第5章 网络应用故障排除

ISSUE 3.0

课程目标

学习完本课程，您应该能够：

- 掌握ACL故障排除
- 掌握NAT故障排除
- 掌握VRRP故障排除
- 掌握DHCP故障排除

目录

ACL故障排除

- ACL概述
- ACL常见故障及排除方法
- ACL排障相关命令介绍
- ACL排障典型案例

ACL概述

- **ACL的定义：**
  →ACL（Access Control List，访问控制列表）是用来实现流识别功能的。网络设备为了对特定的报文进行操作，需要配置一系列的匹配规则，以识别出特定的报文，然后根据预先设定的策略对该报文进行操作。
- **ACL常见的应用：**
  →报文过滤；
  →QoS；
  →NAT地址转换；
  →路由策略；

ACL常见故障

- 配置ACL过滤，但没有生效；
- 配置ACL过滤报文后，网络连通性产生影响；
- 配置了MQC，但所引用的ACL没有匹配到相关流；

ACL故障排除步骤（1）

- ACL不生效问题的故障处理步骤
  - → 更新计时器
  - → 查看防火墙功能是否开启
  - → 检查防火墙的缺省过滤方式
  - → 检查ACL规则配置是否正确
  - → 检查ACL规则的匹配顺序是否合理
  - → 检查报文匹配到哪条规则

ACL故障排除步骤（2）

- 网络连通性产生影响的故障处理步骤
  - → 确定是包过滤导致的问题
  - → 检查防火墙的缺省过滤方式
  - → 检查ACL规则配置是否正确
  - → 检查是否ACL配置不当导致正常协议交互中断

ACL故障排除步骤（3）

- **配置了MQC，但所引用的ACL没有匹配到相关流的故障处理步骤**
  - → 检查QOS策略是否已经应用到端口
  - → 检查ACL规则配置是否正确
  - → 查看报文匹配到哪条规则

ACL排障相关命令（1）

- **display acl { acl-number | all | name acl-name }**

  → 该命令用来显示当前ACL的配置信息

```
<H3C >display acl all
Advanced ACL  3004, named to-gss_permit, 18 rules,
ACL's step is 1
rule 0 permit ip source 219.141.226.1 0 destination 219.141.226.2 0
rule 1 permit ip source 219.141.136.10 0 destination 219.141.226.2 0
rule 2 permit ip source 219.141.140.10 0 destination 219.141.226.2 0
rule 3 permit ip source 21.1.116.18 0 destination 219.141.226.2 0
rule 4 permit ip source 219.141.226.64 0.0.0.63 destination 219.141.226.2 0
rule 5 permit ip source 219.141.226.128 0.0.0.127 destination 219.141.226.2 0
rule 6 permit ip source 209.99.10.64 0.0.0.63 destination 219.141.226.2 0
rule 7 permit ip source 209.99.10.128 0.0.0.127 destination 219.141.226.2 0
rule 8 permit icmp source 202.108.189.12 0 destination 219.141.226.2 0

Advanced ACL  3014, named to-gss_deny, 1 rule,
ACL's step is 1
rule 5 permit ip
```

ACL排障相关命令介绍（2）

- **display qos policy interface**

  → 该命令用来显示指定端口或所有端口上策略的配置信息和运行情况

```
<H3C >display qos policy interface
  Interface: Serial0/2/0
  Direction: Inbound
  Policy: filter
Classifier: permit
     Matched : 0(Packets)
     Operator: AND
     Rule(s) : If-match acl 3004
     Behavior: permit
      Filter Enable: permit
  Classifier: deny
     Matched : 0(Packets)
     Operator: AND
     Rule(s) : If-match acl 3014
     Behavior: deny
      Filter Enable: deny
```

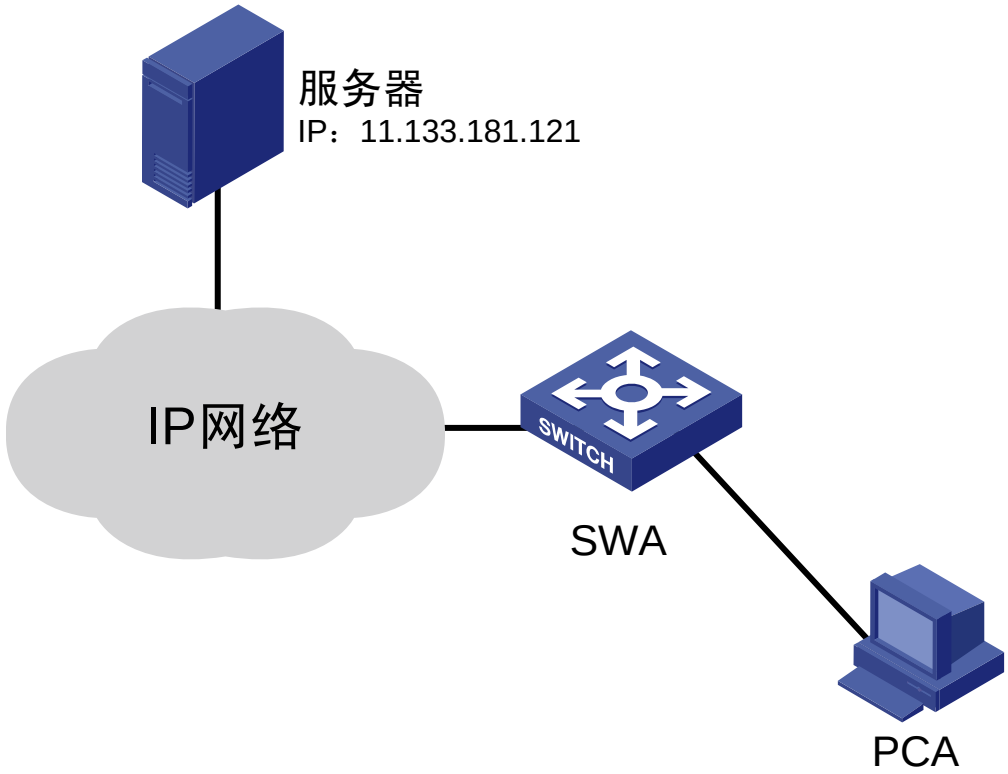
ACL排障相关命令介绍（3）

- **display firewall-statistics { all | interface interface-type interface-number | fragments-inspect }**

  → 该命令用来查看防火墙的统计信息

```
<H3C>display firewall-statistics all
  Firewall is enable, default filtering method is 'deny'.
  Interface: Serial0/0
  In-bound Policy: acl 2001
  Fragments matched normally
  From 2008-11-17 10:33:46  to 2008-11-18 13:59:46
     0 packets, 0 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     0 packets, 0 bytes, 0% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

ACL典型案例一（1）



- **故障现象:**
  - → 要求终端PCA只能访问服务器，不能访问其它网段。
  - → ACL应用后，发现PCA访问不到网络中的任何设备

ACL典型案例一（2）

- SWA上的相关配置：

