

## 组网及说明

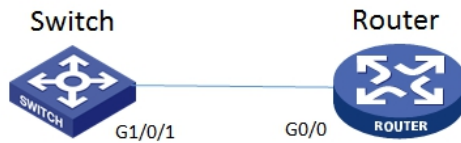
### 1.1 适用产品系列

本案例适用于如S5024PV3-EI-HPWR、S5048PV3-EI、S5120V2-52P-LI、S5120V2-28P-SI、S5130-52S-EI、S5130S-28S-EI、S5150X-16ST-EI等S5000PV3、S5120V2、S5130、S5150系列的交换机。

### 1.2 配置需求

Switch管理VLAN是VLAN2，开启了Telnet功能。Telnet用户主机与Switch相连，需要实现Switch对不同的Telnet用户进行分权管理。其中，admin用户拥有最高管理权限，user1用户只有ping、tracert和display interface 查看接口信息权限。

## 2 组网图



## 配置步骤

### 3.1 Switch配置

```
# 创建管理VLAN。
<H3C> system-view
#设置交换机系统名称为Switch
[H3C]sysname Switch
[Switch] vlan 2
[Switch-vlan2]quit
# 设置交换机管理地址。
[Switch]interface Vlan-interface 2
[Switch-Vlan-interface2]ip address 1.1.1.1 255.255.255.0
[Switch-Vlan-interface2]quit
# 设置交换机连接Router的接口加入VLAN2。
[H3C]interface g1/0/1
[H3C-GigabitEthernet1/0/1]port link-type access
[H3C-GigabitEthernet1/0/1]port access vlan 2
[H3C-GigabitEthernet1/0/1]quit
# 开启telnet功能。
[Switch]telnet server enable
# 配置使用帐号+密码方式进行telnet认证。
[Switch]line vty 0 4
[Switch-line-vty0-4]authentication-mode scheme
[Switch-line-vty0-4]quit
# 创建admin帐号。
[Switch]local-user admin
# 配置帐号的服务类型为telnet。
[Switch-luser-manage-admin]service-type telnet
# 配置帐号的密码为admin。
[Switch-luser-manage-admin]password simple admin
#赋予帐号最高权限。
[Switch-luser-manage-admin]authorization-attribute user-role level-15
[Switch-luser-manage-admin]quit
# 配置user1角色，定义只能使用ping、tracert和display interface相关命令
[Switch]role name user1
[Switch-role-user1]rule 1 permit command ping *
[Switch-role-user1]rule 2 permit command tracert *
[Switch-role-user1]rule 3 permit command display interface *
[Switch-role-user1]quit
# 创建账号user1。
```

```
[Switch]local-user user1
# 配置帐号的服务类型为telnet。
[Switch-luser-manage-user1]service-type telnet
# 配置帐号的密码为用户1。
[Switch-luser-manage-user1]password simple user1
#赋予帐号拥有user1角色的权限。
[Switch-luser-manage-user1]authorization-attribute user-role user1
# 为保证用户仅使用授权的用户角色role1，删除用户user1具有的缺省用户角色network-operator。
[Switch-luser-manage-user1]undo authorization-attribute user-role network-operator
[Switch-luser-manage-user1]quit
#保存配置
[Switch]save force
```

### 3.5 Router配置

```
#设置交换机系统名称为Router
[H3C]sysname Router
#Router配置接口地址，保证能和Switch互通
[Router]interface GigabitEthernet 0/0
[Router-GigabitEthernet0/0]ip address 1.1.1.2 255.255.255.0
[Router-GigabitEthernet0/0]quit
#保存配置
[Router]save force
```

### 3.2 验证配置

1) Router使用user1帐号 telnet登录Switch测试，display 只能查看接口的信息：

```
<Router>telnet 1.1.1.1
Trying 1.1.1.1 ...
Press CTRL+K to abort
Connected to 1.1.1.1 ...

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

login: user1
Password:
<Switch>dis
<Switch>display ?
    interface Specify the interface configuration view
<Switch>display [ ]
```

2) Router使用admin帐号 telnet登录Switch测试，可以查看所有信息：

```
<Router>telnet 1.1.1.1
Trying 1.1.1.1 ...
Press CTRL+K to abort
Connected to 1.1.1.1 ...

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

login: admin
Password:
<Switch>
<Switch>dis ?
    aaa AAA module
    acl Specify ACL configuration information
    adjacent-table Display adjacent table information
    alias Command alias configuration information
    archive Display archive information
    arp ARP module
    attack-defense Attack defense function
    bfd BFD module
    bgp Border Gateway Protocol (BGP) module
    boot-loader Display software image files
    bootp BOOTP information
    bootrom-access Display bootrom access control information
    buffer Buffer management function
    cfd Connectivity Fault Detection (CFD) module
    clock Clock status and configuration information
    cloud Cloud management module
    cmtunnel Cloud management tunnel information
    configuration Configuration information
    copyright Display Copyright
    counters Statistics information
    cpu-usage CPU usage information
    crypto-engine Crypto engine module
    current-configuration Current configuration
    --- More --- [ ]
```

