SR6600系列路由器OSPF接口启用portal的注意事项

OSPF Portal 张盛楠 2011-07-07 发表

一、 组网：

组网说明：左侧路由器为SR6600系列路由器，右侧为MSR路由器 在两台路由器的互联网段上使能了OSPF，使其它网段可以通过OSPF学习到路由。
在网络连通后，在MSR上下挂一测试PC访问内网网络资源，同时在SR6600路由器的接口上（如图所示）下发可跨三层的portal认证，使PC访问内网资源需经过Portal认证
案例中SR6600使用版本：R2507P01

二、 问题描述：
在未配置Portal认证前，两台路由器间的OSPF邻居关系正常：
[SR6600]display ospf peer

OSPF Process 1 with Router ID 1.1.1.1
Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	Interface	State
2.2.2.2	192.168.1.2	1	35	GE0/0	Full/DR

在配置了如下Portal的相关配置后：
[SR6600] portal server test ip 100.1.1.1 port 9200 key h3c url http://100.1.1.1:8080/portal
[SR6600-GigabitEthernet0/0]ip address 192.168.1.1 255.255.255.0
[SR6600-GigabitEthernet0/0]portal server test method layer3
OSPF邻居出现停留在initial 状态，一直不能达到Full，导致路由学习异常

三、 问题原因分析：
Portal 认证的机制是经过Portal网关接口的报文，如不符合免认证规则，则一律须重定向到Portal 认证服务器进行认证。
在OSPF接口上启用了Portal 以后，MSR上的OSPF Hello报文（源为192.168.1.2 目的地址为224.0.0.5）因认证不能通过被丢弃，导致OSPF邻居40秒后down，由于SR6600 一直在发送Hello报文却无法接收到对端的Hello报文，因此状态一直停留在Initial 状态。

四、 解决方法：
将MSR的接口地址（192.168.1.2）下发到Portal认证的Free-rule 中（作为免认证源地址），使Hello报文得以通过。
配置方法：
[SR6600]portal free-rule 0 source ip 192.168.1.2 mask 32

五、 问题引申：
此时用户如果在MSR的与SR6600的互联接口上下发NAT 使PC访问内网的源地址采用192.168.1.2进行访问，则所有的PC访问将全部被免认证，Portal认证的意义就不存在了。
思考：是否可以在Free-rule中下发目的地址为224.0.0.5/224.0.0.6来避免将源地址192.168.1.2 下发到免认证规则中，确保经过nat转换的用户访问仍然需要Portal认证？
设备上的操作结果：
[SR6600]portal free-rule 1 destination ip 224.0.0.5 mask 32
Error: The IP address is invalid
可见我们在设备上无法配置目的地址为组播地址的free-rule（广播地址是允许的），因此这种Nat组网是无法实现的，只有依靠改变Nat 转换的地址池地址来实现。