```
acl number 3001
 rule 0 permit icmp
 rule 1 permit ip destination 11.133.181.121 0
acl number 3999
 rule 0 permit ip
#
traffic classifier deny operator and
 if-match acl 3999
traffic classifier permit operator and
 if-match acl 3001
#
traffic behavior deny
 filter deny
traffic behavior permit
 filter permit
#
qos policy filter
 classifier deny behavior deny
 classifier permit behavior permit
#
interface Ethernet1/0/1
 qos apply policy filter inbound
```

ACL典型案例一（3）

●排障过程

→使用“display acl all”和“display qos policy interface”命令来检查ACL的配置，可以看到配置正确下发；

→怀疑是qos policy filter中的classifier deny behavior deny先生效。在流行为中增加Accounting行为，用于查看报文匹配到哪条规则。

```
<SWA>display qos policy interface
  Interface: Ethernet1/0/1
  Direction: Inbound
  Policy: filter
  Classifier: deny
    Operator: AND
    Rule(s) : If-match acl 3999
    Behavior:
      Accounting Enable:
       1326 (Bytes)
  Classifier: permit
    Operator: AND
    Rule(s) : If-match acl 3001
    Behavior: permit
     Accounting Enable:
       0 (Bytes)
     Filter Enable: permit
```

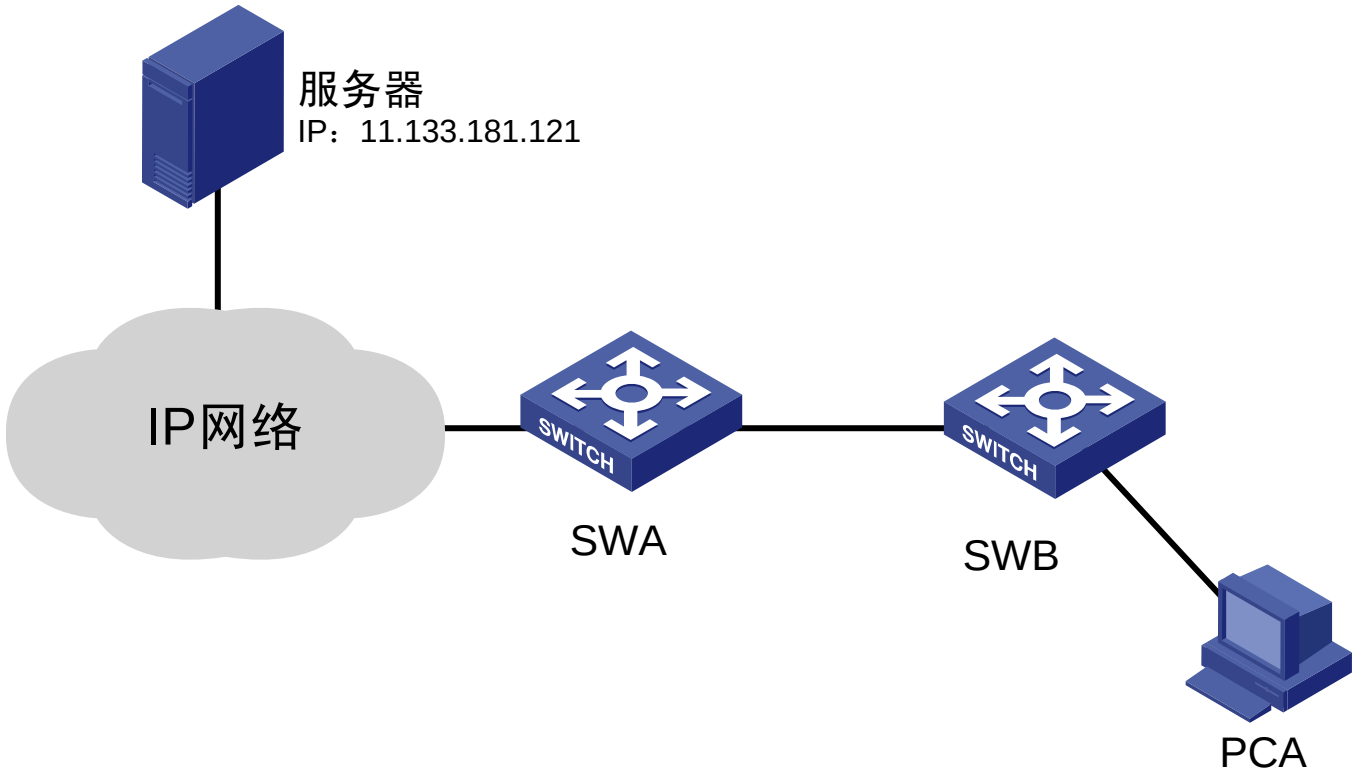
ACL典型案例一（4）

●解决方案

→更改SWA上qos policy filter的相关下发顺序可以解决问题。

```
traffic behavior permit
filter permit
traffic behavior deny
filter deny
#
qos policy filter
classifier permit behavior permit
classifier deny behavior deny
```

ACL典型案例二（1）



- 故障现象
  - → 要求SWB下接终端PCA只能访问服务器；
  - → 应用ACL十多分钟后，PCA访问不到网络中的任何设备。

ACL典型案例二（2）

- SWB上的相关配置：

```
acl number 3001
rule 0 permit ip destination 11.133.181.121 0
#
traffic classifier permit operator or
 if-match acl 3001
traffic classifier deny operator and
 if-match any
#
traffic behavior permit
 filter permit
traffic behavior deny
 filter deny
#
qos policy filter
 classifier permit behavior permit
 classifier deny behavior deny
#
interface GigabitEthernet1/0/1
 qos apply policy filter inbound
```

ACL典型案例二（3）

- 排障过程

→在交换机SWB的相应端口上取消ACL，故障消失。由此确定是ACL导致问题。

→使用“display acl all”和“display qos policy interface”命令查看相关配置

→发现交换机上配置的ACL规则是只允许目的地址为11.133.181.121的报文通过，阻断所有其它报文。所以基本可以断定是ACL阻断了ARP报文

→在ACL下发十多分钟后，使用“display arp all”查看ARP表项，发现没有PCA的ARP表项。由此确认是ACL配置不当导致ARP报文被阻断。

ACL典型案例二（4）

- 解决方案

→ 在SWB上添加相关ARP的ACL如下：

