端口。下面分别介绍各步的处理机制。

第 1 步：选举根桥（Root Bridge，RB）。

网络内具有最小桥 ID（BID）的交换机将被选举为该生成树的根桥（即根交换机），作为生成树的树根。

桥ID由桥优先级和MAC地址两部分组成，竞选根桥时先比较各交换机桥ID的优先级，一个网络中桥ID优先级最小的交换机会被选举为根桥，如果所有交换机桥ID相同（每台交换机默认桥ID均为32 768）则比较MAC地址，MAC地址最小的会被选为根桥。桥优先级必须为4096的倍数，默认值为32 768，最小为0，最大值为61 440。在一个网络中，处于核心位置而且转发性能较强的交换机往往是理想的根桥，但如果让交换机自由选举，因优先级均相同，往往会依据MAC地址选举，这样选举出来的根桥通常是不理想的。所以在实际中，往往通过手工修改桥优先级为较小值使某交换机成为根桥，或直接用命令指定根桥，也可以用类似的方法指定备用根桥。

根桥的选举是通过交换机相互交换配置BPDU（Bridge Protocol Data Unit，网桥协议数据单元），比较配置BPDU中携带的桥ID的大小实现的。每台交换机启动后，会向所在的网络广播配置BPDU，其中携带了根ID和自己的桥ID（此时暂以自己的桥ID作为根ID），供交换机相互比较桥ID的大小，如果交换机收到的配置BPDU中的桥ID比自己的桥ID大，就将自己的桥ID作为根ID填到自己的配置BPDU中继续向网络中发送；如果交换机收到的配置BPDU中的桥ID比自己的桥ID小，就将该BPDU中的桥ID作为根ID填到自己的BPDU中继续广播……最终整个网络中最小桥ID会被填到根ID字段，具有最小桥ID的交换机会被选为根桥。

安全警示：网络收敛后，如果有桥ID更小的交换机接入网络，或者有攻击者故意修改桥ID为更小并接入网络，新加入的交换机就会把自己当作根桥向网络中广播配置BPDU，这时网络会重新选举根桥，将会影响网络的稳定性，所以除非实际需要更换根桥，否则应采取相应的保护根桥的措施，如将相应端口开启BPDU防护功能（参见3.2.4节），维护网络的稳定性。

第2步：选举根端口（Root Port，RP）。

根端口即非根交换机上所有端口中去往根桥路径开销最小的端口。每个非根桥上均须选举一个根端口，且仅可选一个根端口，根桥上没有根端口。

路径开销（Path Cost）即一个网络节点到另一个网络节点的整条链路中每段链路的开销之和。每段链路的开销是由链路的端口开销（Cost）决定的。端口开销与端口速率和工作模式有关，还与交换机使用的STP Cost计算标准有关。华为交换机支持3种端口开销计算标准，以便与其他厂商设备兼容，如在IEEE 802.1t标准下，速率为1000Mb/s的端口在全双工（Full-Duplex）模式下端口开销值为20 000。端口开销值可以通过命令修改，其默认值请参考表3-2。

表3-2　不同端口默认Cost值参考

端口速率	端口模式	STP开销（默认值）		
		IEEE 802.1d—1998标准	IEEE 802.1t—2001标准	华为计算方法
100Mb/s	Half-Duplex	19	200 000	200
	Full-Duplex	18	199 999	199
1000Mb/s	Full-Duplex	4	20 000	20
10Gb/s	Full-Duplex	2	2000	2
40Gb/s	Full-Duplex	1	500	1
100Gb/s	Full-Duplex	1	200	1

根路径开销(Root Path Cost,RPC)即非根交换机的某一个端口到达根桥的“成本”,其值等于从根桥到该设备沿途所有入方向端口的 Cost 值的累加。如图 3-10 所示,LSW3 从 GE 0/0/3 端口到达根桥 LSW1 的 RPC 等于端口①的 Cost 值加上端口②的 Cost 值。

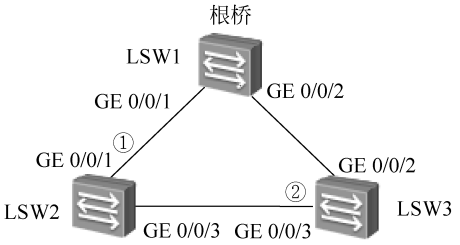

图 3-10　根路径开销计算示意

如果非根交换机上的两个端口的 RPC 相等,可以继续比较发送端桥 ID,发送端桥 ID 小的会被选举为根端口(也可以使用命令修改端口的 Cost 值以改变相应端口的 RPC,使根端口的选择更符合网络规划)。如果发送端桥 ID 也相同,则比较发送端的端口 ID,发送端的端口 ID 小的会被选为根端口。

端口 ID 由端口优先级和端口号组成,端口优先级为 16 的倍数,默认值为 128,可以通过命令修改端口优先级的值。端口优先级越小越优先,端口优先级相同则端口号越小越优先。

如上所述,选择根端口依据的顺序如下。

(1) 根路径开销最小。

(2) 发送端桥 ID 最小。

(3) 发送端口 ID 最小。

第 3 步:选举指定端口(Designated Port,DP)。

每条链路上都要选择一个指定端口,选择指定端口依据的顺序如下。

(1) 根路径开销最小。

(2) 所在交换机桥 ID 最小。

(3) 发送端口 ID 最小。

由于根桥上各端口的根路径开销为 0,因此根桥上的所有端口均为指定端口。

第 4 步:阻塞非根、非指定接口。

以上选举过程中,既没被选举为根端口也没被选举为指定端口的端口将会被阻塞,那么该端口所在链路也就被阻塞了,于是网络中的二层环路就此被消除,形成逻辑上无环的树型网络。

4. 生成树的端口状态

生成树端口有 5 种状态,如表 3-3 所示。

表 3-3　生成树端口状态

端口状态名称	端口状态描述
禁用(Disable)	该端口因故障或被设定为 Down,不能收发 BPDU,也不能收发业务数据帧
阻塞(Blocking)	该端口被 STP 阻塞。处于阻塞状态的端口不能发送 BPDU,不能收发业务数据帧,也不会进行 MAC 地址学习,但是会持续侦听 BPDU,该状态默认会停留 20s
监听(Listening)	当端口处于该状态时,表明 STP 初步认定该端口为根端口或指定端口,但端口依然处于 STP 计算的过程中,此时端口可以收发 BPDU,但是不能收发业务数据帧,也不会进行 MAC 地址学习,该状态默认会停留 15s

续表

端口状态名称	端口状态描述
学习(Learning)	当端口处于该状态时,会侦听业务数据帧(但是不能转发业务数据帧),并且在收到业务数据帧后进行 MAC 地址学习,该状态默认会停留 15s
转发(Forwarding)	处于该状态的端口可以正常地收发业务数据帧,也会进行 BPDU 收发。端口的角色需是根端口或指定端口才能进入转发状态

交换机的端口状态转换过程如图 3-11 所示。

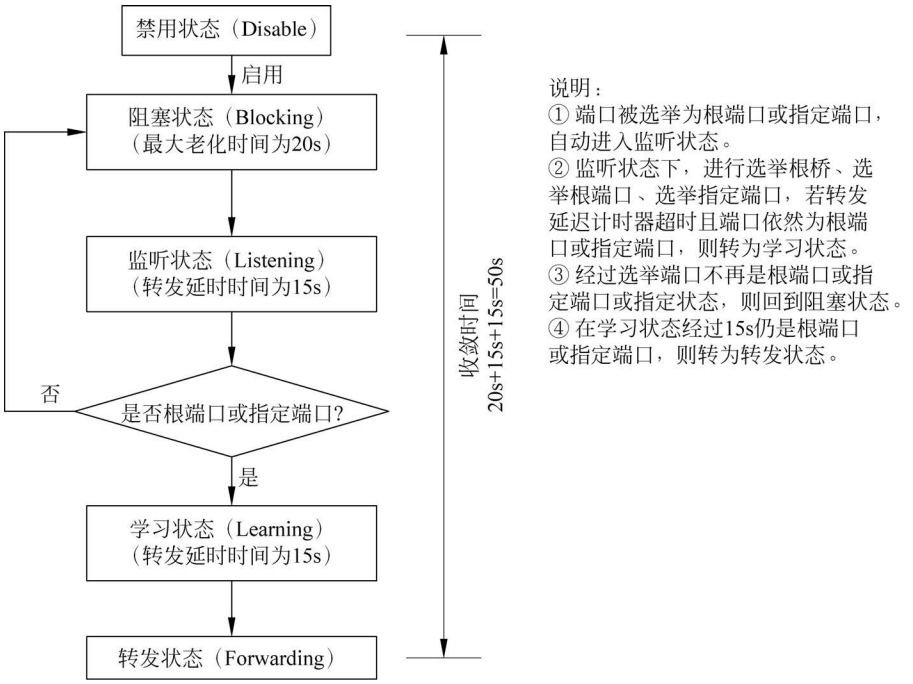

图 3-11　交换机的端口状态转换过程

5. 生成树拓扑变化

在部署生成树后,交换机之间通过根桥、根端口、指定端口的选举最后阻塞相应端口消除逻辑上的环路,使网络收敛。当网络收敛后,生成树中所有交换机端口都处于转发状态或阻塞状态,转发端口接收和发送用户数据和 BPDU,阻塞端口则只接收 BPDU。

当生成树状态发生变化时,最先感知到变化的交换机还会周期性发送 TCN BPDU(拓扑变更通告),上游交换机收到 TCN BPDU 后继续向上游传递 TCN BPDU,直到根交换机收到 TCN BPDU,然后将配置 BPDU 的 Flags 字段的 TC(拓扑变更)位置 1 后发往下游交换机,通知下游交换机把 MAC 地址表项的老化时间由默认的 300s 修改为 15s,于是下游交换机 15s 后 MAC 地址表项会被自动清除,然后重新开始 MAC 表项的学习。

6. RSTP 对 STP 的改进

STP 收敛速度慢,也不能及时响应网络拓扑的变化。RSTP 对 STP 进行了优化,收敛速度快,而且能够兼容 STP。以下是 RSTP 对 STP 的改进分析。

(1) RSTP 引入了新的端口角色——替代端口和备份端口,使非根交换机的根端口或指定端口失效时,均能够快速切换,秒级收敛。

(2) RSTP 还根据端口是否转发用户流量和学习 MAC 地址把 STP 的 5 种端口状态缩减为 3 种：Discarding、Learning 和 Forwarding，如表 3-4 所示，从而缩减了端口状态转换时延。而且，RSTP 还引入了边缘端口的概念，使交换机连接终端的端口在启用后无须等待直接进入转发状态。

(3) RSTP 改进了配置 BPDU 格式，其 Flags 字段能够表名端口的角色，配置 BPDU 还使用了更短的超时计时，发送方式也进行了改进。

(4) 相比 STP，RSTP 对拓扑变化的处理机制进行了改进，能更快地响应拓扑变更。

表 3-4　STP 与 RSTP 端口状态比较

STP 端口状态	RSTP 端口状态	端口在拓扑中的角色
Forwarding	Forwarding	包括根端口、指定端口
Learning	Learning	包括根端口、指定端口
Listening	Discarding	包括根端口、指定端口
Blocking		包括 Alternate 端口、Backup 端口
Disable		包括 Disable 端口

