某局点使用SR8804-X配置IPOE+web认证，仅针对ipv4做认证，ipv4业务正常，但是ipv6业务不通经验案例

IPv6 Portal Web页面 ipoe **徐猛** 2018-11-08 发表

组网及说明

现场在SR8804-X上起子接口，在该子接口上配置了ipv4地址和ipv6的地址，并使用该子接口的作为终端的网关。

组网配置说明：

1. 用户主要实现ipv4的无感知，第一次登陆弹出portal认证界面进行认证；

2.下次用户接入网络时，直接使用mac地址作为用户向AAA发送radius报文，认证成功直接上线；

3. 若认证不成功，终端弹出portal页面；

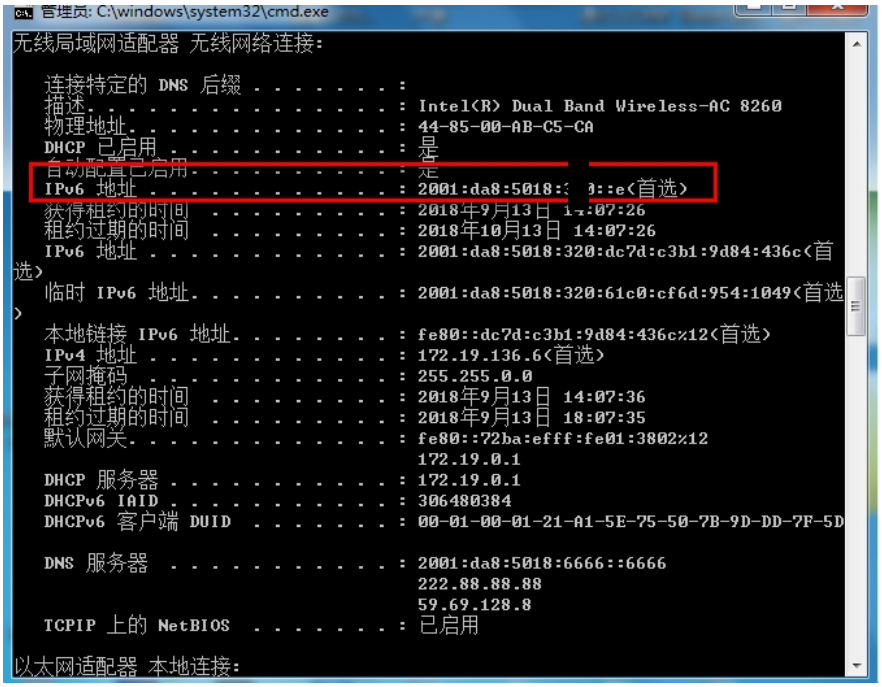
4. 对于ipv6地址不做认证要求，IPv6资源放通访问；

问题描述

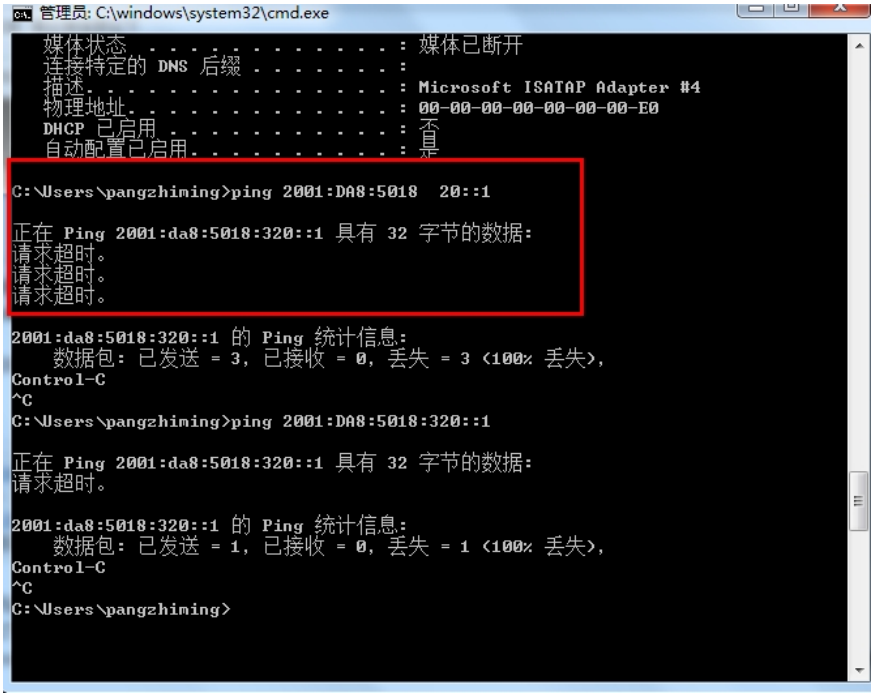
该局点使用SR8804-X配置IPOE+web认证，现场仅需要针对ipv4做认证，当前ipv4业务正常，但是ipv6业务不通，终端无法ping通自己的IPV6网关，取消 ip subscriber l2-connected enable后（即关闭IPOE认证），ipv6业务正常。

具体现场测试情况如下：

1、用户终端能够获取IPV6地址截图：



2、客户端测试ipv6不能ping通网关



过程分析

1. 首先检查设备侧配置：

现场测试终端下联在3101子接口，且3101子接口为测试终端网关：

```
#
interface Route-Aggregation1.3101
 ip address 172.19.0.1 255.255.248.0
 arp send-gratuitous-arp
 vlan-type dot1q vid 3101
 vlan-termination user-mode
 ipv6 dhcp select server
 ipv6 address 2001:DA8:5018:320::1/64
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable        //开启ipoe功能，并配置二层接入模式
 ip subscriber initiator dhcp enable
 ip subscriber initiator unclassified-ip enable matching-user        //只配置了未知源IPv4报文触发生成IPoE会话的功能，并未配置ipv6的。
 ip subscriber user-detect ip arp retry 2 interval 60
 ip subscriber authentication-method web mac-auth
 ip subscriber pre-auth domain dm1
 ip subscriber mac-auth domain dm2
 ip subscriber web-auth domain dm2
#
```