```
acl number 4000
  rule 0 permit type 0806 ffff
traffic classifier permit operator or
  if-match acl 3001
  if-match acl 4000
```

→ 允许ARP报文通过后，PCA和SWA都能进行正常的ARP学习。

目录

- ACL故障排除
- NAT故障排除
- VRRP故障排除
- DHCP故障排除

NAT故障排除

- NAT概述
- NAT常见故障及排除方法
- NAT故障排除相关命令
- NAT排障案例

NAT概述

- **NAT（Network Address Translation）网络地址转换，又称地址代理。NAT的过程即是将IP数据包中的IP头部地址转换成其他IP地址的过程。NAT用于实现私有网络与外部网络的互通，节省了IP地址资源，同时向外隐藏了私有网络的内部结构，在远程接入等网络环境中得到了很多应用。**
- **网络中常见的NAT应用有：**
  - → NAT easy IP
  - → NATP
  - → NAT static
  - → NAT server

NAT常见故障

- 网络中所有主机都无法进行地址转换；
- 网络中部分主机不能进行地址转换；
- 配置NAT后，外部主机无法访问内部服务器。

NAT故障排除的一般步骤（1）

- 网络中所有主机都无法进行地址转换的故障处理步骤
  - → 检查ACL是否配置了允许进行NAT转换的内网地址段
  - → 检查NAT的配置是否正确
  - → 检查设备的NAT session的建立情况
  - → 确认对端设备是否有到地址池IP地址段的路由

NAT故障排除的一般步骤（2）

- 网络中部分主机不能进行地址转换的故障处理步骤
  - →检查ACL是否配置了允许进行NAT转换的内网地址段
  - →检查NAT配置是否正确

NAT故障排除的一般步骤（3）

- 配置NAT后，外部主机无法访问内部服务器的故障处理步骤
  - →检查路由器上NAT Server的配置
  - →添加ICMP报文的NAT Server转换进行辅助排障
  - →通过debug命令查看详细的debug信息

NAT排障相关命令 （1）

- **display nat [all | address-group | outbound | server | session]**

  → 该命令用来查看当前NAT的所有配置信息

```
<H3C >display nat all
  NAT address-group information:
  There are currently 1 nat address-group(s)
    1 : from       100.1.1.1   to      100.1.1.10
  NAT outbound information:
  There are currently 1 nat outbound rule(s)
    Serial0/2/0: acl(2000) --- NAT address-group(1)
  NAT server in private network information:
  There are currently 1 internal server(s)
  Interface:Serial0/2/0, Protocol:6(tcp),
    [global]      100.1.1.100:  23(teln)   [local]      192.168.1.1:  23(teln)
  NAT static information:
    No NAT static have been configured
  NAT aging-time value information:
     tcp ---- aging-time value is  86400 (seconds)
     udp ---- aging-time value is    300 (seconds)
     icmp ---- aging-time value is     60 (seconds)
     pptp ---- aging-time value is  86400 (seconds)
     dns ---- aging-time value is     60 (seconds)
     tcp-fin ---- aging-time value is     60 (seconds)
     tcp-syn ---- aging-time value is     60 (seconds)
     ftp-ctrl ---- aging-time value is   7200 (seconds)
     ftp-data ---- aging-time value is    300 (seconds)
  NAT log information:
    NAT log is not configured
```

NAT排障相关命令 （2）

- **display nat session**
  - → 显示当前NAT设备进行NAT地址转换的表项信息

```
<H3C>display nat session
There are currently 1 NAT session:
 Protocol     GlobalAddr      Port     InsideAddr     Port      DestAddr      Port
    6       219.141.226.2   12289    192.168.1.1   1025      200.0.0.1       23
 VPN:  0,      status:    11,      TTL: 24:00:00,      Left: 23:59:53
```

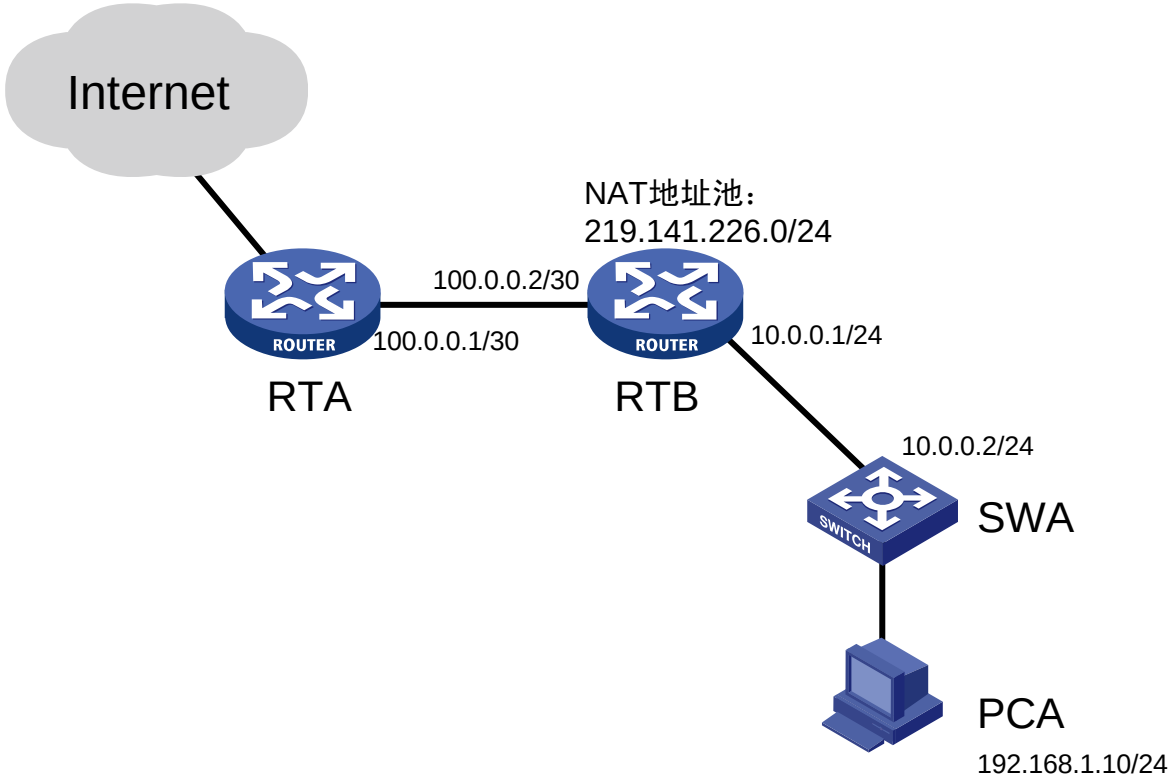
NAT排障相关命令 （3）

- **debugging nat packet**

  → 打开NAT调试信息开关

```
*Dec 16 14:43:36:601 2008 Router NAT/7/debug:
(Serial0/2/0-out :)Pro : ICMP
(    192.168.1.1:  512 -       200.0.0.1:  512) ------>
(      100.1.1.2:12288 -       200.0.0.1:  512)
*Dec 16 14:43:36:611 2008 Router NAT/7/debug:
(Serial0/2/0-in  :)Pro : ICMP
(      200.0.0.1:  512 -       100.1.1.2:12288) ------>
(      200.0.0.1:  512 -     192.168.1.1:  512)
```

NAT典型案例一（1）



- 故障现象

  → 在RTB上配置NAT后，发现内网主机PCA不能访问Internet。

NAT典型案例一（2）

- RTB上的相关配置：