7. 配置命令

(1) 配置生成树工作模式。

```
[Huawei] stp mode { stp | rstp | mstp }
```

说明：交换机支持 STP、RSTP 和 MSTP(Multiple Spanning Tree Protocol)3 种生成树工作模式，默认情况工作在 MSTP 模式。

(2) 配置根桥和备份根桥。

```
[Huawei] stp root primary
[Huawei] stp root secondary
```

说明：配置根桥后该设备优先级数值自动为 0，配置备份根桥后该设备优先级数值自动为 4096，并且不能更改设备优先级。

(3) 配置交换机的 STP 优先级。

```
[Huawei] stp priority priority
```

说明：优先级数值须为 4096 的倍数，最小为 0。

(4) 配置端口路径开销。

```
[Huawei] stp pathcost-standard {dot1d-1998 |dot1t |legacy }
```

说明：配置端口路径开销计算方法。默认情况下，路径开销值的计算方法为 IEEE 802.1t(dot1t)标准。同一网络内所有交换机的端口路径开销应使用相同的计算方法。

```
[Huawei-GigabitEthernet0/0/1] stp cost cost
```

说明：设置当前端口的路径开销值。

(5) 配置端口优先级。

```
[Huawei-intf] stp priority priority
```

(6) 启用 STP/RSTP/MSTP。

```
[Huawei] stp enable
```

(7) 配置边缘端口实例。

```
[LLSW1 - GigabitEthernet0/0/1]stp edged - port enable
```

(8) 生成树查看命令。

```
[Huawei] display stp [brief]
```


视频讲解

3.2.3 配置与测试

注意该模块拓扑 LSW1 和 LSW2 之间有 3 条链路,需要在 LSW1 和 LSW2 上配置链路聚合,所以这里保留模块 1 的链路聚合配置,把 LSW1 和 LSW2 之间看成用 Eth-Trunk 端口连接的单链路。同时这里也给出了 LSW1 和 LSW2 之间仅保留一条链路(用 GigabitEthernet 0/0/24 端口相连)的配置。

这里仅介绍 RSTP 配置,STP 配置与 RSTP 仅仅模式不同,可参照 RSTP 配置,这里不做介绍。

1. LSW1 配置

(1) 初始配置:见模块 1,这里从略。

(2) 基础配置。

```
< huawei > system - view
[ huawei]sysname LSW1
[LSW1]vlan batch 10 20
//手工链路聚合,从下一行起共 4 行
[LSW1]interface Eth - Trunk 1
[LSW1 - Eth - Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24
[LSW1 - Eth - Trunk1] port link - type trunk
[LSW1 - Eth - Trunk1] port trunk allow - pass vlan all
[LSW1 - Eth - Trunk1] quit
```

```
//如果 LSW1 和 LSW2 间仅用 GE 0/0/24 口做单链路连接,可用以下 4 行命令
[LSW1]interface GigabitEthernet 0/0/24 //单链路端口配置
[LSW1 - GigabitEthernet0/0/24]port link - type trunk
[LSW1 - GigabitEthernet0/0/24]port trunk allow - pass vlan all
[LSW1 - GigabitEthernet0/0/24]quit
```

```
[LSW1]interface GigabitEthernet 0/0/1
[LSW1 - GigabitEthernet0/0/1]port link - type trunk
[LSW1 - GigabitEthernet0/0/1]port trunk allow - pass vlan all
[LSW1 - GigabitEthernet0/0/1]quit
[LSW1]interface vlanif 1
[LSW1 - Vlanif1]ip address 192.168.1.254 24
[LSW1 - Vlanif1]quit
[LSW1]interface vlanif 10
[LSW1 - Vlanif10]ip address 192.168.10.254 24
[LSW1 - Vlanif10]quit
[LSW1]interface vlanif 20
[LSW1 - Vlanif20]ip address 192.168.20.254 24
[LSW1 - Vlanif20]quit
[LSW1]
```

(3) RSTP 配置。

```
[LSW1]stp mode rstp                      //选择快速生成树模式
[LSW1]stp priority 4096                  //配置生成树优先级
[LSW1]stp pathcost - standard dot1t      //配置路径开销计算标准
[LSW1]interface GigabitEthernet 0/0/1
```

```
[LSW1-GigabitEthernet0/0/1]stp cost 100              //设置端口开销
[LSW1-GigabitEthernet0/0/1]stp port priority 16     //配置端口优先级
[LSW1-GigabitEthernet0/0/1]quit
[LSW1]
```

2. LSW2 配置

(1) 初始配置(见模块 1,这里从略)。

(2) 基础配置。

```
<huawei>system-view
[huawei]sysname LSW2
[LSW2]vlan batch 10 20
//手工链路聚合,从下一行起共 4 行
[LSW2]interface Eth-Trunk 1
[LSW2-Eth-Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24
[LSW2-Eth-Trunk1] port link-type trunk
[LSW2-Eth-Trunk1] port trunk allow-pass vlan all
[LSW2-Eth-Trunk1] quit
//或(单链路适用,从下一行起共 4 行)
[LSW2]interface GigabitEthernet 0/0/24
[LSW2-GigabitEthernet0/0/24]port link-type trunk
[LSW2-GigabitEthernet0/0/24]port trunk allow-pass vlan all
[LSW2-GigabitEthernet0/0/24]quit
[LSW2]interface GigabitEthernet 0/0/1
[LSW2-GigabitEthernet0/0/1]port link-type trunk
[LSW2-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW2-GigabitEthernet0/0/1]quit
[LSW2]interface vlanif 1
[LSW2-Vlanif1]ip address 192.168.1.253 24
[LSW2-Vlanif1]quit
[LSW2]
```

(3) RSTP 配置。

```
[LSW2]stp mode rstp                    //选择快速生成树模式
[LSW2]stp pathcost-standard dot1t //配置路径开销计算标准
[LSW2]
```

3. LSW3 配置

(1) 初始配置(见模块 1,这里从略)。

(2) 基础配置。

```
<huawei>system-view
[huawei]sysname LSW3
[LSW3]vlan batch 10 20
[LSW3]interface GigabitEthernet 0/0/1
[LSW3-GigabitEthernet0/0/1]port link-type trunk
[LSW3-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/1]quit
[LSW3]interface GigabitEthernet 0/0/2
[LSW3-GigabitEthernet0/0/2]port link-type trunk
[LSW3-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/2]quit
[LSW3]port-group group-member Ethernet 0/0/1 to Ethernet 0/0/10 //该 10 个端口加入 VLAN 10
[LSW3-port-group]port link-type access
[LSW3-port-group]port default vlan 10
[LSW3-port-group]stp edged-port enable                    //开启边缘端口
```

```
[LSW3-port-group]quit
[LSW3]port-group group-member Ethernet 0/0/11 to Ethernet 0/0/20    //该10个端口加入VLAN 20
[LSW3-port-group]port link-type access
[LSW3-port-group]port default vlan 20
[LSW3-port-group]stp edged-port enable                              //开启边缘端口
[LSW3-port-group]quit
[LSW3]
```

(3) RSTP配置。

```
[LSW3]stp mode rstp
[LSW3]stp pathcost-standard dot1t                //定义路径开销计算标准为dot1t
[LSW3]interface Ethernet 0/0/1
[LSW3-Ethernet0/0/1]stp edged-port enable        //将端口配置为边缘端口
[LSW3-Ethernet0/0/1]quit
[LSW3]interface Ethernet 0/0/11
[LSW3-Ethernet0/0/11]stp edged-port enable       //将端口配置为边缘端口
[LSW3-Ethernet0/0/11]quit
[LSW3]
```

4. 测试

(1) 查看快速生成树状态。

命令1：

```
[LSW1]display stp
```

查看结果如图3-12所示，可以看到LSW1的MAC地址和根桥的MAC地址相同，说明LSW1被选为根桥。

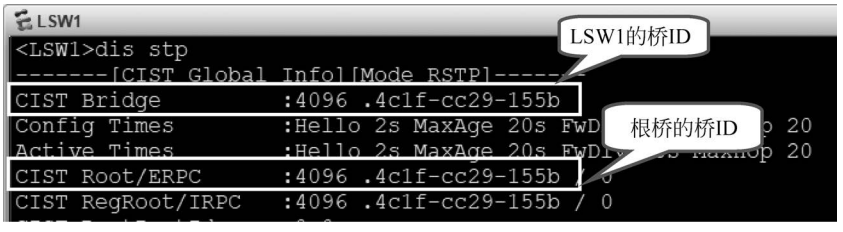

图3-12 交换机LSW1的桥ID和根桥ID

命令2：

```
[LSW1]display stp brief
```

查看结果如图3-13所示，可以看到LSW1各端口角色均为指定端口(DESI)，均处于转发状态(Forwarding)，这也是根桥的特征。

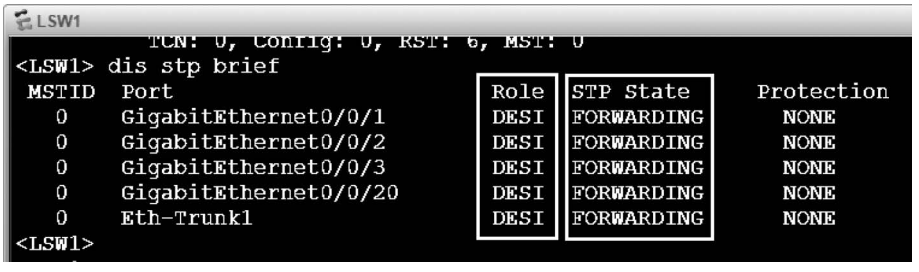

图3-13 交换机LSW1的生成树摘要信息

其他交换机可用同样的方法，查看桥的角色、端口的角色和状态。

(2) 测试链路选用情况。

在 LSW3 与 LSW1 和 LSW2 连接的两个端口 GE 0/0/1 和 GE 0/0/2 分别开启 Wireshark 抓包功能，然后用 PC1 ping 192.168.1.1，发现 GE 0/0/1 口对应的抓包器捕获到了 ICMP 数据流，如图 3-14 所示，而 GE 0/0/2 口对应的抓包器并没有捕获到 ICMP 数据流，说明此时没有链路故障的情况下，终端发往上游的数据是走 LSW3—LSW1 这条路径的。

No.	Time	Source	Destination	Protocol	Length	Info
3121	868.093000	192.168.10.1	192.168.1.1	ICMP	78	Echo (ping) request
3122	868.109000	192.168.1.1	192.168.10.1	ICMP	78	Echo (ping) reply
3123	868.343000	IETF-VRRP-VRID_28	Broadcast	ARP	64	ARP Announcement for
3124	868.515000	192.168.30.254	224.0.0.18	VRRP	64	Announcement (v2)
3125	868.703000	192.168.10.254	224.0.0.18	VRRP	64	Announcement (v2)
3126	868.796000	192.168.20.254	224.0.0.18	VRRP	64	Announcement (v2)
3127	869.140000	192.168.10.1	192.168.1.1	ICMP	78	Echo (ping) request
3128	869.156000	192.168.1.1	192.168.10.1	ICMP	78	Echo (ping) reply
3129	869.218000	HuaweiTe_29:15:5b	Spanning-tree-(for-…	STP	151	MST. Root = 32768/0/4
3130	869.515000	192.168.30.254	224.0.0.18	VRRP	64	Announcement (v2)
3131	869.703000	192.168.10.254	224.0.0.18	VRRP	64	Announcement (v2)
3132	869.796000	192.168.20.254	224.0.0.18	VRRP	64	Announcement (v2)
3133	870.171000	192.168.10.1	192.168.1.1	ICMP	78	Echo (ping) request
3134	870.203000	192.168.1.1	192.168.10.1	ICMP	78	Echo (ping) reply
3135	870.515000	192.168.30.254	224.0.0.18	VRRP	64	Announcement (v2)

