

《HCIA – Datacom 实验手册》目录

01、配置网络设备的明文密钥实验组网	-----	003
02、配置网络设备的密文密钥实验组网	-----	004
03、配置 VLAN 实验组网 (一)	-----	005
04、配置 VLAN 实验组网 (二)	-----	008
05、配置 VLAN 实验组网 (三)	-----	012
06、配置 STP 实验组网	-----	015
07、配置二层链路手动负载均衡模式下的链路聚合实验组网	-----	018
08、配置三层链路手动负载均衡模式下的链路聚合实验组网	-----	020
09、配置二层链路 LACP 模式下的链路聚合实验组网	--	022
10、配置三层链路 LACP 模式下的链路聚合实验组网	--	025
11、配置广播型网络上的静态路由实验组网	-----	028
12、配置串行接口下的静态路由实验组网	-----	030
13、配置静态路由等价负载分担实验组网	-----	032
14、配置缺省路由实验组网	-----	034
15、配置单臂路由实验组网	-----	036
16、配置 RIP 实验组网	-----	038
17、配置 OSPF 单区域实验组网	-----	041
18、配置基本 ACL 实验组网	-----	044

19、配置高级 ACL 实验组网	-----	047
20、配置静态 NAT 实验组网	-----	050
21、配置动态 NAT 实验组网	-----	052
22、配置 NAT Easy IP 实验组网	-----	054
23、配置 NAT 服务器实验组网	-----	056
24、配置 PPP PAP 认证实验组网	-----	058
25、配置 PPP CHAP 认证实验组网	-----	060
26、配置 PPPoE 实验组网 (一)	-----	062
27、配置 PPPoE 实验组网 (二)	-----	065
28、配置 AAA 本地认证及授权实验组网	-----	067
29、配置 AAA 在 ACS 上进行远端认证实验组网	-----	074
30、配置基于 CLI 的远程登录操作实验组网	-----	079
31、配置基于 Web 方式登录防火墙实验组网	-----	081
32、配置 SNMPv1 实验组网	-----	084
33、配置 SNMPv2c 实验组网	-----	093
34、配置 SNMPv3 实验组网	-----	103
35、配置无线 AC 控制器实验组网	-----	117
36、使用 Python 的 Telnetlib 登录设备实验组网	-----	133
37、配置 FTP 实验组网	-----	135

一、配置网络设备的明文密钥实验组网

一、实验拓扑：



二、实验目的：

通过在设备上配置明文密钥，令用户通过 Console 线缆连接设备时，需要登录密钥

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

user-interface console 0 #进入用户接口配置界面

authentication-mode password #配置认证模式为密码认证

set authentication password simple huawei #配置认证方式为明文认证，并创建密钥

二、配置网络设备的密文密钥实验组网

一、实验拓扑：



二、实验目的：

通过在设备上配置密文密钥，令用户通过 Console 线缆连接设备时，需要登录密钥

三、实验步骤：

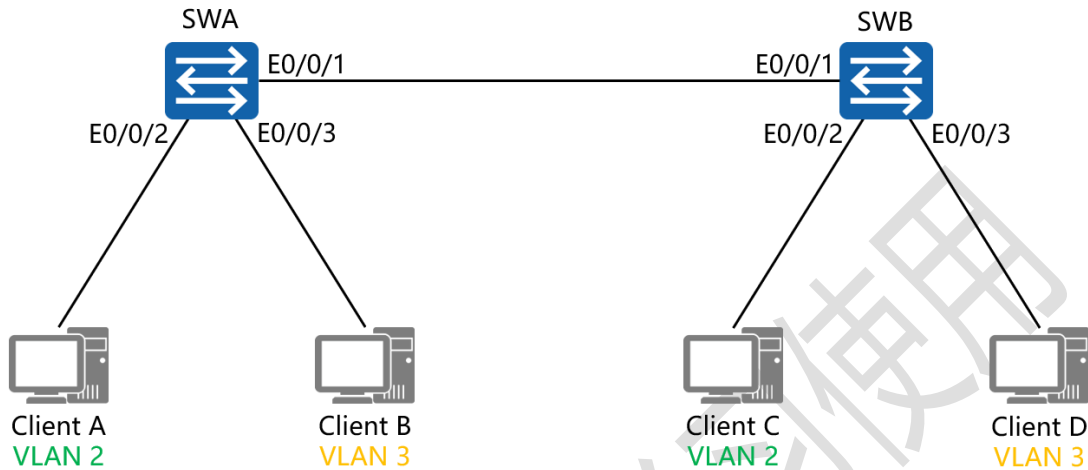
RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
user-interface console 0    #进入用户接口配置界面
authentication-mode password    #配置认证模式为密钥认证
set authentication password cipher 123qwe`    #配置认证方式为密文认证，并创建密钥
    
```

三、配置 VLAN 实验组网（一）

一、实验拓扑：



二、实验目的：

令同 VLAN 之间的主机能够相互通信，不同 VLAN 之间的主机不能相互通信

三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

vlan 2 #创建 VLAN 2

vlan 3 #创建 VLAN 3

interface E0/0/2 #进入相应的端口

port link-type access #将端口的链路类型配置为接入模式

```

port default vlan 2      #将端口加入进 VLAN 2
interface E0/0/3        #进入相应的端口
port link-type access    #将端口的链路类型配置为接入模式
port default vlan 3      #将端口加入进 VLAN 3
interface E0/0/1        #进入相应的端口
port link-type trunk     #将端口配置为中继模式
port trunk allow-pass vlan all #允许该中继端口传递所有 VLAN 的信息

```

SWB:

```

system-view
sysname SWB
vlan 2
vlan 3
interface E0/0/2
port link-type access
port default vlan 2
interface E0/0/3
port link-type access
port default vlan 3
interface E0/0/1

```

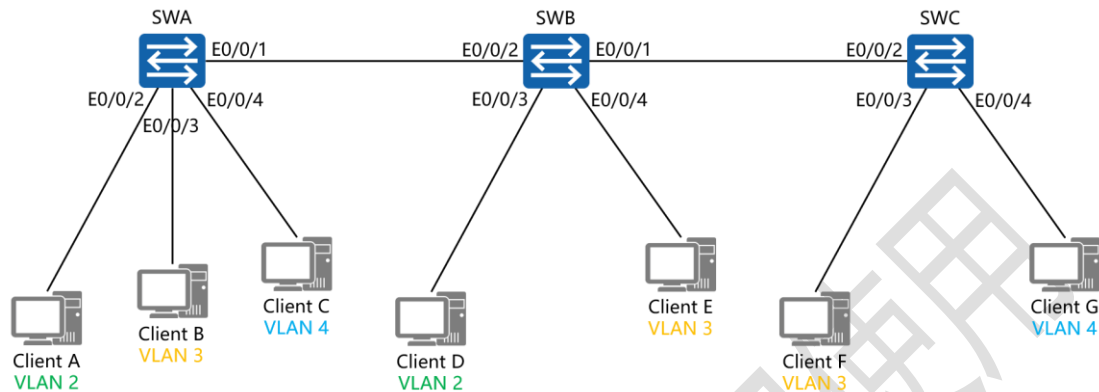
port link-type trunk

port trunk allow-pass vlan all

仅供瑞通学员学习使用

四、配置 VLAN 实验组网（二）

一、实验拓扑：



二、实验目的：

令同 VLAN 之间的主机能够相互通信，不同 VLAN 之间的主机不能相互通信

三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

vlan 2 #创建 VLAN 2

vlan 3 #创建 VLAN 3

vlan 4 #创建 VLAN 4

interface E0/0/2 #进入相应的端口

port link-type access #将端口的链路类型配置为接入模式


```

port default vlan 2      #将端口加入进 VLAN 2
interface E0/0/3        #进入相应的端口
port link-type access   #将端口的链路类型配置为接入模
式
port default vlan 3      #将端口加入进 VLAN 3
interface E0/0/4        #进入相应的端口
port link-type access   #将端口的链路类型配置为接入模
式
port default vlan 4      #将端口加入进 VLAN 4
interface E0/0/1        #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all #允许该中继端口传递所有
VLAN 的信息

```

```

SWB:
system-view
sysname SWB
vlan 2
vlan 3
vlan 4
interface E0/0/3
port link-type access

```

```
port default vlan 2
interface E0/0/4
port link-type access
port default vlan 3
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
```

SWC:

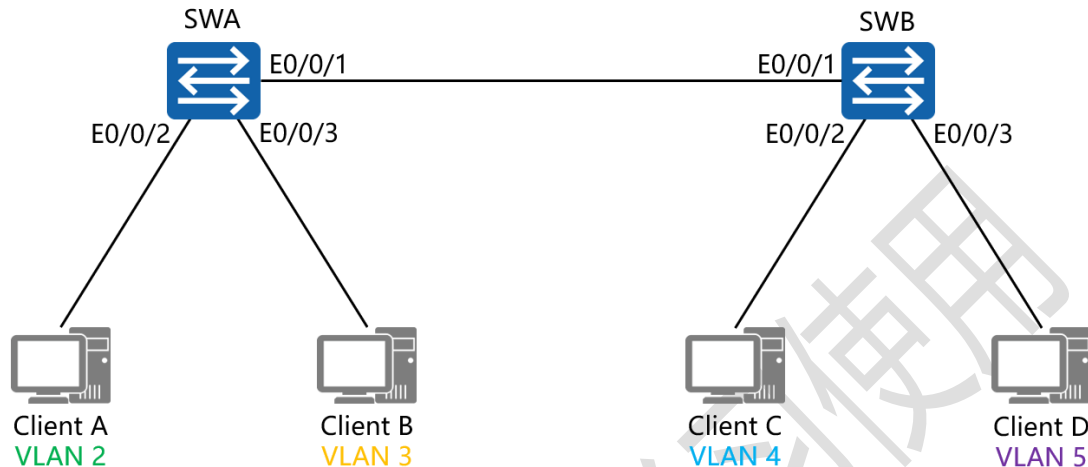
```
system-view
sysname SWC
vlan 3
vlan 4
interface E0/0/3
port link-type access
port default vlan 3
interface E0/0/4
port link-type access
port default vlan 4
```

```
interface E0/0/2  
port link-type trunk  
port trunk allow-pass vlan all
```

仅供瑞通学员学习使用

五、配置 VLAN 实验组网（三）

一、实验拓扑：



二、实验目的：

令 VLAN 2 中的 Client A 能够与 Client B, Client C, Client D 通信；令 VLAN 3 中的 Client B 能够与 Client A, Client C, Client D 通信；令 VLAN 4 中的 Client C 不能与 VLAN 5 中的 Client D 通信

三、实验步骤：

SWA:

system-view #进入系统视图模式

sysname SWA #给设备命名

vlan 2 #创建 VLAN 2

vlan 3 #创建 VLAN 3

vlan 4 #创建 VLAN 4

```

vlan 5          #创建 VLAN 5

interface E0/0/2    #进入相应的端口

port link-type hybrid    #将端口的链路类型配置为混杂模式

port hybrid untagged vlan 2 to 5    #指定该端口不对来自 VLAN 2 到 VLAN 5 中的主机发出的数据帧打标记

port hybrid pvid vlan 2    #配置该端口的本地 VLAN 为 VLAN 2

interface E0/0/3    #进入相应的端口

port link-type hybrid    #将端口的链路类型配置为混杂模式

port hybrid untagged vlan 2 to 5    #指定该端口不对来自 VLAN 2 到 VLAN 5 中的主机发出的数据帧打标记

port hybrid pvid vlan 3    #配置该端口的本地 VLAN 为 VLAN 3

interface E0/0/1    #进入相应的端口

port link-type trunk    #将端口配置为中继模式

port trunk allow-pass vlan all    #允许该中继端口传递所有 VLAN 的信息

```

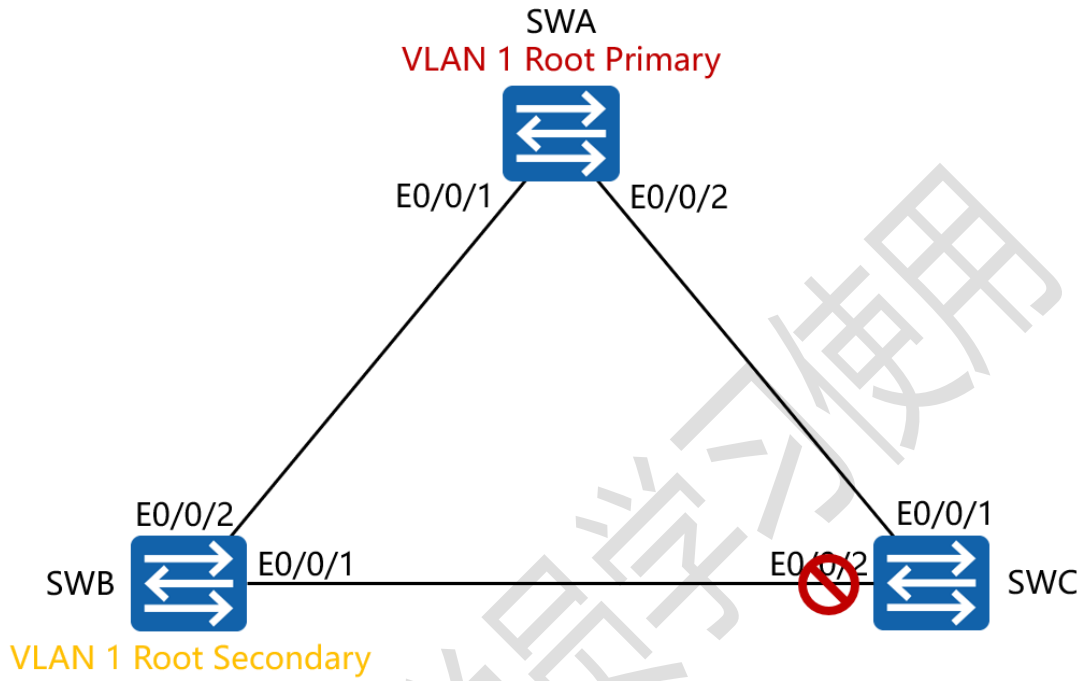
SWB:

system-view

```
sysname SWB
vlan 2
vlan 3
vlan 4
vlan 5
interface E0/0/2
port link-type hybrid
port hybrid untagged vlan 2 to 4
port hybrid pvid vlan 4
interface E0/0/3
port link-type hybrid
port hybrid untagged vlan 2 to 3 5
port hybrid pvid vlan 5
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
```

六、配置 STP 实验组网

一、实验拓扑：



二、实验目的：

令 SWA 是 VLAN 1 的主根网桥，在 VLAN 1 的 STP 中，阻塞 SWC 的 E0/0/2 端口；当 SWA 失效时，令 SWB 接替 SWA 成为 VLAN 1 的主根网桥

三、实验步骤：

SWA:

```
system-view      #进入系统视图模式
sysname SWA     #给设备命名
stp enable      #全局启用 STP
stp mode stp    #将 STP 的工作模式配置为 STP
```

```
interface E0/0/1    #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
```

VLAN 的信息

```
interface E0/0/2    #进入相应的端口
port link-type trunk    #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
```

VLAN 的信息

```
stp priority 4096    #将 SWA 的 STP 优先级配置为 4096
```

SWB:

```
system-view
sysname SWB
stp enable
stp mode stp
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
interface E0/0/2
port link-type trunk
port trunk allow-pass vlan all
stp priority 8192
```


SWC:

system-view

sysname SWC

stp enable

stp mode stp

interface E0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface E0/0/2

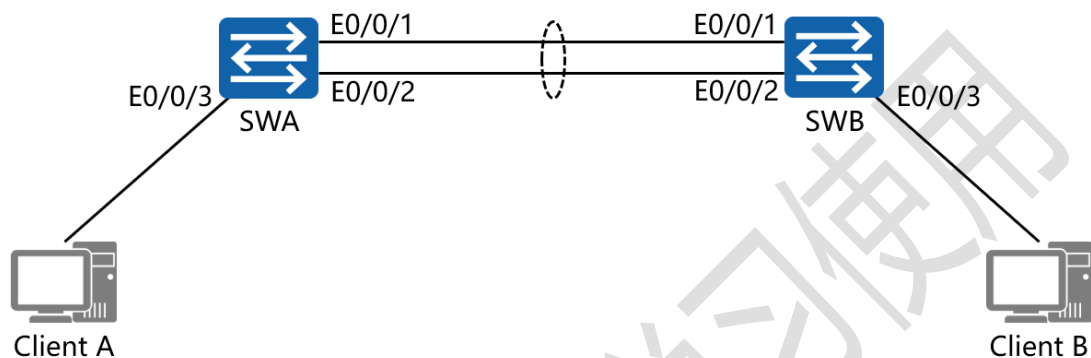
port link-type trunk

port trunk allow-pass vlan all

仅供学习使用

七、配置二层链路手动负载均衡模式下的链路聚合实验组网

一、实验拓扑：



二、实验目的：

通过使用手动负载均衡的模式，将 SWA 与 SWB 的两条以太网链路绑定为同一个以太网隧道

三、实验步骤：

SWA:

```

system-view          #进入系统视图模式
sysname SWA         #给设备命名
interface Eth-Trunk 1    #创建 Eth-Trunk 端口组
interface E0/0/1        #进入 E0/0/1 端口
Eth-Trunk 1          #将该端口加入进 Eth-Trunk 端口组
interface E0/0/2        #进入 E0/0/2 端口
Eth-Trunk 1          #将该端口加入进 Eth-Trunk 端口组
    
```

SWB:

system-view

sysname SWB

interface Eth-Trunk 1

interface E0/0/1

Eth-Trunk 1

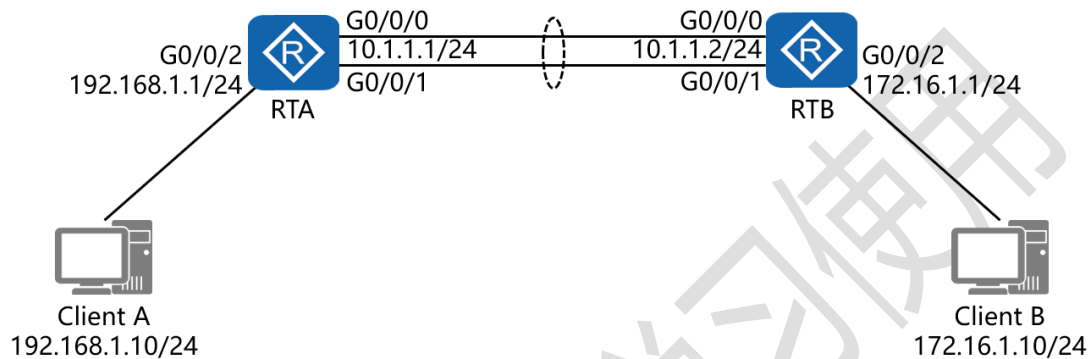
interface E0/0/2

Eth-Trunk 1

仅供瑞通学员学习使用

八、配置三层链路手动负载均衡模式下的链路聚合实验组网

一、实验拓扑：



二、实验目的：

通过使用手动负载均衡的模式，将 RTA 与 RTB 的两条以太网链路绑定为同一个以太隧道，令 Client A 与 Client B 正常通信

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface Eth-Trunk 1    #创建 Eth-Trunk 端口组
undo portswitch      #将聚合链路由 2 层转换为 3 层
ip address 10.1.1.1 24  #为端口组配置 IP 地址
interface G0/0/0      #进入 E0/0/0 接口
Eth-Trunk 1         #将该接口加入进 Eth-Trunk 端口组
    
```

```
interface G0/0/1    #进入 E0/0/1 接口
Eth-Trunk 1    #将该端口加入进 Eth-Trunk 端口组
interface G0/0/2    #进入相应的接口
ip address 192.168.1.1 24    #配置接口的 IP 地址及子网掩
码
ip route-static 172.16.1.0 24 10.1.1.2    #配置静态路由,
指定去往的目的网段及下一跳接口 IP 地址
```

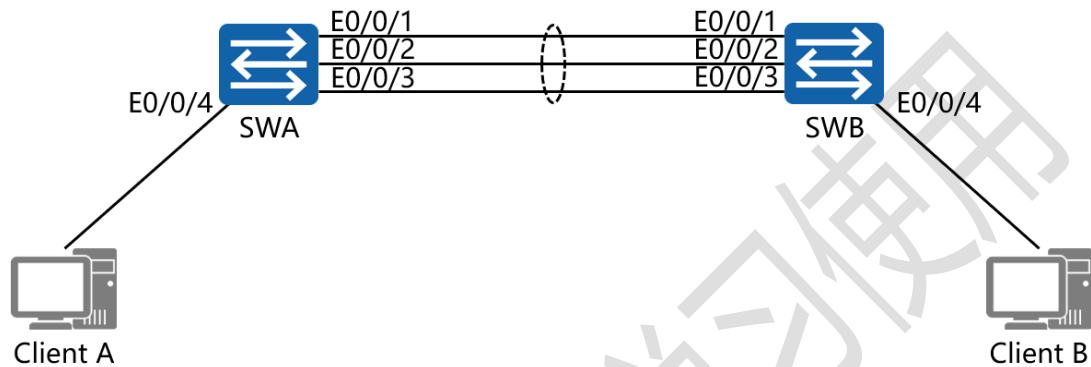
RTB:

```
system-view
sysname RTB
interface Eth-Trunk 1
undo portswitch
ip address 10.1.1.2 24
interface G0/0/0
Eth-Trunk 1
interface G0/0/1
Eth-Trunk 1
interface G0/0/2
ip address 172.16.1.1 24
ip route-static 192.168.1.0 24 10.1.1.1
```

九、配置二层链路 LACP 模式下的链路

聚合实验组网

一、实验拓扑：



二、实验目的：

通过使用 LACP 的模式，将 SWA 与 SWB 的三条以太网链路绑定为同一个以太网隧道

三、实验步骤：

SWA:

```

system-view          #进入系统视图模式
sysname SWA         #给设备命名

interface Eth-Trunk 1    #创建 Eth-Trunk 端口组
mode lacp-static      #将该端口组的模式配置为 LACP

interface E0/0/1        #进入 E0/0/1 端口
Eth-Trunk 1           #将该端口加入进 Eth-Trunk 端口组

interface E0/0/2        #进入 E0/0/2 端口
    
```

```

Eth-Trunk 1    #将该端口加入进 Eth-Trunk 端口组
interface E0/0/3    #进入 E0/0/3 端口
Eth-Trunk 1    #将该端口加入进 Eth-Trunk 端口组
lacp priority 100    #配置 SWA 的 LACP 优先级为 100
interface Eth-Trunk 1    #进入 Eth-Trunk 端口组
max active-linknumber 2    #配置活跃端口的上限阈值为 2
interface E0/0/1    #进入 E0/0/1 端口
lacp priority 100    #配置端口优先级确定活跃链路
interface E0/0/2    #进入 E0/0/2 端口
lacp priority 100    #配置端口优先级确定活跃链路

```

SWB:

```

system-view
sysname SWB
interface Eth-Trunk 1
mode lacp-static
interface E0/0/1
Eth-Trunk 1
interface E0/0/2
Eth-Trunk 1
interface E0/0/3
Eth-Trunk 1

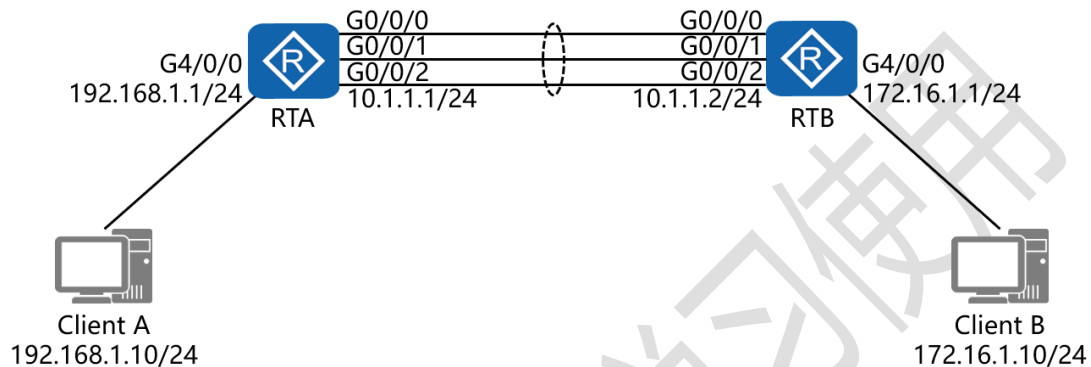
```

```
lacp priority 100
interface Eth-Trunk 1
max active-linknumber 2
interface E0/0/1
lacp priority 100
interface E0/0/2
lacp priority 100
```


十、配置三层链路 LACP 模式下的链路

聚合实验组网

一、实验拓扑：



二、实验目的：

通过使用 LACP 的模式，将 RTA 与 RTB 的三条吉比特以太网链路绑定为同一个以太隧道，令 Client A 与 Client B 正常通信

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名

interface Eth-Trunk 1    #创建 Eth-Trunk 端口组
undo portswitch       #将聚合链路由 2 层转换为 3 层
mode lacp-static       #将该端口组的模式配置为 LACP
max active-linknumber 2    #配置活跃端口的上限阈值为 2
ip address 10.1.1.1 24    #为端口组配置 IP 地址
    
```

```

lacp priority 100      #配置 RTA 的 LACP 优先级为 100
interface G0/0/0      #进入 G0/0/0 接口
Eth-Trunk 1          #将该接口加入进 Eth-Trunk 端口组
lacp priority 100    #配置接口优先级确定活跃链路
interface G0/0/1      #进入 G0/0/1 接口
Eth-Trunk 1          #将该接口加入进 Eth-Trunk 端口组
lacp priority 100    #配置接口优先级确定活跃链路
interface G0/0/2      #进入 G0/0/2 接口
Eth-Trunk 1          #将该接口加入进 Eth-Trunk 端口组
interface G4/0/0      #进入相应的接口
ip address 192.168.1.1 24 #配置接口的 IP 地址及子网掩
码
ip route-static 172.16.1.0 24 10.1.1.2 #配置静态路由,
指定去往的目的网段及下一跳接口 IP 地址

```

```

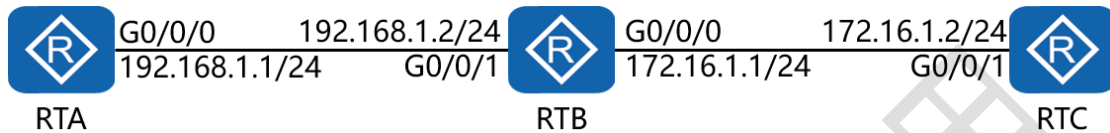
RTB:
system-view
sysname RTB
interface Eth-Trunk 1
undo portswitch
mode lacp-static
max active-linknumber 2

```

```
ip address 10.1.1.2 24
lacp priority 100
interface G0/0/0
Eth-Trunk 1
lacp priority 100
interface G0/0/1
Eth-Trunk 1
lacp priority 100
interface G0/0/2
Eth-Trunk 1
interface G4/0/0
ip address 172.16.1.1 24
ip route-static 192.168.1.0 24 10.1.1.1
```

十一、配置广播型网络上的静态路由实验组网

一、实验拓扑：



二、实验目的：

通过配置静态路由，令 RTA 与 RTC 能够正常互访

三、实验步骤：

RTA:

```

system-view #进入系统视图模式
sysname RTA #给设备命名
interface G0/0/0 #进入相应的接口
ip address 192.168.1.1 24 #配置接口的 IP 地址及子网掩码
ip route-static 172.16.1.0 24 192.168.1.2 #配置静态路由，指定去往的目的网段及下一跳接口 IP 地址
    
```

RTB:

```

system-view
sysname RTB
    
```

```
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
ip address 192.168.1.2 24
```

RTC:

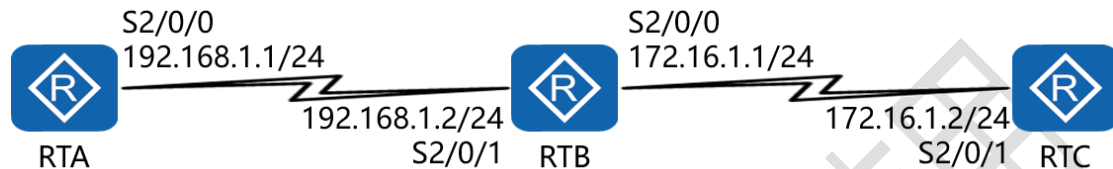
```
system-view
sysname RTC
interface G0/0/1
ip address 172.16.1.2 24
ip route-static 192.168.1.0 24 172.16.1.1
```

仅供学习使用

十二、配置串行接口下的静态路由实验

组网

一、实验拓扑：



二、实验目的：

通过配置静态路由，令 RTA 与 RTC 能够正常互访

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface S2/0/0     #进入相应的接口
ip address 192.168.1.1 24    #配置接口的 IP 地址及子网掩码
ip route-static 172.16.1.0 24 S2/0/0    #配置静态路由，指定
    去往的目的网段及本地外出接口
    
```