```
nat address-group 1 219.141.226.1 219.141.226.254
#
acl number 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
#
interface Serial0/2/0
 link-protocol ppp
 nat outbound 2000 address-group 1
 ip address 100.0.0.2 255.255.255.252
#
interface Ethernet0/1/0
 ip address 10.0.0.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
 ip route-static 192.168.1.0 255.255.255.0 10.0.0.2
```

NAT典型案例一（3）

- 排障过程

→在交换机检查ACL是否配置了允许进行NAT转换的内网地址段，正常；

→检查公网IP地址池的配置是否正确，正常；

→检查NAT session的建立情况，发现只有出方向报文，没有入方向报文，所以怀疑是没有回程路由所致；

→在对端设备上查看，确认对端设备上没有配置回程路由，问题原因找到。

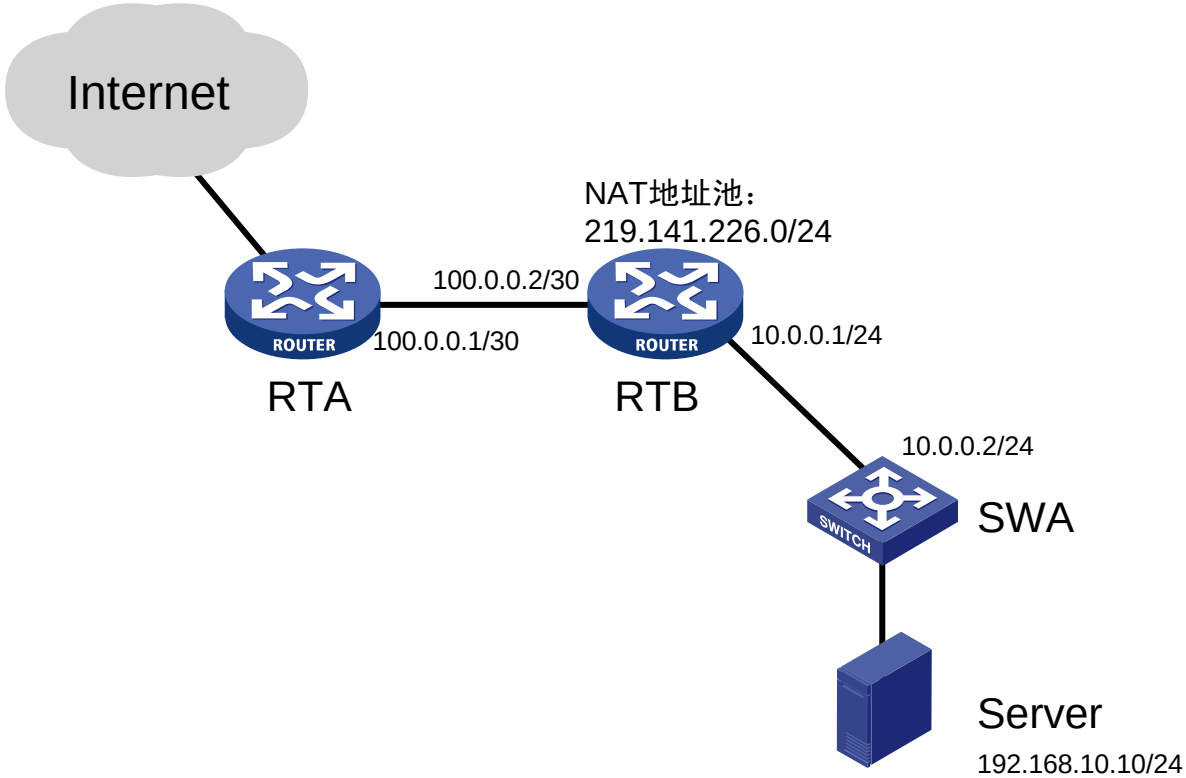
NAT典型案例一（4）

- 解决方案

→在对端设备RTA上配置路由，目的地址为RTB上的地址池。

```
[RTA] ip route-static 219.141.226.0 255.255.255.0 100.0.0.2
```

NAT典型案例二（1）



- 故障现象

  → 在RTB上配置NAT后，发现外部主机不能访问内部服务器。

NAT典型案例二（2）

- RTB上的相关配置：

```
nat address-group 1 219.141.226.1 219.141.226.254
#
acl number 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
#
interface Serial0/2/0
 link-protocol ppp
 nat outbound 2000 address-group 1
nat server protocol tcp global 192.168.10.10 www inside
219.141.226.10 www
ip address 100.0.0.2 255.255.255.252

#
interface Ethernet0/1/0
 ip address 10.0.0.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
 ip route-static 192.168.10.0 255.255.255.0 10.0.0.2
```

NAT典型案例二（3）

- 排障过程

→因为内部主机能够访问外部网络，外部主机无法访问内部服务器，所以判定不是地址池配置错误或没有回程路由；

→使用“display nat server”查看NAT Server的配置信息；发现global和local配置的IP地址有误，global是指内部服务器映射的外部公有地址，local (inside)是指内部服务器的实际IP地址。

```
<RTB>display nat server
NAT server in private network information:
  There are currently 2 internal server(s)
  Interface: Serial0/2/0, Protocol:6(tcp),
    [global]   192.168.10.10:   80(www)   [local]   219.141.226.10:   80(www)
```

NAT典型案例二（4）

- 解决方案

→在RTB上重新配置NAT Server，指定正确的global地址和inside地址。

```
interface Serial0/2/0
   nat server protocol tcp global 219.141.226.10
www inside 192.168.10.10 www
```

目录

VRRP故障排除

- VRRP概述
- VRRP故障排除方法
- VRRP故障排除相关命令
- VRRP故障案例分析

VRRP概述

- VRRP(Virtual Router Redundancy Protocol，虚拟路由器冗余协议)是一种容错协议，是由一台以上的路由器或三层交换机虚拟成一台路由器，而增加网关可靠性的协议。
- VRRP协议的实现有VRRPv2和VRRPv3两个版本。其中，VRRPv2基于IPv4，VRRPv3基于IPv6。

VRRP常见故障

- 设备Log日志里出现VRRP配置错误的信息
- 同一个VRRP组内出现多个主设备；
- 主从设备的VRRP状态同时频繁切换；
- 主设备状态不变，从设备状态频繁切换；

VRRP故障排除的一般步骤（1）

- 设备Log日志里出现VRRP配置错误信息的处理步骤
  - →查看各交换机的VRRP配置信息，保证VRRP组中所有设备的VRRP配置参数一致
  - →查看接收到的VRRP调试信息，可以找出配置错误VRRP参数的设备

VRRP故障排除的一般步骤（2）

- 同一个VRRP组内出现多个主设备的故障处理步骤
  - →若短时间内存在多个Master，属于正常情况
  - →若多个Master长时间共存，这很有可能是由于VRRP组内各设备之间收不到VRRP报文，或者收到不合法的报文造成的
    - 在VRRP设备之间执行“ping 接口实际IP地址” 来测试设备间的可达性
    - 查看设备系统CPU资源的使用情况，如果设备CPU使用率过高，查找相关原因

VRRP故障排除的一般步骤（3）

- 主从设备的VRRP状态同时频繁切换的故障处理步骤

→执行命令display vrrp verbose查看VRRP的参数设置，检查是否在VRRP组中启用了监视端口的功能

→排查被监视端口连接线路状态或使用VRRP的非抢占模式

VRRP故障排除的一般步骤（4）

- **Backup设备的状态频繁切换的故障处理步骤**

  →在VRRP设备之间执行“ping 接口实际IP地址” 来测试设备间的可达性

  →查看设备系统CPU资源的使用情况，如果设备CPU使用率过高，查找相关原因

VRRP排障相关命令（1）

- **display vrrp [verbose]**
  - → 该命令用来显示VRRP当前运行状态及配置信息