图 3-14　抓取到的 LSW3—LSW1 的数据流

现在模拟故障，将 LSW3 的 GE 0/0/1 端口用 shutdown 命令关闭，再在 LSW3 与 LSW2 连接的端口 GE 0/0/2 开启 Wireshark 抓包功能，然后再用 PC1 ping 192.168.1.1 (LSW1 的管理地址)，发现 GE 0/0/2 端口对应的抓包器捕获到了 ICMP 数据流，说明此时终端发往上游的数据是走了 LSW3—LSW2—LSW1 这条备用路径的。

用 undo shutdown 命令重新启用 LSW3 的 GE 0/0/1 端口，再次在 LSW3 与 LSW1 和 LSW2 连接的两个端口 GE 0/0/1 和 GE 0/0/2 分别开启 Wireshark 抓包功能，然后用 PC1 ping 192.168.1.1，发现 ICMP 数据流又选择了 LSW3—LSW1 这条路径作为最优路径。还可以用 PC1 ping PC2，发现数据流走了 LSW3—LSW1—LSW3 的路径，说明这时两台 PC 是经过三层路由访问的，而二层是隔离的。

3.2.4　知识拓展——生成树的安全防御

1. BPDU 保护

正常情况下，交换机与终端相连的端口只要设置为边缘端口，就不会接收 BPDU 报文。但是，如果有攻击者伪造 BPDU 攻击交换设备，当伪造的 BPDU 发送到交换机边缘端口时，交换机会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络的振荡，严重影响网络的正常运行。同理，攻击者也可伪造 TCN BPDU 报文恶意攻击交换设备，交换设备收到很多 TCN BPDU 报文后会频繁地删除 MAC 地址表项或 ARP 地址表项而重新学习相应表项，也会造成网络的振荡，同时会给交换设备带来很大的负担。针对这些攻击可采用配置 BPDU 保护来进行防御。

BPDU 保护配置的示例如下：

```
[huawei]stp bpdu-protection                          //全局开启 BPDU 保护
[huawei]interface GigabitEthernet 0/0/1              //进入端口视图
```

```
[huawei-GigabitEthernet0/0/1]stp edged-port enable  //将端口配置为边缘端口
[huawei-GigabitEthernet0/0/1]stp bpdu-filter enable //使能端口过滤 BPDU 的功能
```

2. 环路保护

由于链路故障或拥塞导致根端口及阻塞端口收不到上游交换设备发送的 BPDU 报文时，生成树中的交换机就会重新选择根端口，原来的阻塞端口会迁移到转发状态，这时没有端口处于阻塞状态，从而可能导致产生环路。这种情况下，为防止环路发生，可部署环路保护功能。

在启用了环路保护功能后，如果根端口及阻塞端口长时间收不到来自上游交换设备发送的 BPDU 报文，会向网管发送通知消息，使阻塞端口转换为指定端口时，依然保持阻塞状态，直到链路不再拥塞或链路故障恢复。

3.3 模块 3：虚拟路由冗余协议

【教学目标】

知识目标：

- 了解 VRRP 应用场景。
- 理解 VRRP 工作原理。
- 掌握 VRRP 基本配置。

技能目标：能够在相应场景正确配置 VRRP，解决网关单点故障的问题。

思政目标：

- 明确单网关设备面临的风险，树立维护网络安全的责任意识，采取必要措施保障企事业单位利益。
- 培养学生溯本求源的探究精神及一丝不苟的工匠精神。

3.3.1 模块拓扑

在图 3-1 中，为了避免单网关故障给企业带来网络故障风险，该项目将 LSW1 和 LSW2 两台 RS 交换机作为各 VLAN 终端的主备网关。VRRP（虚拟路由冗余协议）是这种场景下常用的协议，这里仅以 VLAN 10 为例，分析 VRRP 的工作原理。为方便研究，由图 3-1 中把主备网关 LSW1 和 LSW2 与上下游设备 R1、PC1 及之间的链路组成的模块独立出来，形成如图 3-15 所示的拓扑，该拓扑在配置 VRRP 时也结合了链路聚合、生成树的配置，便于掌握 3 个功能模块的综合应用，而这 3 种技术结合使用在实际中也是比较多见的，有较大的借鉴意义。

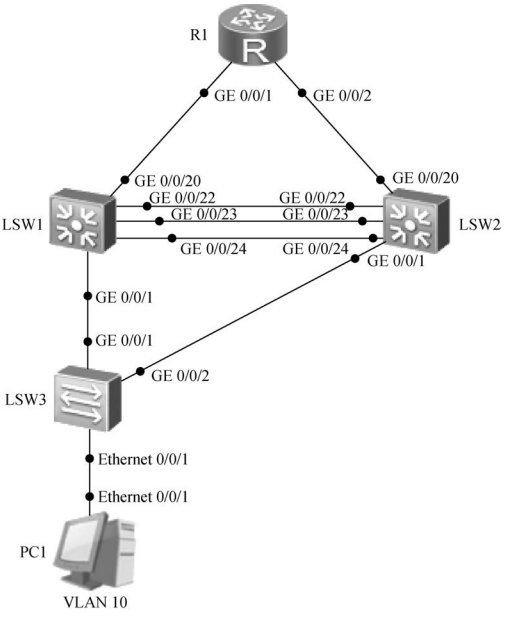

图 3-15　VRRP＋链路聚合＋生成树应用示例

在正常的网络状态下，VLAN 10 的终端

均以 LSW1 为默认网关设备，网关地址为 192.168.10.254，当 LSW1 故障或 LSW3—LSW1 链路故障时，希望 VLAN 10 的所有终端能自动把网关地址切换为 LSW2 上 vlanif 10 的地址 192.168.10.253，但如果要求普通用户在很短时间能步调一致地把网关改过来几乎是不可能的。如果将两台设备 vlanif 10 地址均配置成相同的 IP 地址，又会导致地址冲突，而 VRRP 可以将主备网关虚拟成一台设备，提供统一的网关地址，所有终端只需设置该虚拟网关地址作为网关即可，即使其中一台设备故障也无须切换网关地址。

3.3.2 知识准备

1. VRRP 概述

局域网中的用户终端要访问外网，就必须配置一个默认网关地址，这个地址意味着终端在访问外网时会先将数据发往该地址所在的网关设备，再由这台设备将数据转发出去，如图 3-16 所示，PC1 想要访问 PC2，网关可以是 R1 的 GE 0/0/1 地址 192.168.1.1 或 R2 的 GE 0/0/2 地址 192.168.1.2。

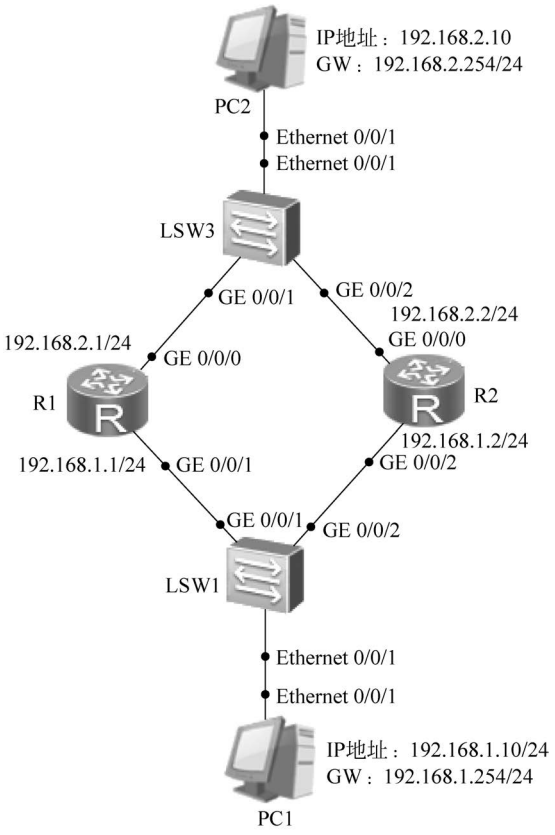

图 3-16 VRRP 应用示例

如果仅以一台设备的相应地址作为默认网关（如 R1 的 GE 0/0/1 地址 192.168.1.1），默认网关设备发生故障后用户终端就无法访问外网，这很可能会给用户带来不可预计的损失。

部署多个网关设备可以解决单点故障问题，但多个设备如果都配置和终端默认网关一样的地址，就会导致 IP 地址冲突问题，如果多个设备配置不一样的网关地址，则原网关故障

后所有用户需要步调一致地把网关地址改成备用网关地址，这几乎是不可能的。那么如何让多个网关能够协同工作但地址又不会相互冲突呢？

VRRP通过将多个网关设备虚拟成一个网关设备，从而只需要设置一个虚拟网关地址（和用户终端的默认网关地址相同），如图3-17所示，两台网关设备虚拟成一台网关设备后拓扑就相当于成了右边单网关的情况，从而可以使终端的默认网关和网关设备上的网关地址始终保持一致，这样成功地在使网关设备冗余的同时解决了网关地址冲突和终端切换网关的问题。

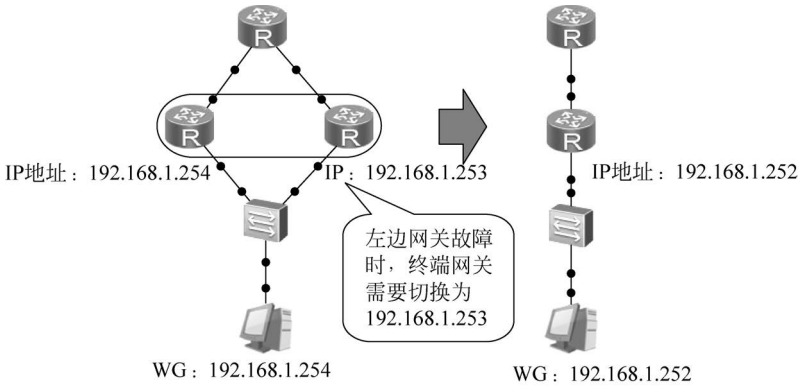

图3-17　VRRP工作原理

VRRP有两个版本，VRRPv2仅适用于IPv4网络，VRRPv3适用于IPv4和IPv6两种网络。

2. VRRP主备网关选举

在虚拟网关组中VRRP会使用选举机制确定路由器（包括三层交换机）的主备（Master或Backup），优先级高的VRRP路由器为主路由器（Master），当优先级相同时通过比较IP地址来进行选择，IP地址大的路由器将成为主路由器。路由器可配置的VRRP优先级为1～254，默认优先级为100。当VRRP虚拟IP地址与某网关地址相同时，与VRRP虚拟IP地址相同的VRRP路由器具有最高优先级255，此时该路由器被称为IP地址拥有者。

3. VRRP的主备切换

Master设备在工作时会周期性地发送VRRP通告报文（Advertisement，也被形象地称为心跳报文）给组内其他设备，以通知自己处于正常工作状态。通告报文目的IP地址是224.0.0.18，目的MAC地址是01-00-5e-00-00-12，协议号是112。Backup在Master_Down_Interval时间内未收到Master发送的状态通告报文，则立即成为Master。因为原Master优先级较高，所以故障恢复后会立即抢占再次成为Master。

