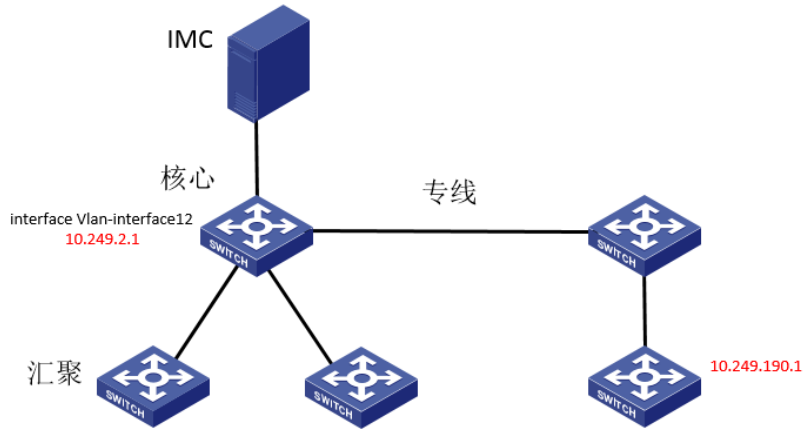


# portal认证+包过滤, 未认证时仍能访问业务地址

Portal packet-filter 郭尧 2021-07-29 发表

## 组网及说明

基本组网



#### 问题描述

故障描述: 终端设备在未通过iMC认证前所有网络都不通, 认证通过后专线对端的内网通, 后将用户强制下线后, 理论上应该是所有网络都不通, 但是实际上是终端ping不通网关10.249.2.1, 10.249.190.1等业务内网地址可以ping通

## 过程分析

测试故障现象

认证通过时:

```
C:\Users\>ping 10.249.2.1

正在 Ping 10.249.2.1 具有 32 字节的数据:
来自 10.249.2.1 的回复: 字节=32 时间=1ms TTL=255
来自 10.249.2.1 的回复: 字节=32 时间=1ms TTL=255
来自 10.249.2.1 的回复: 字节=32 时间<1ms TTL=255
来自 10.249.2.1 的回复: 字节=32 时间=1ms TTL=255

10.249.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\>ping 10.249.190.1

正在 Ping 10.249.190.1 具有 32 字节的数据:
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252

10.249.190.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms, 最长 = 3ms, 平均 = 3ms
```

未进行认证时:

```
C:\Users\>ping 10.249.2.1

正在 Ping 10.249.2.1 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

10.249.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\>ping 10.249.190.1

正在 Ping 10.249.190.1 具有 32 字节的数据:
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=3ms TTL=252
来自 10.249.190.1 的回复: 字节=32 时间=5ms TTL=252

10.249.190.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms, 最长 = 5ms, 平均 = 3ms
```

终端网卡配置:

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网  
删除包过滤后portal业务恢复正常配置。

应该把包过滤掉在上行接口，不要和portal使能在同一接口，否则流量优先匹配包过滤影响portal正  
常业务) 自动获得 IP 地址(O)

使用下面的 IP 地址(S):

IP 地址(I): 10 . 249 . 2 . 2

子网掩码(U): 255 . 255 . 255 . 0

默认网关(D): 10 . 249 . 2 . 1

自动获得 DNS 服务器地址(B)

使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): 10 . 249 . 1 . 59

备用 DNS 服务器(A): . . .

终端接汇聚下，网关在核心，在网关接口起二层portal认证，正常情况下，portal认证通过后，网关和  
对端业务地址才能访问，此时现象是正常的，但是当终端在未进行认证时，网关无法ping通，对端  
的业务地址却能够ping通，到对端业务地址是跨三层走网关转发的，网关不同如何能够进行转发报文呢  
？

检查交换机侧配置：

```
interface Vlan-interface12
description IT
ip address 10.249.2.1 255.255.255.0
packet-filter 3000 inbound
dhcp select relay
dhcp relay server-address 10.249.1.47
portal enable method direct
portal bas-ip 10.249.2.1
portal apply web-server myportal fail-permit
#
radius session-control enable
#
radius scheme imc
primary authentication 10.249.125.48
primary accounting 10.249.125.48
key authentication cipher $c$3$bJCEm0nIHcBxUcz4b1DQjdbxX37FjQY=
key accounting cipher $c$3$oQwuXCtskHZJgnJ87YO4RVuILWL35UQ=
nas-ip 10.249.127.3
#
domain tportal
authorization-attribute idle-cut 30 10240000
authentication portal radius-scheme imc
authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
portal free-rule 10 source ip any destination ip 10.249.1.59 255.255.255.255
portal free-rule 20 source mac 10e7-c62b-1e85
portal free-rule 21 source mac 907e-ba50-e3b7
portal free-rule 22 source mac 907e-ba50-e402
portal free-rule 23 source mac 5803-fb96-1062
portal free-rule 24 source mac 5803-fb96-1082
portal free-rule 25 source mac 5803-fb96-107e
portal free-rule 26 source mac 5803-fb96-1241
portal free-rule 27 source mac 5803-fb96-12dc
portal free-rule 28 source mac bcad-28dc-2557
portal free-rule 29 source mac 00e3-4f68-0ce7
```

portal free-rule 30 source mac 7af6-7aa7-b968  
portal free-rule 31 source mac 0017-61c7-8ca1