```
<H3C >display vrrp verbose
 IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Total number of virtual routers: 1
Interface       : Vlan-interface100
VRID            : 10              Adver. Timer    : 1
Admin Status    : UP                State         : Backup
Config Pri      : 100             Run Pri         : 100
Preempt Mode    : YES               Delay Time    : 0
Auth Type       : NONE
Virtual IP      : 192.168.0.254
Master IP       : 192.168.0.253
```

VRRP排障相关命令（2）

- **debugging vrrp packet**
  - → 该命令用来显示了解当前各接口收发VRRP协议报文的情况

```
<H3C >debugging vrrp packet
IPv4 Vlan-interface10 | Virtual Router 10:receiving from
192.168.0.253, version = 2, type = 1, priority = 110, count ip
addrs = 1, timer = 1, auth type is no, checksum = 3061
```

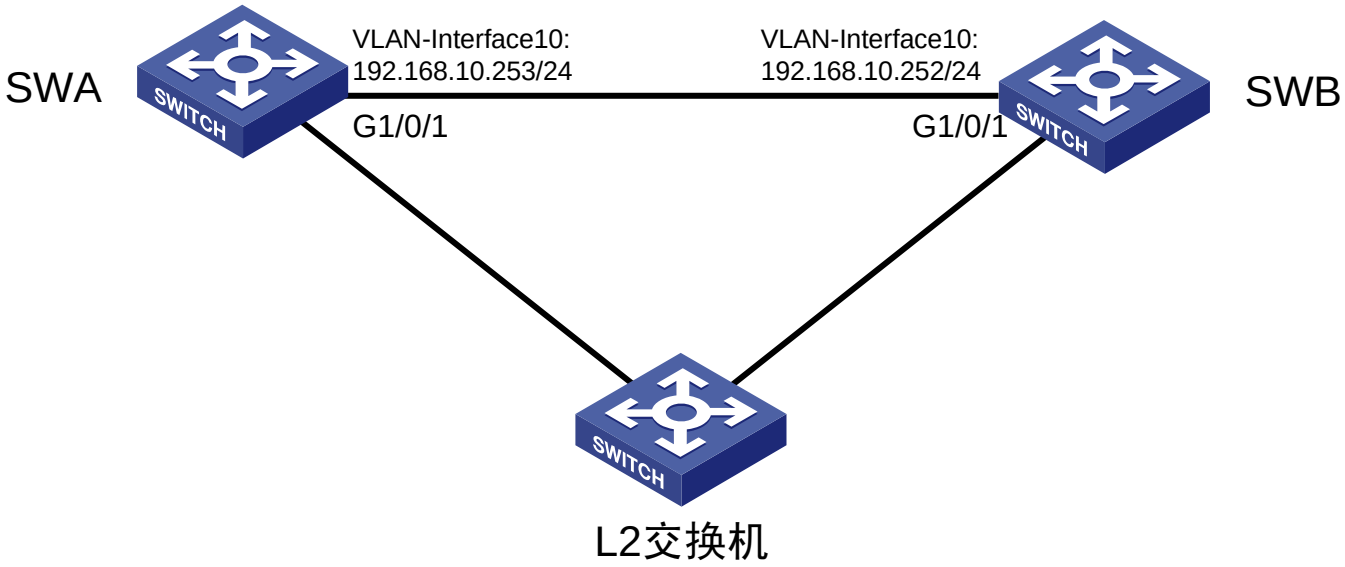
VRRP相关log的介绍

- 一般系统log的格式是：**timestamp sysname module/level/digest:content**，所分别对应中文格式为：时间戳 主机名 模块名/信息级别/信息摘要：信息内容。

%Nov 17 16:58:45:334 2008 SW_A ARP/3/DUPVRRPIP:Slot=4;IP address 192.168.0.254 collision with VRRP virtual IP address on interface Vlan-interface100, sourced by 0000-5e00-010a

→ 以上log显示信息表示：在接口Vlan-interface100上发生了IP地址192.168.0.254的地址冲突，这个冲突信息是由MAC地址为0000-5e00-010a的设备发出的。

VRRP典型案例一（1）



- 故障现象

  → VRRP状态正常，但在控制台上频繁报VRRP配置错误信息。

VRRP典型案例一（2）

- SWA上相关配置：

```
interface Vlan-interface10
ip address 192.168.10.253
255.255.255.0
vrrp vrid 10 virtual-ip 192.168.10.254
vrrp vrid 10 priority 110
#
interface GigabitEthernet1/0/1
port access vlan 10
```

- SWB上相关配置：