4. VRRP的负载分担

如果流量都经由单个Master转发，Master负担过重，而备份设备得不到利用。VRRP支持通过配置不同的备份组，使RouterA为组1的Master，而使RouterB成为组2的Master，这样就可以让RouterA和RouterB共同分担网络中流量了。

5. 配置命令（端口模式）

（1）设置虚拟网关地址。

```
vrrp vrid VRID virtual-ip X.X.X.X
```

说明：VRID 为 VRRP 分组的编号，X. X. X. X 代表该 VRIP 组虚拟的网关地址。

(2) 配置 VRRP 优先级。

```
vrrp vrid VRID priority priority
```

说明：priority 用于设置优先级，并按优先级竞选主备网关，取值范围为 1～254。

(3) 设置抢占时延示例(单位为秒)。

```
vrrp vrid 1 preempt - mode timer delay 20
```

说明：该命令设置主网关恢复功能后经过一定延时再将主网关的角色抢回。

(4) 监听上游端口示例。

```
vrrp vrid 1 track interface GigabitEthernet 0/0/0 reduce 30
```

说明：监听上游端口，如果故障则将优先级降低 30，则让备用设备成为主网关。

(5) 显示 VRRP 信息。

```
display vrrp brief
```

3.3.3 配置与测试

由于图 3-15 所示模块拓扑中综合了 VRRP、链路聚合和生成树 3 大功能，对初学者来说，可能会对领会 VRRP 配置有所干扰。为便于领会 VRRP 单项功能配置，这里先对图 3-16 所示拓扑进行配置，之后再配置图 3-15 所示的拓扑。


视频讲解

1. 对如图 3-16 所示拓扑配置 VRRP

该实例对上下两个网段分别作了 VRRP 虚拟网关设置。上面 PC2 地址设置为 192. 168. 2. 10/24，默认网关为 192. 168. 2. 254，而它的两个网络出接口分别为 R1 的 GE 0/0/0 (192. 168. 2. 1)和 R2 的 GE 0/0/0(192. 168. 2. 2)，均与终端默认网关不同，无法通信。现在为了 R1 和 R2 的 GE 0/0/0 对终端均表现为与终端默认网关相同的地址，使 PC2 通过两个出接口均可实现跨网段访问，这里采用 VRRP 将两台路由器的 GE 0/0/0 接口(与 PC2 相连)虚拟成一个 VRRP 组，这个 VRRP 组对应唯一的 IP 地址 192. 168. 2. 254(与终端默认网关相同)，这个地址将成为 R1 和 R2 面对 192. 168. 2. 0/24 网段所有终端提供的唯一网关地址，这样 PC2 跨网段访问 PC1 时不管数据经哪台路由器转发，面对的只有一个网关地址。类似地，下面的终端 PC1 与 R1 和 R2 连接的两个接口地址均与终端默认网关不同，也需要用 VRRP 将两个出接口虚拟成一个 VRRP 组，设置其对应 IP 地址为 192. 168. 1. 254 (与终端默认网关相同)，该地址将成为两个出接口对终端表现的唯一的地址，从而 PC1 访问 PC2 时不管数据经哪台路由器转发，面对的只有一个网关地址。以下是该实例相应的配置。

(1) R1 配置。

```
< Huawei > sys
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/0
[R1 - GigabitEthernet0/0/0]ip address 192.168.2.1 24
[R1 - GigabitEthernet0/0/0]vrrp vrid 1 virtual - ip 192.168.2.254 //配置组 1 虚拟网关
[R1 - GigabitEthernet0/0/0]vrrp vrid 1 priority 150               //配置优先级使 R1 为主设备
[R1 - GigabitEthernet0/0/0]quit
[R1]interface GigabitEthernet 0/0/1
[R1 - GigabitEthernet0/0/1]ip address 192.168.1.1 24
```

```
[R1-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 192.168.1.254  //配置组2虚拟网关
[R1-GigabitEthernet0/0/1]vrrp vrid 2 priority 150     //配置优先级使R1为主设备
[R1-GigabitEthernet0/0/1]vrrp vrid 2 preempt-mode timer delay 10     //配置抢占时延
[R1-GigabitEthernet0/0/1]vrrp vrid 2 track interface GigabitEthernet 0/0/0 reduced 60
//上游接口失效时降低该设备优先级将主设备角色让给备用设备
[R1-GigabitEthernet0/0/1]quit
```

(2) R2配置。

```
<Huawei>sys
[Huawei]sysname R2
[R2]undo info-center enable
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 192.168.2.2 24
[R2-GigabitEthernet0/0/0]vrrp vrid 1 virtual-ip 192.168.2.254 //配置组1虚拟网关
[R2-GigabitEthernet0/0/0]quit
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 192.168.1.2 24
[R2-GigabitEthernet0/0/2]vrrp vrid 2 virtual-ip 192.168.1.254 //配置组2虚拟网关
[R2-GigabitEthernet0/0/2]quit
[R2]
```

(3) 终端配置。

PC1：IP地址为192.168.1.10，掩码为255.255.255.0，默认网关为192.168.1.254。

PC2：IP地址为192.168.2.10，掩码为255.255.255.0，默认网关为192.168.2.254。

(4) VRRP信息查看。

在R1用display vrrp命令查看VRRP信息，显示如图3-18所示，可以看出在VRRP虚拟组1(虚拟路由器1)中R1为主设备，在VRRP虚拟组2(虚拟路由器2)中R1也为主设备，这样保证了数据流去和回都是经R1转发。这种情况下，如果R1工作正常，数据流只要能到达目的地就能将应答信息返回，如果R1不能正常工作，也会将去往目的地的数据流和返回的数据流一并转由R2转发，降低故障率。

图3-18　VRRP虚拟组信息

再用 display vrrp brief 命令查看 VRRP 摘要信息，显示结果如图 3-19 所示，也可以看出在两个虚拟 VRRP 组中，R1 均为主设备，虚拟 IP 地址分别为 192.168.2.254 和 192.168.1.254。

```
<R1>dis vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Master       GE0/0/0                  Normal   192.168.2.254
2     Master       GE0/0/1                  Normal   192.168.1.254
------------------------------------------------------------------
Total:2     Master:2     Backup:0     Non-active:0
<R1> User interface con0 is available
```

图 3-19　VRRP 摘要信息

在 R2 上可用同样的方法查看 VRRP 信息，分别分析两个 VRRP 组的相应信息。

(5) 测试。

在 R1 与 PC1 相连的接口 GE 0/0/1 开启抓包，然后用 PC1 ping PC2 地址 192.168.2.10，可以 ping 通，而且抓到了 PC1 ping PC2 的往返 ICMP 报文，说明此时 R1 为工作网关；现模拟故障宕掉 R1 与 PC2 相连的 GE 0/0/0 接口，在 R2 的 GE 0/0/2 接口开启抓包，再用 PC1 长 ping PC2 地址 192.168.2.10，发现经过短暂延时后 PC1 收到 Reply 报文，在 R2 的 GE 0/0/2 接口也抓取到了 ICMP 报文，说明此时工作网关由 R1 切换为了 R2。

2. 对如图 3-15 所示拓扑配置 VRRP


视频讲解

该模块由图 3-1 所示拓扑分解而来，综合了 VRRP、链路聚合及生成树多个功能。这里仅以 VLAN 10 为例说明 VRRP 配置方法，其他 VLAN 可参照 VLAN 10 配置。

分析拓扑结构，可以看出 PC1(VLAN 10)访问上游路由器的数据流既可以经 LSW1 转发，也可以经 LSW2 转发，所以 LSW1 和 LSW2 均可以作为 PC1 网关设备，但如果这两个网关设置同一个 IP 地址(SVI 接口地址)做 VLAN 10 的终端网关，会引起地址冲突问题，如果设置不同网关地址，又需要在工作网关失效后瞬间修改所有 VLAN 10 的客户端网关地址与备用设备所设网关地址一致，这是很不现实的。所以这里采用 VRRP 技术把 LSW1 和 LSW2 虚拟成一个网关设备，从而使两台网关设备对同一 VLAN 的终端只提供一个统一的虚拟网关(这里使用 LSW1 的网关 192.168.10.252)，以解决两个网关不一致或 IP 冲突问题，同时通过主备网关增强网络的可靠性。以下是实现 VRRP 的相关配置(含链路聚合及生成树配置)，各部分配置以浅灰色标示。

(1) LSW1 配置。

```
<Huawei>sys
[Huawei]sysname LSW1
[LSW1]undo info-center enable
[LSW1]stp mode rstp          //设置生成树模式
[LSW1]vlan 10
[LSW1-vlan10]quit
//以下 5 行为端口聚合设置
[LSW1]interface Eth-Trunk 1                          //设置聚合端口
[LSW1-Eth-Trunk1]port link-type trunk
[LSW1-Eth-Trunk1]port trunk allow-pass vlan all
[LSW1-Eth-Trunk1]load-balance dst-ip          //设置负载分担模式
[LSW1-Eth-Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24 //给 Eth-Trunk 1 添加成员端口
[LSW1-Eth-Trunk1]quit
[LSW1]interface GigabitEthernet 0/0/1
```

```
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW1-GigabitEthernet0/0/1]quit
[LSW1]interface vlanif 10
[LSW1-Vlanif10]ip address 192.168.10.254 24                    //设置 vlanif 接口地址
//以下 3 行为 VRRP 相关配置
[LSW1-Vlanif10]vrrp vrid 1 virtual-ip 192.168.10.252   //设置虚拟网关地址
[LSW1-Vlanif10]vrrp vrid 1 priority 120                //设置优先级使该设备成为主设备
[LSW1-Vlanif10]vrrp vrid 1 preempt-mode timer delay 10  //设置抢占延时为 10s
[LSW1-Vlanif10]quit
```

(2) LSW2 配置。

```
<Huawei>sys
[Huawei]sysname LSW2
[LSW2]undo info-center enable
[LSW2]stp mode rstp                          //设置生成树模式
[LSW2]vlan 10
[LSW2-vlan10]quit
//以下 5 行为端口聚合设置(手工模式)
[LSW2]interface Eth-Trunk 1                  //设置链路聚合
[LSW2-Eth-Trunk1]port link-type trunk
[LSW2-Eth-Trunk1]port trunk allow-pass vlan all
[LSW2-Eth-Trunk1]load-balance dst-ip    //设置负载分担模式
[LSW2-Eth-Trunk1]trunkport GigabitEthernet 0/0/22 to 0/0/24 //给 Eth-Trunk 1 添加成员端口
[LSW2-Eth-Trunk1]quit
[LSW2]interface GigabitEthernet 0/0/1
[LSW2-GigabitEthernet0/0/1]port link-type trunk
[LSW2-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW2-GigabitEthernet0/0/1]quit
[LSW2]interface vlanif 10
[LSW2-Vlanif10]ip address 192.168.10.253 24                    //设置 vlanif 接口地址
//以下 1 行为 VRRP 相关配置(备用设备不用配置优先级和抢占时延)
[LSW2-Vlanif10]vrrp vrid 1 virtual-ip 192.168.10.252 //设置虚拟网关地址
[LSW2-Vlanif10]quit
```

