19 常见 NAC 操作

关于本章

介绍NAC的常见操作。

19.1 配置 MAC 旁路认证

在同时存在PC以及少量哑终端（如打印机）的网络环境中，可配置802.1X认证MAC旁路认证功能保证哑终端同样能够接入802.1X认证网络。例如接口GE1/0/1和GE1/0/5下均接有大量PC以及少量哑终端，为保证PC以及哑终端都能够接入网络，可在接口下使能802.1X认证MAC旁路认证功能。以接口GE1/0/1为例，GE1/0/5的配置与之类似。

NAC传统模式下配置MAC旁路认证功能：

- 在系统视图下对多个接口进行批量配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
[HUAWEI] dot1x mac-bypass interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
```

- 在接口视图下对每个接口进行单个配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dot1x enable
[HUAWEI-GigabitEthernet1/0/1] dot1x mac-bypass
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/5
[HUAWEI-GigabitEthernet1/0/5] dot1x enable
[HUAWEI-GigabitEthernet1/0/5] dot1x mac-bypass
```

NAC统一模式下配置MAC旁路认证功能：

- 对于V200R009C00之前的版本

  需要在接口下同时配置802.1X和MAC认证，并且802.1X认证配置在前。


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication dot1x mac-authen
[HUAWEI-GigabitEthernet1/0/1] quit
```

- 对于V200R009C00及其之后的版本

  需要在认证模板下同时绑定802.1X接入模板和MAC接入模板，并且配置命令**authentication dot1x-mac-bypass**。之后将认证模板绑定到接口上。

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] quit
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] mac-access-profile m1
[HUAWEI-authen-profile-p1] dot1x-access-profile d1
[HUAWEI-authen-profile-p1] authentication dot1x-mac-bypass
[HUAWEI-authen-profile-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication-profile p1
[HUAWEI-GigabitEthernet1/0/1] quit
```

相关信息

技术论坛

一个门卫的故事（一）

一个门卫的故事（二）

19.2 配置 Guest VLAN 功能

为了满足用户不进行认证即能访问某些网络资源需求，譬如下载客户端软件、升级客户端、更新病毒库等，可配置Guest VLAN功能。例如为保证接口GE1/0/1和GE1/0/5下的用户能够实时更新病毒库，可在接口下是配置Guest VLAN功能。假设病毒库服务器在VLAN10中。

说明

交换机V200R005C00及其之后版本，仅NAC传统模式支持Guest VLAN功能。

- 在系统视图下对多个接口进行批量配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
[HUAWEI] authentication guest-vlan 10 interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
```

- 在接口视图下对每个接口进行单个配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dot1x enable
[HUAWEI-GigabitEthernet1/0/1] authentication guest-vlan 10
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/5
[HUAWEI-GigabitEthernet1/0/5] dot1x enable
[HUAWEI-GigabitEthernet1/0/5] authentication guest-vlan 10
```

相关信息

技术论坛

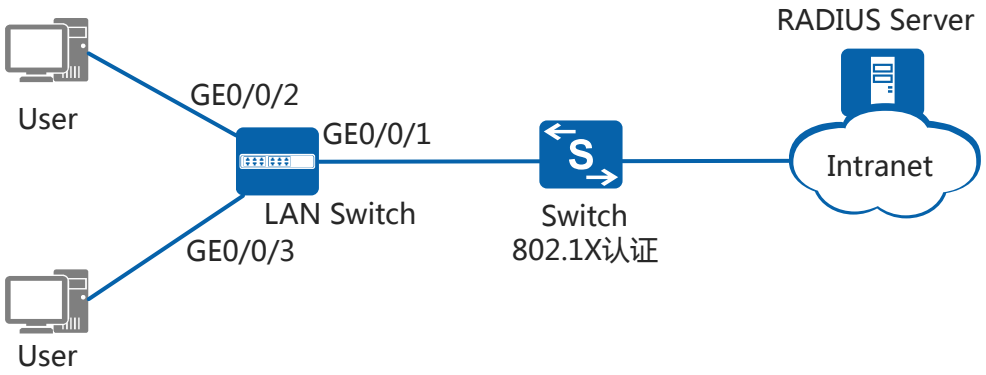
一个门卫的故事（一）

一个门卫的故事（二）

19.3 配置 802.1X 认证报文二层透明传输功能

802.1X认证过程中的EAP协议报文，是一种BPDU报文。对于BPDU报文，华为公司的交换机设备当前缺省是不做二层转发的。因此如果使能802.1X的设备和用户之间还存在二层交换机，就必须在其上配置二层透明传输，否则用户发送的EAP报文将无法到达认证设备，用户自然无法通过认证。

图 19-1 配置 802.1X 认证报文二层透明传输功能示意图



如图19-1所示，使能802.1X认证的接入设备Switch与用户之间存在二层交换机LAN Switch，为保证用户的802.1X认证报文能够通过LAN Switch到达Switch，需要在LAN Switch上进行如下配置（二层交换机以S5700LI为例进行说明）。

```
<HUAWEI> system-view
[HUAWEI] sysname LAN Switch
[LAN Switch] l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002   //group-mac不能设置为保留的组播MAC地址（0180-C200-0000～0180-C200-002F）以及其他几种特殊MAC地址，其余MAC地址均可。
[LAN Switch] interface gigabitethernet 0/0/1 //需要在二层交换机连接上行网络以及用户的所有接口上进行配置
[LAN Switch-GigabitEthernet0/0/1] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/1] bpdu enable
[LAN Switch-GigabitEthernet0/0/1] quit
[LAN Switch] interface gigabitethernet 0/0/2
[LAN Switch-GigabitEthernet0/0/2] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/2] bpdu enable
[LAN Switch-GigabitEthernet0/0/2] quit
[LAN Switch] interface gigabitethernet 0/0/3
[LAN Switch-GigabitEthernet0/0/3] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/3] bpdu enable
[LAN Switch-GigabitEthernet0/0/3] quit
```

相关信息

技术论坛

一个门卫的故事（一）

一个门卫的故事（二）

19.4 限制 802.1X 认证接口可以学习的 MAC 地址数量

由于802.1X认证功能与**mac-limit**命令（配置接口能够学习的最大MAC地址数量）以及**mac-address learning disable**命令（关闭接口的MAC地址学习功能）冲突，因此当接口使能802.1X认证功能之后，无法再通过执行**mac-limit**命令和**mac-address learning disable**命令限制接口可以学习的MAC地址数量，下面是几种替代方法。

NAC 传统模式

- （适用于所有版本）通过限制接口下允许接入的802.1X认证用户数量，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x max-user 3
```

- （适用于V200R012及之后版本）在接口下配置端口安全功能，并限制该接口能够学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 3
```

NAC 统一模式

- （适用于V200R005-V200R008版本）通过限制接口下允许接入的用户数量，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1]  authentication mode multi-authen max-user 3
```

- （适用于V200R009及之后版本）通过在认证模板下配置允许接入的802.1X认证用户数量并将该模板应用到指定接口，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] quit   //缺省的802.1X认证方式为EAP中继认证
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] dot1x-access-profile d1
[HUAWEI-authen-profile-p1] authentication mode multi-authen max-user 3 dot1x
[HUAWEI-authen-profile-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication-profile p1
```

- （适用于V200R012及之后版本）在接口下配置端口安全功能，并限制该接口能够学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 3
```