```
interface Vlan-interface10
ip address 192.168.10.252
255.255.255.0
vrrp vrid 10 virtual-ip 192.168.10.254
#
interface GigabitEthernet1/0/1
port access vlan 10
```

VRRP典型案例一（3）

- 排障过程

→执行命令display vrrp命令来查看VRRP组状态。状态正常；

→执行命令display vrrp verbose检查VRRP组的配置是否一致。可以看到所有设备上的VRRP配置都正确；

→打开设备上的debug vrrp packet开关，查看设备调试信息。发现IP地址为192.168.0.252的设备发送了具有相同的VRID号的VRRP通告报文。

***Nov 18 15:28:55:265 2008 SWA VRRP/7/DebugPacket:**

IPv4 Vlan-interface1000 | Virtual Router 10:sending from 192.168.10.253, version = 2, type = 1, priority = 110, count ip addrs = 1, timer = 1, auth type is no, checksum = 42316

***Nov 18 15:28:55:331 2008 SWA VRRP/7/DebugPacket:**

IPv4 Vlan-interface1000 | Virtual Router 10:receiving from 192.168.0.252, version = 2, type = 1, priority = 100, count ip addrs = 1, timer = 1, auth type is no, checksum = 47436

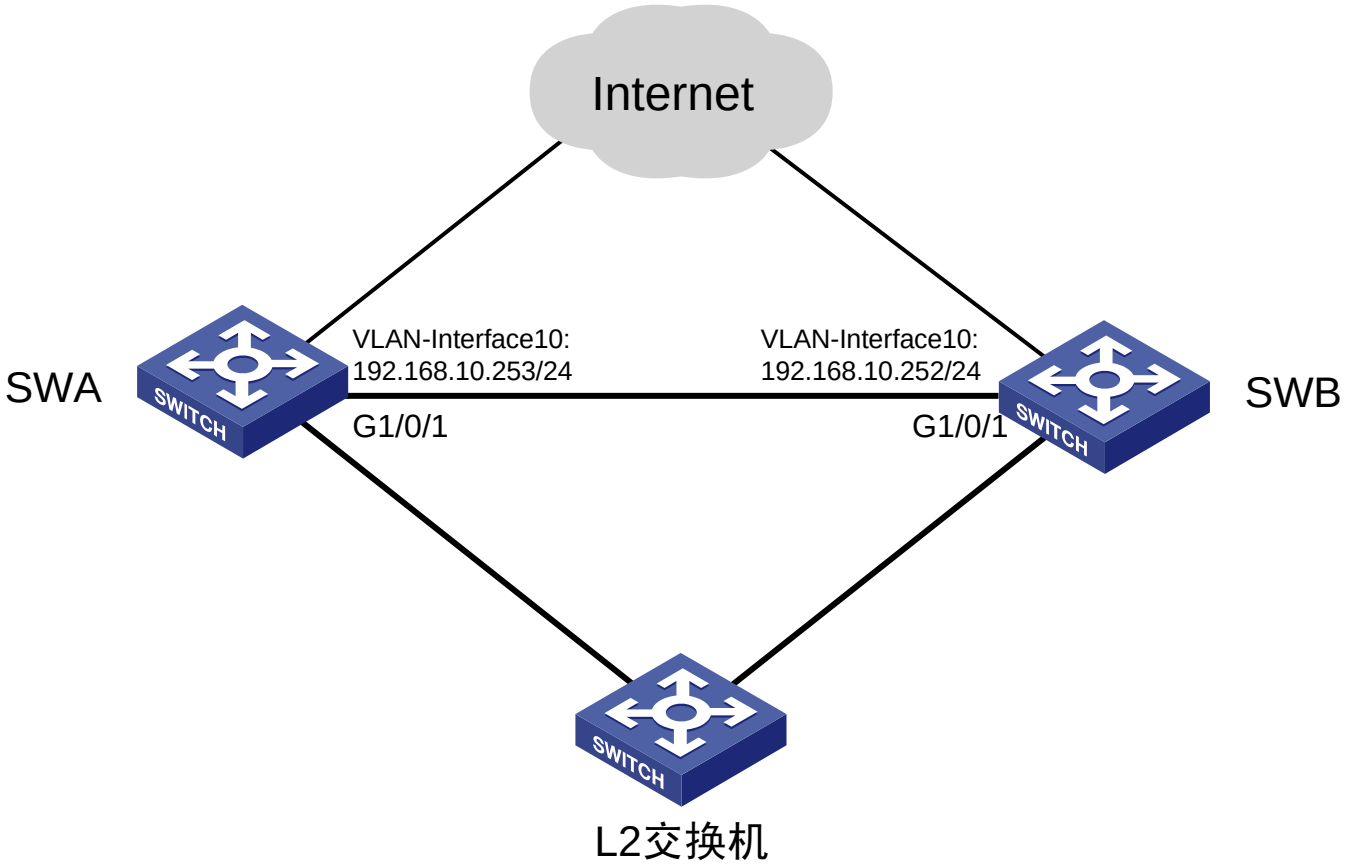
VRRP典型案例一（4）

- 解决方案

→根据IP地址找到该设备，取消VRRP组配置或修改VRRP组为另一个不同的VRID号，问题解决。

如果从IP地址不容易找到出问题的设备，可以根据MAC地址来查找。在VRRP设备上，Virtual Router的MAC地址是00-00-5E-00-01-{vrid}，所以IP地址为192.168.0.252的设备的虚MAC地址是0000-5e00-010a。

VRRP典型案例二（1）



- 故障现象

  → 设备的VRRP主备状态频繁切换。

VRRP典型案例二（2）

H3C

- SWA上相关配置：

```
interface Vlan-interface10
ip address 192.168.10.253
255.255.255.0
vrrp vrid 10 virtual-ip 192.168.10.254
vrrp vrid 10 priority 110
vrrp vrid 10 track interface Vlan-
interface20 reduced 20
#
interface GigabitEthernet1/0/1
port access vlan 10
```

- SWB上相关配置：

```
interface Vlan-interface10
ip address 192.168.10.252
255.255.255.0
vrrp vrid 10 virtual-ip 192.168.10.254
#
interface GigabitEthernet1/0/1
port access vlan 10
```

VRRP典型案例二（3）

- 排障过程

→执行display vrrp verbose查看VRRP的参数设置，可以看到VRRP启用了对Vlan-interface 20接口监控功能；

```
<SWA>display vrrp verbose
Run Method      : VIRTUAL-MAC
Virtual Ip Ping : Enable
Interface       : Vlan-interface10
VRID            : 10                Adver. Timer    : 1
Admin Status    : UP                State           : Master
Config Pri      : 110               Run Pri         : 110
Preempt Mode    : YES               Delay Time      : 0
Auth Type       : NONE
Track IF        : Vlan-interface20  Pri Reduced     : 20
Virtual IP      : 192.168.10.254
Virtual MAC     : 0000-5e00-010a
Master IP       : 192.168.10.253
```

VRRP典型案例二（4）

- 排障过程

→执行命令display logbuffer查看设备的log日志，发现日志中有大量如下的信息：