(3) LSW3 配置。

```
<Huawei>sys
[Huawei]sysname LSW3
[LSW3]undo info-center enable
[LSW3]stp mode rstp      //设置生成树模式
[LSW3]vlan 10
[LSW3-vlan10]quit
[LSW3]interface GigabitEthernet 0/0/1
[LSW3-GigabitEthernet0/0/1]port link-type trunk
[LSW3-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/1]quit
[LSW3]interface GigabitEthernet 0/0/2
[LSW3-GigabitEthernet0/0/2]port link-type trunk
[LSW3-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/2]quit
[LSW3]port-group group-member Ethernet 0/0/1 to Ethernet 0/0/10
[LSW3-port-group]port link-type access
[LSW3-port-group]port default vlan 10
[LSW3-port-group]quit
[LSW3]
```

(4) 查看 VRRP 信息。

用 display vrrp brief 命令查看 LSW1 的 VRRP 摘要信息，如图 3-20 所示，可以看到虚拟网关地址为 192.168.10.252，LSW1 为主设备(Master)。

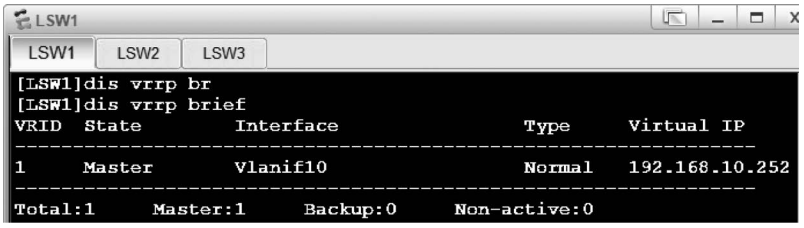

图 3-20 LSW1 上 VRRP 摘要信息

用 display vrrp 命令查看 LSW1 的 VRRP 信息，如图 3-21 所示，可以看到 LSW1 为主设备(Master)、虚拟网关地址为 192.168.10.252、优先级为 120 等信息。

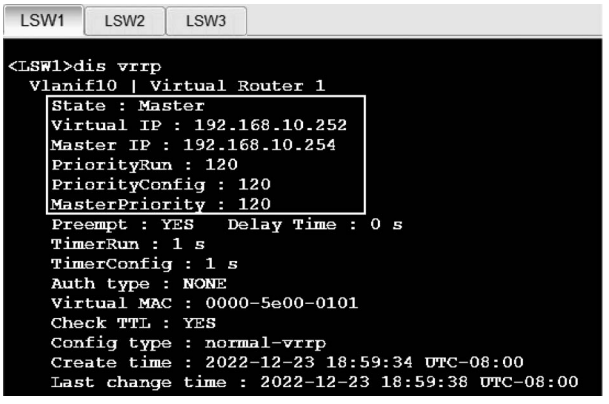

图 3-21 LSW1 上 VRRP 信息

类似地，用 display vrrp brief 和 display vrrp 命令查看 LSW2 的 VRRP 信息，可以看到 VLAN 10 的虚拟网关地址为 192.168.10.252，LSW2 为备用设备(Backup)。

(5) ping 测试。

用 PC1 ping 网关 192.168.10.252，收到应答消息，说明能够 ping 通虚拟网关，如图 3-22 所示。

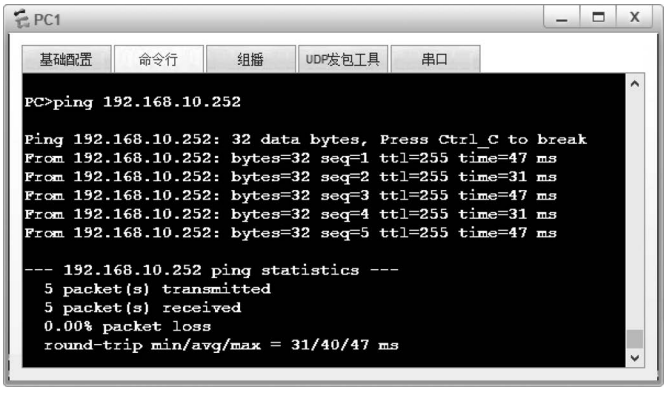

图 3-22 对虚拟网关的连通性测试

现模拟故障关闭LSW1和LSW3相连的端口，在LSW3的GE 0/0/2端口开启抓包，再在PC1上执行ping 192.168.10.252 -t命令长ping虚拟网关，发现经过一定延时后，在LSW3的GE 0/0/2端口抓取到了ICMP数据流，如图3-23所示，说明此时网关由LSW1切换为LSW2。

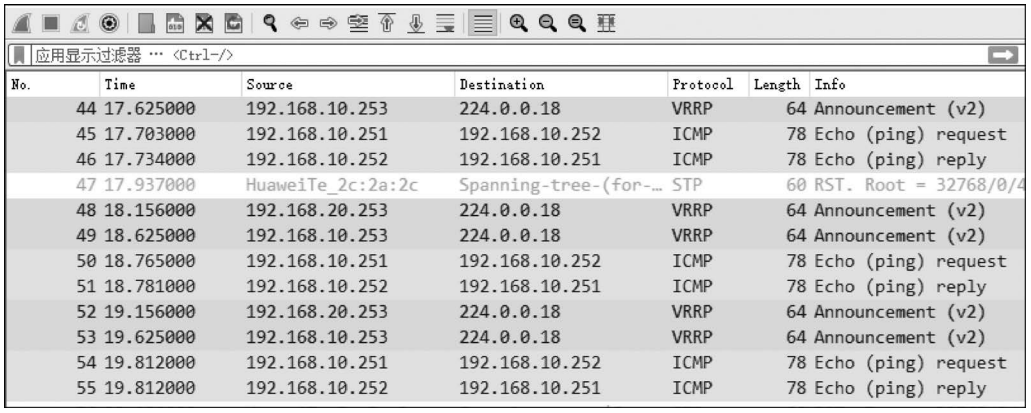

图3-23　LSW3的GE 0/0/2端口抓到的ICMP数据流

3.3.4　能力提升——抓包分析VRRP

按照前文3.3.3节对图3-16所示拓扑做VRRP配置后，在R1和R2的GE 0/0/0接口开启抓包，然后用PC1 ping PC2，发现R1的GE 0/0/0接口抓到了ICMP数据流，而R2的GE 0/0/0接口却没有抓到ICMP数据流，说明PC1 ping PC2的往返数据流均是经R1转发的，此时R1为主网关。

现在为了模拟主设备故障，将R1的GE 0/0/0接口关闭，重新在R1的GE 0/0/1接口和R2的GE 0/0/2接口开启抓包，然后用PC1长ping PC2，发现经短暂延时后，R2的GE 0/0/2接口抓到了ICMP数据流，说明这时PC1 ping PC2的往返数据流均是经R2转发的，此时原来作为主设备的R1已经失效，R2原来作为备用设备现已接替了主设备转发数据的工作。

用undo shutdown命令恢复R1的GE 0/0/0接口功能，并将R1的GE 0/0/1接口关闭，然后在R2的GE 0/0/0接口开启抓包，然后用PC1长ping PC2，发现不能ping通，而且R2的GE 0/0/0接口只能抓到ICMP Request报文再用tracert命令，并没有抓到Reply报文，而R1的GE 0/0/0却抓到了Reply报文，说明PC1 ping PC2的往返数据流均是经R2转发的，此时原来作为主设备的R1已经失效，R2作为备用设备已接替了主设备转发数据的工作。

分析：如果让PC1访问PC2，PC1发出的报文首先会交给R2转发给PC2，PC2返回的应答报文则会首先交给R1，然后由R1转发给PC1。

这时因为数据流去往目的的路径和回包的路径不同，所以必须保证两条链路都没有故障的情况下，两端才能正常通信；任意一条链路的任意节点故障，都将导致两端通信失败，所以这种配置故障率较高。

如果将两个 VRRP 组的主设备配置为同一台设备，则该设备工作正常时往返数据流全部经该设备转发，如果该设备或该设备相连的链路或接口故障，VRRP 就会启用备用设备，而且往返数据流同步切换为备用设备转发。显然这种情况只要两端有一条链路工作正常，通信就正常，这样就能保证两端通信的低故障率，明显优于两个 VRRP 组的主设备不一致的情况。

所以，在网络构建和配置中，如果存在多种方案，一定要权衡利弊，选择最优的方案。

3.4 模块 4：DHCP

【教学目标】

知识目标：

- 了解 DHCP 的应用场景。
- 理解 DHCP 工作原理。
- 掌握 DHCP 基本配置。
- 了解 DHCP 的安全威胁与防御。

技能目标：能够在相应场景正确配置 DHCP，使众多主机能够自动获取 IP 地址等参数。

思政目标：

- 了解 DHCP 的安全威胁与防御，树立维护网络安全的责任意识，保障企事业单位利益。
- 培养学生溯本求源的探究精神及一丝不苟的工匠精神。

3.4.1 模块拓扑

按照如图 3-1 所示项目整体规划，VLAN 10 对应网段 192.168.10.0/24，VLAN 20 对应网段 192.168.20.0/24，其他 VLAN 也映射了相应网段。所以，VLAN 10 的用户需要配置 192.168.10.0/24 网段的 IP 地址及相应网关，而且要保证每个终端的 IP 地址不同。同理，VLAN 20 的用户需要配置 192.168.20.0/24 网段的 IP 地址及相应网关，而且也要保证每个终端的 IP 地址不同，其他 VLAN 的情况类似。这样，在用户数量较多的网络中，不仅配置工作量大，还容易产生地址配置错误或冲突的情况，影响用户正常通信。

为避免以上问题，该模块将利用 DHCP 服务器实现自动为终端分配 IP 地址，保证终端地址不会重复，而且可以大大节约工作量。为避免重复性配置工作以节约篇幅，这里仅研究 VLAN 10 和 VLAN 20 内的主机获取地址的方法，其他 VLAN 的终端自动获取 IP 地址的配置方法可参照 VLAN 10 或 VLAN 20。

该模块拓扑由项目 3 拓扑图 3-1 分解而来，如图 3-24 所示。将 LSW1 部署为 DHCP Server1，可以为 VLAN 10 的终端 PC1 和 VLAN 20 的终端 PC2 自动分配 IP 地址，为防止 LSW1 故障导致终端不能获取 IP 地址，将 LSW2 部署为 DHCP Server2，作为 DHCP Server1 的备份。

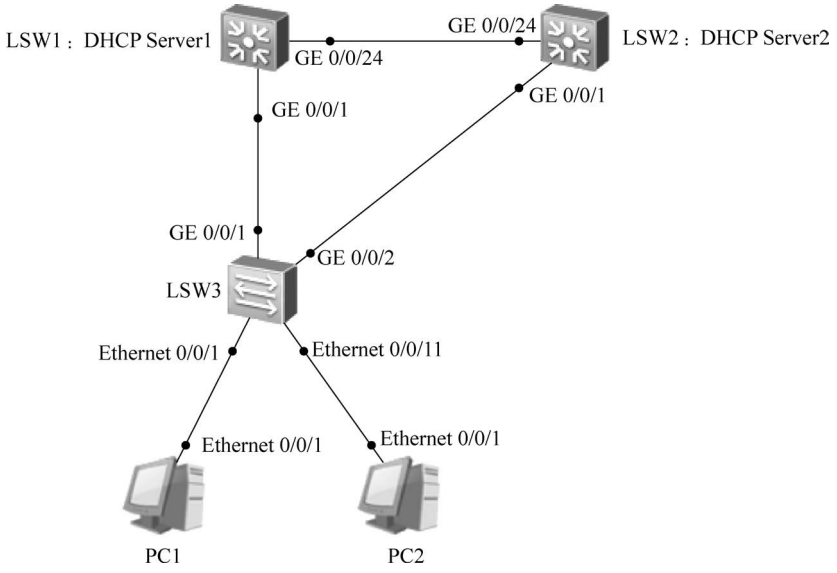

图 3-24　DHCP Server 备份

3.4.2　知识准备

1. DHCP 概述

DHCP(Dynamic Host Configuration Protocol,动态主机配置协议)是一种由 DHCP 服务器对 IP 地址集中管理和自动分配的技术,采用 C/S 构架,终端可以自动从 DHCP 服务器获取 IP 地址以及网关、DNS 服务器地址,简化网络配置,减少 IP 地址冲突,实现接入网络后即插即用。DHCP 广泛用于有线网络和无线局域网终端的地址分配,是影响用户上网体验的重要因素。