RTB:

```

system-view
    
```

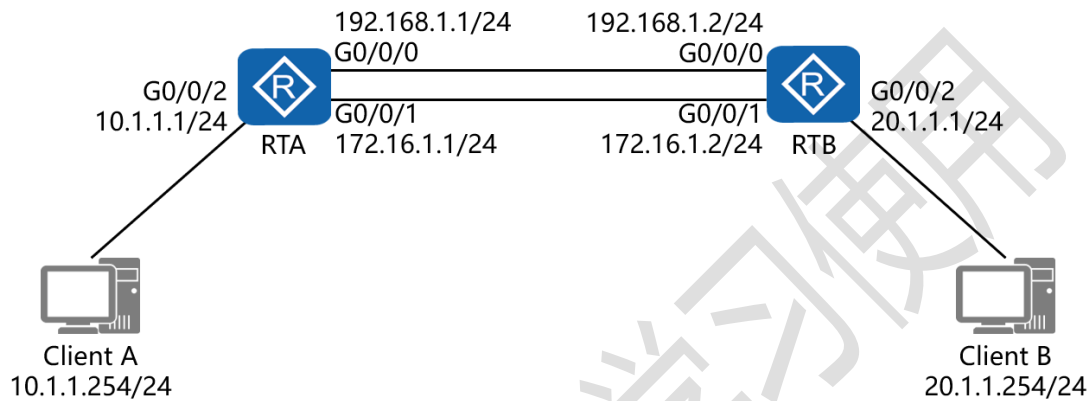
```
sysname RTB  
interface S2/0/0  
ip address 172.16.1.1 24  
interface S2/0/1  
ip address 192.168.1.2 24
```

```
RTC:  
system-view  
sysname RTC  
interface S2/0/1  
ip address 172.16.1.2 24  
ip route-static 192.168.1.0 24 S2/0/1
```

十三、配置静态路由等价负载分担实验

组网

一、实验拓扑：



二、实验目的：

RTA 与 RTB 通过 2 条吉比特以太网链路相连，通过配置静态路由的等价负载分担，令 Client A 与 Client B 能够正常互通，且同时使用 2 条链路传输数据

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应的接口

ip address 192.168.1.1 24 #配置接口的 IP 地址及子网掩码


```

interface G0/0/1    #进入相应的接口
ip address 172.16.1.1 24    #配置接口的 IP 地址及子网掩
码
interface G0/0/2    #进入相应的接口
ip address 10.1.1.1 24    #配置接口的 IP 地址及子网掩码
ip route-static 20.1.1.0 24 192.168.1.2    #配置静态路由,
指定去往的目的网段及下一跳接口 IP 地址
ip route-static 20.1.1.0 24 172.16.1.2    #配置静态路由,
指定去往的目的网段及下一跳接口 IP 地址

```

RTB:

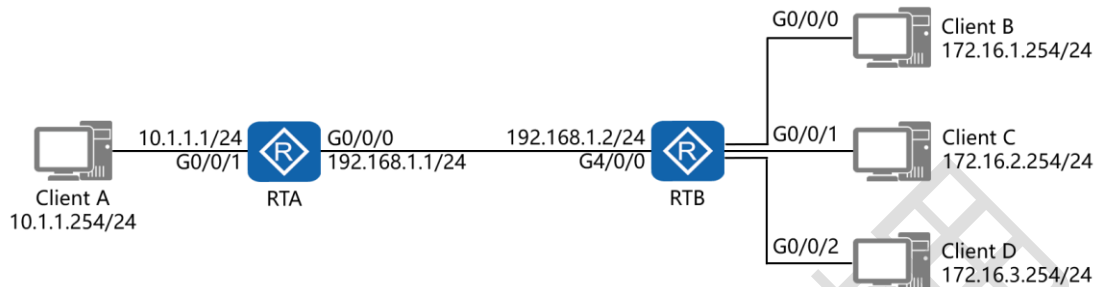
```

system-view
sysname RTB
interface G0/0/0
ip address 192.168.1.2 24
interface G0/0/1
ip address 172.16.1.2 24
interface G0/0/2
ip address 20.1.1.1 24
ip route-static 10.1.1.0 24 192.168.1.1
ip route-static 10.1.1.0 24 172.16.1.1

```

十四、配置缺省路由实验组网

一、实验拓扑：



二、实验目的：

在 RTA 上配置缺省路由，在 RTB 上配置静态路由，令 Client A 能够与 Client B、Client C、Client D 正常互通

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应的接口

ip address 192.168.1.1 24 #配置接口的 IP 地址及子网掩码

interface G0/0/1 #进入相应的接口

ip address 10.1.1.1 24 #配置接口的 IP 地址及子网掩码

ip route-static 0.0.0.0 0 192.168.1.2 #配置缺省路由，指定去往任意网段的下一跳接口 IP 地址

RTB:

system-view

sysname RTB

interface G0/0/0

ip address 172.16.1.1 24

interface G0/0/1

ip address 172.16.2.1 24

interface G0/0/2

ip address 172.16.3.1 24

interface G4/0/0

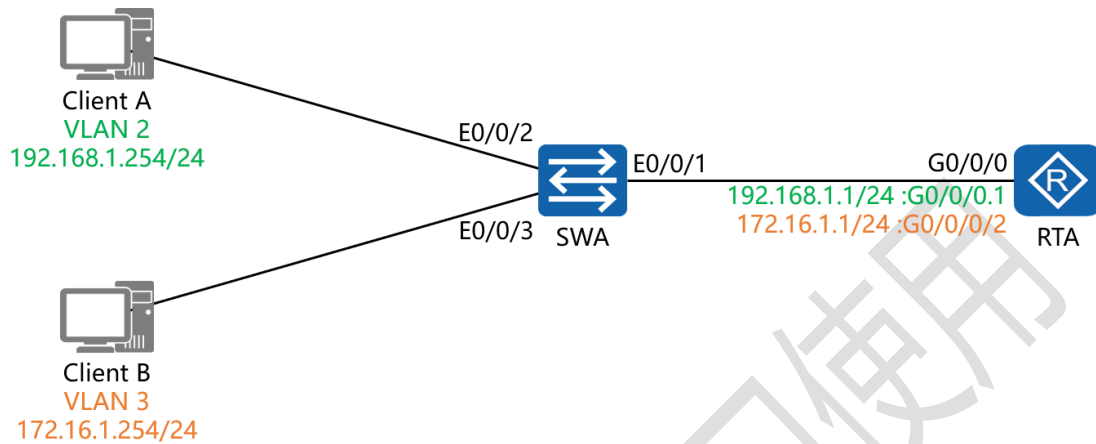
ip address 192.168.1.2 24

ip route-static 10.1.1.0 24 192.168.1.1

仅供学习使用

十五、配置单臂路由实验组网

一、实验拓扑：



二、实验目的：

通过配置单臂路由，令 VLAN 2 中的 Client A 能够与 VLAN 3 中的 Client B 通讯

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0.1 #进入第 1 个子接口

dot1q termination vid 2 #配置其 VLAN 的封装方式为 802.1Q, 并且令该子接口为 VLAN 2 的主机提供路由转发服务

ip address 192.168.1.1 24 #配置接口的 IP 地址及子网掩码

arp broadcast enable #在子接口下开启 ARP 广播功能

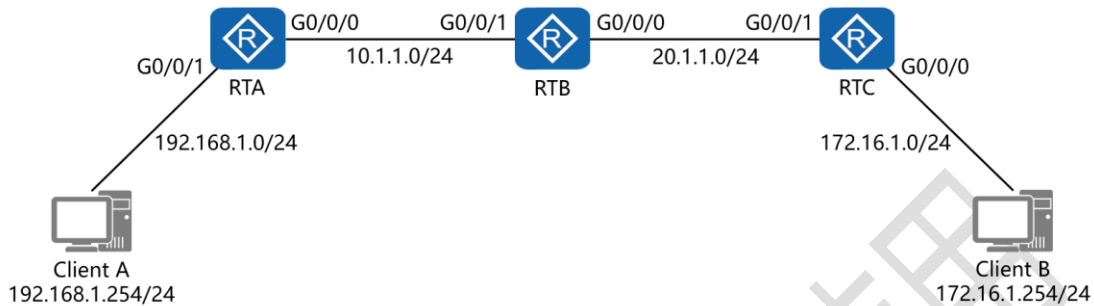
```
interface G0/0/0.2      #进入第 2 个子接口
dot1q termination vid 3    #配置其 VLAN 的封装方式为
802.1Q, 并且令该子接口为 VLAN 3 的主机提供路由转发服务
ip address 172.16.1.1 24    #配置接口的 IP 地址及子网掩
码
arp broadcast enable      #在子接口下开启 ARP 广播功能
```

SWA:

```
system-view
sysname SWA
vlan 2
vlan 3
interface E0/0/2
port link-type access
port default vlan 2
interface E0/0/3
port link-type access
port default vlan 3
interface E0/0/1
port link-type trunk
port trunk allow-pass vlan all
```

十六、配置 RIP 实验组网

一、实验拓扑：



二、实验目的：

通过在 3 台路由器上进行 RIPv2 的配置，令 Client A 能够与 Client B 正常通讯

三、实验步骤：

RTA:

```

system-view      #进入系统视图模式
sysname RTA      #给设备命名
interface G0/0/0  #进入相应接口
ip address 10.1.1.1 24  #配置 IP 地址及子网掩码
interface G0/0/1  #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
rip 1            #进入 RIP 进程 1
version 2        #配置使用版本 2
network 10.0.0.0 #通告其直连网段
  
```

```
network 192.168.1.0    #通告其直连网段  
undo summary         #关闭自动汇总
```

RTB:

```
system-view  
sysname RTB  
interface G0/0/0  
ip address 20.1.1.1 24  
interface G0/0/1  
ip address 10.1.1.2 24  
rip 1  
version 2  
network 10.0.0.0  
network 20.0.0.0  
undo summary
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 172.16.1.1 24  
interface G0/0/1
```

ip address 20.1.1.2 24

rip 1

version 2

network 20.0.0.0

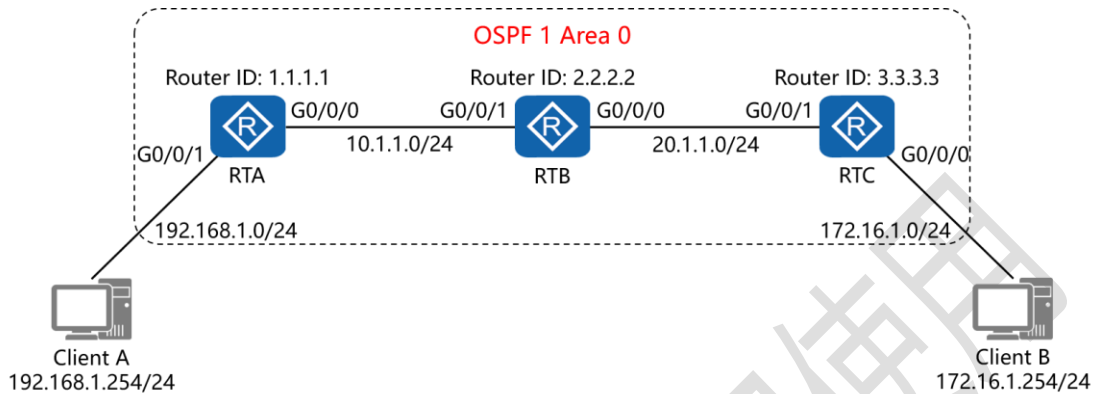
network 172.16.0.0

undo summary

仅供瑞通学员学习使用

十七、配置 OSPF 单区域实验组网

一、实验拓扑：



二、实验目的：

通过 OSPF 单区域的配置，令 Client A 能与 Client B 正常通讯

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
interface Loopback0  #创建环回接口 0
ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1 #进入 OSPF 进程 1, 并指定其路由
    
```

器 ID

```
area 0      #创建 OSPF 区域 0
network 10.1.1.0 0.0.0.255  #通告其直连网段
network 192.168.1.0 0.0.0.255  #通告其直连网段
```

RTB:

```
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
```

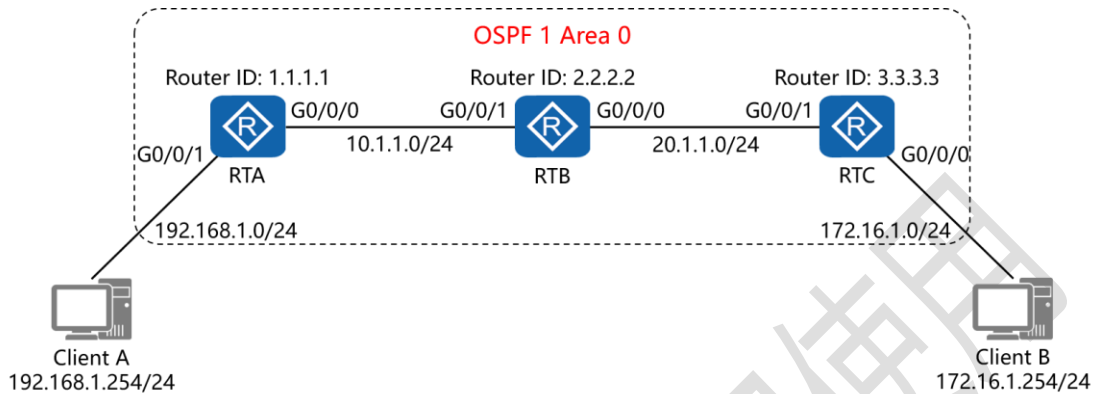
RTC:

```
system-view
sysname RTC
```

```
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
area 0
network 20.1.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
```

十八、配置基本 ACL 实验组网

一、实验拓扑：



二、实验目的：

通过 OSPF 单区域的配置, 令 Client A 能与 Client B 正常互访;
之后在 RTA 上配置基本 ACL, 令 Client A 与 Client B 不能再相互通讯

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
interface Loopback0  #创建环回接口 0
    
```

```

ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
器 ID
area 0    #创建 OSPF 区域 0
network 10.1.1.0 0.0.0.255    #通告其直连网段
network 192.168.1.0 0.0.0.255    #通告其直连网段
acl 2001    #创建基本 ACL
rule deny source 192.168.1.0 0.0.0.255    #定义其规则为拒
绝网段 192.168.1.0/24
interface G0/0/1    #进入相应接口
traffic-filter inbound acl 2001    #在接口的入方向上应用该
基本 ACL

```

RTB:

```

system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24
interface G0/0/1
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32

```

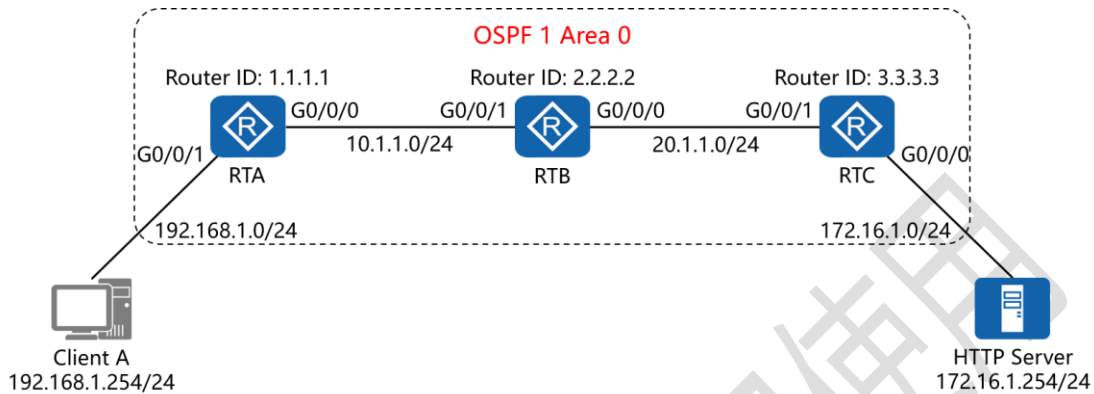
```
ospf 1 router-id 2.2.2.2  
area 0  
network 10.1.1.0 0.0.0.255  
network 20.1.1.0 0.0.0.255
```

RTC:

```
system-view  
sysname RTC  
interface G0/0/0  
ip address 172.16.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
interface Loopback0  
ip address 3.3.3.3 32  
ospf 1 router-id 3.3.3.3  
area 0  
network 20.1.1.0 0.0.0.255  
network 172.16.1.0 0.0.0.255
```

十九、配置高级 ACL 实验组网

一、实验拓扑：



二、实验目的：

通过 OSPF 单区域的配置, 令 Client A 能够访问 HTTP Server; 之后在 RTA 上配置高级 ACL, 令 Client A 能够 ping 通 HTTP Server, 但无法访问其 HTTP 服务

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 10.1.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1     #进入相应接口
ip address 192.168.1.1 24  #配置 IP 地址及子网掩码
interface Loopback0  #创建环回接口 0
    
```

```

ip address 1.1.1.1 32    #配置 IP 地址及子网掩码
ospf 1 router-id 1.1.1.1    #进入 OSPF 进程 1, 并指定其路由
器 ID
area 0    #创建 OSPF 区域 0
network 10.1.1.0 0.0.0.255    #通告其直连网段
network 192.168.1.0 0.0.0.255    #通告其直连网段
acl 3001    #创建高级 ACL
rule deny tcp source 192.168.1.0 0.0.0.255 destination
172.16.1.254 0 destination-port eq 80    #定义其规则为拒
绝来自网段 192.168.1.0/24 访问目标主机 172.16.1.254 的 TCP
服务的 80 端口
rule permit icmp source any destination any    #允许任
何源地址访问任何目的地址的 ICMP 服务
interface G0/0/1    #进入相应接口
traffic-filter inbound acl 3001    #在接口的入方向上应用该
高级 ACL

RTB:
system-view
sysname RTB
interface G0/0/0
ip address 20.1.1.1 24

```



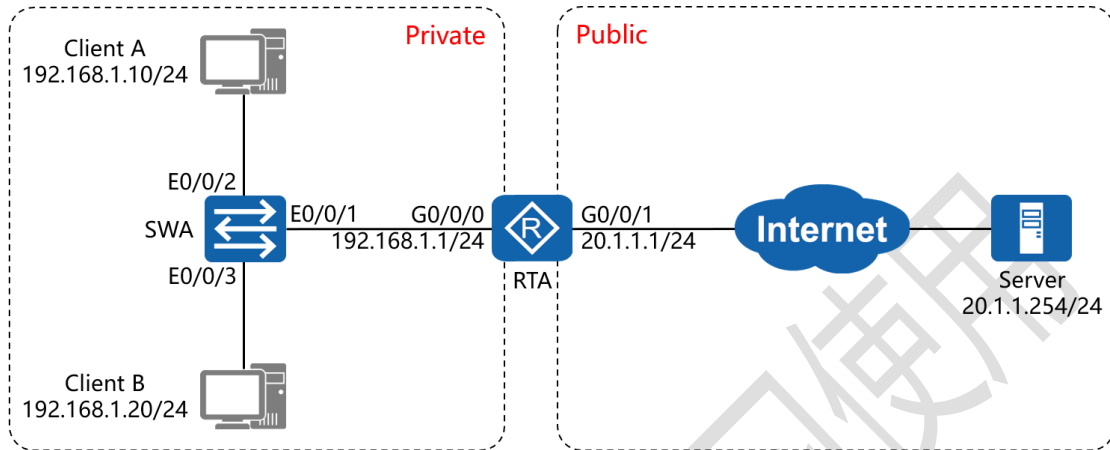
```
interface G0/0/1
ip address 10.1.1.2 24
interface Loopback0
ip address 2.2.2.2 32
ospf 1 router-id 2.2.2.2
area 0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
```

RTC:

```
system-view
sysname RTC
interface G0/0/0
ip address 172.16.1.1 24
interface G0/0/1
ip address 20.1.1.2 24
interface Loopback0
ip address 3.3.3.3 32
ospf 1 router-id 3.3.3.3
area 0
network 20.1.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
```

二十、配置静态 NAT 实验组网

一、实验拓扑：



二、实验目的：

通过静态 NAT 的配置, 令 Client A 与 Client B 能够访问 Public 内的 Server

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

interface G0/0/0 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码

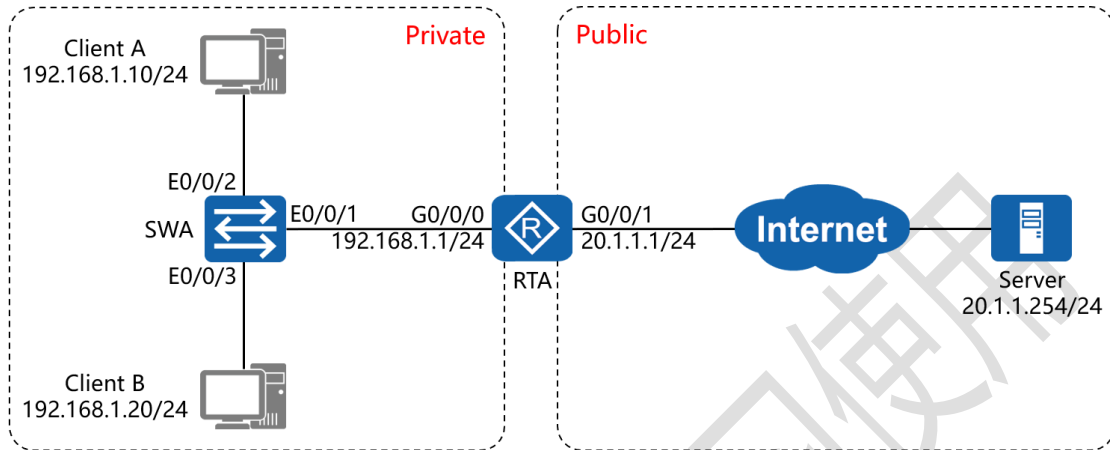
nat static global 20.1.1.10 inside 192.168.1.10 #将内部地址 192.168.1.10 静态转换为公有地址 20.1.1.10

```
nat static global 20.1.1.11 inside 192.168.1.20    #将内部  
地址 192.168.1.20 静态转换为公有地址 20.1.1.11  
nat static enable    #开启 NAT 静态转换服务
```

仅供瑞通学员学习使用

二十一、配置动态 NAT 实验组网

一、实验拓扑：



二、实验目的：

通过动态 NAT 的配置, 令 Client A 与 Client B 能够访问 Public 内的 Server

三、实验步骤：

RTA:

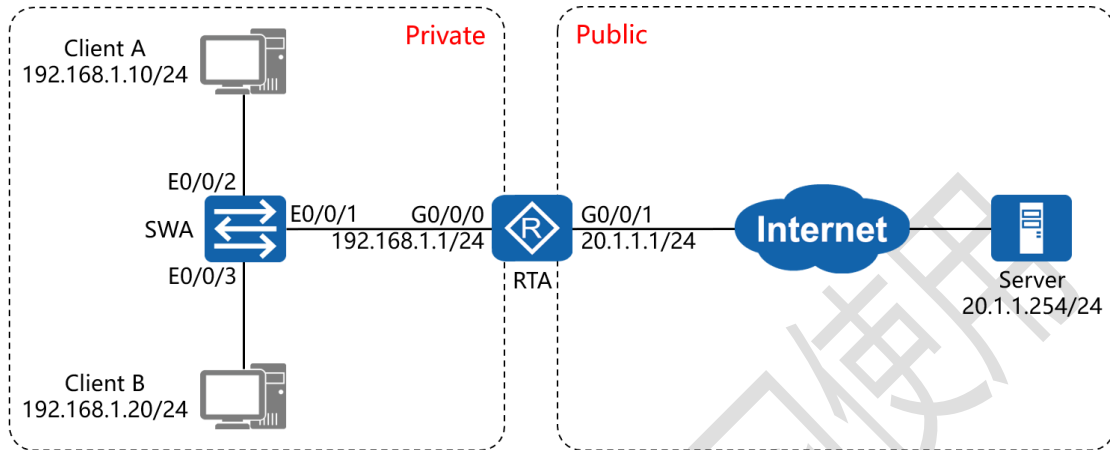
```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
nat address-group 1 20.1.1.10 20.1.1.20    #创建 NAT 地址池
acl 2001             #创建标准访问控制列表
rule permit source 192.168.1.0 0.0.0.255    #匹配内部源网段
interface G0/0/0     #进入相应接口
    
```

```
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
interface G0/0/1          #进入相应接口
ip address 20.1.1.1 24     #配置 IP 地址及子网掩码
nat outbound 2001 address-group 1    #在外部接口的出
方向上调用访问控制列表，并匹配 NAT 地址池
```

二十二、配置 NAT Easy IP 实验组网

一、实验拓扑：



二、实验目的：

通过 NAT Easy IP 的配置，令 Client A 与 Client B 能够访问 Public 内的 Server

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

acl 2001 #创建标准访问控制列表

rule permit source 192.168.1.0 0.0.0.255 #匹配内部源网

段

interface G0/0/0 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

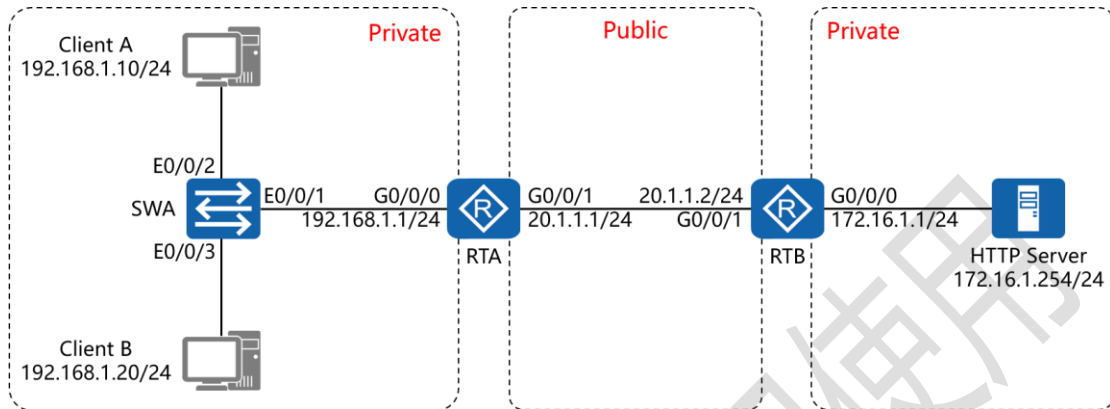
interface G0/0/1 #进入相应接口

ip address 20.1.1.1 24 #配置 IP 地址及子网掩码
nat outbound 2001 #在外部接口的出方向上调用访问控制列表

仅供瑞通学员学习使用

二十三、配置 NAT 服务器实验组网

一、实验拓扑：



二、实验目的：

通过 NAT 服务器的配置,令 Client A 与 Client B 能够通过 Web 浏览器访问 HTTP Server

三、实验步骤：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

acl 2001 #创建标准访问控制列表

rule permit source 192.168.1.0 0.0.0.255 #匹配内部源网

段

interface G0/0/0 #进入相应接口

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

interface G0/0/1 #进入相应接口

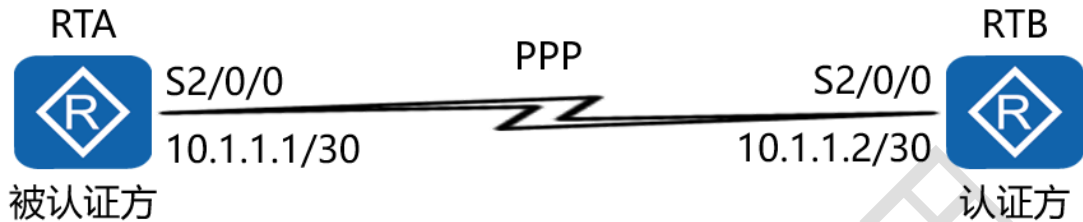

```
ip address 20.1.1.1 24      #配置 IP 地址及子网掩码  
nat outbound 2001        #在外部接口的出方向上调用访问控制列表
```

RTB:

```
system-view  
sysname RTB  
acl 2001  
rule permit source 172.16.1.0 0.0.0.255  
interface G0/0/0  
ip address 172.16.1.1 24  
interface G0/0/1  
ip address 20.1.1.2 24  
nat outbound 2001  
nat server protocol tcp global 20.1.1.3 www inside  
172.16.1.254 80      #开启 NAT 服务器功能，将内部地址  
172.16.1.254 及其端口 80 映射到全局地址 20.1.1.3 的 80 端口
```

二十四、配置 PPP PAP 认证实验组网

一、实验拓扑：



二、实验目的：

将 RTA 与 RTB 之间的串行链路封装协议配置为 PPP，并在两端配置 PPP (PAP) 认证，最终实现 RTA 能够与 RTB 相互通讯

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface S2/0/0     #进入相应的接口
link-protocol ppp   #配置链路封装协议为 PPP
ip address 10.1.1.1 30    #配置 IP 地址及子网掩码
ppp pap local-user easthome password cipher P@ssw0rd
#配置认证时所使用的用户名及密钥
    
```

RTB:

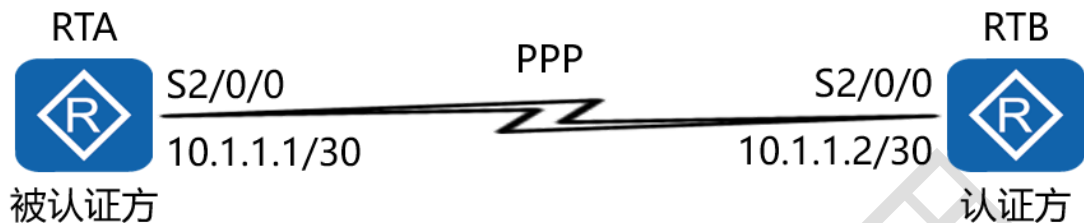
```

system-view
    
```

```
sysname RTB
aaa      #开启 AAA 服务
local-user easthome password cipher P@ssw0rd
#在主认证方的数据库中创建用户及其密钥
local-user easthome service-type ppp      #配置该用户的服
务类型为 PPP
interface S2/0/0
link-protocol ppp
ip address 10.1.1.2 30
ppp authentication-mode pap      #在接口下启用 PPP 的
PAP 认证
```