```
%Nov 18 17:35:23:466 2008 SWA  IFNET/4/UPDOWN:
Line protocol on the interface Vlan-interface20 is DOWN
```

→问题原因找到了，是因为VRRP监控接口状态频繁变化，导致VRRP组中的主备状态频繁切换。

- 解决方案

→修复Vlan-interface20 对应的上行链路，问题解决。

→也可以使用VRRP的非抢占模式来进行规避。在上行链路频繁切换的情况下，能够减少VRRP主备状态频繁切换次数。

目录

DHCP故障排除

- DHCP概述
- DHCP故障排除方法
- DHCP故障排除相关命令
- DHCP故障案例分析

DHCP概述

- **DHCP（Dynamic Host Configuration Protocol）协议是在Bootstrap Protocol（BOOTP）的基础上提出，并增加了重新使用的网络地址的自动分配能力和附加配置选项（Configuration Options）。**
- **网络中常见的DHCP应用有：**
  - →DHCP Server
  - →DHCP relay
  - →DHCP snooping

DHCP常见故障

- 设备作为DHCP Server后，DHCP Client无法得到IP地址；
- 设备作为DHCP Relay后，DHCP Client无法得到IP地址；
- 二层交换机配置DHCP snooping后，DHCP Client无法获得IP地址；
- DHCP Client可以得到IP地址，但却无法通过域名或主机名访问网络资源。

DHCP排障的一般步骤（1）

- **设备作为DHCP Server，DHCP Client无法得到IP地址的故障处理步骤**
  - →检查DHCP Server设备是否启动了DHCP任务；
  - →检查DHCP Server的地址池中是否有IP地址可供分配;
  - →检查DHCP Server到DHCP Client网关地址是否路由可达

DHCP排障的一般步骤（2）

- **设备作为DHCP Relay，DHCP Client无法得到IP地址的故障处理步骤**
  - →检查DHCP Relay及DHCP Server设备是否启动了DHCP任务；
  - →检查设备DHCP Relay相关配置是否正确；
  - →检查 DHCP Relay设备和DHCP Server是否配置有相互可达的路由；
  - →检查设备DHCP Server上是否配置了DHCP Client所在网段的地址池

DHCP排障的一般步骤（3）

- **二层交换机配置DHCP snooping后，DHCP Client无法获得IP地址的故障处理步骤**

  →确认是否是DHCP snooping导致的故障；

  →确认设备的DHCP snooping配置是否正确

DHCP排障的一般步骤（4）

- 无法通过域名或主机名访问网络资源的故障处理步骤
  - →确认终端PC是从正确的DHCP Server得到的IP地址；
  - →检测网络的连通性;
  - →检测DNS服务器

DHCP排障相关命令（1）

- **display dhcp server tree all**
  - → 该命令用来显示DHCP地址池的配置信息

```
<H3C >display dhcp server tree all
Global pool:
Pool name: pool-1
 network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.254
 dns-list 1.1.1.1 1.1.1.2
 domain-name h3c.com
 expired 1 0 0
```

DHCP排障相关命令（2）

- **display dhcp server ip-in-use all**
  - → 该命令用来显示DHCP Server地址池中已经分配的IP地址信息。

```
<H3C >display dhcp server ip-in-use all
Global pool:
 IP address      Client-identifier/          Lease expiration          Type
                 Hardware address
 192.168.1.2     0015-c506-99c4      Jan  2 2009 18:38:46
Auto:COMMITTED
 --- total 1 entry ---
```

DHCP排障相关命令（3）

- **display dhcp relay server-group all**
  - → 该命令用来显示DHCP服务器组中服务器的IP地址。

```
<H3C >display dhcp relay server-group all
  Server-group          Group IP
      1             192.168.207.251
      2             192.168.207.252
<H3C >display current-configuration interface Vlan-interface 192
interface Vlan-interface192
 ip address 192.168.1.254 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
```

DHCP排障相关命令（4）

- **display dhcp-snooping**
  - → 该命令用来显示DHCP snooping的有效表项。

```
<H3C >display dhcp-snooping
DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Type      IP Address       MAC Address      Lease       VLAN      Interface
   D    192.168.207.101   0015-c506-99c4     86310        10
GigabitEthernet1/0/20
```

DHCP排障相关命令（5）

- **debugging dhcp relay packet**
  - → 该命令用来打开DHCP relay调试信息开关。

```
<H3C >debugging dhcp relay packet
  Rx, DHCP request packet, interface Vlan-interface20.
  From client to server(Server-group 1):
  Message type: request
  Hardware type: 1, Hardware address length: 6
  Hops: 0, Transaction ID: 3452412148
  Seconds: 0, Broadcast flag: 0
  Client IP address: 0.0.0.0   Your IP address: 0.0.0.0
  Server IP address: 0.0.0.0   Relay agent IP address: 192.168.1.254
  Client hardware address: 0000-215c-e232 //客户端MAC地址
  Server host name: Not Configured, Boot file name: Not Configured
  DHCP message type: DHCP Discover //DHCP消息类型：DHCP Discover
```

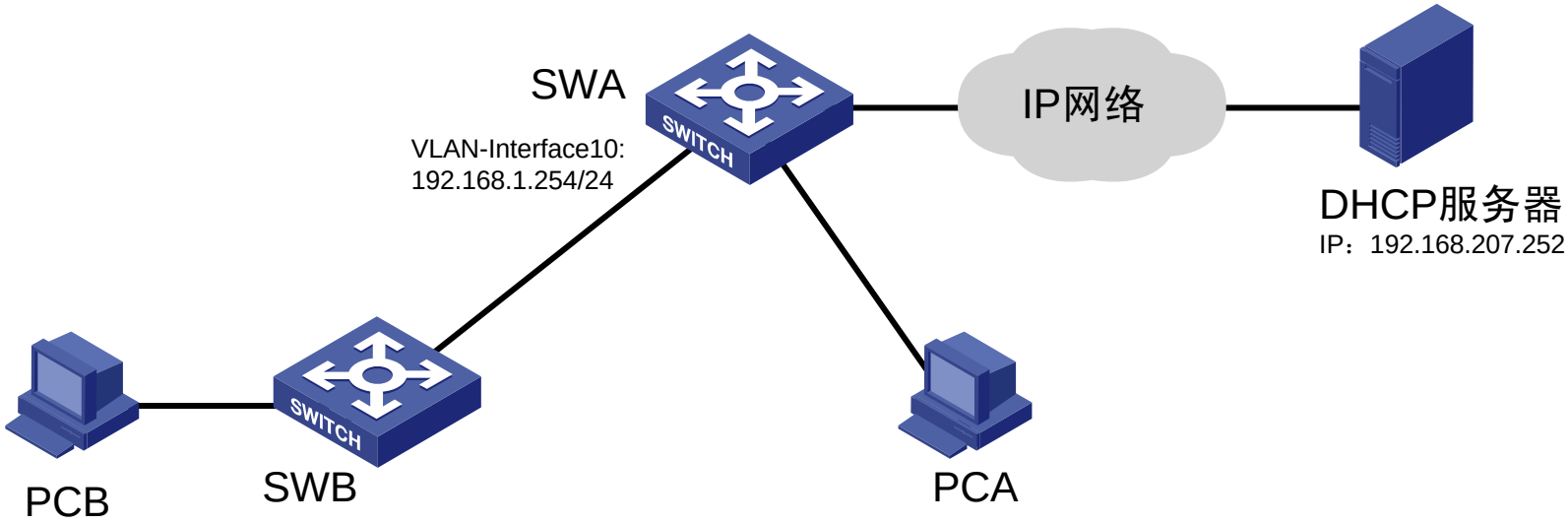
DHCP排障相关命令（6）

- **debugging dhcp-snooping { all | error | event | packet }**

  → 该命令用来打开DHCP snooping调试信息开关。

```
<H3C >debugging dhcp-snooping event
……
*Dec 16 16:35:38:108 2008 H3C DHCPSP/7/EVENT:
 Succeed in sending DHCP snooping packet to trusted port
GigabitEthernet1/0/1 in VLAN 10.
……
*Dec 16 16:35:40:02 2008 H3C DHCPSP/7/EVENT:
 Add DHCP snooping security item(IP address: 192.168.207.101).
```

DHCP典型案例一（1）



- 故障现象

  → 终端PCA和PCB无法动态获得IP地址。

DHCP典型案例一（2）

- SWA上相关配置：

