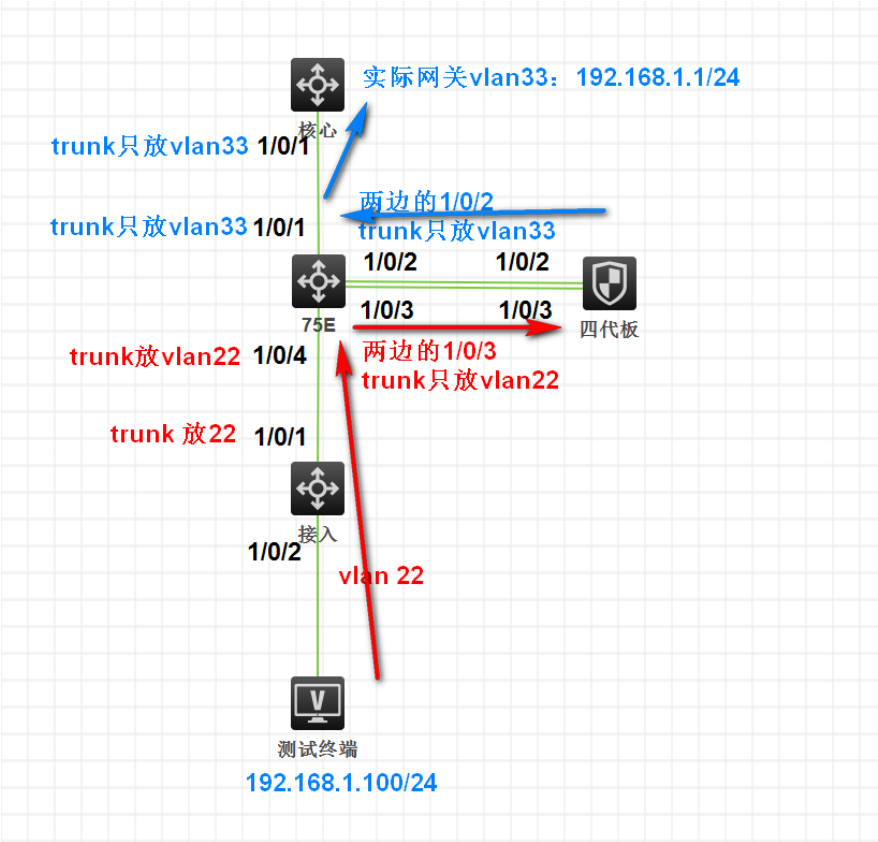
secblade IV板卡--透明部署--跨vlan二层转发案例

二层转发 周凯 2020-09-11 发表

组网及说明

四代板插在75上，需要将内网流量经过四代板过一遍。



问题描述

测试发现流量泛洪到四代板以后被丢掉了，debug aspf packet有如下日志，发现包被ASPF丢掉（关注源目安全域即可，vlan和地址请忽略）：

*Sep 8 15:50:46:574 2020 H3C ASPF/7/PACKET: -COntext=1; The packet was dropped by ASPF for nonexistent zone pair. Src-ZOne=-, Dst-ZOne=-;If-In=Ten-GigabitEthernet1/0/2(3), If-Out=Ten-GigabitEthernet1/0/1(2), VLAN-In=100, VLAN-Out=304; Packet Info:Src-IP=10.149.4.128, Dst-IP=10.149.4.1, VPN-Instance=none,Src-Port=1, Dst-Port=2048. Protocol=ICMP(1).

过程分析

首先四代板透明部署的方案是：跨vlan二层转发，如图测试终端在75下边，都是属于vlan22，所以只能在vlan22二层泛洪，故流量最终到四代板上；

四代板使用桥模式，替换标签命令如下：

bridge 2 inter-vlan

add vlan 22 33

假定安全策略无问题，此时数据进入四代板的1/0/3口标签为22，从四代板1/0/2出来的时候，标签换成33，泛洪到75E，最终找到实际网关vlan33；

安全策略配置如下：

#

security-zone name Untrust

import interface GigabitEthernet1/0/2 vlan 1 to 4094

import interface GigabitEthernet1/0/3 vlan 1 to 4094

import vlan 22 33

#

security-policy ip

rule 4 name 测试

action pass

counting enable

source-zone Untrust

destination-zone Untrust

解决方法

1、四代板透明部署方案为：跨vlan二层转发
2、引流思路：二层泛洪
3、桥模式实质上是替换二层标签
4、四代板有四个内联口，可以只用一个内联口同时放行vlan22与vlan33，图中方案是用两条线得注意放通vlan不能重合，防止环路；
5、安全域不一定要加到一个域，按照trust-UNtrust操作也可以；
6、两台75E、两块四代板堆叠思路一致，测试没问题；
7、重点注意，安全域中必须加入二层vlan，即import vlan 22，下边这个ASPF报错就是当时没有加二层vlan，所以出现源目域都为空的情况；
*Sep 8 15:50:46:574 2020 H3C ASPF/7/PACKET: -COntext=1; The packet was dropped by ASPF for nonexistent zone pair. Src-ZOne=-, Dst-ZOne=-;If-In=Ten-GigabitEthernet1/0/2(3), If-Out=Ten-GigabitEthernet1/0/1(2), VLAN-In=100, VLAN-Out=304; Packet Info:Src-IP=10.149.4.128, Dst-IP=10.149.4.1, VPN-Instance=none,Src-Port=1, Dst-Port=2048. Protocol=ICMP(1).