二十五、配置 PPP CHAP 认证实验组网

一、实验拓扑：



二、实验目的：

将 RTA 与 RTB 之间的串行链路封装协议配置为 PPP，并在两端配置 PPP (CHAP) 认证，最终实现 RTA 能够与 RTB 相互通讯

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
aaa                 #进入 aaa 的配置模式
local-user RTB password cipher P@ssw0rd    #在被认证
方的数据库中创建主认证方的用户及其密钥
local-user RTB service-type ppp           #配置该用户的服务类型
为 PPP
interface S2/0/0    #进入相应的接口
link-protocol ppp  #配置链路封装协议为 PPP
ip address 10.1.1.1 30    #配置 IP 地址及子网掩码
    
```

ppp chap user *RTA* #配置被认证方认证时所使用的用户名

RTB:

system-view

sysname RTB

aaa #开启 AAA 服务

local-user *RTA* password cipher *P@ssw0rd* #在主认证方的数据库中创建被认证方的用户及其密钥

local-user *RTA* service-type ppp #配置该用户的服务类型为 PPP

interface S2/0/0

link-protocol ppp

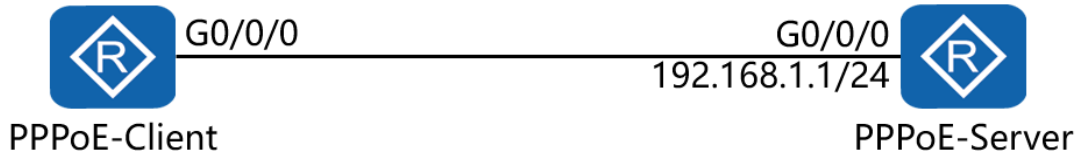
ip address 10.1.1.2 30

ppp authentication-mode chap #在接口下启用 PPP 的 CHAP 认证

ppp chap user *RTB* #配置主认证方认证时所使用的用户名

二十六、配置 PPPoE 实验组网（一）

一、实验拓扑：



二、实验目的：

通过 PPPoE 的配置，令 PPPoE-Client 能够成功获取 IP 地址，并与 PPPoE-Server 正常通讯

三、实验步骤：

PPPoE-Client:

```

system-view          #进入系统视图模式
sysname PPPoE-Client #给设备命名
dialer-rule          #进入拨号规则视图
dialer-rule 1 ip permit #允许在 IP 网络环境下发起拨号连接请求
interface Dialer1    #创建并进入拨号接口 1
link-protocol ppp    #配置链路封装协议为 PPP
ppp chap user easthome #配置使用 PPP 的 CHAP 认证并创建用户
ppp chap password cipher P@ssw0rd #配置认证时使用的密钥
    
```

ip address ppp-negotiate #配置 IP 地址的获取方式为通过 PPP 协商获得

dialer user *pppoe* #创建拨号用户

dialer bundle 1 #将设备的物理接口与拨号接口做绑定

dialer timer idle 300 #配置用户超时时间为 300 秒

dialer-group 1 #将物理接口与拨号接口置于一个拨号访问组中

interface G0/0/0 #进入相应的接口

pppoe-client dial-bundle-number 1 on-demand # 将设备的物理接口与拨号接口做绑定，指定 PPPoE 会话对应的拨号接口；命令 (on-demand) 表示 PPPoE 会话工作在按需拨号模式下

ip route-static 0.0.0.0 0 Dialer1 #配置缺省路由，并指定外出接口为拨号接口

PPPoE-Server:

system-view

sysname PPPoE-Server

aaa #开启 AAA 服务

local-user *easthome* password cipher *P@ssw0rd*

#创建认证时使用的用户名及密钥

local-user *easthome* service-type ppp #配置该用户的服

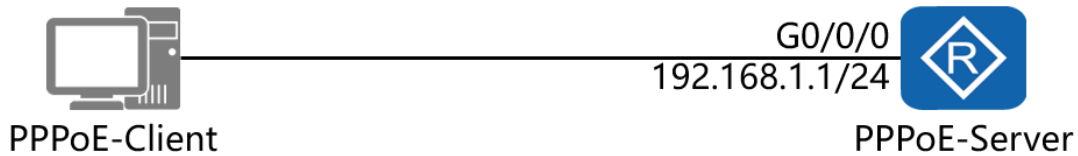
务类型为 PPP

```

ip pool pppoe #创建 DHCP 地址池
gateway-list 192.168.1.1 #指定分配的网关地址
network 192.168.1.0 mask 24 #指定分配的网段及掩码
dns-list 202.106.49.151 #指定分配的 DNS 地址
interface Virtual-Template1 #创建并进入虚拟模板接口
1
ppp authentication-mode chap #指定使用的 PPP 认证模
式为 CHAP
remote address pool pppoe #指定远端设备从名为
pppoe 的地址池中获取 IP 地址
ip address 192.168.1.1 24 #配置虚拟模板接口的 IP 地址
及子网掩码
interface G0/0/0 #进入物理接口
pppoe-server bind Virtual-Template 1 #指定该接口为
PPPoE 的服务器端，并与虚拟模板接口 1 进行绑定
    
```


二十七、配置 PPPoE 实验组网（二）

一、实验拓扑：



二、实验目的：

通过 PPPoE 的配置，令 PPPoE-Client 能够成功获取 IP 地址，并与 PPPoE-Server 正常通讯

三、实验步骤：

PPPoE-Server:

```
system-view
```

```
sysname PPPoE-Server
```

```
aaa #开启 AAA 服务
```

```
local-user easthome password cipher P@ssw0rd
```

#创建认证时使用的用户名及密钥

```
local-user easthome service-type ppp #配置该用户的服务类型为 PPP
```

```
ip pool pppoe #创建 DHCP 地址池
```

```
network 192.168.1.0 mask 24 #指定分配的网段及掩码
```

```
interface Virtual-Template1 #创建并进入虚拟模板接口
```

1

ppp authentication-mode pap #指定使用的 PPP 认证模式为 PAP

remote address pool *pppoe* #指定远端设备从名为 *pppoe* 的地址池中获取 IP 地址

ppp ipcp dns 151.49.106.202 #指定分配的 DNS 地址（反向书写）

ip address 192.168.1.1 24 #配置虚拟模板接口的 IP 地址及子网掩码

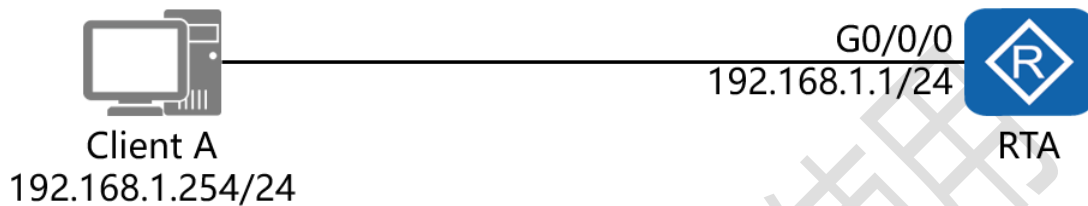
interface G0/0/0 #进入物理接口

pppoe-server bind Virtual-Template 1 #指定该接口为 PPPoE 的服务器端，并与虚拟模板接口 1 进行绑定

二十八、配置 AAA 本地认证及授权实验

组网

一、实验拓扑：



二、实验目的：

在 RTA 上开启 AAA 服务，配置为本地认证及授权，并为 Client A 上的用户授权可通过 Telnet 远程登录路由器，同时为该用户逐条开放可操作的命令权限

三、实验步骤：

RTA:

```
system-view #进入系统视图模式
```

```
sysname RTA #给设备命名
```

```
aaa #开启 AAA 服务
```

```
local-user easthome password cipher P@ssw0rd
```

```
#创建本地用户并设置密钥
```

```
local-user easthome privilege level 0 #指定该用户级别为 0
```

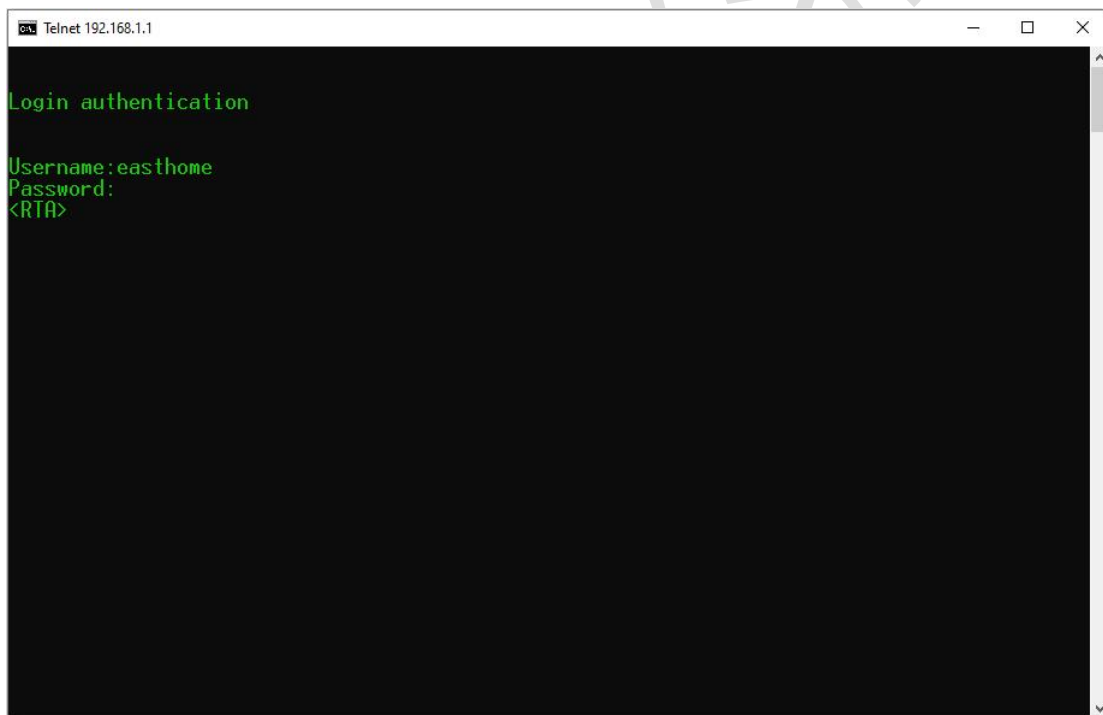
```
local-user easthome service-type telnet #指定该用户的
```

服务类型为 Telnet

```
interface G0/0/0    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
user-interface vty 0 4    #进入虚拟终端配置接口
authentication-mode aaa    #配置认证模式为 AAA
```

以下为开放命令授权测试：

在 Client A 上发起 Telnet：



由于在路由器上为用户 easthome 分配的级别为 0，因此该用户无法进入系统视图：

```

Telnet 192.168.1.1
Login authentication
Username: easthome
Password:
<RTA>system-view
Error: Unrecognized command found at '^' position.
<RTA>
    
```

此时，在路由器上为级别 0 的用户开放命令授权，允许其进入系统视图：

```
command-privilege level 0 view user system-view
```

当为级别 0 的用户开放完命令授权之后，再返回至 Client A，发现已经可以正常进入系统视图：

```

Telnet 192.168.1.1

Login authentication

Username: easthome
Password:
<RTA>system-view

Error: Unrecognized command found at '^' position.
<RTA>system-view
Enter system view, return user view with Ctrl+Z.
[RTA]
    
```

此时，若希望在 RTA 上配置 OSPF 路由选择协议，则需要键入命令 “ospf 1”，但命令无法被接受：

```

Telnet 192.168.1.1

Login authentication

Username: easthome
Password:
<RTA>system-view

Error: Unrecognized command found at '^' position.
<RTA>system-view
Enter system view, return user view with Ctrl+Z.
[RTA]ospf 1

Error: Unrecognized command found at '^' position.
[RTA]
    
```

返回路由器，继续开放授权：

command-privilege level 0 view system ospf

再返回至 Client A，发现已经可以正常进入 OSPF 配置模式：

```

Telnet 192.168.1.1
Login authentication
Username: easthome
Password:
<RTA>system-view
Error: Unrecognized command found at '^' position.
<RTA>system-view
Enter system view, return user view with Ctrl+Z.
[RTA]ospf 1
Error: Unrecognized command found at '^' position.
[RTA]ospf 1
[RTA-ospf-1]
    
```

在 OSPF 下若想进入区域 0，则需要键入命令 “area 0”，但命令依旧无法被接受：

```
Telnet 192.168.1.1

Login authentication

Username: easthome
Password:
<RTA>system-view

Error: Unrecognized command found at '^' position.
<RTA>system-view
Enter system view, return user view with Ctrl+Z.
[RTA]ospf 1

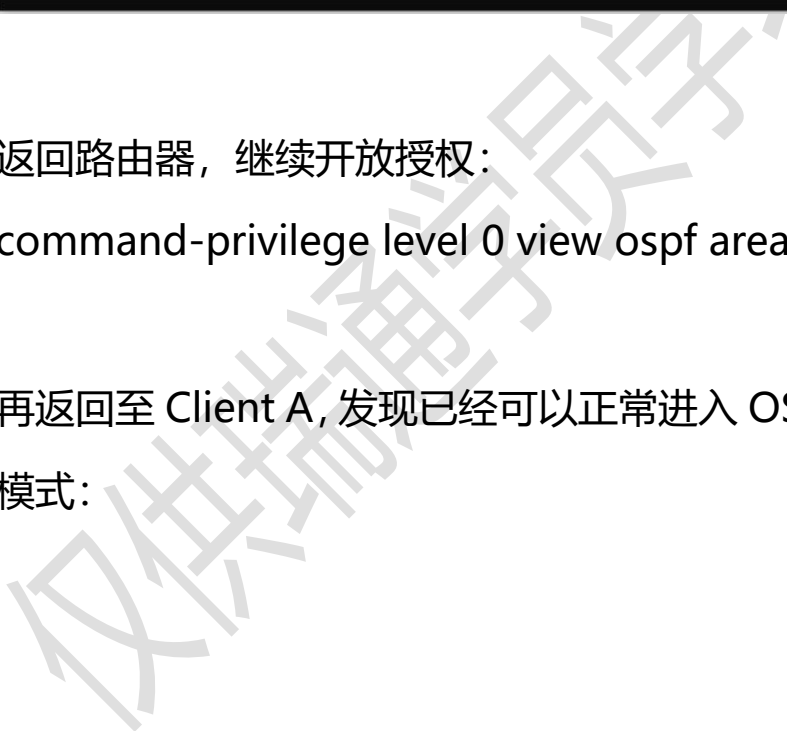
Error: Unrecognized command found at '^' position.
[RTA]ospf 1
[RTA-ospf-1]area 0

Error: Unrecognized command found at '^' position.
[RTA-ospf-1]
```

返回路由器，继续开放授权：

command-privilege level 0 view ospf area

再返回至 Client A, 发现已经可以正常进入 OSPF 的区域 0 配置模式：




```
Telnet 192.168.1.1

Login authentication

Username: easthome
Password:
<RTA>system-view

Error: Unrecognized command found at '^' position.
<RTA>system-view
Enter system view, return user view with Ctrl+Z.
[RTA]ospf 1

Error: Unrecognized command found at '^' position.
[RTA]ospf 1
[RTA-ospf-1]area 0

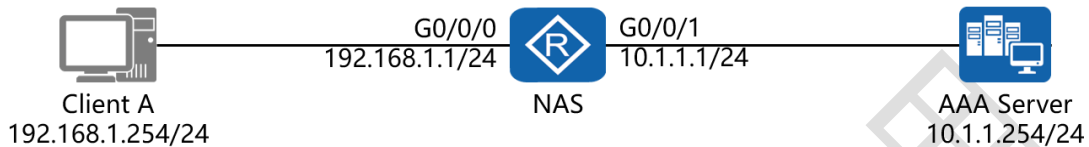
Error: Unrecognized command found at '^' position.
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]
```

仅供瑞通学员学习

二十九、配置 AAA 在 ACS 上进行远端

认证实验组网

一、实验拓扑：



二、实验目的：

在 NAS 上开启 AAA 服务，配置为使用 Cisco ACS 服务器进行远端认证

三、实验步骤：

NAS:

system-view #进入系统视图模式

sysname NAS #给设备命名

aaa #开启 AAA 服务

local-user *easthome* password cipher *P@ssw0rd*

#创建本地用户并设置密钥

local-user *easthome* privilege level 15 #指定该用户级别为 15

local-user *easthome* service-type telnet #指定该用户的服务类型为 Telnet

authentication-scheme 1 #配置认证模板 1

```

authentication-mode radius local      #指定认证模式为先
在 RADIUS 服务器上验证，若服务器不可达再在本地做验证

radius-server template 1             #创建 RADIUS 服务器模板 1

radius-server authentication 10.1.1.254 1812      # 指 定
RADIUS 服务器的 IP 地址及使用的端口号码

radius-server shared-key cipher P@ssw0rd        #指定路由
器与 RADIUS 服务器之间使用的预共享密钥

undo radius-server user-name domain-included
#禁用 RADIUS 服务器在用户名中包含域名

aaa      #再次进入 AAA 的配置模式

domain default_admin      #进入默认的域

radius-server 1           #调用 RADIUS 服务器模板 1

authentication-scheme 1   #调用认证模板 1

interface G0/0/0          #进入相应接口

ip address 192.168.1.1 24  #配置 IP 地址及子网掩码

interface G0/0/1          #进入相应接口

ip address 10.1.1.1 24    #配置 IP 地址及子网掩码

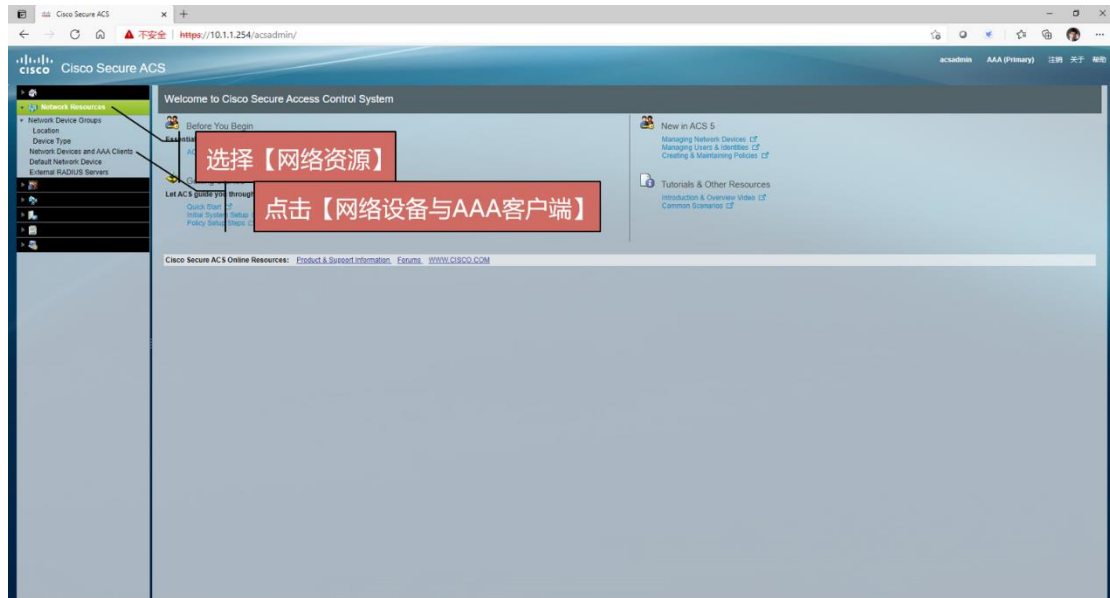
user-interface vty 0 4    #进入虚拟终端配置接口

authentication-mode aaa   #配置认证模式为 AAA

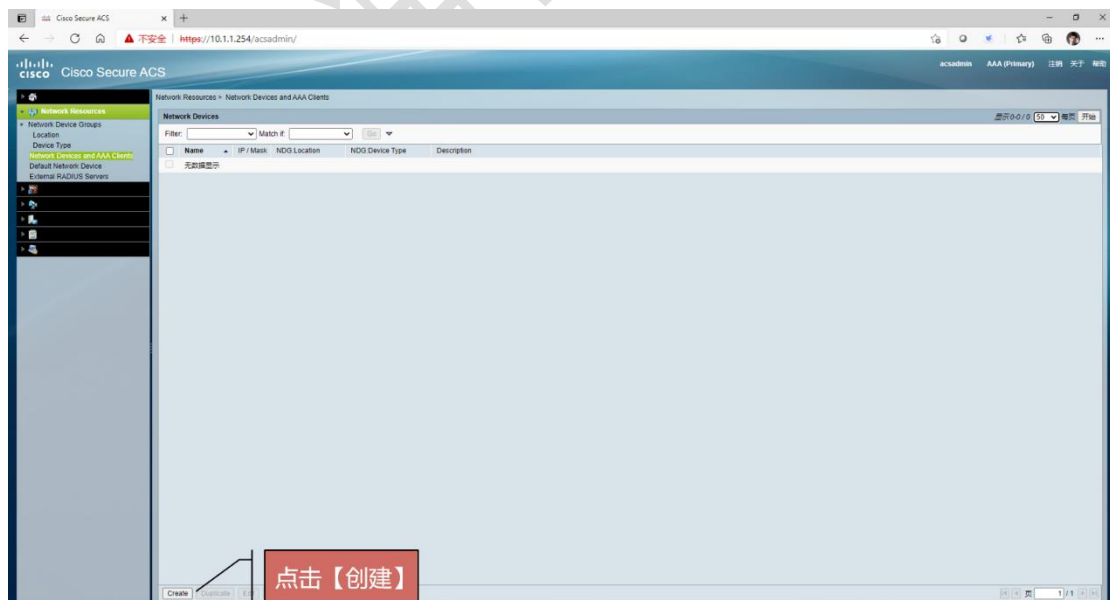
```

Cisco ACSv5.2 的配置:

进入 Cisco ACSv5.2 的配置界面, 点击【网络资源】, 点击【网络设备与 AAA 客户端】:



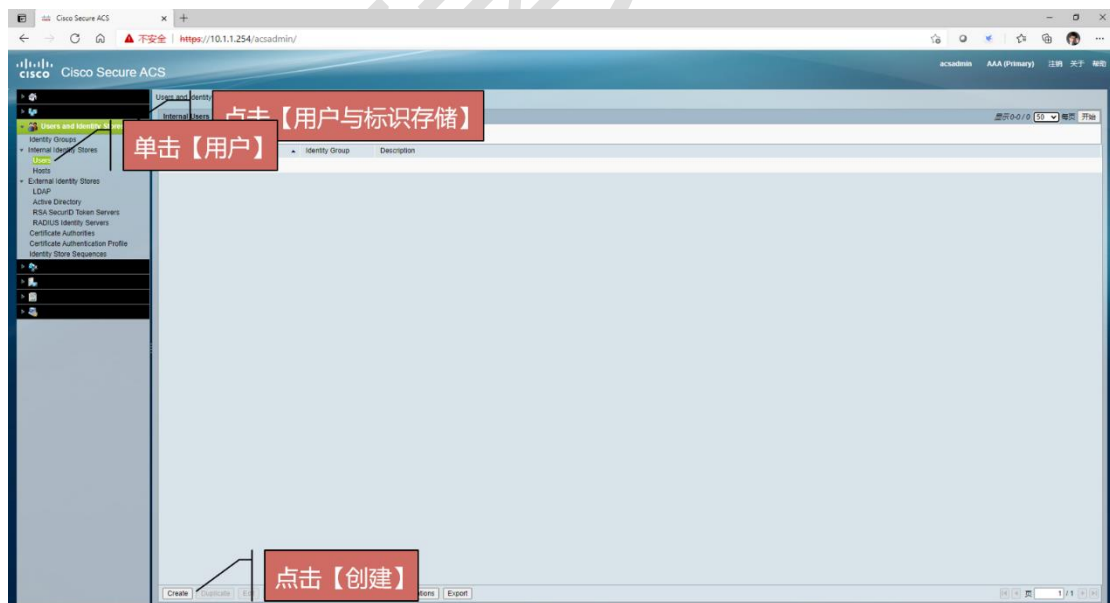
创建 AAA 客户端:



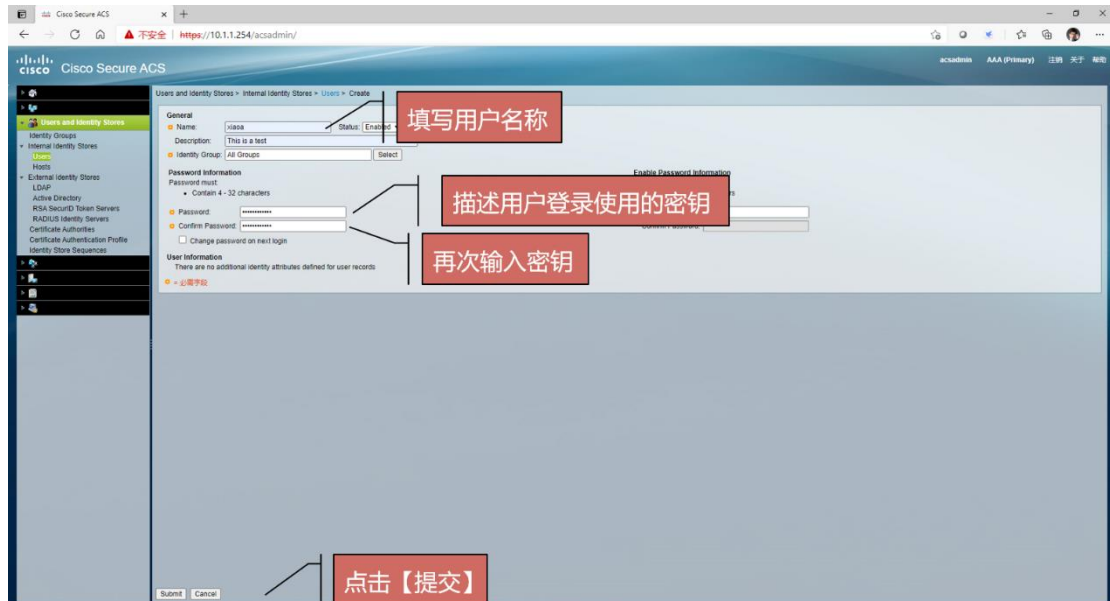
填写 AAA 客户端的相应配置信息：



点击【用户与标识存储】，点击【用户】，在下方点击【创建】，去创建被认证的用户账户：



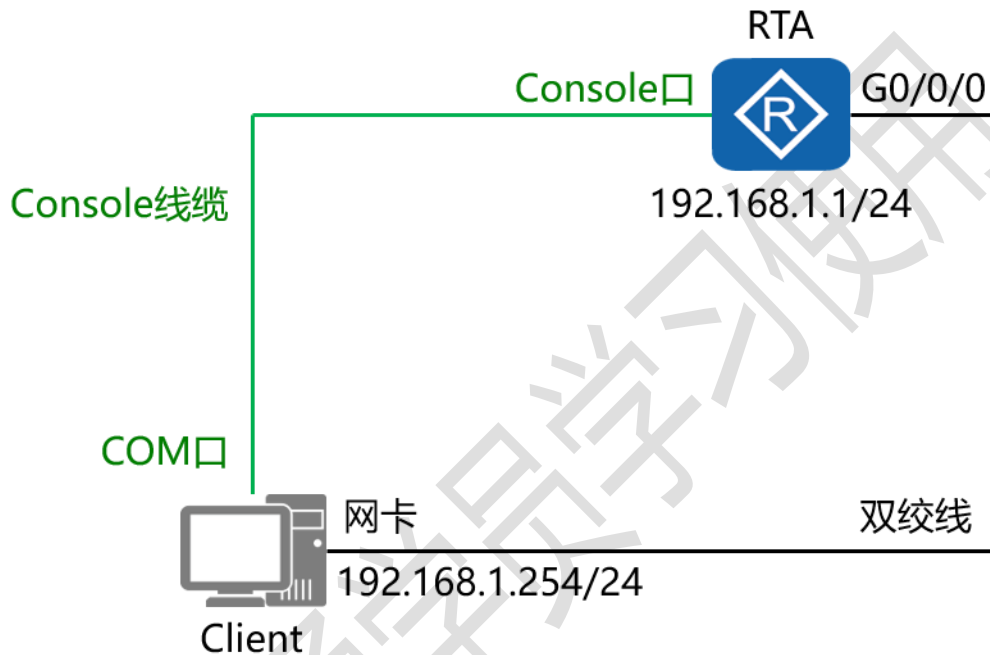
填写用户的基本信息【用户名及密钥】，点击下方的【提交】：



仅供瑞通学员学习

三十、配置基于 CLI 的远程登录操作实验组网

一、实验拓扑：



二、实验目的：

令 Client 通过 Telnet 远程登录设备并做调试

三、实验步骤：

Telnet 方式（一）：

RTA:

system-view #进入系统视图模式

sysname RTA #给设备命名

telnet server enable #开启 Telnet 服务