```
dhcp relay server-group 1 ip
192.168.207.251
#
interface Vlan-interface10
 ip address 192.168.1.254 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
#
interface Vlan-interface20
 ip address 192.168.207.120
255.255.255.0
#
dhcp enable
```

- SWB上相关配置：

```
#
 dhcp-snooping
#
```

DHCP典型案例一（3）

- 排障过程

→在交换机SWA上检查设备的配置，看到设备已经启动了DHCP功能；

→检查DHCP relay的配置，可以看到DHCP 服务器组的IP 地址及客户端网关接口的DHCP relay配置都正确；

→检查 DHCP Relay设备和DHCP Server之间的连通性。发现DHCP中继设备到DHCP服务器没有可达的路由；

→在交换机SWB上检查相关DHCP-Snooping配置，发现上行接口上没有配置成dhcp-snooping 的信任端口。

DHCP典型案例一（4）

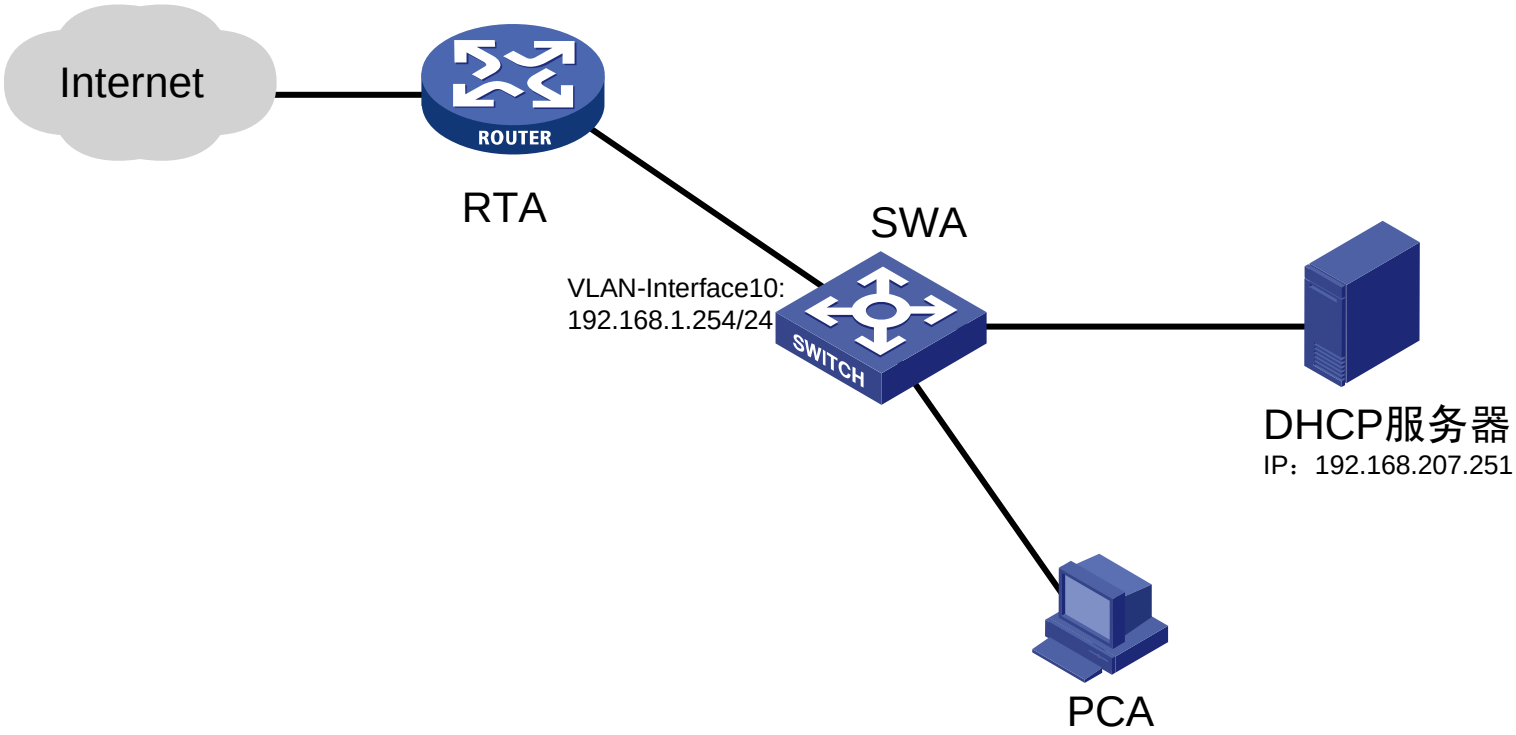
- 解决方案

→在网络中配置了相应的路由后，PCA可以通过DHCP中继动态获得IP地址；

→将SWB的上行端口配置成dhcp-snooping的信任端口，PCB也能够获得IP地址。

```
<SWB>display current-configuration interface GigabitEthernet 1/0/20
interface GigabitEthernet1/0/20
 port access vlan 10
 dhcp-snooping trust
```

DHCP典型案例二（1）



- 故障现象

  → PCA可以获得IP地址，但无法访问外部网站。

DHCP典型案例二（2）

- SWA上相关配置：

```
dhcp server ip-pool pool1
 network 192.168.1.0 mask
255.255.255.0
 gateway-list 192.168.1.254
 domain-name h3c.com.cn
#
interface Vlan-interface10
  ip address 192.168.1.254
255.255.255.0
#
dhcp enable
```

DHCP典型案例二（3）

- 排障过程

→在交换机上查看DHCP地址池IP地址的分配情况，看到PCA的MAC地址与IP的映射，证明PCA是从正确的DHCP服务器分配到了地址；

```
<H3C >display dhcp server ip-in-use all
Global pool:
 IP address       Client-identifier/          Lease expiration          Type
                  Hardware address
 192.168.1.2      0015-c506-99c4              Jan  27 2009 20:38:46
Auto:COMMITTED
 --- total 1 entry ---
```

→Ping命令检测到DHCP服务器的连通性，成功；但以域名方式访问时，解析不成功；

→在PC机上查看，发现没有获得DNS服务器；检查交换机上相关配置，果然没有配置DNS服务器。

DHCP典型案例二（4）

- 解决方案

  →在作为DHCP Server的交换机上增加DNS服务器的地址

```
dhcp server ip-pool pool1
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.254
 dns-list 202.106.0.20 202.106.46.151
 domain-name h3c.com.cn
#
```

本章总结

- ACL常见故障和排除方法
- NAT常见故障和排除方法
- VRRP常见故障和排除方法
- DHCP常见故障和排除方法

ITоIP解决方案专家

杭州华三通信技术有限公司

www.h3c.com