H3C S9500交换机URPF功能的配置

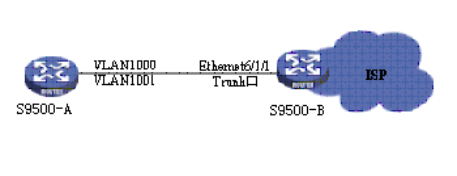
楼依帆　2006-10-08 发表

H3C S9500交换机URPF功能的配置

一、组网需求:

如下组网中，S9500 B上连接ISP，在S9500 B的Ethernet6/1/1 Trunk的VLAN 1000和VLAN1001上启动URPF功能。S9500 B的Slot 5为LSB1NATB0板。端口Ethernet6/1/1分别对VLAN1000和VLAN 1001的报文进行URPF检查。

二、组网图



三、配置步骤：

软件版本：S9500交换机1250之后软件版本

硬件版本：S9500交换机LSB1NATB0业务板

1）配置相关VLAN及VLAN接口地址

[S9500-B] vlan 1000

[S9500-B] vlan 1001

[S9500-B] interface vlan-interface 1000

[S9500-B -Vlan-interface1000] ip address 10.10.10.1 24

[S9500-B] interface vlan-interface 1001

[S9500-B -Vlan-interface1001] ip address 11.11.11.1 24

2）配置端口相关VLAN信息

[S9500-B] interface Ethernet 6/1/1

[S9500-B -Ethernet6/1/1] port link-type trunk

[S9500-B -Ethernet6/1/1] port trunk permit vlan 1000 1001

[S9500-B -Ethernet6/1/1] undo port trunk permit vlan 1

3）配置二层的ACL规则，把需要做URPF检查的相应VLAN的三层报文重定向到LSB1NATB0业务板（配置DMAC为VLAN虚接口MAC，使后续重定向报文到NAT业务板时只重定向三层报文，其他报文不会重定向过去）

[S9500-B] acl number 4000

[S9500-B-acl-link-4000] rule 0 permit ip ingress 1000 egress 00e0-fc39-a9b8 0000-0000-0000

[S9500-B-acl-link-4000] rule 1 permit ip ingress 1001 egress 00e0-fc39-a9b8 0000-0000-0000

4）配置自定义流模板（需要用到字段Ethernet-protocol、DMAC和VLAN ID）和端口重定向到LSB1NATB0业务板。

[S9500-B] flow-template user-defined slot 6 vlanid ethernet-protocol dmac 00-00-00

5）端口下发自定义流模板，且配置相应重定向规则，把三层报文重定向到NAT板

[S9500-B] interface ethernet 6/1/1

[S9500-B-Ethernet6/1/1] flow-template user-defined

[S9500-B-Ethernet6/1/1] traffic-redirect inbound link-group 4000 rule 0 slot 5 1000

[S9500-B-Ethernet6/1/1] traffic-redirect inbound link-group 4000 rule 1 slot 5 1001

6）在VLAN接口下使能URPF功能

[S9500-B] interface vlan-interface 1000

[S9500-B-Vlan-interface1000] urpf enable to slot 5

[S9500-B] interface vlan 1001

[S9500-B-Vlan-interface1001]urpf enable to slot 5

四、配置关键点:

1）URPF是三层的概念，配置重定向时注意只把三层报文（一般报文目的MAC为S9500的VLAN虚接口MAC）重定向到LSB1NATB0业务板处理。注意ACL定义目的IP和VLAN ID时，需要在业务板配置自定义流模板，不然ACL不能生效；

2）S9500的URPF为严格URPF，即FIB和对应的VLAN必须完全一致，才允许检查通过；

3）URPF不支持三层VPN，即私网VPN绑定的VLAN接口不可以做URPF；

4）URPF不支持二层报文。