```
interface G0/0/0    #进入相应的接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
user-interface vty 0 4    #进入用户视图界面
user privilege level 15    #配置用户登录后的使用等级
set authentication password cipher P@ssw0rd    #设置密码
```

Telnet 方式 (二):

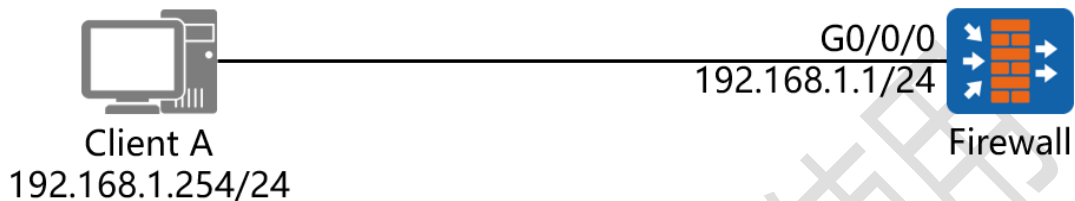
RTA:

```
system-view    #进入系统视图模式
sysname RTA    #给设备命名
telnet server enable    #开启 Telnet 服务
aaa    #开启 AAA 服务
local-user easthome password cipher P@ssw0rd
#配置登录时使用的用户名及密钥
local-user easthome service-type telnet    #设置通过
AAA 登录时使用的服务类型为 TELNET
user-interface vty 0 4    #进入用户视图界面
authentication-mode aaa    #配置认证模式为 AAA
user privilege level 15    #配置用户登录后的使用等级
interface G0/0/0    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
```


三十一、配置基于 Web 方式登录防火墙

实验组网

一、实验拓扑：



二、实验目的：

配置 Firewall【USG6000V1】的管理接口，令 Client A 可以通过 Web 的方式进行登录并管理设备

三、实验步骤：

USG6000V1:

system-view #进入系统视图模式

interface G0/0/0 #进入相应接口

undo ip binding vpn-instance default #关闭默认的接口
与 VPN 实例的绑定关系

ip address 192.168.1.1 24 #配置 IP 地址及子网掩码

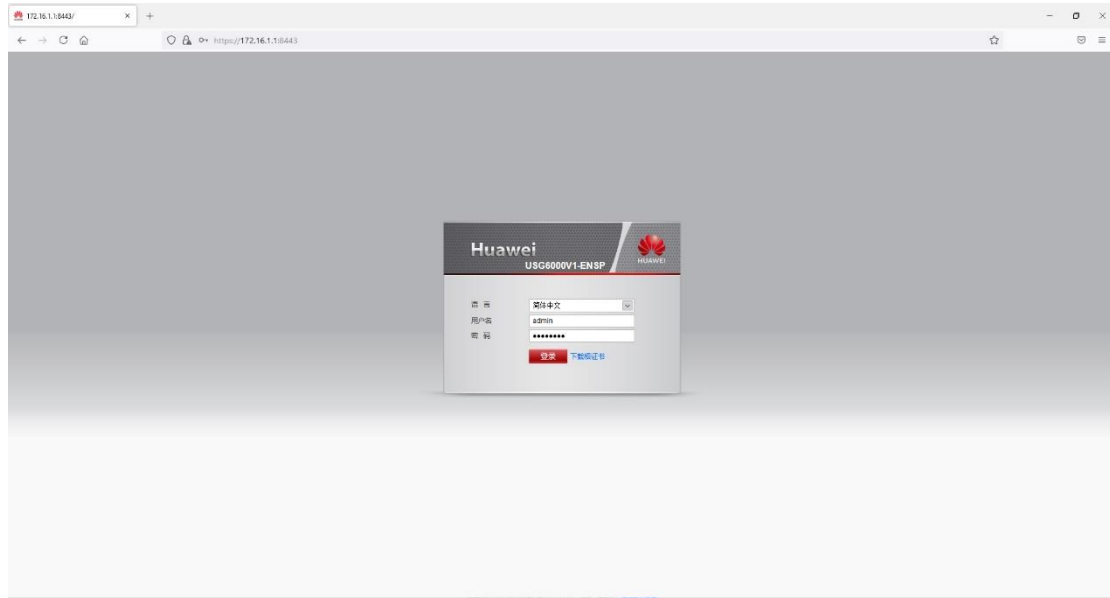
service-manage all permit #配置允许所有服务管理

service-manage enable #开启服务管理功能

web-manager enable #开启基于 Web 的服务管理

Client A:

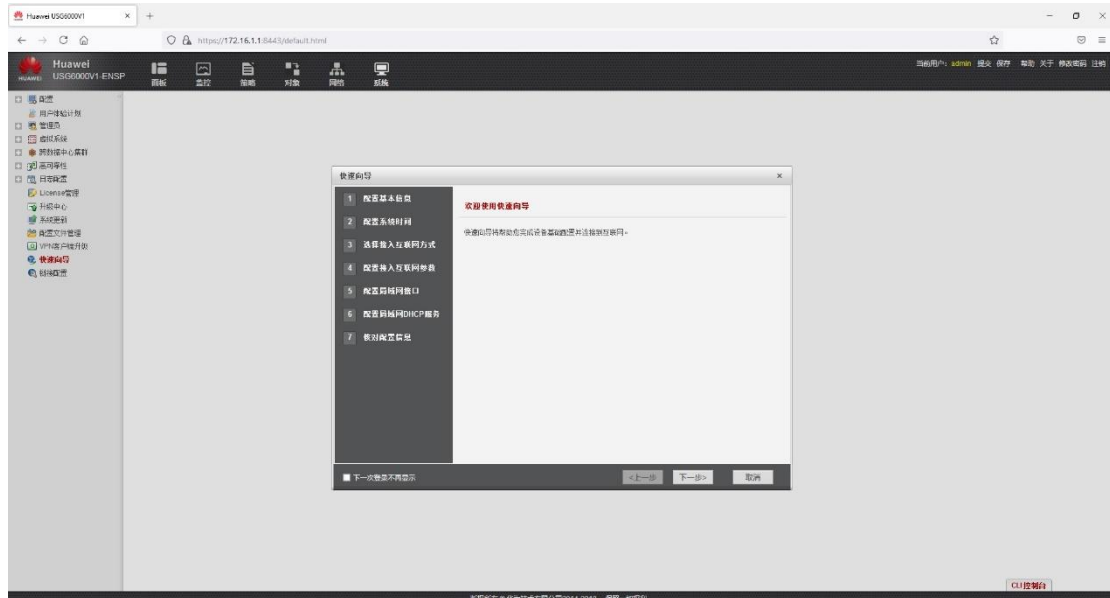
打开 Web 浏览器，输入 <https://172.16.1.1:8443>



输入用户名及密钥，登录设备

仅供学习使用

首次进入会开启【快速向导】，可不使用，勾选【下一次登录不再显示】或直接【取消】

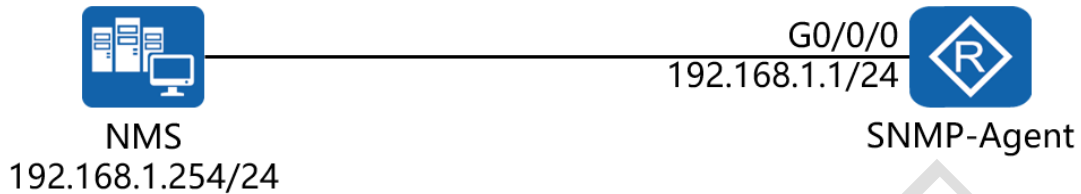


之后弹出【用户体验计划】，管理员可根据企业实际情况选择【参与】或【不参与】



三十二、配置 SNMPv1 实验组网

一、实验拓扑：



二、实验目的：

在 NMS 上安装 MIB Browser，在 SNMP-Agent 上开启 SNMPv1 功能，令 NMS 服务器可以远程管理该路由器

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
snmp-agent          #开启 SNMP 代理功能
snmp-agent sys-info version v1    #配置使用 SNMP 代理版本 1
snmp-agent community read readro    #配置团体名为 readro，并且只允许进行只读访问
snmp-agent community write writerw    #配置团体名为 writerw
    
```

writerw, 并且允许进行读写访问

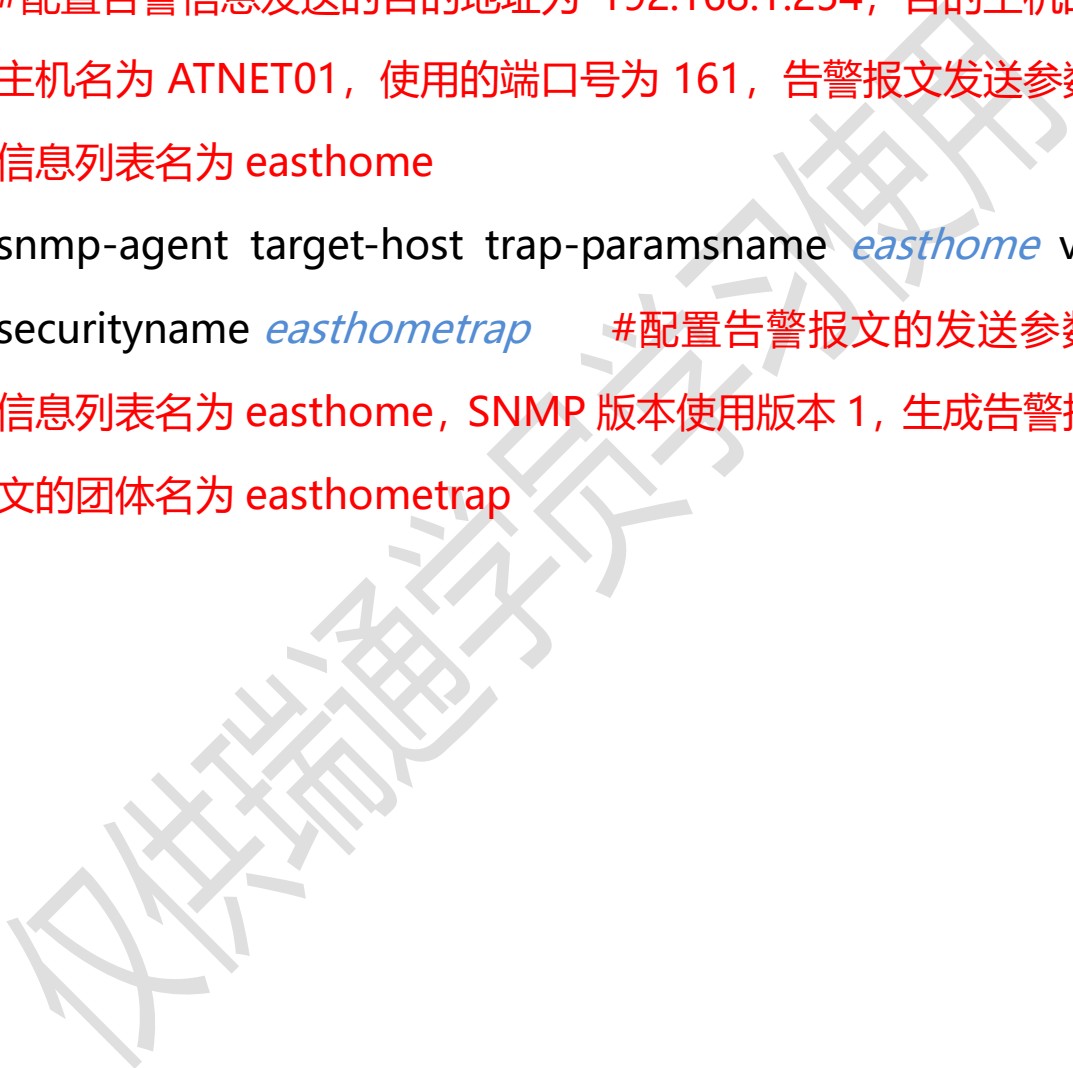
```
snmp-agent trap enable      #开启 SNMP 代理的告警功能
```

```
snmp-agent target-host trap-hostname ATNET01 address  
192.168.1.1254 udp-port 161 trap-paramsname easthome
```

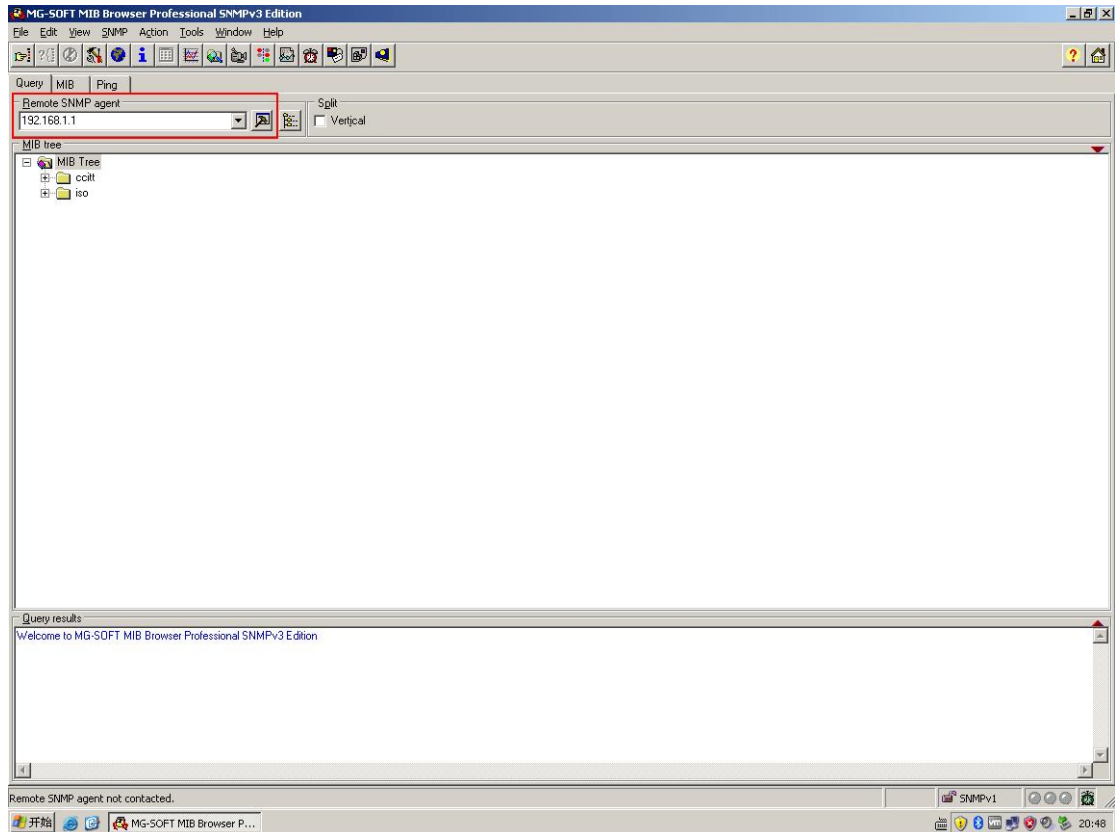
#配置告警信息发送的目的地址为 192.168.1.254, 目的主机的主机名为 ATNET01, 使用的端口号为 161, 告警报文发送参数信息列表名为 easthome

```
snmp-agent target-host trap-paramsname easthome v1  
securityname easthometrap  #配置告警报文的发送参数
```

信息列表名为 easthome, SNMP 版本使用版本 1, 生成告警报文的团体名为 easthometrap

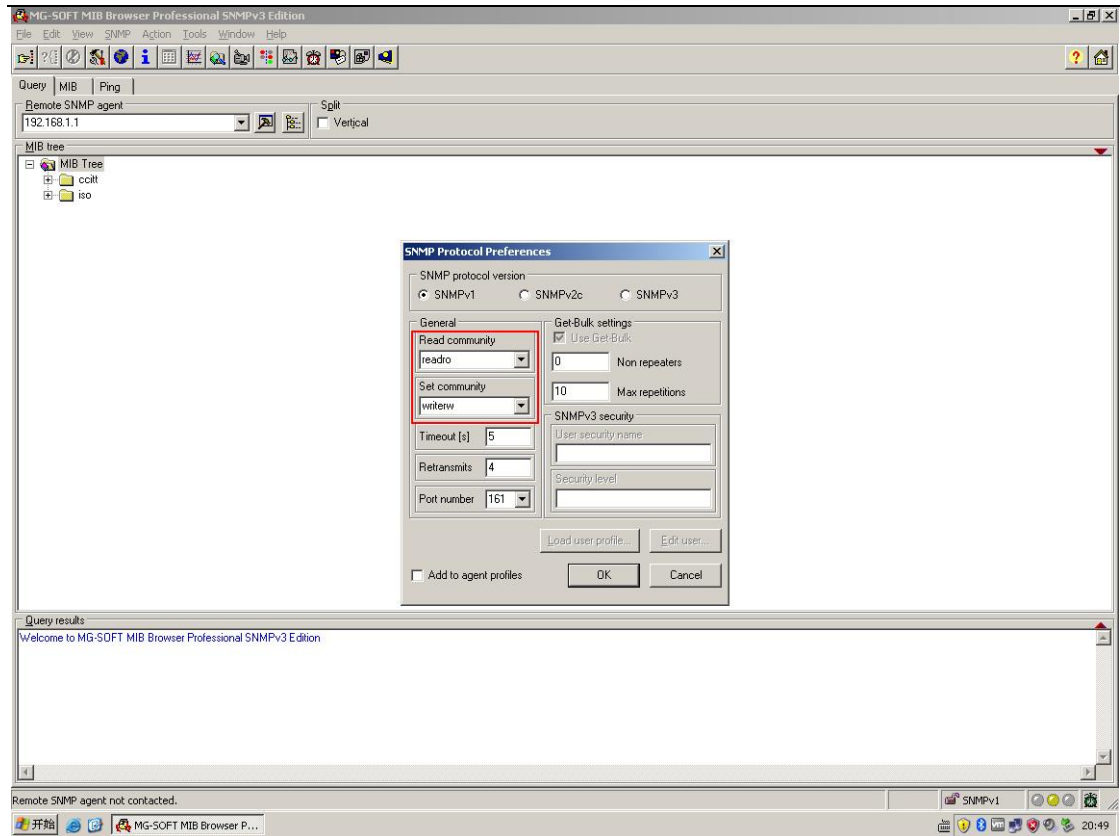


NMS 端安装【MG-SOFT MIB Browser Professional SNMPv3 Edition】软件并开启：

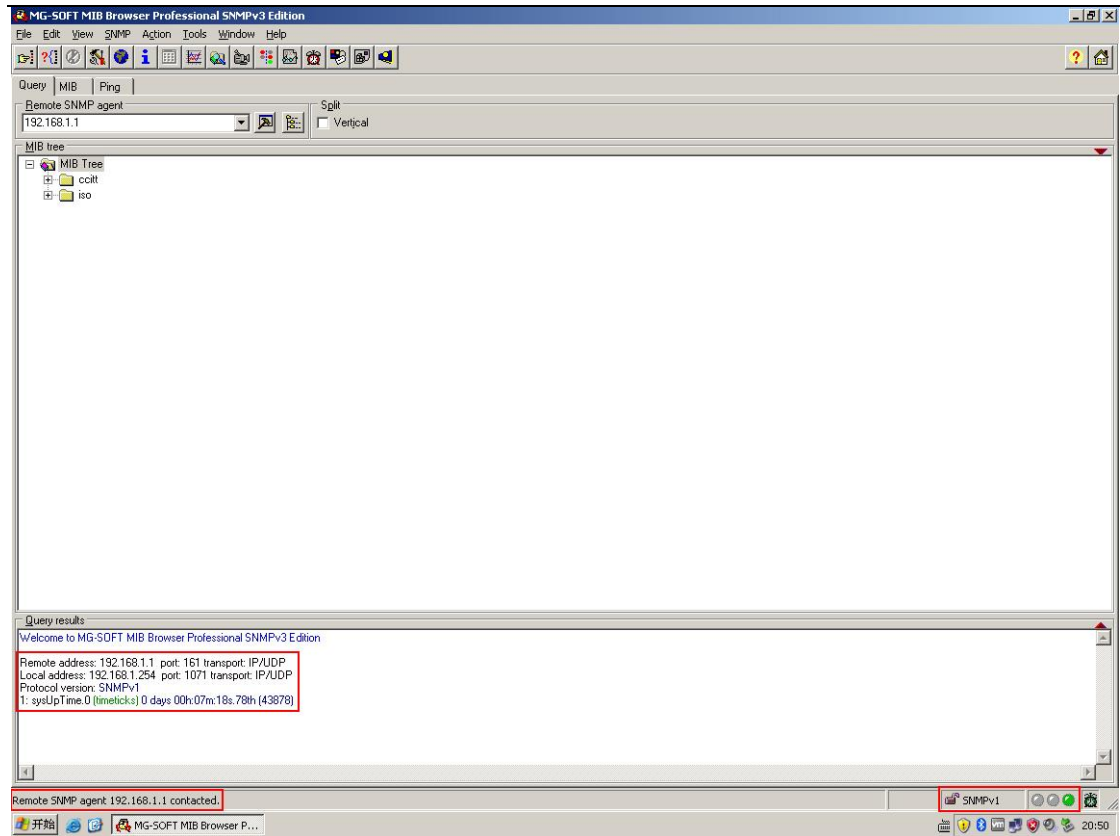


在 Remote SNMP agent 处填写 SNMP-agent (RTA) 的 IP 地址，并单击右侧的“锤子”按钮

仅供学习参考



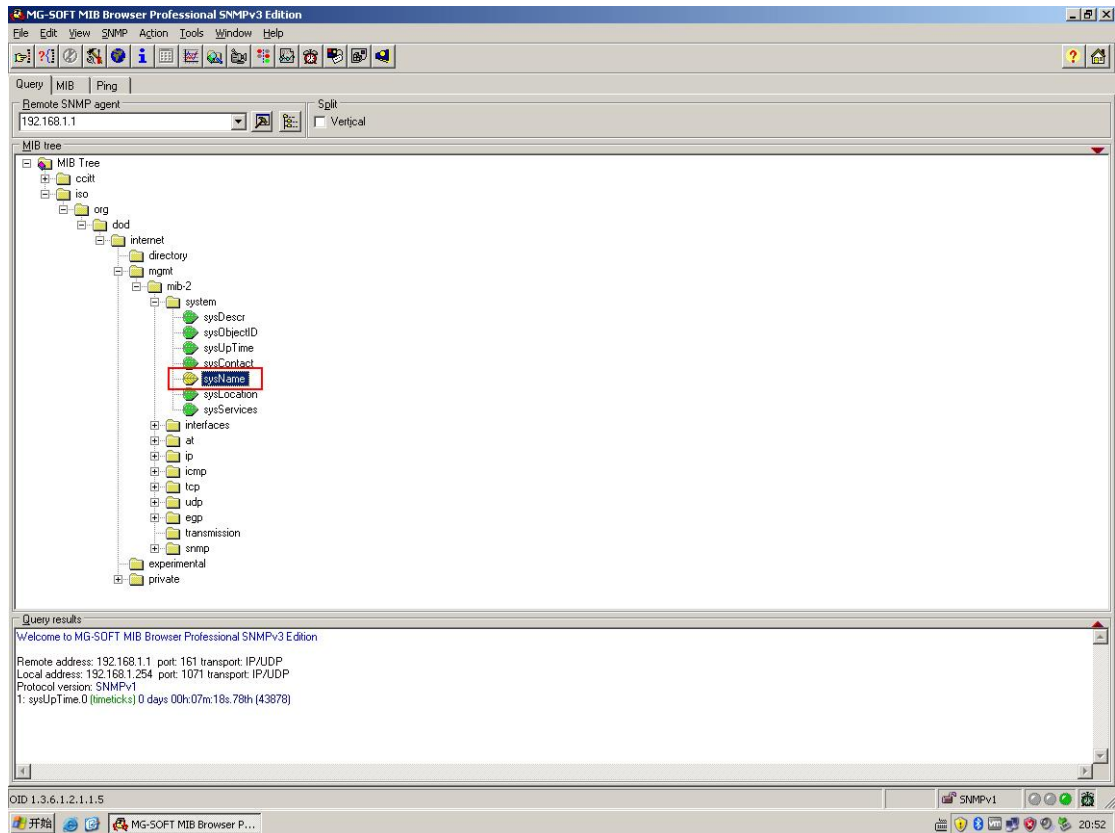
在弹出的选项页中选择 SNMPv1，Read community 处填写 readro，Set community 处填写 writerw，其它参数保持默认值即可，单击 OK