2. DHCP 工作原理

DHCP 客户端首次向 DHCP 服务器获取地址的交互过程如图 3-25 所示,分为 4 个阶段。

图 3-25　DHCP 工作原理

(1) 发现阶段：DHCP 客户端启动时，如果没有 IP 地址，就会以广播方式发送 DHCP Discover 报文，用于寻找 DHCP 服务器，这时由于客户端还没有 IP 地址，所以源 IP 地址为 0.0.0.0，目的 IP 地址为广播地址 255.255.255.255。

(2) 提供阶段：网络中的 DHCP 服务器收到客户端发送的 DHCP Discover，会在自己的地址池中选择一个可用地址封装在 DHCP Offer 报文中发送给客户端，告知客户端自己可以为其提供 IP 地址。

(3) 选择阶段：由于网络中可能存在多个 DHCP 服务器，故 DHCP 客户端可能会收到多个 Offer 报文，但 DHCP 客户端通常会选择最先收到的 Offer 报文携带的 IP 地址，并以广播方式发送 DHCP Request 报文通告自己选择的 IP 地址。

(4) 确认阶段：被客户端选择的 DHCP 服务器收到客户端发送的 DHCP Request 报文，再发送 DHCP ACK 报文确认正式将刚才提供的 IP 地址分配给客户端。其他 DHCP 收到客户端通告的 Request，知道了客户端已选择别的 DHCP 服务器提供的地址，故收回自己提供的地址。

在经过以上 4 个阶段的交互协商，客户端真正获得了 DHCP 服务器提供的 IP 地址。这时，DHCP 客户端还会以广播方式发送免费 ARP 报文，以探测网络中是否有与该 IP 地址重复的 IP 地址，如果没有，则会正式启用该地址。所以，也可以认为，DHCP 工作过程分为 5 步(含发送免费 ARP 报文)。

客户端的 IP 地址是有租期的，如果客户端在租期内重新登录网络，则不再发送 Discover 报文，而是直接发送 DHCP Request 报文。服务器收到客户端发送的 Request 报文，回复 DHCP ACK 报文进行确认，或回复 DHCP NAK 报文拒绝其请求。

3. DHCP 地址池

DHCP 地址池用于定义 DHCP 服务器可以给客户端分配的地址范围及网关等网络参数。华为设备地址池有两种定义方式：全局地址池和接口地址池。

(1) 全局地址池。

全局地址池是独立的，不需要与接口绑定，其定义示例如下：

```
[Huawei]dhcp enable                                          //使能 DHCP 功能
[Huawei]ip pool vlan10                                       //定义地址池名称并进入地址池配置视图
[Huawei-ip-pool-pool2]network 192.168.10.0 mask 24 //定义可分配的地址为 192.168.10.0/24
//网段，可以通过命令排除已用地址
[Huawei-ip-pool-pool2]gateway-list 192.168.10.254   //定义网关
[Huawei-ip-pool-pool2]lease day 10                   //定义租期为 10 天
[Huawei-ip-pool-pool2]quit
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]dhcp select global     //定义该接口为全局地址池输出接口
```

(2) 接口地址池。

接口地址池需要与接口绑定，其定义示例如下：

```
[Huawei]dhcp enable          //使能 DHCP 功能
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]dhcp select interface //选择该接口为地址池接口(这时接口地址
//为网关地址)
[Huawei-GigabitEthernet0/0/1]dhcp server dns-list 8.8.8.8 //定义 DNS 服务器地址
[Huawei-GigabitEthernet0/0/1]dhcp server excluded-ip-address 192.168.10.1 //定义排除地址
[Huawei-GigabitEthernet0/0/1]dhcp server lease day 3 //定义地址租期
```

3.4.3 配置与测试

这里以全局地址池为例介绍DHCP服务的相关配置，并同时在LSW1和LSW2上部署DHCP服务，使两台设备形成DHCP服务的备份。各设备具体配置如下。


视频讲解

1. LSW1配置

```
<Huawei>sys
[Huawei]sysname LSW1
[LSW1]undo info-center enable
[LSW1]stp mode rstp                                          //设置生成树模式
[LSW1]vlan batch 10 20
[LSW1]interface GigabitEthernet 0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW1-GigabitEthernet0/0/1]quit
[LSW1]interface GigabitEthernet 0/0/24
[LSW1-GigabitEthernet0/0/24]port link-type trunk
[LSW1-GigabitEthernet0/0/24]port trunk allow-pass vlan all
[LSW1-GigabitEthernet0/0/24]quit
//配置DHCP地址池
[LSW1]dhcp enable                                            //使能DHCP服务
[LSW1]ip pool vlan10                                         //定义VLAN 10的地址池
[LSW1-ip-pool-vlan10]network 192.168.10.0 mask 255.255.255.0 //定义地址池网段
[LSW1-ip-pool-vlan10]gateway-list 192.168.10.252             //定义VLAN 10的网关
[LSW1-ip-pool-vlan10]excluded-ip-address 192.168.10.253      //定义排除的地址
[LSW1-ip-pool-vlan10]dns-list 8.8.8.8                        //定义DNS服务器地址
[LSW1-ip-pool-vlan10]lease 30                                //定义地址租期为30天
[LSW1-ip-pool-vlan10]quit
[LSW1]ip pool vlan20                                         //定义VLAN 20的地址池
[LSW1-ip-pool-vlan20]network 192.168.20.0 mask 255.255.255.0 //定义地址池网段
[LSW1-ip-pool-vlan20]gateway-list 192.168.20.252             //定义VLAN 20的网关
[LSW1-ip-pool-vlan20]excluded-ip-address 192.168.20.253      //定义排除的地址
[LSW1-ip-pool-vlan20]dns-list 8.8.8.8                        //定义DNS服务器地址
[LSW1-ip-pool-vlan20]lease 30                                //定义地址租期
[LSW1-ip-pool-vlan20]quit
[LSW1]interface vlanif 10
[LSW1-Vlanif10]ip address 192.168.10.254 24                  //设置vlanif接口地址
//以下3行为VRRP虚拟组1设置
[LSW1-Vlanif10]vrrp vrid 1 virtual-ip 192.168.10.252         //设置虚拟网关地址
[LSW1-Vlanif10]vrrp vrid 1 priority 120                      //设置优先级
[LSW1-Vlanif10]vrrp vrid 1 preempt-mode timer delay 10       //设置VRRP抢占延时10s
[LSW1-Vlanif10]dhcp select global        //设置VLAN 10的地址池为全局地址池
[LSW1-Vlanif10]quit
[LSW1]interface vlanif 20
[LSW1-Vlanif20]ip address 192.168.20.254 24                  //设置vlanif接口地址
//以下1行为VRRP虚拟组2设置
[LSW1-Vlanif20]vrrp vrid 2 virtual-ip 192.168.20.252         //设置虚拟网关地址
[LSW1-Vlanif20]dhcp select global        //设置VLAN 20的地址池为全局地址池
[LSW1-Vlanif20]quit
[LSW1]
```

2. LSW2 配置

```
<Huawei>sys
[Huawei]sysname LSW2
[LSW2]undo info-center enable
[LSW2]stp mode rstp                                                    //设置生成树模式
[LSW2]vlan batch 10 20
[LSW2]interface GigabitEthernet 0/0/1
[LSW2-GigabitEthernet0/0/1]port link-type trunk
[LSW2-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW2-GigabitEthernet0/0/1]quit
[LSW2]interface GigabitEthernet 0/0/24
[LSW2-GigabitEthernet0/0/24]port link-type trunk
[LSW2-GigabitEthernet0/0/24]port trunk allow-pass vlan all
[LSW2-GigabitEthernet0/0/24]quit
//配置 DHCP 地址池
[LSW2]dhcp enable                                                      //使能 DHCP 服务
[LSW2]ip pool vlan10                                                   //定义 VLAN 10 的地址池
[LSW2-ip-pool-vlan10]network 192.168.10.0 mask 255.255.255.0           //定义地址池网段
[LSW2-ip-pool-vlan10]gateway-list 192.168.10.252                       //定义 VLAN 10 的网关
[LSW2-ip-pool-vlan10]excluded-ip-address 192.168.10.254                //定义排除的地址
[LSW2-ip-pool-vlan10]dns-list 8.8.8.8                                  //定义 DNS 服务器地址
[LSW2-ip-pool-vlan10]lease 30                                          //定义地址租期
[LSW2-ip-pool-vlan10]quit
[LSW2]ip pool vlan20                                                   //定义 VLAN 20 的地址池
[LSW2-ip-pool-vlan20]network 192.168.20.0 mask 255.255.255.0           //定义地址池网段
[LSW2-ip-pool-vlan20]gateway-list 192.168.20.252                       //定义 VLAN 20 的网关
[LSW2-ip-pool-vlan20]excluded-ip-address 192.168.20.254                //定义排除的地址
[LSW2-ip-pool-vlan20]dns-list 8.8.8.8                                  //定义 DNS 服务器地址
[LSW2-ip-pool-vlan20]lease 30                                          //定义地址租期
[LSW2-ip-pool-vlan20]quit
[LSW2]interface vlanif 10
[LSW2-Vlanif10]ip address 192.168.10.253 24                            //设置 vlanif 接口地址
//以下 1 行为 VRRP 虚拟组 1 设置
[LSW2-Vlanif10]vrrp vrid 1 virtual-ip 192.168.10.252                   //设置虚拟网关地址
[LSW2-Vlanif10]dhcp select global        //设置 VLAN 10 的地址池为全局地址池
[LSW2-Vlanif10]quit
[LSW2]interface vlanif 20
[LSW2-Vlanif20]ip address 192.168.20.253 24                            //设置 vlanif 接口地址
//以下 3 行为 VRRP 虚拟组 2 设置
[LSW2-Vlanif20]vrrp vrid 2 virtual-ip 192.168.20.252                   //设置虚拟网关地址
[LSW2-Vlanif20]vrrp vrid 2 priority 120                                //设置优先级
[LSW2-Vlanif20]vrrp vrid 2 preempt-mode timer delay 10                 //设置 VRRP 抢占延时 10s
[LSW2-Vlanif20]dhcp select global      //设置 VLAN 20 的地址池为全局地址池
[LSW2-Vlanif20]quit
[LSW2]
```