命令说明：

1.1.36 ip subscriber enable

ip subscriber enable命令用来在接口上开启IPoE功能并指定用户的接入模式。

undo ip subscriber enable命令用来关闭接口上的IPoE功能。

【命令】

ip subscriber { **l2-connected** | **routed** } **enable**

undo ip subscriber { **l2-connected** | **routed** } **enable**

【缺省情况】

接口上的IPoE功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图

三层聚合接口视图/三层聚合子接口视图

L3VE接口视图/L3VE子接口视图

检查了下现场的配置：

全局下发了qos策略，且这里确认了下：· 在基于端口、基于VLAN和基于全局三种应用QoS策略的方式中，基于端口的方式优先级高于基于VLAN的方式，
而基于全局的方式优先级最高。即设备对于接收/发送的流量，首先匹配全局应用的QoS策略中的流分类条件，如果匹配则直接执行全局的QoS策略而不再执
行基于端口和VLAN的策略。
#
qos apply policy web global inbound
 qos apply policy out global outbound
#

以下是出入方向的qos明细内容：
#
acl ipv6 advanced name neiwang
rule 0 permit ipv6 user-group web
rule 5 permit ipv6
#
traffic classifier neiwang operator or
if-match acl name neiwang
if-match acl ipv6 name neiwang
#
traffic behavior neiwang
filter permit
#
qos policy web
classifier web_permit behavior web_permit
classifier neiwang behavior neiwang　　//入方向的qos通过流分类neiwang已经放通进来的ipv6报文
classifier web_http behavior web_http
classifier web_https behavior web_https
classifier ip_cpu behavior web_cpu
classifier ip_deny behavior web_deny
#
acl ipv6 advanced name neiwang_out
rule 0 permit ipv6 user-group web
rule 5 permit ipv6
#
traffic classifier neiwang_out operator or
if-match acl name neiwang_out
if-match acl ipv6 name neiwang_out
#
traffic behavior neiwang_out
filter permit
#
qos policy out
classifier web_out behavior web_out
classifier neiwang_out behavior neiwang_out　　//出方向的qos通过流分类neiwang_out放通ipv6报文
classifier ip_deny behavior web_deny
#

后续针对ipv6 的报文进行了debug，收集debugging ip subscriber all，debugging portal all的信息。用测试终端测试，并收集debug，发现有相应IPOEdebug信息，但是现场qos都是放通的，且触发认证配置中并未配置ipv6报文触发认证。
*Sep 13 14:18:30:437 2018 SR8804-X IPOE/7/TIMER: -MDC=1-Chassis=2-Slot=4; User detection timer expired: Interface=Route-Aggregation1.3101, IP=2001:DA8:5018:320::E, VLAN=3101, CVLAN=65535.
*Sep 13 14:18:30:438 2018 SR8804-X IPOE/7/EVENT: -MDC=1-Chassis=2-Slot=4; Sent NS packet successfully: Interface=Route-Aggregation1.3101, IP=2001:DA8:5018:320::E, VLAN=3101, CVLAN=65535.
*Sep 13 14:18:30:440 2018 SR8804-X IPOE/7/EVENT: -MDC=1-Chassis=2-Slot=4; Received an NA reply: Interface=Route-Aggregation1.3101, IP=2001:DA8:5018:320::E, VLAN=3101, CVLAN=65535.

后续协调产品线工程师一同进行定位后，发现如下官网有如下说明：
对于IPoE Web认证，在IPv6网络中，为避免终端使用临时IPv6地址进行认证，从而导致认证失败，可

在用户上线接口配置ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length } no-advertise命令禁止终端生成临时IPv6地址。

解决方法

lpoe的v4认证参考典型配置即可，v6只能配置成dhcpv6的方式获取地址，再通过全局mqc中放行所有ipv6的用户来达到不认证的效果，同时借口需要关闭ra报文的功能，相关关键配置如下标红

1. 入出方向mqc下增加以下针对ipv6报文的cb对，对ipv6计费报文不计费

```
classifier ipv6 behavior ipv6

traffic classifier ipv6 operator and
 if-match acl ipv6 name ipv6
#
traffic behavior ipv6
 filter permit
 free account
#
acl ipv6 advanced name ipv6
 rule 0 permit ipv6
```

2. 接口增加配置，关闭ra报文，使pc不生成ipv6临时地址

```
interface Route-Aggregation1.1001
description YeWu-vlan
ip address 10.63.0.1 255.255.192.0
vlan-type dot1q vid 1001
dhcp server apply ip-pool vlan1001
ipv6 dhcp select server
ipv6 dhcp server apply pool vlan1001
ipv6 nd ra prefix 2001:250:4402:1112::/64 no-advertise
 ipv6 address FE80:101::1 link-local
ipv6 address 2001:250:4402:1112::1/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
ipv6 nd ra no-advlinkmtu
ip subscriber l2-connected enable
ip subscriber user-detect ip arp retry 3 interval 270
ip subscriber authentication-method web mac-auth
ip subscriber http-fast-reply enable
ip subscriber captive-bypass enable ios optimize
ip subscriber pre-auth domain ipoe
```