图中红框内显示，SNMP 代理（192.168.1.1）已连接成功

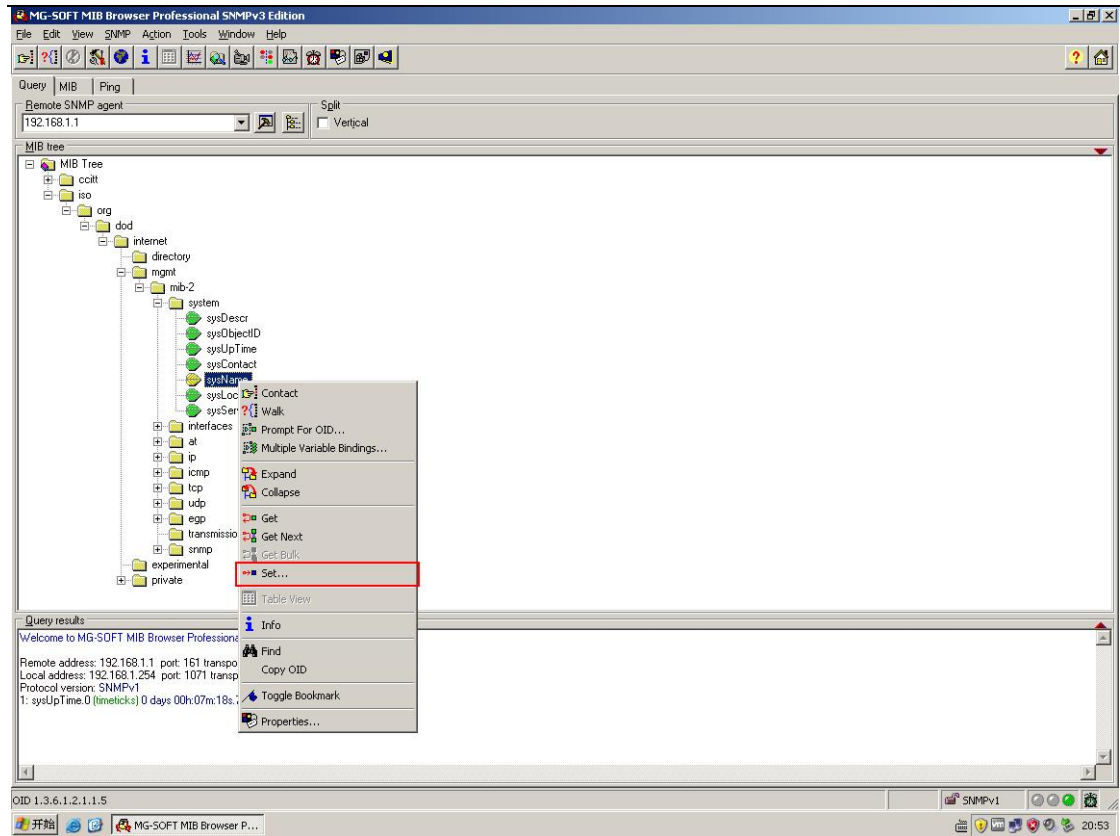
仅供瑞通字

测试是否可以通过 SNMP 远程管理并更改路由器名称：

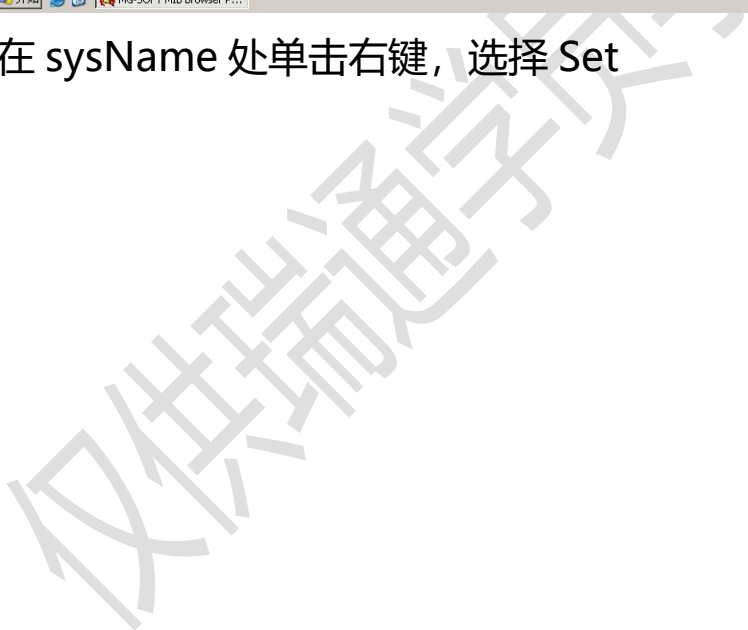


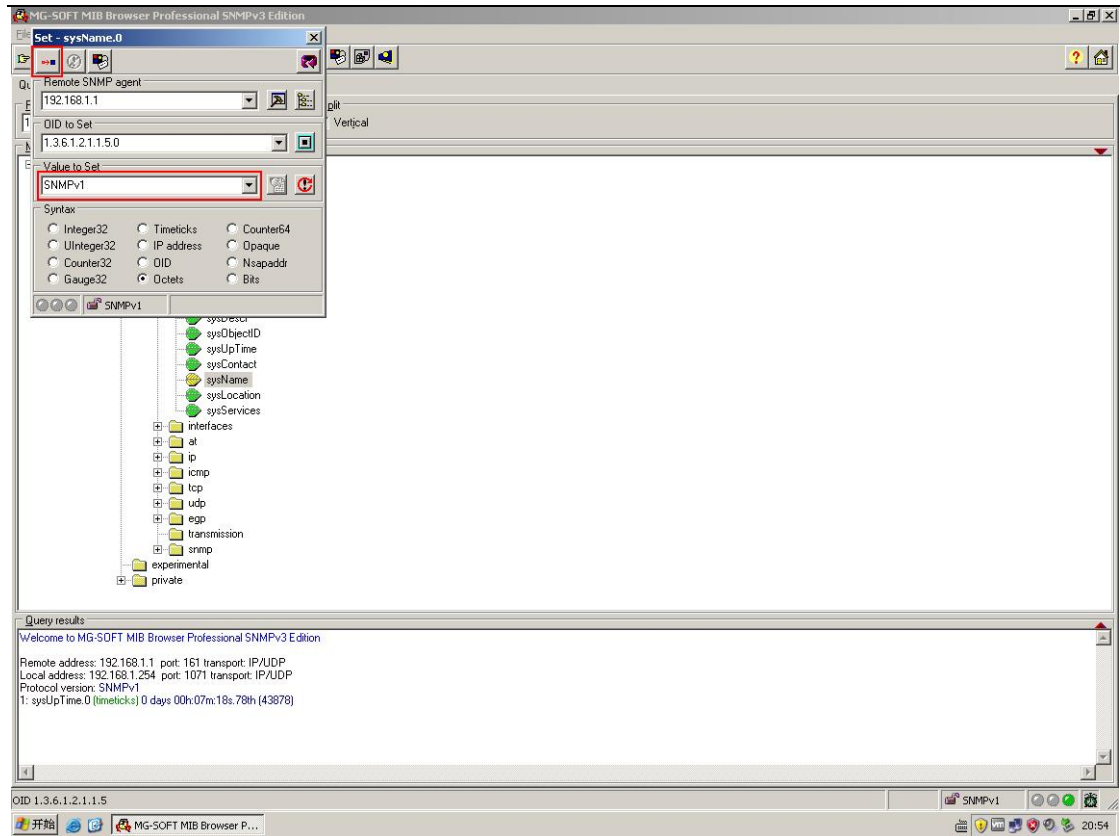
按照上图所示路径，找到 sysName（系统名称）

仅供学习参考

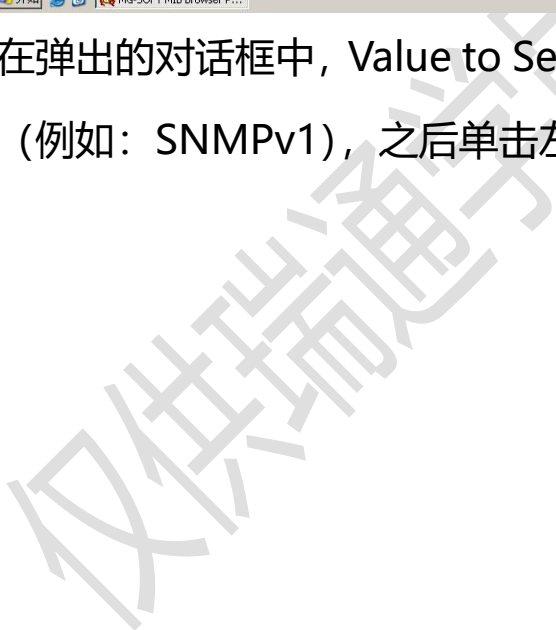


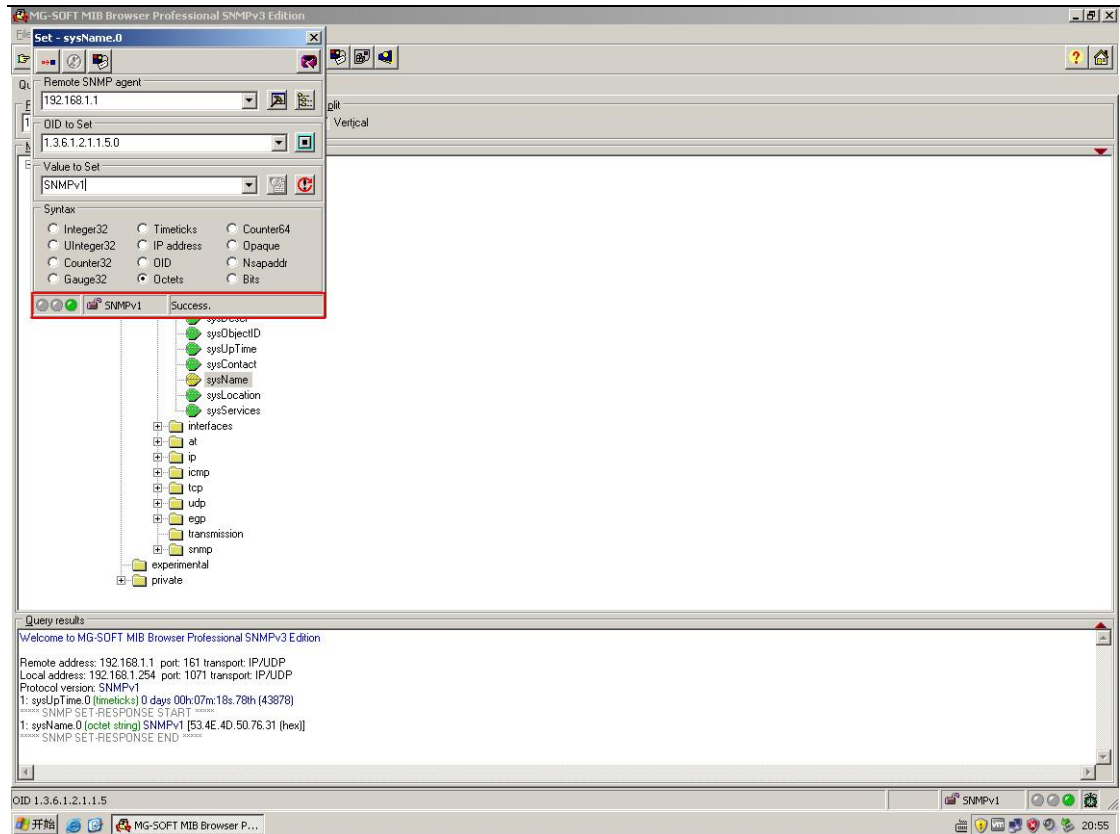
在 sysName 处单击右键，选择 Set





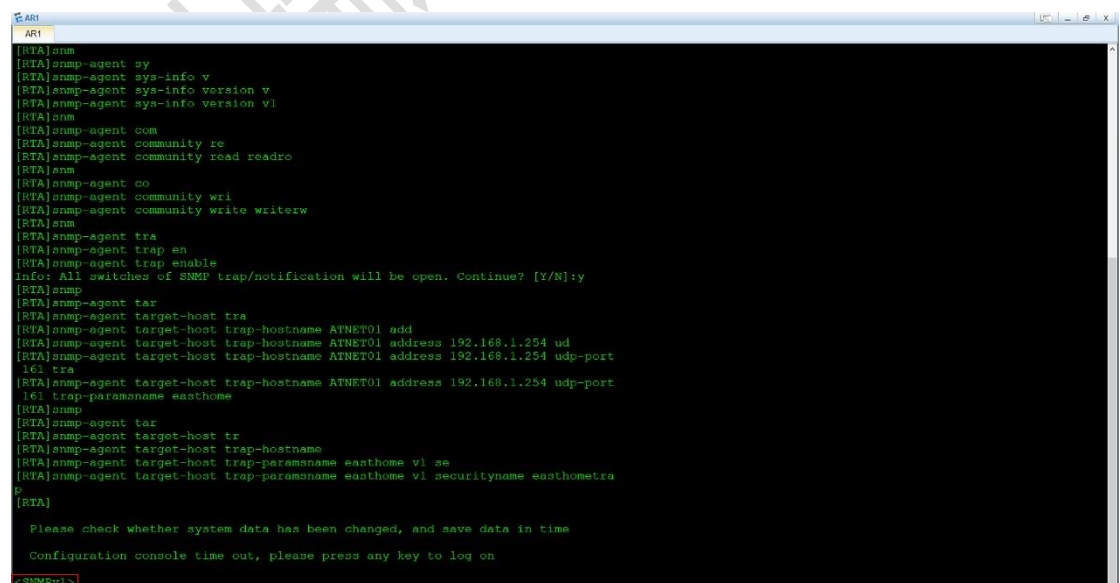
在弹出的对话框中，Value to Set 处填写希望更改的路由器名称（例如：SNMPv1），之后单击左上角红框处的按钮





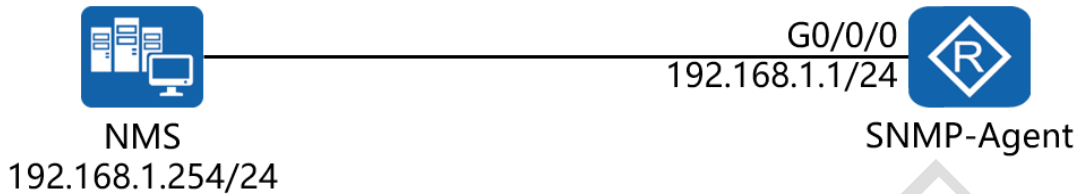
上图红框处已表明修改成功

此时，返回路由器的配置界面，点击“回车”键，查看路由器名称是否已经更改：（已修改）



三十三、配置 SNMPv2c 实验组网

一、实验拓扑：



二、实验目的：

在 NMS 上安装 MIB Browser，在 SNMP-Agent 上开启 SNMPv2 功能，令 NMS 服务器可以远程管理该路由器

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0    #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
snmp-agent          #开启 SNMP 代理功能
snmp-agent sys-info version v2c    #配置使用 SNMP 代理版本 v2c
snmp-agent community read readro    #配置团体名为 readro，并且只允许进行只读访问
snmp-agent trap enable    #开启 SNMP 代理的告警功能
    
```

```
snmp-agent target-host trap-hostname ATNET01 address
192.168.1.254 udp-port 161 trap-paramsname easthome
#配置告警信息发送的目的地址为 192.168.1.254，目的主机的主机名为 ATNET01，使用的端口号为 161，告警报文发送参数信息列表名为 easthome

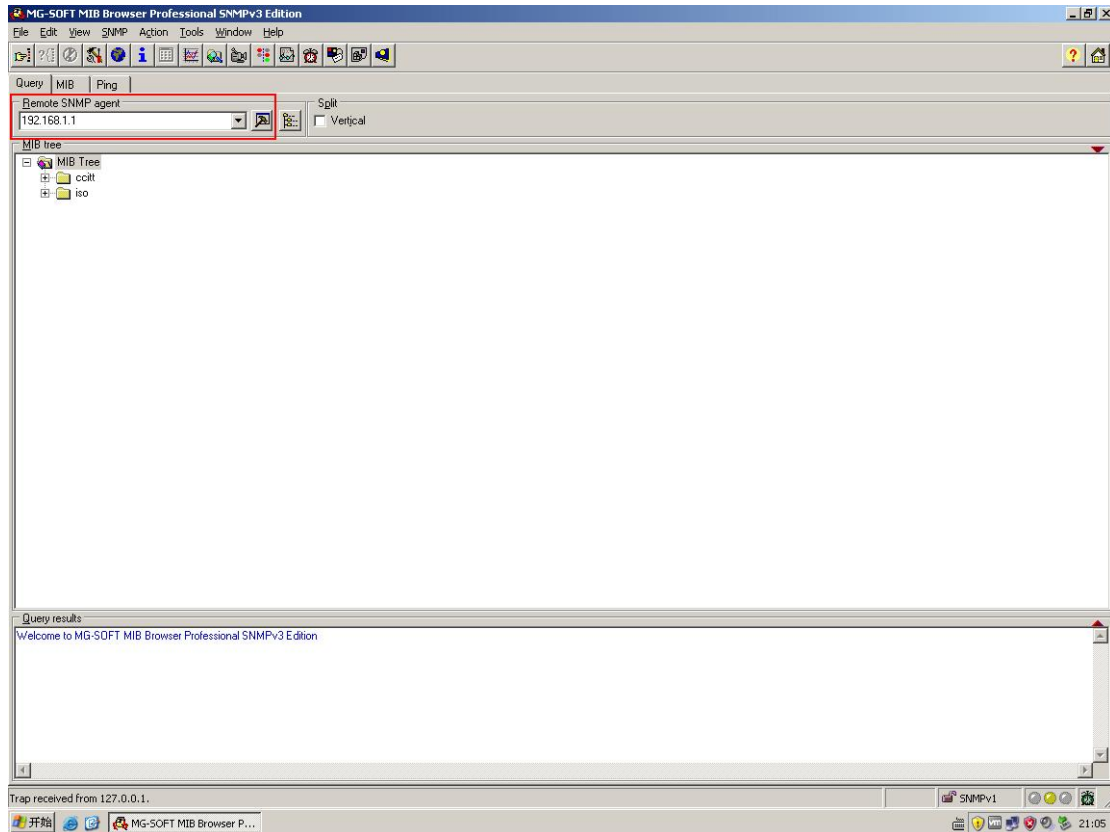
snmp-agent target-host trap-paramsname easthome v2c
securityname easthometrap #配置告警报文的发送参数信息列表名为 easthome，SNMP 版本使用版本 v2c，生成告警报文的团体名为 easthometrap

acl 2001 #创建并配置基本 ACL
rule permit source 192.168.1.254 0 #匹配源主机地址 192.168.1.254
rule deny source any #其它主机地址不匹配

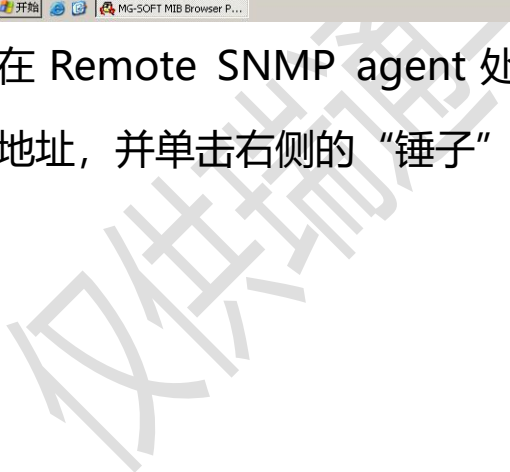
snmp-agent mib-view testview excluded system
#创建并配置名为 testview 的 MIB 视图，限制 NMS 可以管理路由器上除 system 以外的节点

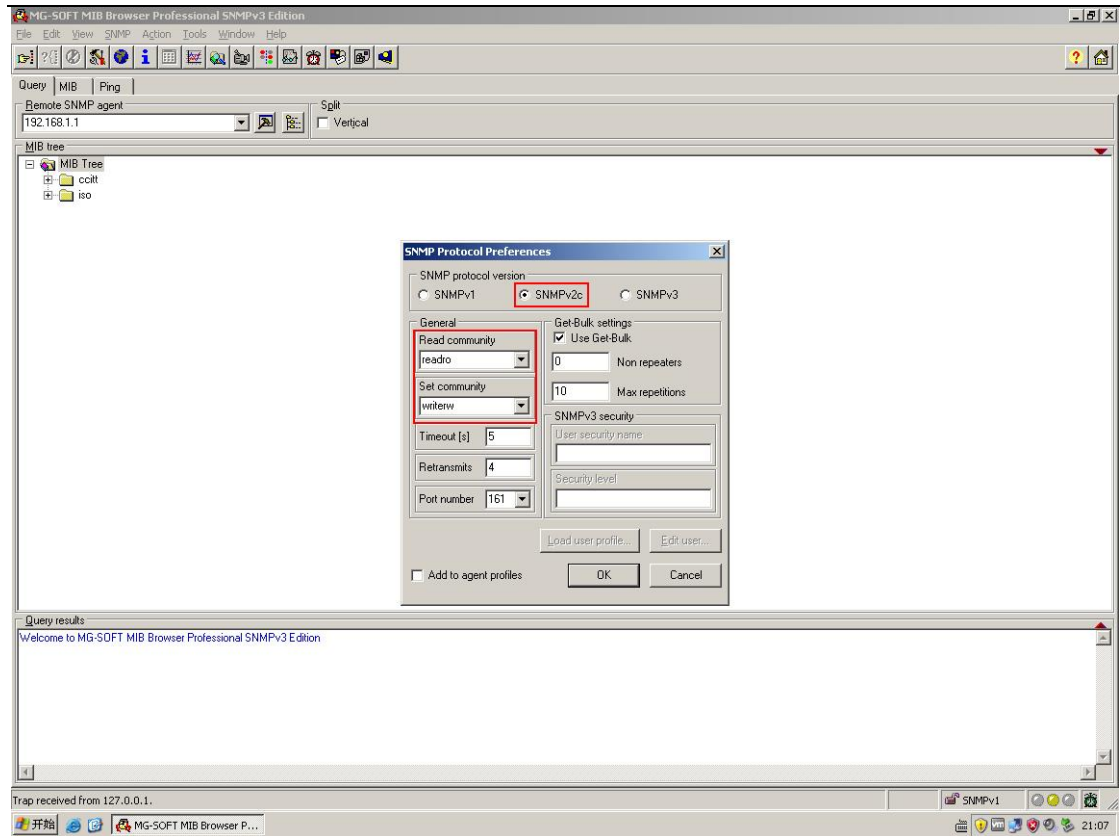
snmp-agent community write writerw mib-view testview
acl 2001
#将名为 testview 的 MIB 视图应用在 write 的团体中，并配置团体名为 writerw，且调用基本 ACL 2001
```

NMS 端安装【MG-SOFT MIB Browser Professional SNMPv3 Edition】软件并开启：

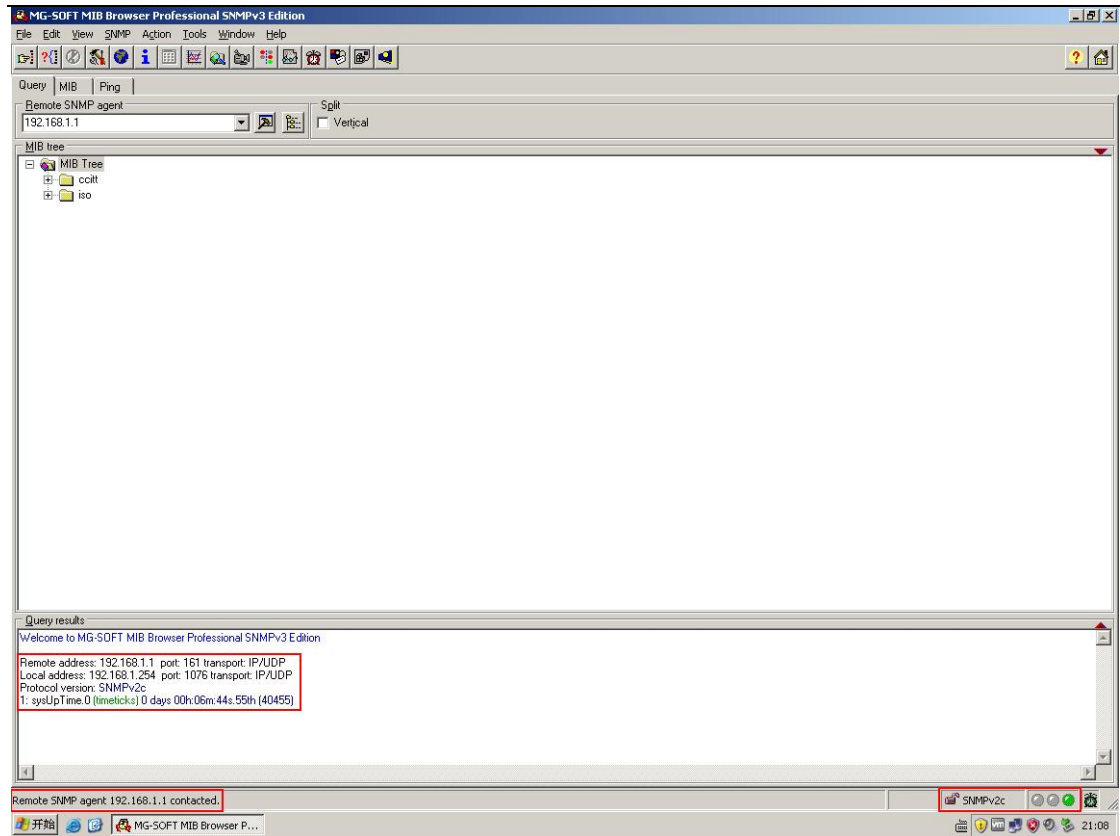


在 Remote SNMP agent 处填写 SNMP-agent (RTA) 的 IP 地址，并单击右侧的“锤子”按钮





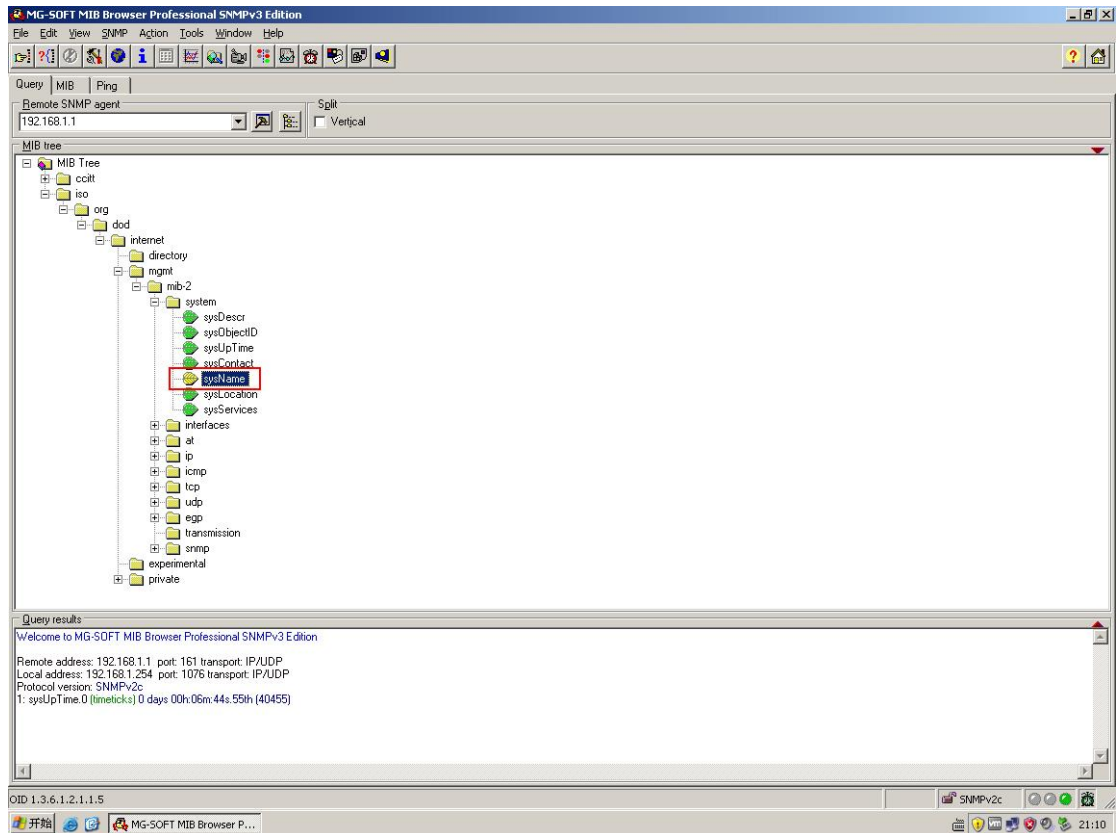
在弹出的选项页中选择 SNMPv2c, Read community 处填写 readro, Set community 处填写 writerw, 其它参数保持默认值即可, 单击 OK



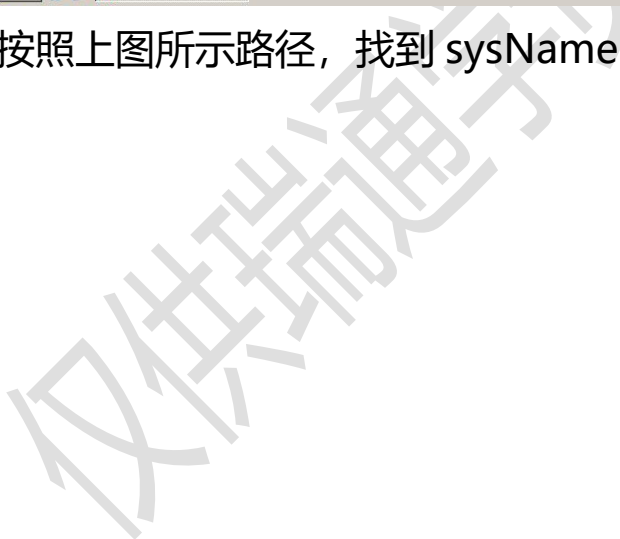
图中红框内显示，SNMP 代理（192.168.1.1）已连接成功

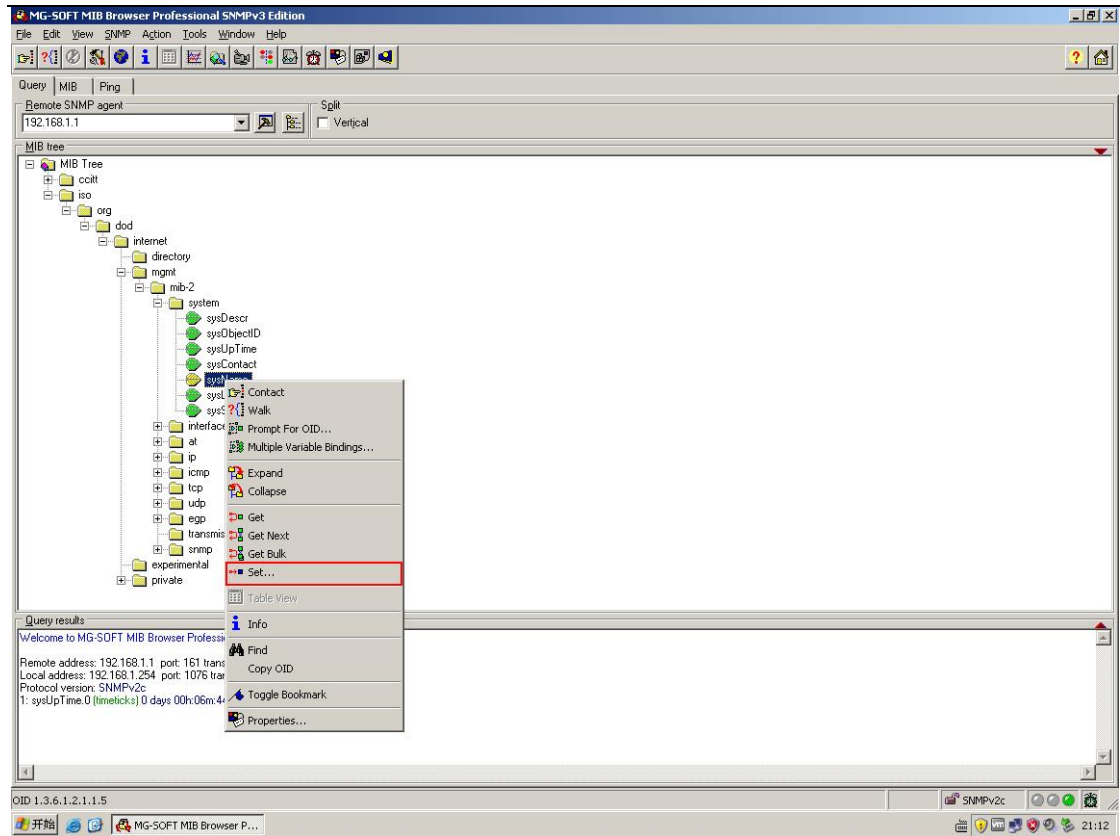
仅供瑞通字

测试是否可以通过 SNMP 远程管理并更改路由器名称：



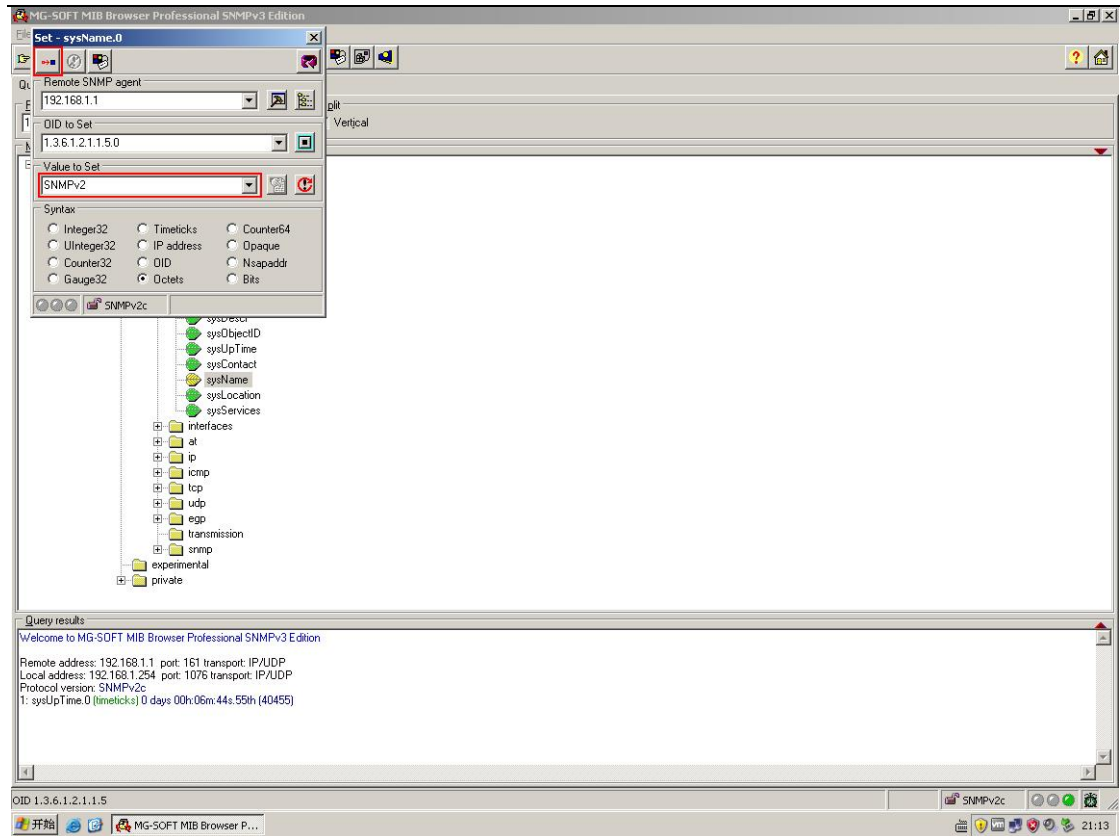
按照上图所示路径，找到 sysName（系统名称）



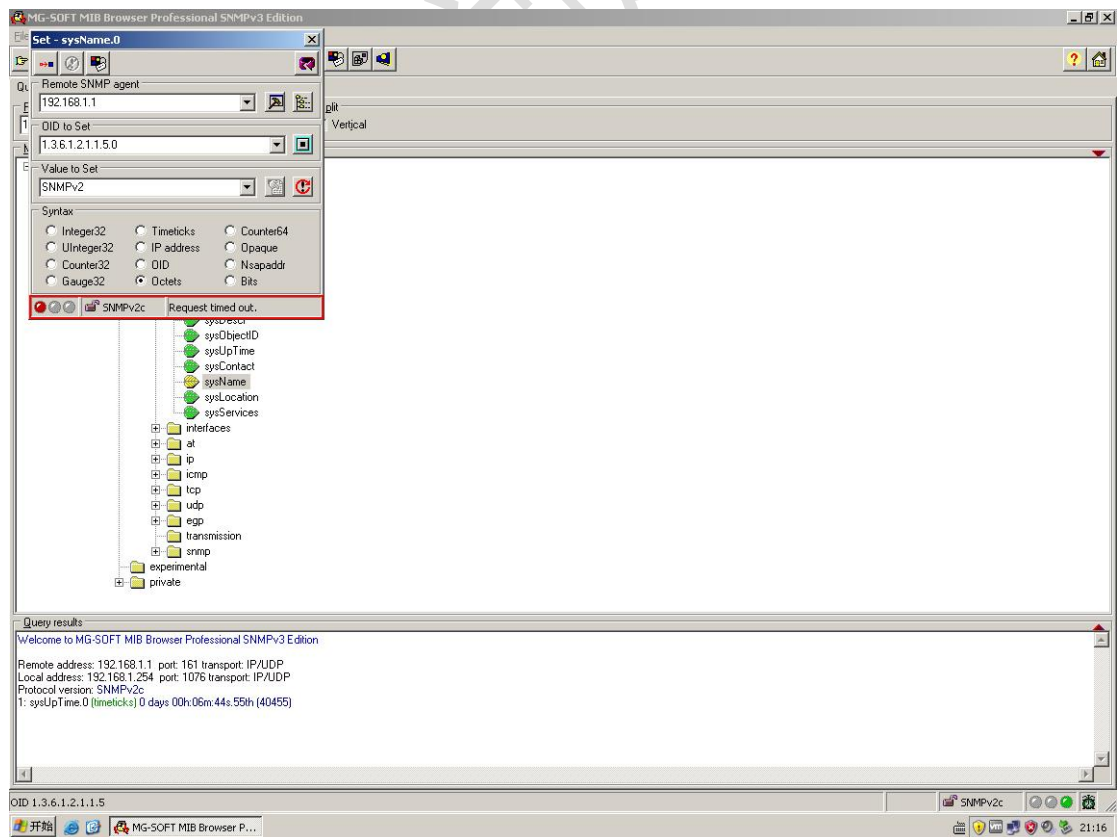
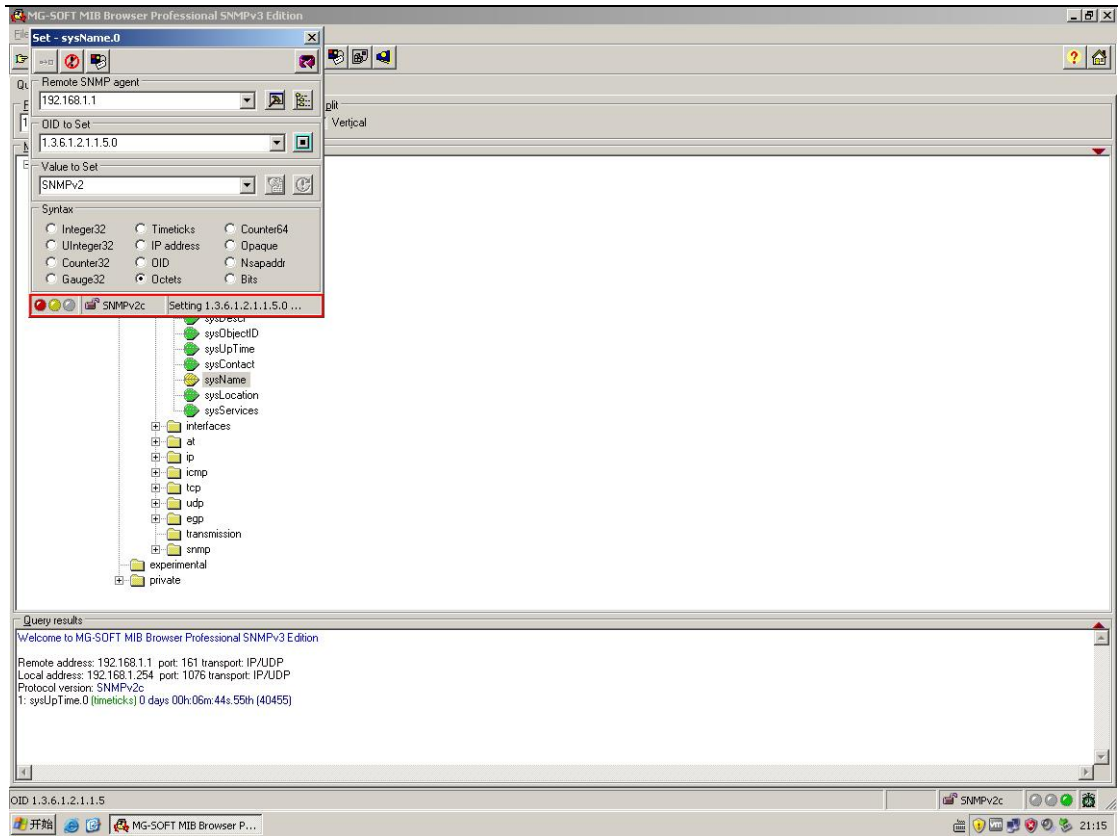


在 sysName 处单击右键，选择 Set





在弹出的对话框中，Value to Set 处填写希望更改的路由器名称（例如：SNMPv2），之后单击左上角红框处的按钮



上述 2 幅图中的红框处表明无法修改此值(Request timed out),

因为在 SNMP-Agent 上做过相应的配置，令 NMS (192.168.1.254) 无法管理 system 中的内容

此时，返回路由器的配置界面，点击“回车”键，查看路由器名称是否已经更改：(未被修改)

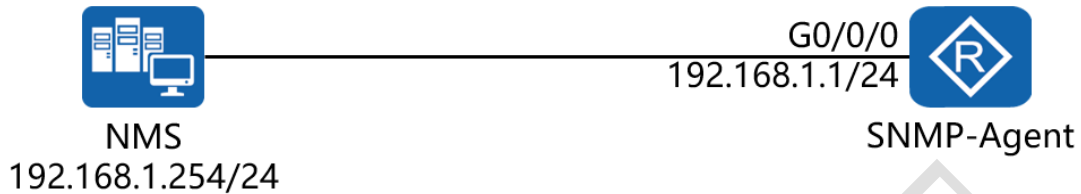
```