3. LSW3 配置

```
<Huawei>sys
[Huawei]sysname LSW3
[LSW3]undo info-center enable
[LSW3]stp mode rstp   //设置生成树模式
[LSW3]vlan batch 10 20
[LSW3-vlan10]quit
[LSW3]interface GigabitEthernet 0/0/1
```

```
[LSW3-GigabitEthernet0/0/1]port link-type trunk
[LSW3-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/1]quit
[LSW3]interface GigabitEthernet 0/0/2
[LSW3-GigabitEthernet0/0/2]port link-type trunk
[LSW3-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[LSW3-GigabitEthernet0/0/2]quit
[LSW3]port-group group-member Ethernet 0/0/1 to Ethernet 0/0/10
[LSW3-port-group]port link-type access
[LSW3-port-group]port default vlan 10
[LSW3-port-group]quit
[LSW3]port-group group-member Ethernet 0/0/11 to Ethernet 0/0/20
[LSW3-port-group]port link-type access
[LSW3-port-group]port default vlan 20
[LSW3-port-group]quit
[LSW3]
```

4. 测试

如图 3-26 所示，选择 PC1 的“基础配置”选项卡，设置 IPv4 配置模式为 DHCP，然后单击右下角的“应用”按钮。

图 3-26　终端自动获取 IP 地址设置

然后选择 PC1 的“命令行”选项卡，输入 ipconfig 命令并按 Enter 键，查看 PC1 的 IP 地址，如图 3-27 所示，发现 PC1 已经获取到了 IP 地址 192.168.10.251，网关为虚拟地址 192.168.10.252，DNS 服务器地址为地址池设置的 8.8.8.8。

类似地，PC2 也获取到了 IP 地址，网关地址为 192.168.10.252，DNS 服务器地址为地址池设置的 8.8.8.8。

模拟故障停止设备 LSW1 或 LSW2，再让 PC1 或 PC2 用 DHCP 方式获取 IP 地址，发现总能获取到地址，说明此时 LSW1 和 LSW2 形成了 DHCP 服务器的备份。

图 3-27　查看由 DHCP 服务器获取的 IP 地址

3.4.4　能力提升——DHCP 攻击与防御

由于 DHCP 缺乏认证机制，这样就可能因错误地接入具有 DHCP 服务功能的设备或者不法分子故意接入网络实施攻击而导致 DHCP 服务异常。

最典型的两类问题就是 DHCP 地址被耗尽和 DHCP 服务器被假冒。

DHCP 地址耗尽攻击也称为 DHCP 饿死攻击，如图 3-28 所示，如果有攻击者伪造不同的 CHADDR 不断地向 DHCP 服务器请求 IP 地址，DHCP 服务器地址池中的地址很快会被耗尽，就不能为正常主机分配地址了。

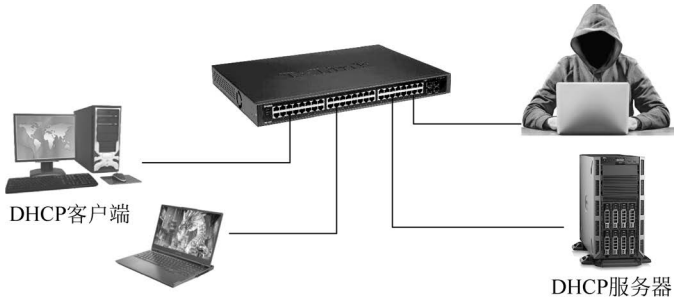

图 3-28　DHCP 地址耗尽攻击

DHCP 服务器假冒即冒充 DHCP 服务器给客户端分配错误的 IP 地址及网关等网络参数，导致客户端通信异常或数据被窃取。如图 3-29 所示，如果有非法 DHCP 服务器冒充正常 DHCP 服务器为客户端分配错误 IP 地址及网关等参数，就会使客户端获取错误 IP、网关并改变数据流向，导致数据被窃取及上网行为被控制。

为了抵御 DHCP 攻击，可采取如下措施。

(1) 在交换机上开启 DHCP snooping 功能。

(2) 防止 DHCP 服务器假冒：将交换机与合法 DHCP 服务器连接的端口设置为信任端口(Trusted)，其他端口设置为非信任端口(Untrusted)。这样，攻击者假冒 DHCP 服务器发送的 Offer 报文会被交换机拒收，终端只能接收到信任的 DHCP 服务器分配的 IP 地址等网络参数。

(3) 防止 DHCP 饿死攻击：根据攻击类型在交换机与攻击者连接的端口设置安全端口或 DHCP 报文检查功能，拒收攻击者对 IP 地址的虚假请求报文，并可以关闭该端口。

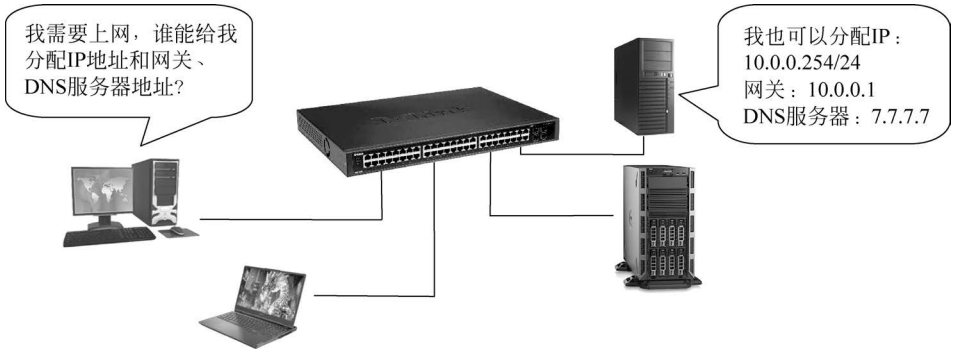

图 3-29　DHCP 服务器假冒

3.5　模块整合与项目整体部署

【教学目标】

知识目标：

- 了解单生成树的缺陷。
- 理解 MSTP 的工作原理。
- 理解 VRRP 的工作原理。
- 掌握 MSTP 基本配置命令。
- 掌握 VRRP 基本配置。
- 掌握 Eth-Trunk 基本配置。
- 掌握 DHCP 基本配置。

技能目标：掌握 MSTP＋VRRP＋Eth-Trunk＋DHCP 综合应用设计思路，并能正确配置实现各项功能。

思政目标：

- 明确网络稳定性的重要性，树立维护网络安全稳定的责任意识，提前做好网络规划与部署，综合运用 MSTP、Eth-Trunk 及 VRRP 等技术实现网络的稳定可靠，并有效防御 DHCP 等各种攻击，维护企事业单位利益。
- 培养学生溯本求源的探究精神及一丝不苟的工匠精神。

3.5.1　模块拓扑

前面对项目 3 所用的几种技术 Eth-Trunk、VRRP、RSTP 分别进行了原理分析和实验测试，该模块将对前面各模块功能进行整合，并引进基于 RSTP 的 MSTP 原理与配置的相关知识，综合运用 MSTP＋VRRP＋Eth-Trunk＋DHCP 技术组合完成项目 3 的整体部署和配置。所以，该模块拓扑及项目 3 的拓扑如图 3-1 所示。

3.5.2　知识准备

1. 多生成树

备份链路和备份设备解决了单链路故障和单点故障给企业带来网络故障或丢包等风

险，而因备份链路和备份设备产生的环路又可以通过生成树或快速生成树解决。但是，STP和RSTP都是单生成树协议，所有VLAN共享一棵生成树转发数据，势必导致工作链路的拥塞和工作设备资源的过多消耗，而非工作链路和设备却没有得到应用，造成资源的浪费。

多生成树协议(MSTP)以快速生成树为基础，可以针对实例(每个实例可理解为一个VLAN组)创建工作链路不同的不同快速生成树，使一个或若干VLAN使用某一棵快速生成树提供的链路转发数据，而另外的一个或若干VLAN使用另外的快速生成树提供的链路转发数据，这样所有的设备和链路都得到了利用，而且实现了负载分担，保证了数据的高效转发。这时就产生了VLAN和生成树的映射关系，这种映射关系形成的每一棵树分别称为一个多生成树实例(MSTI)。MSTI具有如下特点。

(1) 每个实例对应一个或一组VLAN。

(2) 每个VLAN只能对应一个实例。

(3) 每个交换机可以运行多个实例(最多16个，编号为0～15)。

(4) 没有配置VLAN与实例的映射关系时，所有VLAN映射到实例0。

(5) MSTI的计算过程和状态机基本与RSTP的计算过程和状态机一致。

2. MSTP配置命令

(1) 使能生成树协议，选择生成树模式为多生成树。

```
[Huawei] stp enable
[Huawei] stp mode mstp
```

(2) 进入MSTP域配置模式，设置域名为GR1。

```
[Huawei] stp region-configuration
[Huawei-mst-region] region-name RG1
```

域名为域的一个标识，具有相同域名、相同修订级别和相同VLAN与实例的映射关系的交换机属同一个域。

(3) 创建实例1并映射相应VLAN(可选)。

```
[Huawei-mst-region]instance 1 vlan n[, m...]
```

(4) 激活域配置。

```
[Huawei-mst-region]active region-configuration
```

(5) 配置实例1的根桥和备用根桥(其他实例参照该配置)。

```
[Huawei] stp instance 1 root primary(或 stp instance 1 priority 4096)
[Huawei] stp instance 1 root secondary
```

或

```
[Huawei] stp instance 1 priority 4096
[Huawei] stp instance 2 priority 8192
```

(6) 配置边缘端口示例。

```
[LLSW1-GigabitEthernet0/0/1]stp edged-port enable
```

(7) 生成树查看命令。

```
[Huawei] display stp [brief]
```


视频讲解

3.5.3 配置与测试

该模块采用VRRP+MSTP+Eth-Trunk+DHCP技术组合对图3-1所示网络进行几

大功能的综合运用和部署，实现带宽扩展、链路备份、负载均衡及网关、根桥和DHCP服务器的备份。下面将对图3-1所示项目拓扑的交换网络进行完整配置。

其中，Eth-Trunk配置依然是将LSW1和LSW2的GE 0/0/22～GE 0/0/24 3个端口进行聚合(手工聚合或LACP模式均可，这里以兼容性最强的手工模式配置)。

生成树配置这里选用MSTP，将VLAN 10、VLAN 20和VLAN 30分为一组，映射为实例1(instance 1)，VLAN 40和VLAN 50分为一组，映射为instance 2，为实现负载均衡，在instance 1中配置LSW1为根桥，在instance 2中配置LSW2为根桥。

通过配置让VRRP与MSTP主备设备保持一致，VLAN 10、VLAN 20和VLAN 30 3个VLAN以LSW1为主设备，而VLAN 40和VLAN 50则以LSW2为主设备，这样实现了负载均衡。

DHCP配置类似模块4，同时在LSW1和LSW2上分别对VLAN 10、VLAN 20、VLAN 30、VLAN 40、VLAN 50配置地址池。

以下是通过display current-configuration命令显示的各交换机的实例配置代码(为节约篇幅，与此实例无关的配置内容已略去)，需要注意该实例各交换机需要用stp mode mstp命令配置生成树模式为多生成树，由于该模式为默认模式，配置代码中并没有显示。因LSW4和LSW5配置与LSW3类似，为节约篇幅，这里只列出LSW3的配置代码，LSW4和LSW5的配置可参照LSW3，也可参照图书配套资源中3.5节各设备的配置源码。