[RTA]snmp
[RTA]snmp-agent tar
[RTA]snmp-agent target-host t
[RTA]snmp-agent target-host trap-hostname
[RTA]snmp-agent target-host trap-paramsname easthome 7
  v1 Specify security model of SNMPv1 to generate SNMP messages
  v2c Specify security model of SNMPv2c to generate SNMP messages
  v3 Specify security model of SNMPv3 to generate SNMP messages
[RTA]snmp-agent target-host trap-paramsname easthome v2
[RTA]snmp-agent target-host trap-paramsname easthome v2c sec
[RTA]snmp-agent target-host trap-paramsname easthome v2c securityname easthome:tr
ap
[RTA]acl 2001
[RTA-acl-basic-2001]ru
[RTA-acl-basic-2001]rule per
[RTA-acl-basic-2001]rule permit sou
[RTA-acl-basic-2001]rule permit source 192.168.1.254 0
[RTA-acl-basic-2001]ru
[RTA-acl-basic-2001]rule de
[RTA-acl-basic-2001]rule deny sou
[RTA-acl-basic-2001]rule deny source n
[RTA-acl-basic-2001]rule deny source an
[RTA-acl-basic-2001]rule deny source any
[RTA-acl-basic-2001]q
[RTA]snmp
[RTA]snmp-agent mi
[RTA]snmp-agent mib-view testview ex
[RTA]snmp-agent mib-view testview exclude sy
[RTA]snmp-agent mib-view testview exclude system
[RTA]snmp
[RTA]snmp-agent com
[RTA]snmp-agent community wri
[RTA]snmp-agent community write writerw mib-view testview acl 2001
[RTA]

Please check whether system data has been changed, and save data in time
Configuration console time out, please press any key to log on
<RTA>
    
```

三十四、配置 SNMPv3 实验组网

一、实验拓扑：



二、实验目的：

在 NMS 上安装 MIB Browser，在 SNMP-Agent 上开启 SNMPv3 功能，令 NMS 服务器可以远程管理该路由器

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
snmp-agent          #开启 SNMP 代理功能
snmp-agent sys-info version v3    #配置使用 SNMP 代理版本 3
snmp-agent sys-info contact Administrator's phone number is +86 135-1111-1111 #配置管理员的联系方式
snmp-agent sys-info location Beijing #配置当前
    
```

SNMP-Agent 的位置

```
snmp-agent mib-view testview include internet
```

#创建并配置名为 *testview* 的 MIB 视图，指定 NMS 可以管理路由器上 *internet* 以下的节点

```
snmp-agent group v3 easthomegroup privacy write-view  
easthomerw read-view easthomero notify-view
```

easthomeno #配置 SNMPv3 用户组，并分别指定获取读写、只读、通知权限的对应名称

```
snmp-agent usm-user v3 easthomeuser easthomegroup
```

```
authentication-mode md5 P@ssw0rd privacy-mode
```

aes128 P@ssw0rd #在 *easthomegroup* 组中创建用户 *easthomeuser*，并配置该用户的认证及数据加密方式

```
snmp-agent trap enable #开启 SNMP 代理的告警功能
```

```
snmp-agent trap source G0/0/0 #指定 SNMP 代理告警的源接口
```

```
snmp-agent trap queue-size 200 #指定每一个 SNMP 代理告警消息的长度
```

```
snmp-agent trap life 60 #指定 SNMP 代理告警的生存时间
```

```
snmp-agent target-host trap-hostname ATNET01 address
```

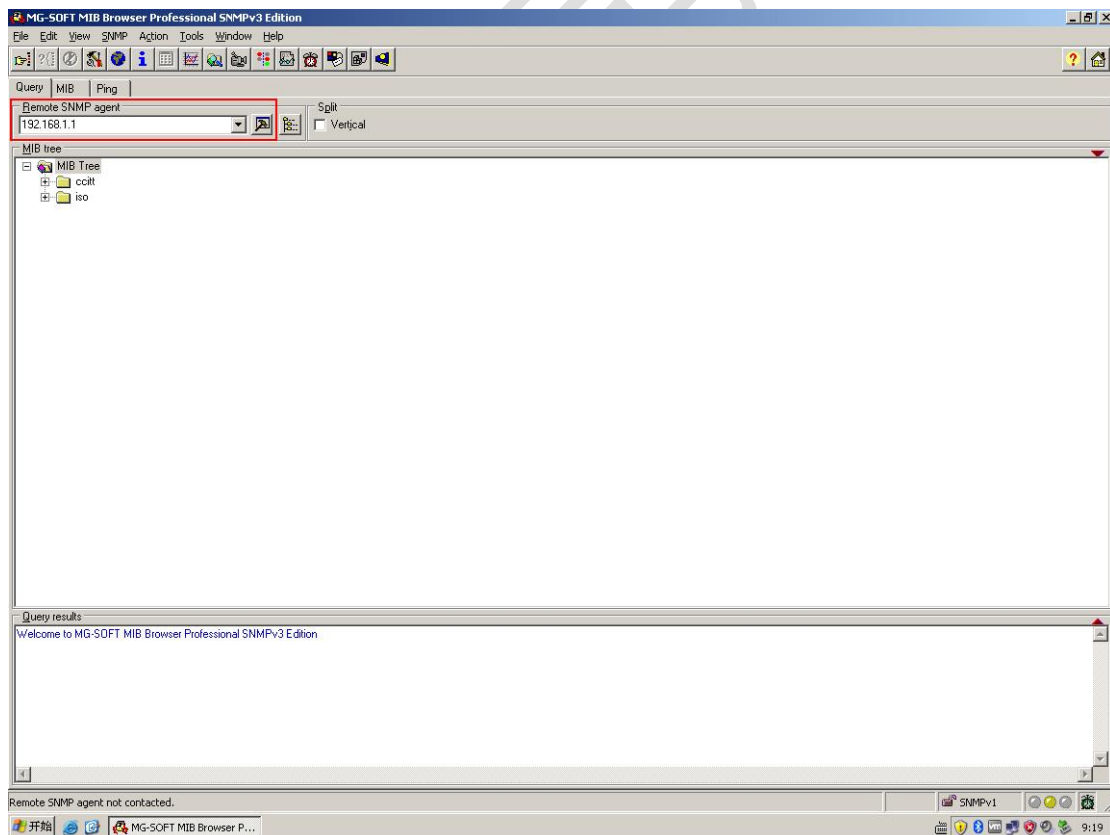
```
192.168.1.254 udp-port 161 trap-paramsname easthome
```

#配置告警信息发送的目的地址为 192.168.1.254，目的主机的

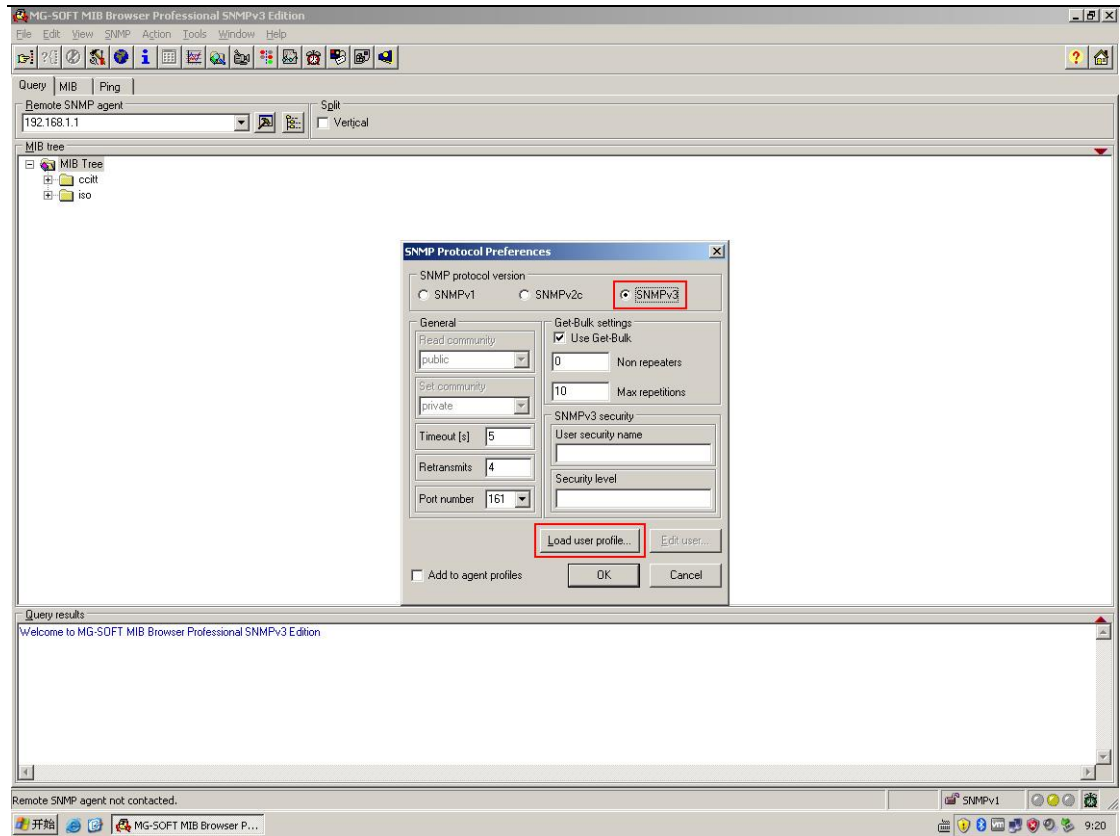
主机名为 ATNET01，使用的端口号为 161，告警报文发送参数信息列表名为 easthome

snmp-agent target-host trap-paramsname *easthome* v3
securityname *easthometrap* privacy #配置告警报文的
发送参数信息列表名为 easthome，SNMP 版本使用版本 3，生
成告警报文的团体名为 easthometrap，并同时使用安全加密与
用户认证

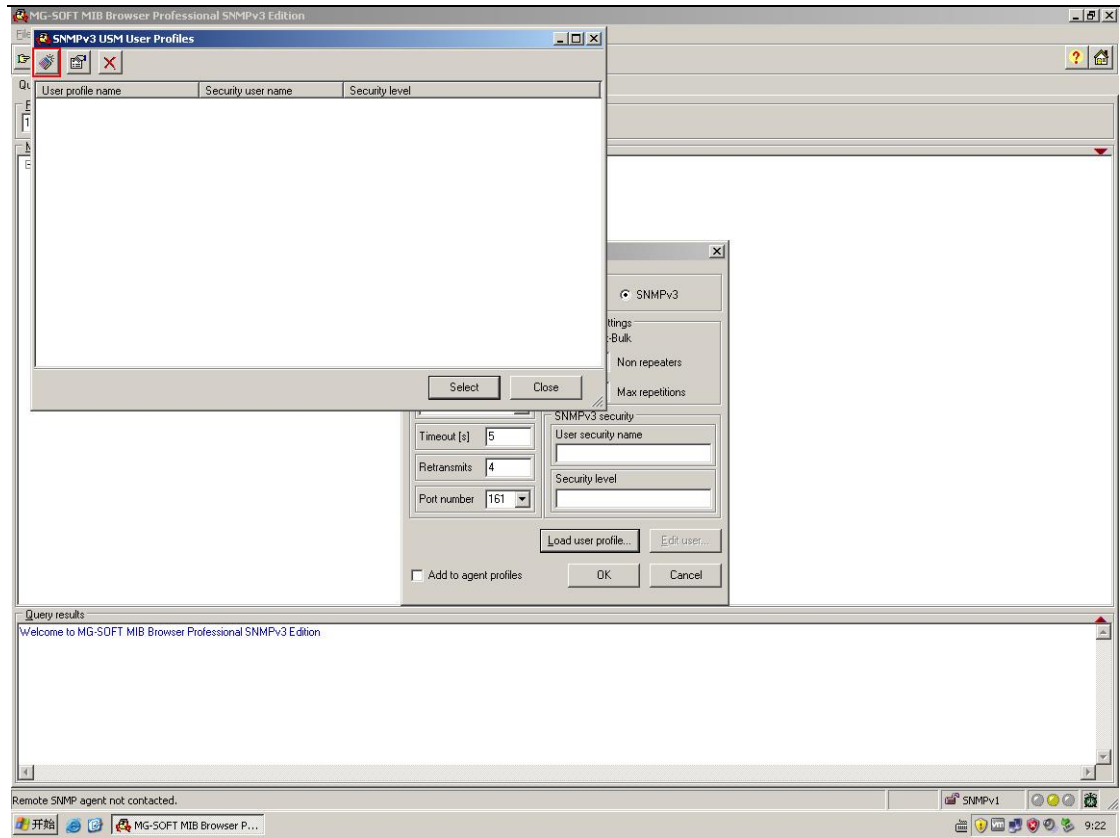
NMS 端安装【MG-SOFT MIB Browser Professional SNMPv3 Edition】软件并开启：



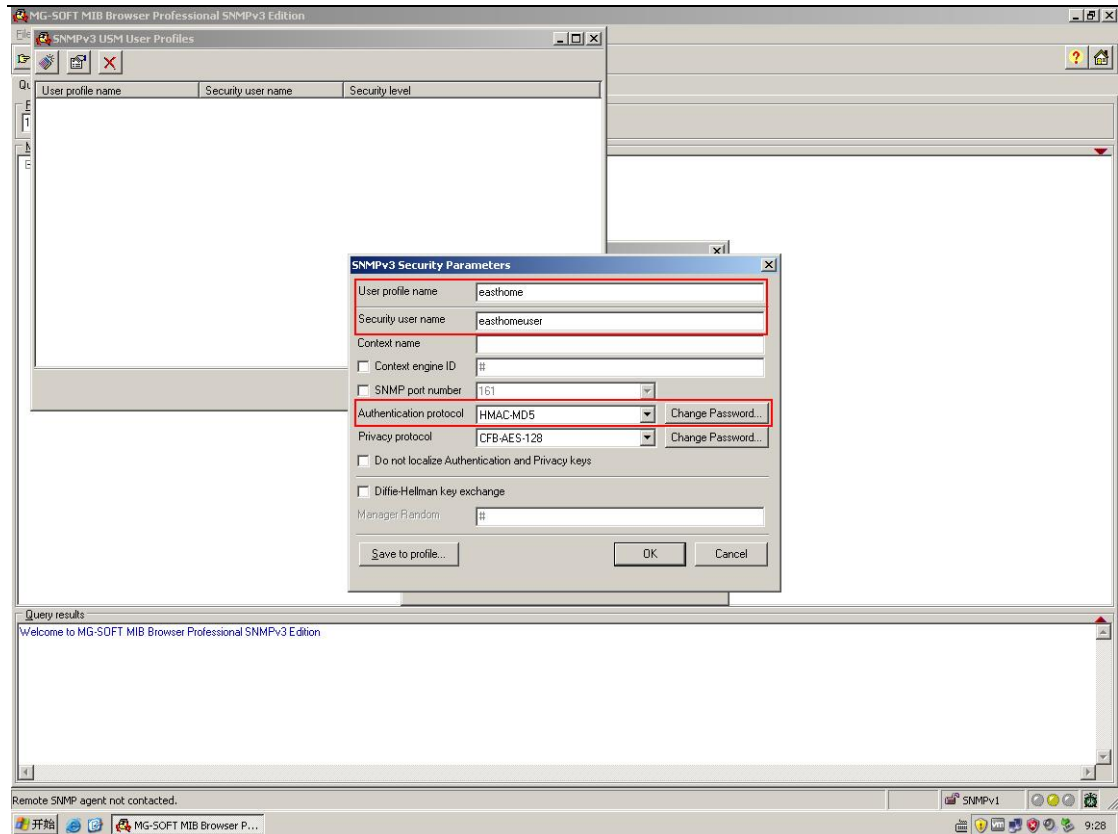
在 Remote SNMP agent 处填写 SNMP-agent (RTA) 的 IP 地址，并单击右侧的“锤子”按钮



在弹出的选项页中选择 SNMPv3，并点击 Load user profile...