1. 终端静态IP配置

这里先配置静态IP，待测试通过后再改成DHCP自动获取方式进行测试。

PC1：IP地址为192.168.10.1/24，网关为192.168.10.252。

PC2：IP地址为192.168.20.1/24，网关为192.168.20.252。

PC3：IP地址为192.168.30.1/24，网关为192.168.30.252。

PC4：IP地址为192.168.40.1/24，网关为192.168.40.252。

PC5：IP地址为192.168.50.1/24，网关为192.168.50.252。

2. LSW1配置

```
<LSW1>display current-configuration
#
sysname LSW1
#
vlan batch 10 20 30 40 50 666
#
dhcp enable
#
ip pool vlan10
  gateway-list 192.168.10.252
  network 192.168.10.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan20
  gateway-list 192.168.20.252
  network 192.168.20.0 mask 255.255.255.0
  excluded-ip-address 192.168.20.253
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
```

```
#
ip pool vlan30
  gateway-list 192.168.30.252
  network 192.168.30.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan40
  gateway-list 192.168.40.252
  network 192.168.40.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan50
  gateway-list 192.168.50.252
  network 192.168.50.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#生成树配置
stp instance 1 priority 4096
stp instance 2 priority 8192
#
stp region-configuration
  region-name RG1
  instance 1 vlan 10 20 30
  instance 2 vlan 40 50
  active region-configuration
#
interface Vlanif1
  ip address 192.168.1.1 255.255.255.0
#
interface Vlanif10
ip address 192.168.10.254 255.255.255.0      //VLAN 10 的原网关
//VLAN 10 的虚拟网关配置
vrrp vrid 10 virtual-ip 192.168.10.252
  vrrp vrid 10 priority 120
  vrrp vrid 10 preempt-mode timer delay 10
    dhcp select global
#
interface Vlanif20
  ip address 192.168.20.254 255.255.255.0      //VLAN 20 的原网关
//VLAN 20 的虚拟网关配置
vrrp vrid 20 virtual-ip 192.168.20.252
  vrrp vrid 20 priority 120
    vrrp vrid 20 preempt-mode timer delay 10
    dhcp select global
#
interface Vlanif30
  ip address 192.168.30.254 255.255.255.0      //VLAN 30 的原网关
//VLAN 30 的虚拟网关配置
vrrp vrid 30 virtual-ip 192.168.30.252
  vrrp vrid 30 priority 120
    vrrp vrid 30 preempt-mode timer delay 10
dhcp select global
#
interface Vlanif40
```

```
  ip address 192.168.40.254 255.255.255.0      //VLAN 40 的原网关
//VLAN 40 的虚拟网关配置
vrrp vrid 40 virtual-ip 192.168.40.252
dhcp select global
#
interface Vlanif50
ip address 192.168.50.254 255.255.255.0            //VLAN 50 的原网关
//VLAN 50 的虚拟网关配置
vrrp vrid 50 virtual-ip 192.168.50.252
dhcp select global
#
interface Vlanif666
  ip address 172.16.1.2 255.255.255.0
#
//链路聚合配置
interface Eth-Trunk1
  port link-type trunk
  port trunk allow-pass vlan 2 to 4094
  load-balance dst-ip
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/2
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/3
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/20
  port link-type access
  port default vlan 666
#
//以下 3 个端口分别加入 Eth-Trunk1,作为其成员端口
interface GigabitEthernet0/0/22
  eth-trunk 1
#
interface GigabitEthernet0/0/23
  eth-trunk 1
#
interface GigabitEthernet0/0/24
  eth-trunk 1
#
return
<LSW1>
```

3. LSW2 配置

```
<LSW2>display current-configuration
#
sysname LSW2
#
undo info-center enable
#
```

```
vlan batch 10 20 30 40 50 666
#
dhcp enable
#
ip pool vlan10
  gateway-list 192.168.10.252
  network 192.168.10.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan20
  gateway-list 192.168.20.252
  network 192.168.20.0 mask 255.255.255.0
  excluded-ip-address 192.168.20.253
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan30
  gateway-list 192.168.30.252
  network 192.168.30.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan40
  gateway-list 192.168.40.252
  network 192.168.40.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
ip pool vlan50
  gateway-list 192.168.50.252
  network 192.168.50.0 mask 255.255.255.0
  lease day 30 hour 0 minute 0
  dns-list 8.8.8.8
#
stp instance 1 priority 8192
stp instance 2 priority 4096
#
stp region-configuration
  region-name RG1
  instance 1 vlan 10 20 30
  instance 2 vlan 40 50
  active region-configuration
#
interface Vlanif1
  ip address 192.168.1.2 255.255.255.0
#
interface Vlanif10
  ip address 192.168.10.253 255.255.255.0
  vrrp vrid 10 virtual-ip 192.168.10.252
dhcp select global
#
interface Vlanif20
  ip address 192.168.20.253 255.255.255.0
  vrrp vrid 20 virtual-ip 192.168.20.252
dhcp select global
#
```

```
interface Vlanif30
  ip address 192.168.30.253 255.255.255.0
  vrrp vrid 30 virtual-ip 192.168.30.252
dhcp select global
#
interface Vlanif40
  ip address 192.168.40.253 255.255.255.0
  vrrp vrid 40 virtual-ip 192.168.40.252
  vrrp vrid 40 preempt-mode timer delay 10
dhcp select global
#
interface Vlanif50
  ip address 192.168.50.253 255.255.255.0
  vrrp vrid 50 virtual-ip 192.168.50.252
  vrrp vrid 50 preempt-mode timer delay 10
dhcp select global
#
interface Vlanif666
  ip address 172.16.2.2 255.255.255.0
#
interface Eth-Trunk1
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
  load-balance dst-ip
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/2
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/3
  port link-type trunk
  port trunk allow-pass vlan 10 20 30 40 50
#
interface GigabitEthernet0/0/20
  port link-type access
  port default vlan 666
#
interface GigabitEthernet0/0/22
  eth-trunk 1
#
interface GigabitEthernet0/0/23
  eth-trunk 1
#
interface GigabitEthernet0/0/24
  eth-trunk 1
#
<LSW2>
```

4. LSW3 配置

```
<LSW3>display current-configuration
#
sysname LSW3
#
undo info-center enable
```

```
#
vlan batch 10 20 30 40 50
#
stp region-configuration
 region-name RG1
 instance 1 vlan 10 20 30
 instance 2 vlan 40 50
 active region-configuration
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
 stp edged-port enable
#
… //Ethernet 0/0/1～Ethernet 0/0/10 均为 Access 端口,默认为 VLAN 10,这里略去中间部分
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 10
 stp edged-port enable
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 20
 stp edged-port enable
#
… //Ethernet 0/0/11～Ethernet 0/0/20 均为 Access 端口,默认为 VLAN 20,这里略去中间部分
#
interface Ethernet0/0/20
 port link-type access
 port default vlan 20
 stp edged-port enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
```

5. 查看 VRRP 信息

查看 LSW1 的 VRRP 信息,结果如图 3-30 所示,在 VLAN 10、VLAN 20 和 VLAN 30 中 LSW1 为主设备(MASTER),在 VLAN 40 和 VLAN 50 中 LSW1 为备用设备(BACKUP),所有 VLAN 网关均为 VRRP 虚拟网关地址。

```
<LSW1>dis vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
10    Master       Vlanif10                 Normal   192.168.10.252
20    Master       Vlanif20                 Normal   192.168.20.252
30    Master       Vlanif30                 Normal   192.168.30.252
40    Backup       Vlanif40                 Normal   192.168.40.252
50    Backup       Vlanif50                 Normal   192.168.50.252
------------------------------------------------------------------
Total:5     Master:3     Backup:2     Non-active:0
<LSW1>
```

图 3-30　LSW1 的 VRRP 信息

```
[LSW1]display vrrp brief
```

类似地，可以查看LSW2的VRRP信息，发现在VLAN 10、VLAN 20和VLAN 30中，LSW2为备用设备(Backup)，在VLAN 40和VLAN 50中LSW2为主设备(Master)。

6. 查看MSTP信息

查看LSW1在各实例中的生成树信息，发现LSW1在instance 1中的桥ID和instance 1根桥的桥ID相同，说明LSW1在instance 1中是根桥，如图3-31所示。

```
[LSW1]display stp instance 1
```

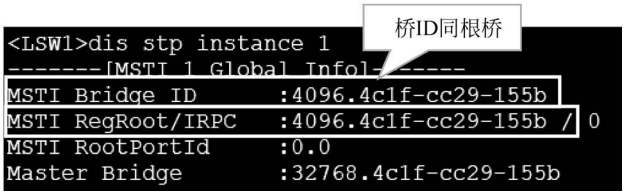

图3-31 LSW1中instance 1根桥选举情况

在instance 2中的桥ID和instance 2根桥的桥ID不同，说明LSW1在instance 2中不是根桥，如图3-32所示。

```
[LSW1]display stp instance 2
```

```
<LSW1>dis stp instance 2
-------[MSTI 2 Global Info]-------
MSTI Bridge ID      :8192.4c1f-cc29-155b
MSTI RegRoot/IRPC   :4096.4c1f-cc97-617c / 6666
MSTI RootPortId     :128.1
Master Bridge       :32768.4c1f-cc29-155b
```

图3-32 LSW1中instance 2根桥选举情况

还可查看各实例的详细信息，了解各实例中端口角色和端口状态信息，如图3-33所示。LSW2可做类似查看，这里从略。

```
<LSW1>dis stp instance 1 brief
 MSTID  Port                        Role  STP State     Protection
   1    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   1    Eth-Trunk1                  DESI  FORWARDING      NONE
<LSW1>dis stp instance 2 brief
 MSTID  Port                        Role  STP State     Protection
   2    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   2    Eth-Trunk1                  ROOT  FORWARDING      NONE
```

图3-33 LSW1 instance 1的摘要信息

7. 查看Eth-Trunk信息

查看LSW1的Eth-Trunk信息，可以看到各成员端口的状态等信息，如图3-34所示。LSW2可做类似查看，这里从略。

```
<LSW1>dis eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL          Hash arithmetic: According to DIP
Least Active-linknumber: 1   Max Bandwidth-affected-linknumber: 8
Operate status: up           Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                      Status      Weight
GigabitEthernet0/0/22         Up          1
GigabitEthernet0/0/23         Up          1
GigabitEthernet0/0/24         Up          1
```

图3-34 LSW1的Eth-Trunk信息

```
[LSW1]display eth-trunk 1
```

用 PC1 ping LSW1 通往 R1 的接口地址 172.16.1.2 或者其他终端地址，可以 ping 通，说明项目 3 的交换网络实现了全网通。

8. 终端动态获取 IP 地址配置与测试

如图 3-35 所示，选择 PC1 的“基础配置”选项卡，设置 IPv4 配置模式为 DHCP，然后单击右下角的“应用”按钮。

图 3-35　终端自动获取 IP 地址设置

选择 PC1 的“命令行”选项卡，输入 ipconfig 命令并按 Enter 键，查看 PC1 的 IP 地址，如图 3-36 所示，发现 PC1 已经由 DHCP 服务器获取到了 IP 地址 192.168.10.251(原静态 IP 地址为 192.168.10.1)，网关为虚拟网关地址 192.168.10.252，DNS 服务器地址为地址池设置的 8.8.8.8。

图 3-36　查看由 DHCP 服务器获取的 IP 地址

类似地，其他PC也获取到了IP地址，网关为相应VRRP虚拟组的IP地址，DNS服务器地址为地址池设置的8.8.8.8。

用PC1 ping LSW1通往R1的接口地址172.16.1.2或者其他终端地址，可以ping通，说明使用动态获取的IP能够正常通信。

由于该项目对DHCP服务器进行了备份，两台DHCP服务器中只要有一台能够正常工作，终端就可以获取到相应地址进行通信，增强了DHCP服务的可靠性。