在弹出的对话框中选择上图红框标注的第一个按钮“New SNMPv3 USM User”



之后再弹出的对话框中按上图所示，填写相应的内容：

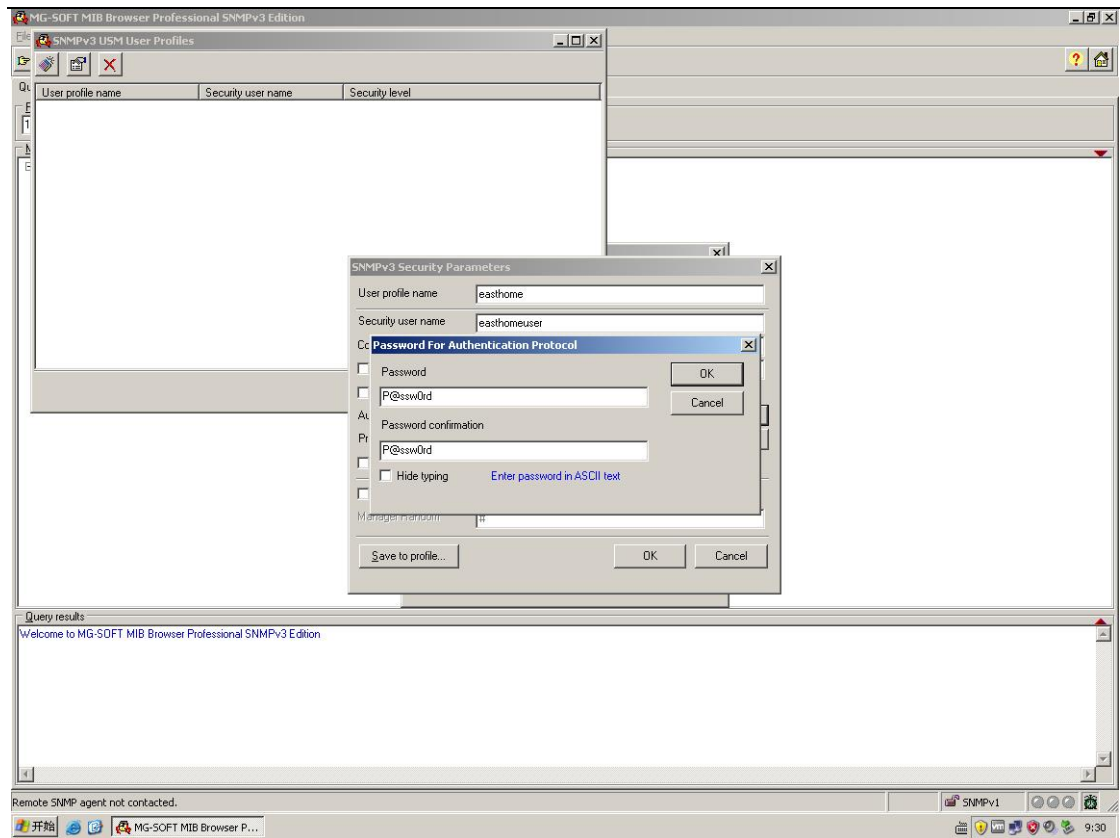
User profile name: 可随意编写，为当前所创建的用户进程命名

Security user name: 此处填写 SNMP-Agent 上所创建的用户名

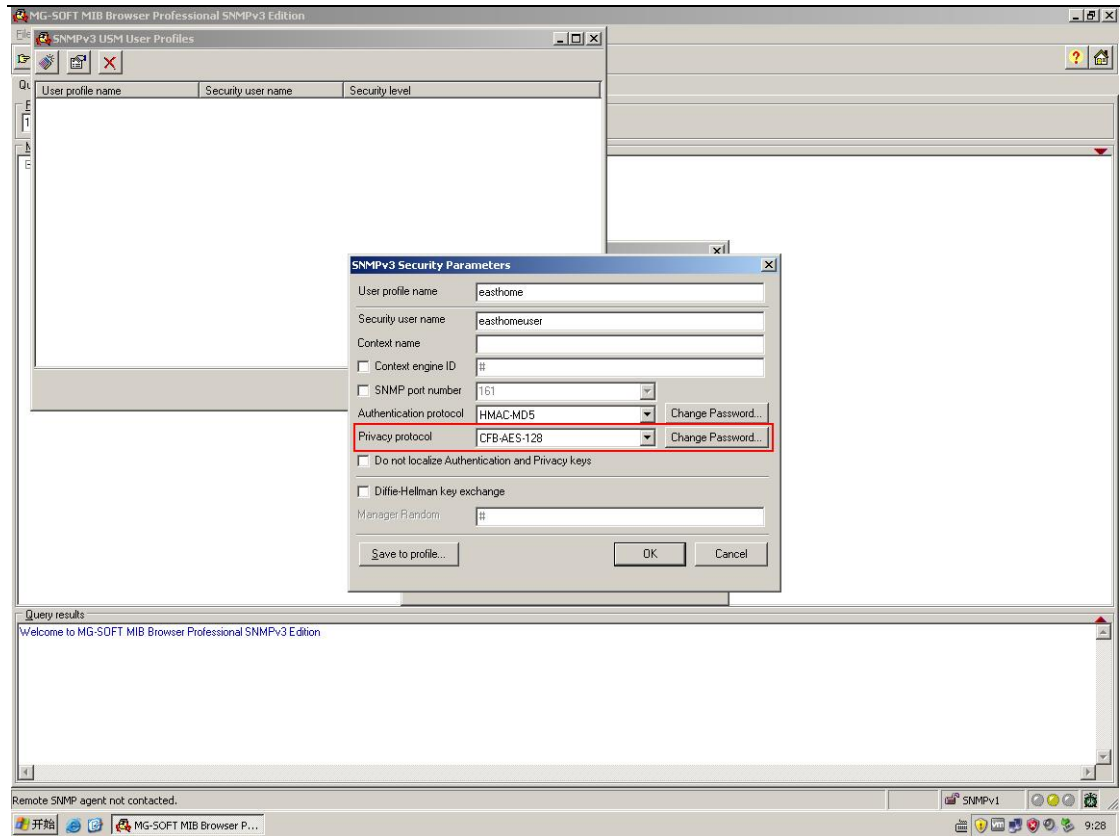
Authentication protocol: 此处选择与 SNMP-Agent 上同样的设置

Privacy protocol: 此处选择与 SNMP-Agent 上同样的设置

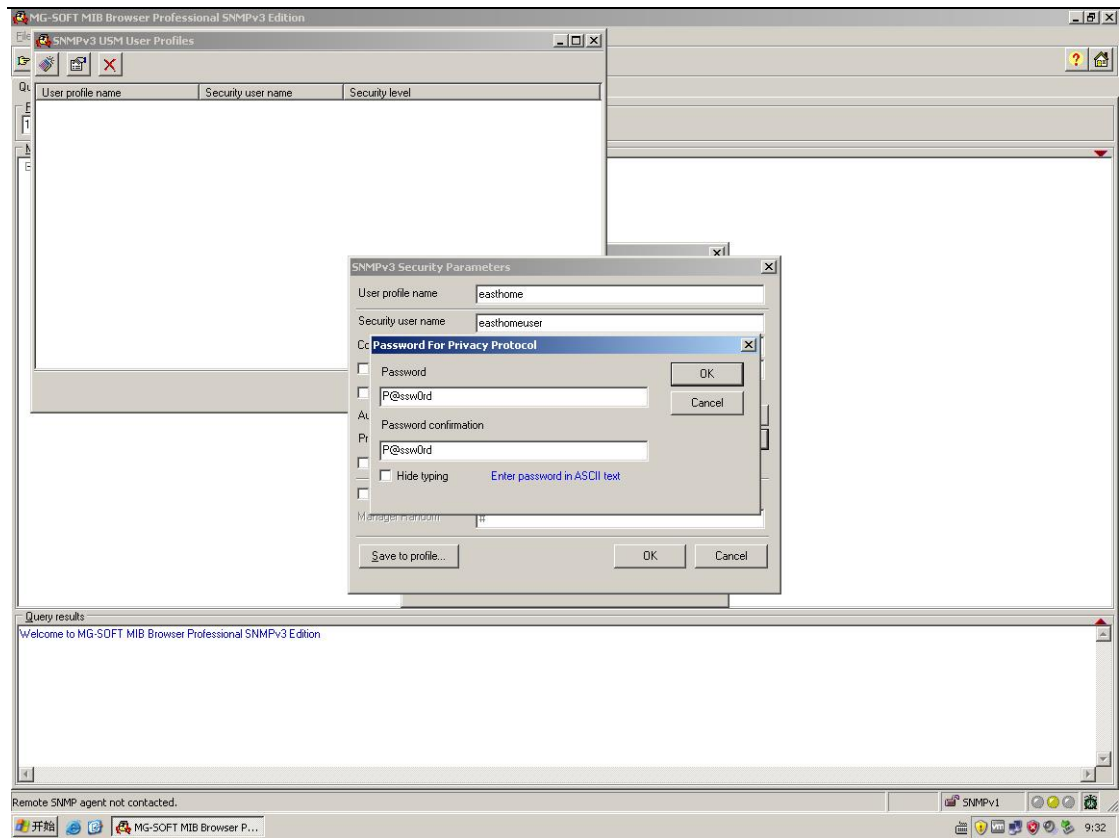
之后单击 Authentication protocol 右侧的 “Change Password...”



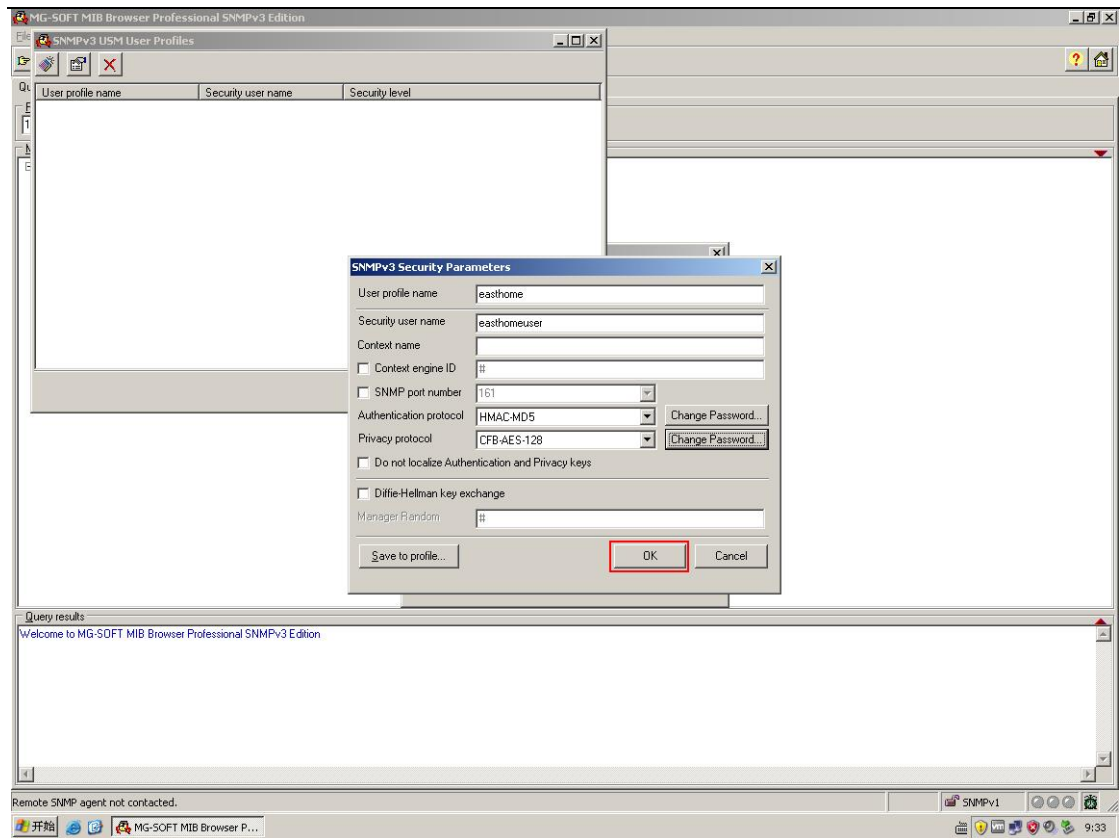
此处填写与 SNMP-Agent 上配置的同样的密钥，之后单击 OK



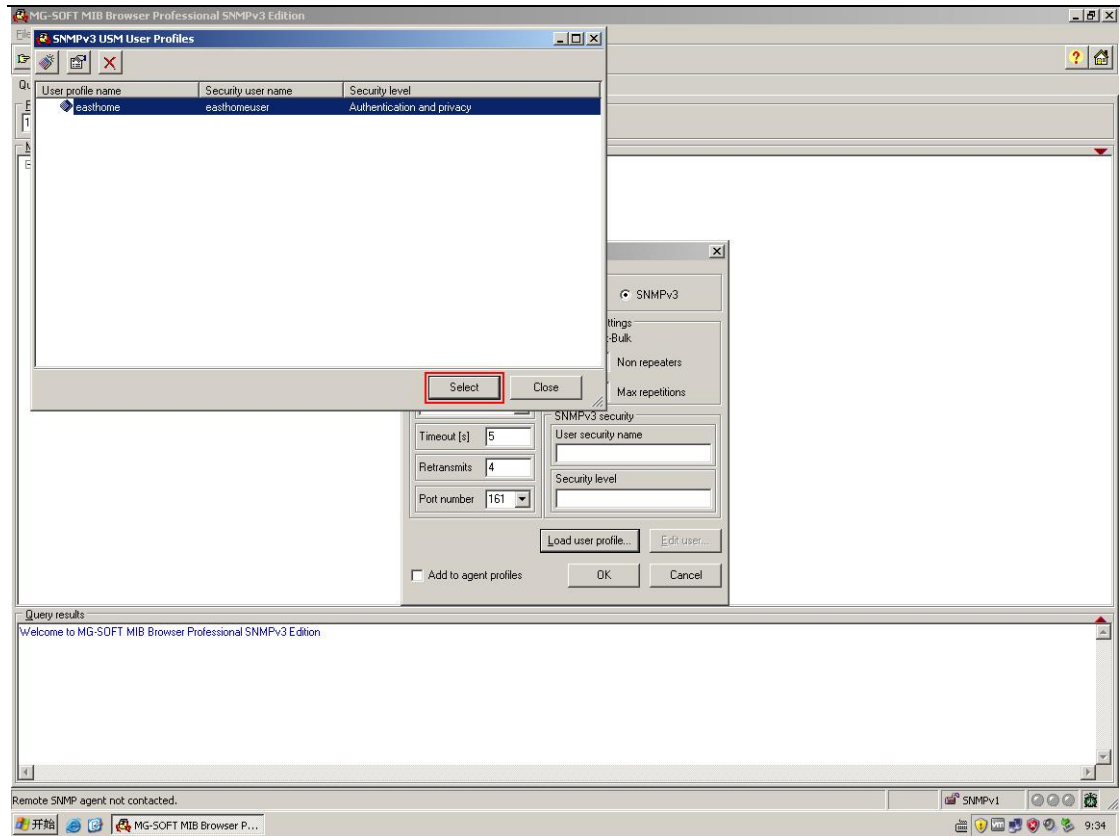
返回上图对话框后，再单击 Privacy protocol 右侧的 “Change Password...”



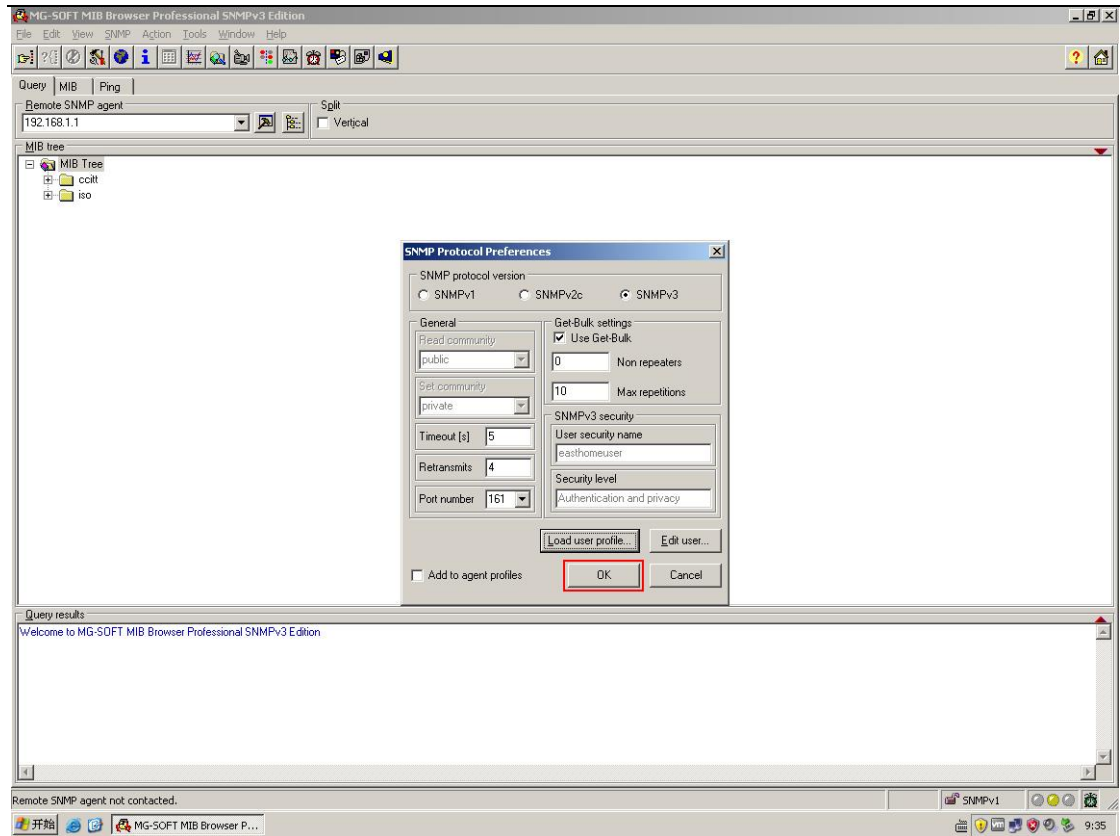
同样，此处填写与 SNMP-Agent 上配置的同样的密钥，之后单击 OK



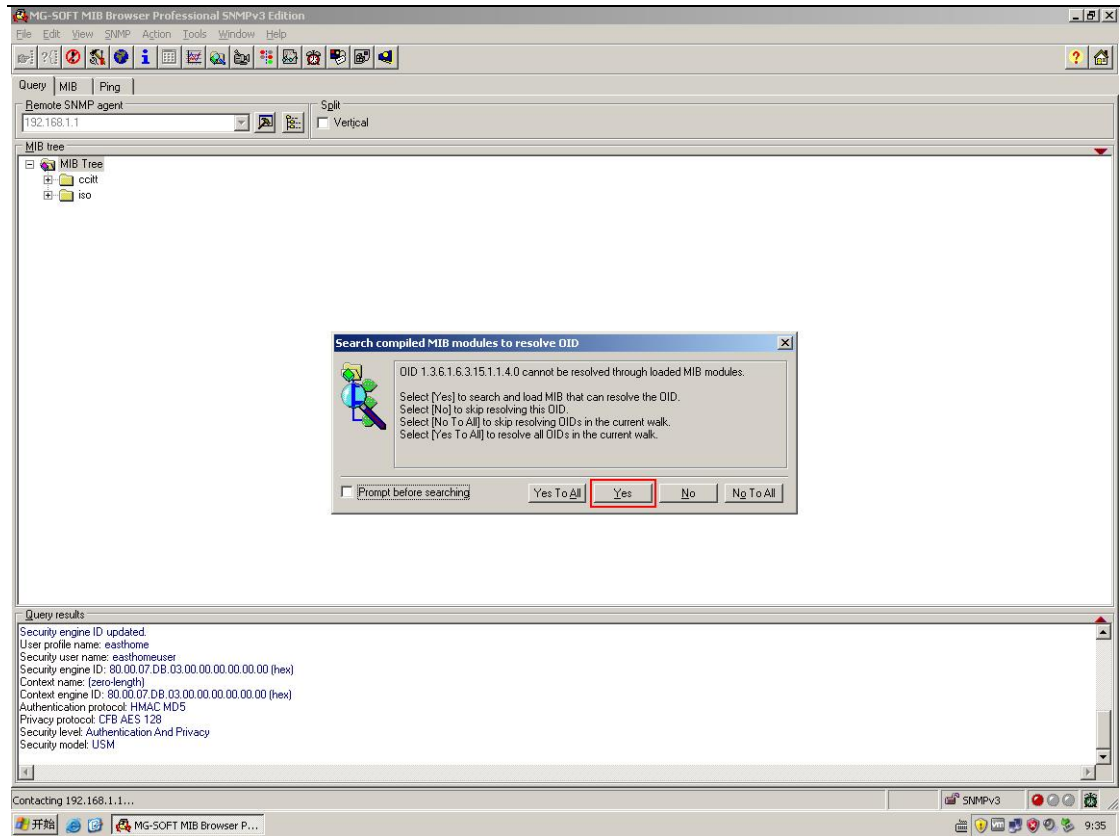
在填写完所有密钥之后，单击上图中对话框内的 OK



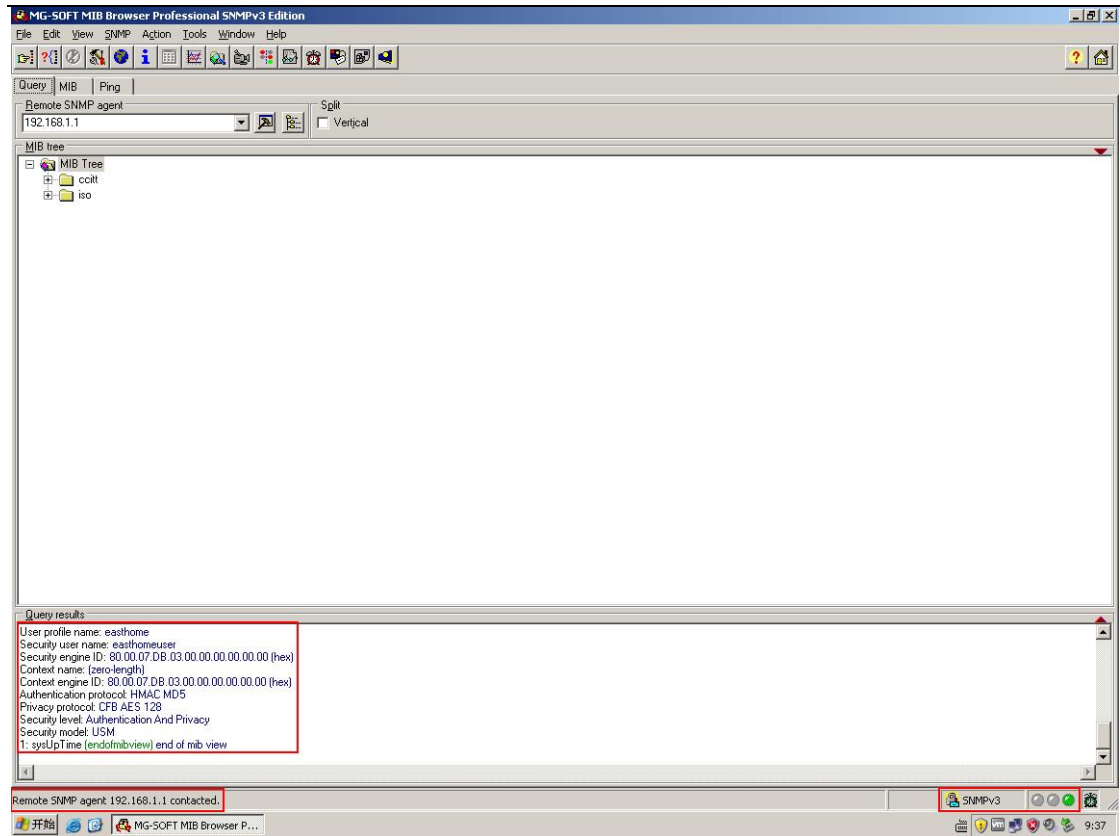
之后返回至上图所示的“SNMPv3 USM User Profiles”对话框，单击 Select



在全部配置结束之后，返回至上图所示的“SNMP Protocol Preferences”界面，单击 OK



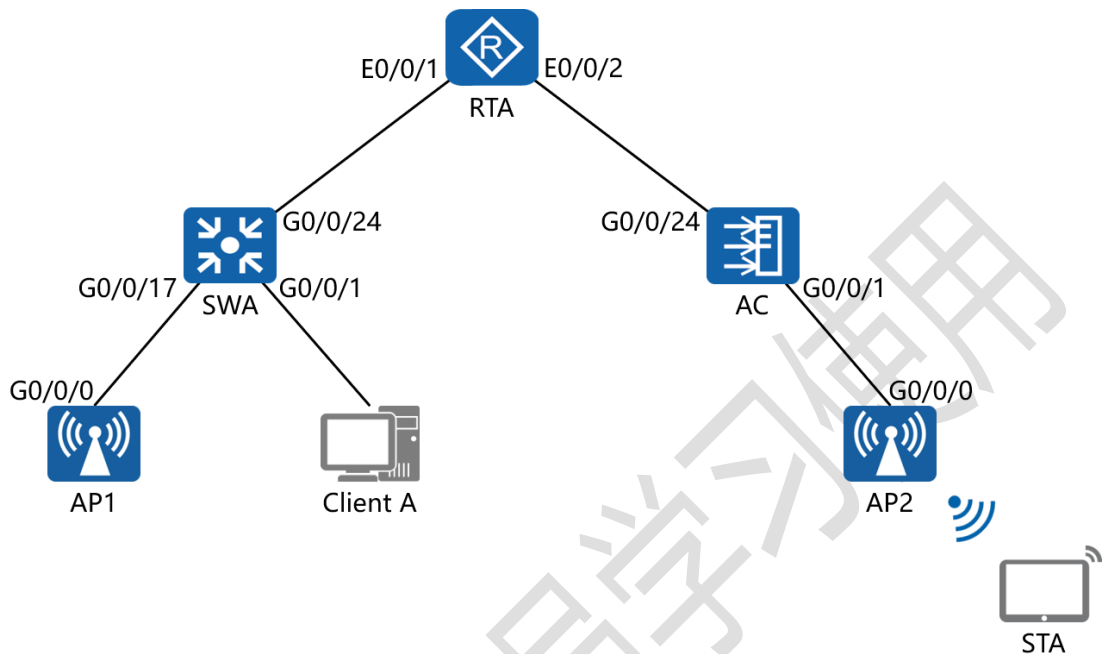
此处弹出的对话框告知用户，软件无法在当前的 MIB 树中找到 OID 为 1.3.6.1.6.3.15.1.1.4.0 的子集。单击 “Yes” 则表示允许查找并加载 MIB 即可解决上述问题



单击“**Yes**”之后, 上图显示, 当前 NMS 服务器与 SNMP-Agent 已经成功建立了连接

三十五、配置无线 AC 控制器实验组网

一、实验拓扑：



二、实验目的：

SWA 作为二层接入交换机，创建 VLAN 100 为有线客户的业务 VLAN；VLAN 200 为 AP 管理 VLAN；VLAN 300 为 AP 的无线客户的业务 VLAN；VLAN 999 为设备管理 VLAN；

SWA 的 G0/0/1 – 16 端口配置业务 VLAN 100；G0/0/17 – 22 端口配置为 AP 的接入端口；G0/0/24 为上联路由器端口；

AC 的 G0/0/1 – 20 端口配置为 AP 的接入端口；G0/0/24 为上联路由器端口；

AC 作为 DHCP 服务器，为有线客户的业务 VLAN 100、AP 的管理 VLAN 200、AP 的无线客户的业务 VLAN 300 提供 IP 地址的分配服务；

RTA 作为边界路由器，与外网建立连接；

AP1 与 AP2 的 SSID 为 HuaWei-AP3030；连接密钥为 P@ssw0rd；

令部署在 SWA 上的 Client A 与连接在 AP1 或 AP2 上的 STA 设备可互相访问；且 Client A 与 STA 均可与 SWA、RTA、AP 及 AC 通讯

三、实验步骤：

RTA:

```

system-view          #进入系统视图模式
sysname RTA         #给设备命名
vlan batch 100 200 300 999    #创建 VLAN 100、200、300
及 999
dhcp enable         #开启 DHCP 功能
interface vlan 100    #进入 VLAN 100 的接口配置模式
description PC_Business_VLAN    #添加接口描述信息
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
dhcp select relay    #开启 DHCP 中继代理功能
interface vlan 200    #进入 VLAN 200 的接口配置模式
description AP_Management_VLAN    #添加接口描述信息
ip address 192.168.2.1 24    #配置 IP 地址及子网掩码
    
```

```

dhcp select relay      #开启 DHCP 中继代理功能
interface vlan 300    #进入 VLAN 300 的接口配置模式
description AP_Business_VLAN    #添加接口描述信息
ip address 192.168.3.1 24    #配置 IP 地址及子网掩码
dhcp select relay      #开启 DHCP 中继代理功能
interface vlan 999    #进入 VLAN 999 的接口配置模式
description Management_VLAN    #添加接口描述信息
ip address 172.16.1.1 24    #配置 IP 地址及子网掩码
interface E0/0/1      进入相应的端口
description To_SWA    #添加端口描述信息
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
VLAN 的信息
interface E0/0/2      进入相应的端口
description To_AC     #添加端口描述信息
port link-type trunk  #将端口配置为中继模式
port trunk allow-pass vlan all    #允许该中继端口传递所有
VLAN 的信息

```

SWA:

```

system-view
sysname SWA

```

```
vlan batch 100 200 300 999
interface vlan 100
description PC_Business_VLAN
interface vlan 200
description AP_Management_VLAN
interface vlan 300
description AP_Business_VLAN
interface vlan 999
description Management_VLAN
ip address 172.16.1.2 24
port-group Business
group-member G0/0/1 to G0/0/16
port link-type access
port default vlan 100
port-group AP-Access
group-member G0/0/17 to G0/0/22
port link-type trunk
port trunk allow-pass vlan all
port trunk pvid vlan 200
interface G0/0/24
description To_RTA
port link-type trunk
```



```
port trunk allow-pass vlan all  
ip route-static 0.0.0.0 0 172.16.1.1
```

AC:

```
system-view  
sysname AC  
vlan batch 100 200 300 999  
dhcp enable  
ip pool ForAP #创建名为 ForAP 的地址池  
network 192.168.2.0 mask 24 #创建地址池中的可用网段  
及分配的子网掩码  
excluded-ip-address 192.168.2.2 #指定在分配地址时  
排除的 IP 地址  
gateway-list 192.168.2.1 #指定分配的网关地址  
dns-list 192.168.2.1 #指定分配的 DNS 地址  
ip pool ForSTA  
network 192.168.3.0 mask 24  
excluded-ip-address 192.168.3.2  
gateway-list 192.168.3.1  
dns-list 192.168.3.1  
ip pool ForPC  
network 192.168.1.0 mask 24
```

```
excluded-ip-address 192.168.1.2
gateway-list 192.168.1.1
dns-list 192.168.1.1
interface vlan 100
description PC_Business_VLAN
ip address 192.168.1.2 24
dhcp select global      #开启基于全局的 DHCP 功能
interface vlan 200
description AP_Management_VAN
ip address 192.168.2.2 24
dhcp select global      #开启基于全局的 DHCP 功能
interface vlan 300
description AP_Business_VLAN
ip address 192.168.3.2 24
dhcp select global      #开启基于全局的 DHCP 功能
interface vlan 999
description Management_VLAN
ip address 172.16.1.3 24
port-group AP-Access
group-member G0/0/1 to G0/0/20
port link-type trunk
port trunk allow-pass vlan all
```

```

port trunk pvid vlan 200

interface G0/0/24

description To RTA

port link-type trunk

port trunk allow-pass vlan all

capwap source interface Vlanif 200    #配置 AC 与 AP 建立
CAPWAP 隧道的源接口

wlan    #进入 WLAN 的配置模式

security-profile name HuaWei-AP3030    #创建并进入安
全模板视图

security wpa2 psk pass-phrase P@ssw0rd aes-tkip
#指定加密使用的方式及密钥

ssid-profile name HuaWei-AP3030    #创建并进入 SSID 模
板视图

ssid HuaWei-AP3030    #指定 SSID 的名称

vap-profile name HuaWei-AP3030    #创建并进入 VAP 模
板视图

service-vlan vlan-id 300    #配置 VAP 的业务 VLAN

ssid-profile HuaWei-AP3030    #绑定 SSID 模板

security-profile HuaWei-AP3030    #绑定安全模板

ap-group name HuaWei-AP3030    #创建并进入 AP 组

radio 0    #指定射频 ID

```

vap-profile *HuaWei-AP3030* wlan 1 #将 VAP 与 WLAN 配置做绑定

ap-id 1 type-id 45 ap-mac 00e0-fce3-7ee0 #配置第一台 AP 的 ID 值, 类型值, 以及 AP 的 MAC 地址

ap-name AP1 #为第一台 AP 命名

ap-group *HuaWei-AP3030* #将 AP 加入进 AP 组

ap-id 2 type-id 45 ap-mac 00e0-fc2c-3620

ap-name AP2

ap-group HuaWei-AP3030

ip route-static 0.0.0.0 0 172.16.1.1

测试:

在 AP1 上检测是否成功获取 IP 地址:

```
[AP1]display arp
IP ADDRESS      MAC ADDRESS      EXPIRE (M)  TYPE  INTERFACE      VPN-INSTANCE
-----
192.168.2.21    00e0-fcd1-2880   I -         Vlanif1
192.168.2.1     00e0-fc5c-2e70   17          D-0   GE0/0/0
192.168.2.2     00e0-fc54-6336   19          D-0   GE0/0/0
-----
Total:3         Dynamic:2        Static:0     Interface:1
[AP1]
```

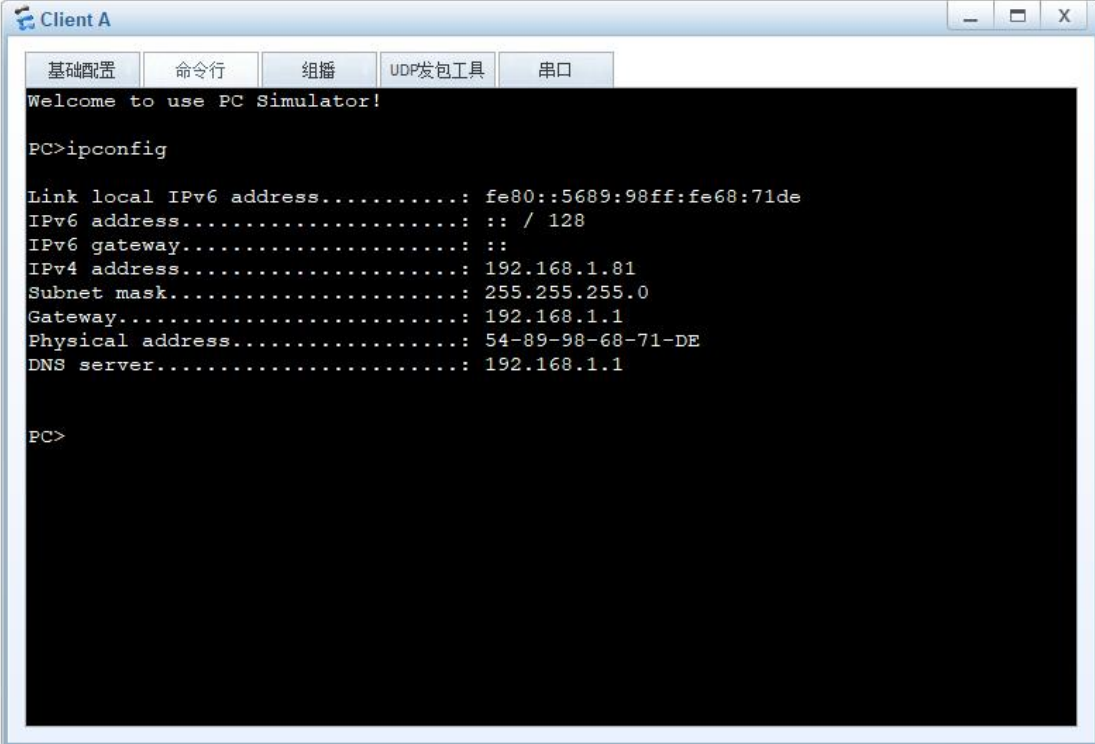
在 AP2 上检测是否成功获取 IP 地址:

```
[AP2]display arp
IP ADDRESS      MAC ADDRESS      EXPIRE (M)  TYPE  INTERFACE      VPN-INSTANCE
-----
192.168.2.75    00e0-fc57-0b90   I -         Vlanif1
192.168.2.1     00e0-fc5c-2e70   14          D-0   GE0/0/0
192.168.2.2     00e0-fc54-6336   17          D-0   GE0/0/0
-----
Total:3         Dynamic:2        Static:0     Interface:1
[AP2]
```

在 AC 上查看与两台 AP 的关联情况:

```
[AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor : normal          [2]
-----
ID   MAC           Name Group      IP           Type          State STA Up
time
-----
1    00e0-fcd1-2880 AP1  Huawei-AP3030  192.168.2.21 AP3030DN      nor   0   5M
:18S
2    00e0-fc57-0b90 AP2  Huawei-AP3030  192.168.2.75 AP3030DN      nor   0   4M
:39S
-----
Total: 2
[AC]
```

首先检测 Client A 是否成功获取 IP 地址：



The screenshot shows a window titled 'Client A' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The terminal window displays the following text:

```

Welcome to use PC Simulator!

PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:fe68:71de
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.1.81
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.1.1
Physical address.....: 54-89-98-68-71-DE
DNS server.....: 192.168.1.1

PC>
    
```

检测 Client A 是否可与 RTA(172.16.1.1)、SWA(172.16.1.2)、AC (172.16.1.3) 正常通讯：

```

Client A
基础配置 命令行 组播 UDP发包工具 串口
Link local IPv6 address.....: fe80::5689:98ff:fe68:71de
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.1.81
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.1.1
Physical address.....: 54-89-98-68-71-DE
DNS server.....: 192.168.1.1

PC>ping 172.16.1.1

Ping 172.16.1.1: 32 data bytes, Press Ctrl_C to break
From 172.16.1.1: bytes=32 seq=1 ttl=255 time=31 ms
From 172.16.1.1: bytes=32 seq=2 ttl=255 time=31 ms
From 172.16.1.1: bytes=32 seq=3 ttl=255 time=31 ms
From 172.16.1.1: bytes=32 seq=4 ttl=255 time=47 ms
From 172.16.1.1: bytes=32 seq=5 ttl=255 time=47 ms

--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/37/47 ms

PC>
    
```

```

Client A
基础配置 命令行 组播 UDP发包工具 串口
From 172.16.1.1: bytes=32 seq=3 ttl=255 time=31 ms
From 172.16.1.1: bytes=32 seq=4 ttl=255 time=47 ms
From 172.16.1.1: bytes=32 seq=5 ttl=255 time=47 ms

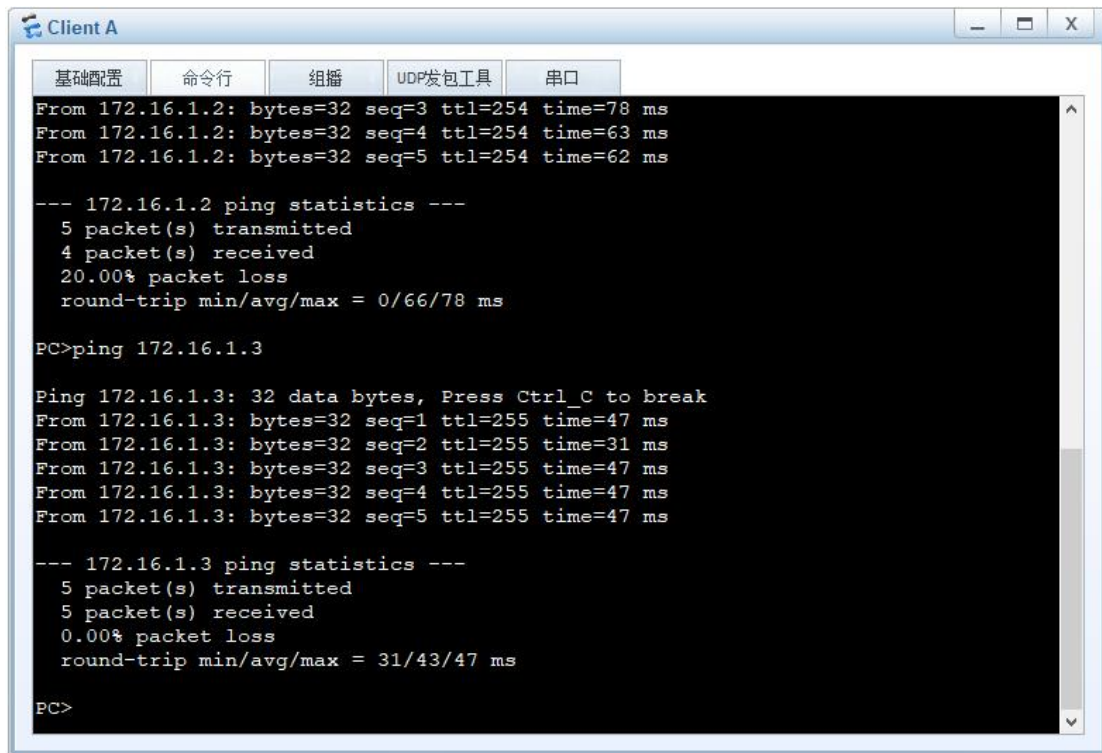
--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/37/47 ms

PC>ping 172.16.1.2

Ping 172.16.1.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 172.16.1.2: bytes=32 seq=2 ttl=254 time=62 ms
From 172.16.1.2: bytes=32 seq=3 ttl=254 time=78 ms
From 172.16.1.2: bytes=32 seq=4 ttl=254 time=63 ms
From 172.16.1.2: bytes=32 seq=5 ttl=254 time=62 ms

--- 172.16.1.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/66/78 ms

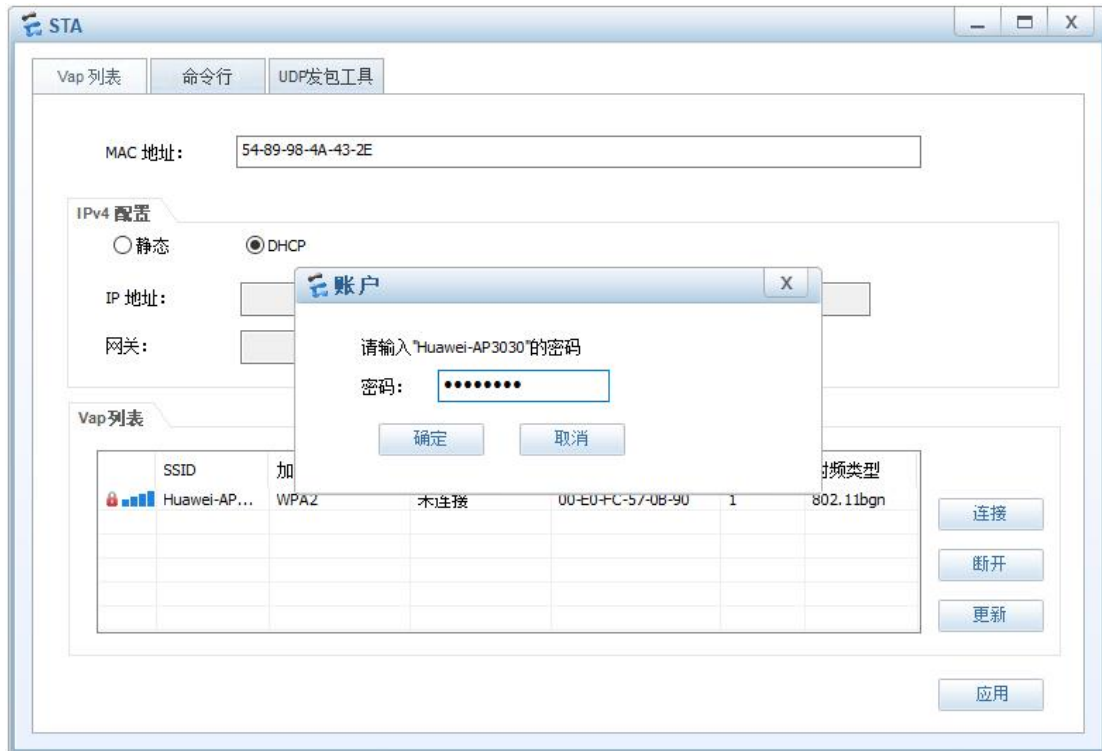
PC>
    
```

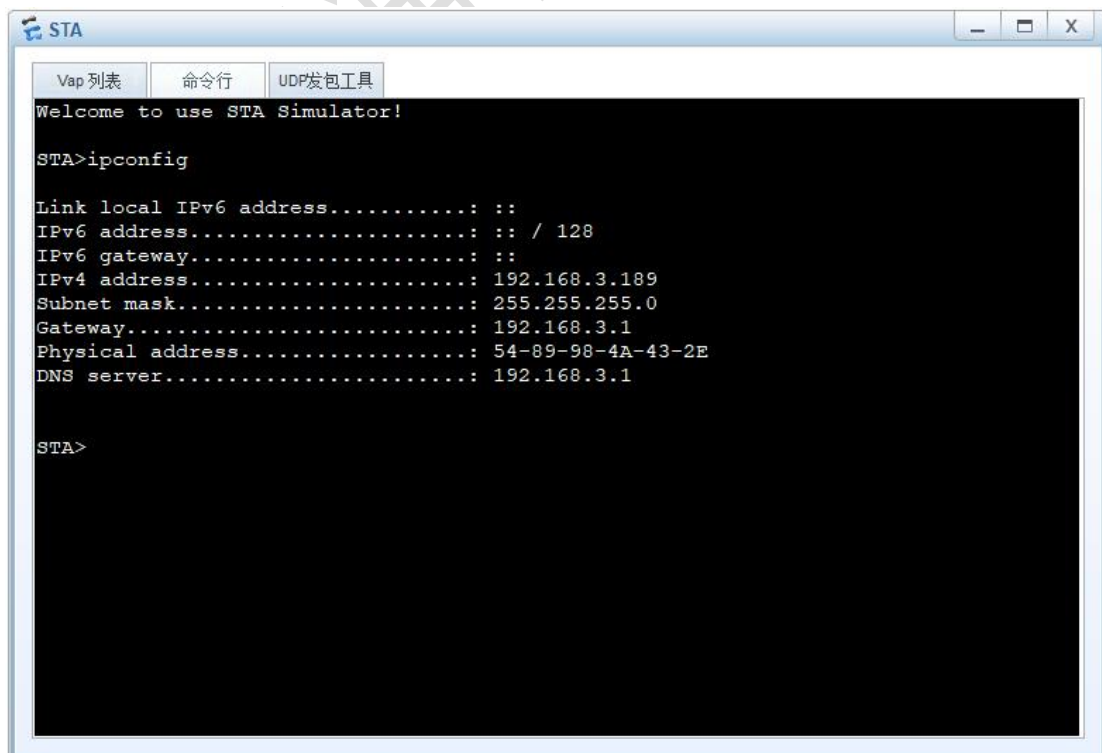
之后检测 STA 是否可搜索到 HuaWei-AP3030 的无线信号:



尝试与 AP 建立连接，获取 IP 地址等网络参数：



查看 STA 获取的 IP 地址：



检测 STA 是否可与 RTA (172.16.1.1)、SWA (172.16.1.2)、AC (172.16.1.3) 正常通讯:

```

STA
Vap 列表  命令行  UDP发包工具
Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.3.189
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.3.1
Physical address.....: 54-89-98-4A-43-2E
DNS server.....: 192.168.3.1

STA>ping 172.16.1.1

Ping 172.16.1.1: 32 data bytes, Press Ctrl_C to break
From 172.16.1.1: bytes=32 seq=1 ttl=255 time=110 ms
From 172.16.1.1: bytes=32 seq=2 ttl=255 time=109 ms
From 172.16.1.1: bytes=32 seq=3 ttl=255 time=110 ms
From 172.16.1.1: bytes=32 seq=4 ttl=255 time=109 ms
From 172.16.1.1: bytes=32 seq=5 ttl=255 time=109 ms

--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/109/110 ms

STA>
    
```

```

STA
Vap 列表  命令行  UDP发包工具
From 172.16.1.1: bytes=32 seq=3 ttl=255 time=110 ms
From 172.16.1.1: bytes=32 seq=4 ttl=255 time=109 ms
From 172.16.1.1: bytes=32 seq=5 ttl=255 time=109 ms

--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/109/110 ms

STA>ping 172.16.1.2

Ping 172.16.1.2: 32 data bytes, Press Ctrl_C to break
From 172.16.1.2: bytes=32 seq=1 ttl=254 time=125 ms
From 172.16.1.2: bytes=32 seq=2 ttl=254 time=109 ms
From 172.16.1.2: bytes=32 seq=3 ttl=254 time=125 ms
From 172.16.1.2: bytes=32 seq=4 ttl=254 time=125 ms
From 172.16.1.2: bytes=32 seq=5 ttl=254 time=125 ms

--- 172.16.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/121/125 ms

STA>
    
```

```

STA
Vap 列表  命令行  UDP发包工具
From 172.16.1.2: bytes=32 seq=3 ttl=254 time=125 ms
From 172.16.1.2: bytes=32 seq=4 ttl=254 time=125 ms
From 172.16.1.2: bytes=32 seq=5 ttl=254 time=125 ms

--- 172.16.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/121/125 ms

STA>ping 172.16.1.3

Ping 172.16.1.3: 32 data bytes, Press Ctrl_C to break
From 172.16.1.3: bytes=32 seq=1 ttl=255 time=109 ms
From 172.16.1.3: bytes=32 seq=2 ttl=255 time=110 ms
From 172.16.1.3: bytes=32 seq=3 ttl=255 time=109 ms
From 172.16.1.3: bytes=32 seq=4 ttl=255 time=110 ms
From 172.16.1.3: bytes=32 seq=5 ttl=255 time=109 ms

--- 172.16.1.3 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/109/110 ms

STA>
    
```

检测 STA 与 Client A 的连通性:

```

STA
Vap 列表  命令行  UDP发包工具
From 172.16.1.3: bytes=32 seq=3 ttl=255 time=109 ms
From 172.16.1.3: bytes=32 seq=4 ttl=255 time=110 ms
From 172.16.1.3: bytes=32 seq=5 ttl=255 time=109 ms

--- 172.16.1.3 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 109/109/110 ms

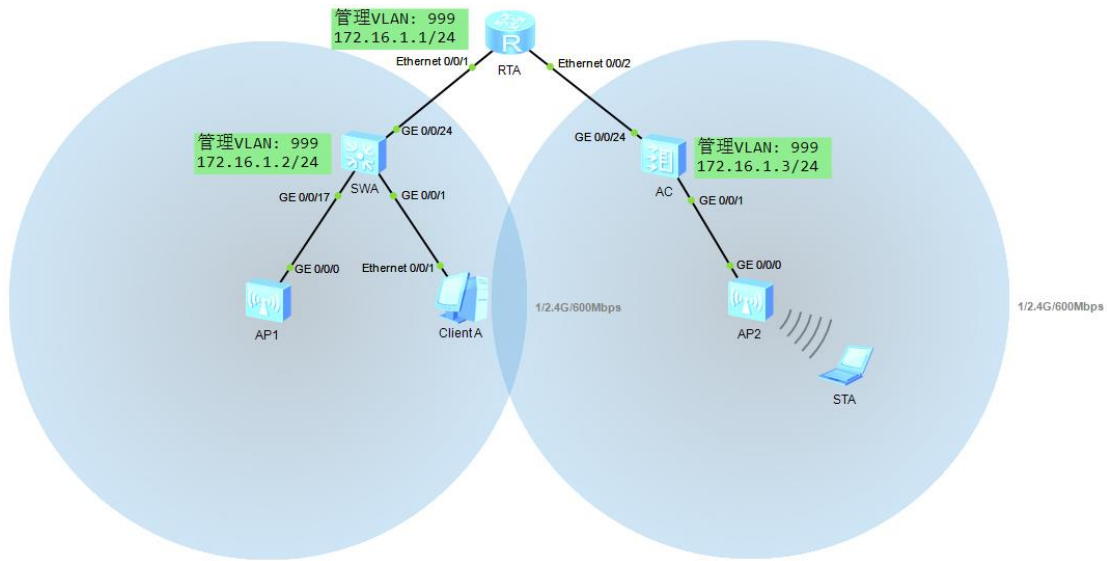
STA>ping 192.168.1.81

Ping 192.168.1.81: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.1.81: bytes=32 seq=2 ttl=127 time=141 ms
From 192.168.1.81: bytes=32 seq=3 ttl=127 time=141 ms
From 192.168.1.81: bytes=32 seq=4 ttl=127 time=141 ms
From 192.168.1.81: bytes=32 seq=5 ttl=127 time=156 ms

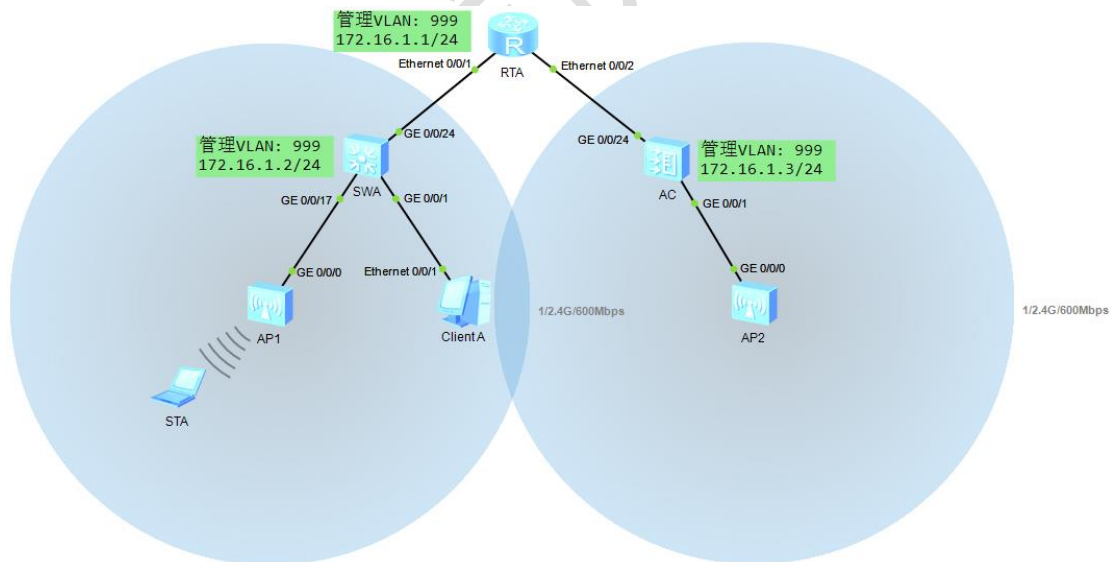
--- 192.168.1.81 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/144/156 ms

STA>
    
```

如下图所示，STA 可正常与 AP2 建立连接并访问网络：

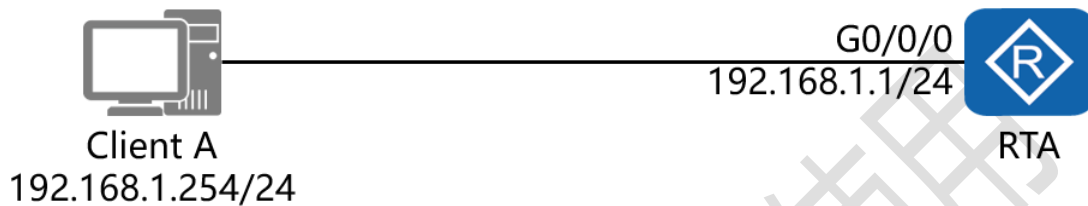


当 STA 进入 AP1 的无线信号覆盖范围内时，可自动与 AP1 建立连接：



三十六、使用 Python 的 Telnetlib 登录设备实验组网

一、实验拓扑：



二、实验目的：

令 Client A 实现使用 Python 的 Telnetlib 登录对端路由器

三、实验步骤：

RTA:

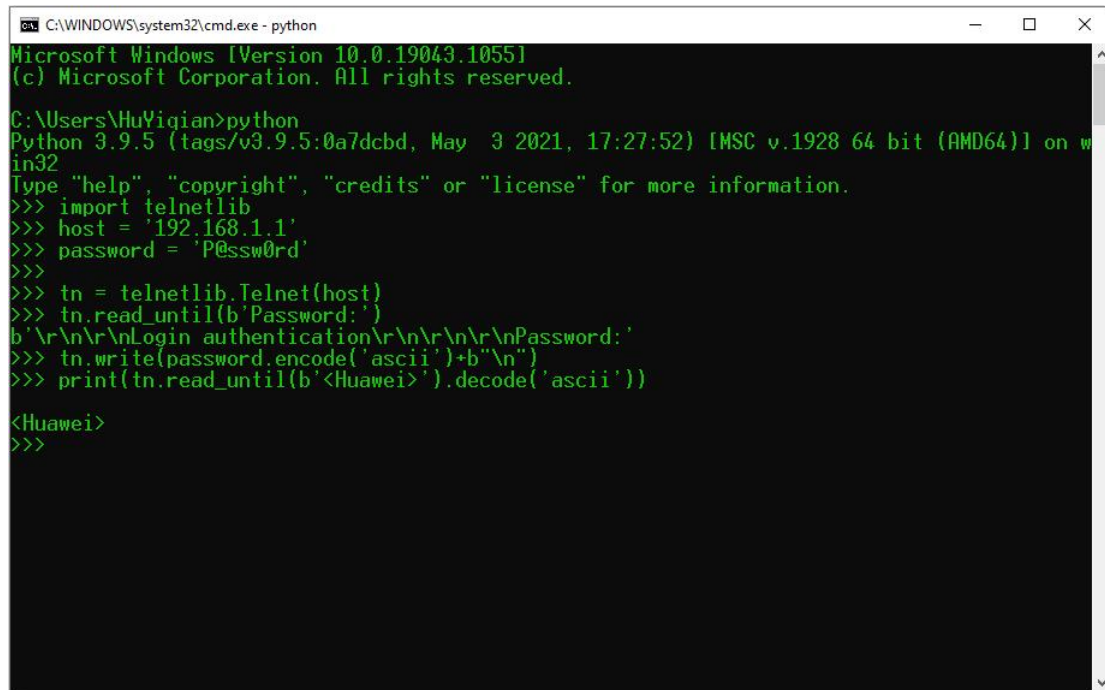
```

system-view          #进入系统视图模式
interface G0/0/0     #进入相应接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
user-interface vty 0 4      #进入 Telnet 的配置模式
authentication-mode password #指定认证方式为密钥验证
set authentication password cipher P@ssw0rd
#配置认证时使用的密钥及加密方式
protocol inbound telnet    #指定使用的远程登录协议为 Telnet
    
```

user privilege level 15 #指定登录后用户的级别

telnet server enable #开启 Telnet 功能

Client A:



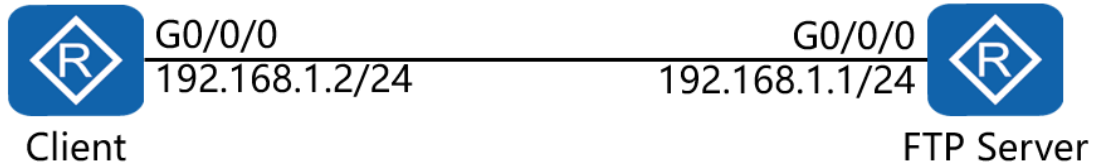
```
C:\WINDOWS\system32\cmd.exe - python
Microsoft Windows [Version 10.0.19043.1055]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HuYiqian>python
Python 3.9.5 (tags/v3.9.5:0a7dcdb, May  3 2021, 17:27:52) [MSC v.1928 64 bit (AMD64)] on w
in32
Type "help", "copyright", "credits" or "license" for more information.
>>> import telnetlib
>>> host = '192.168.1.1'
>>> password = 'P@ssw0rd'
>>>
>>> tn = telnetlib.Telnet(host)
>>> tn.read_until(b'Password:')
b'\r\n\r\nLogin authentication\r\n\r\n\r\n\r\nPassword:'
>>> tn.write(password.encode('ascii')+b"\n")
>>> print(tn.read_until(b'<Huawei>').decode('ascii'))

<Huawei>
>>>
```


三十七、配置 FTP 实验组网

一、实验拓扑：



二、实验目的：

通过在 FTP Server 上配置 FTP 服务，令 Client 可以正常访问 FTP Server 的指定目录

三、实验步骤：

FTP Server:

```

system-view          #进入系统视图模式
sysname FTP Server  #给设备命名
interface G0/0/0    #进入相应的接口
ip address 192.168.1.1 24    #配置 IP 地址及子网掩码
ftp server enable   #开启 FTP 服务
set default ftp-directory flash:/    #设置默认的 FTP 可访问
目录
aaa                 #开启 AAA 服务
local-user easthome password cipher P@ssw0rd
#创建本地用户及密钥
local-user easthome service-type ftp    #指定该用户可使
    
```

用的服务类型为 FTP

local-user *easthome* ftp-directory flash:/ #指定该用户通过 FTP 访问时可访问的目录

local-user *easthome* access-limit 200 #指定该用户可建立的最大连接数目

local-user *easthome* idle-timeout 0 0 #指定该用户的登录超时时间

local-user *easthome* privilege level 15 #指定该用户登录后的授权级别

Client:

system-view

sysname Client

interface G0/0/0

ip address 192.168.1.2 24

Client 测试:

<Client> ftp 192.168.1.1

Trying 192.168.1.1 ...

Press CTRL+K to abort

Connected to 192.168.1.1.

220 FTP service ready.

User(192.168.1.1:(none)):*easthome*

331 Password required for easthome.

Enter password:*P@ssw0rd*

230 User logged in.

[Client-ftp] *binary* #当网络设备作为 FTP 客户端时，设置文件传输方式为 Binary 模式（二进制模式）

200 Type set to I.

[Client-ftp]