1 系统管理典型配置案例

关于本章

1.1 配置用户登录
用户可以通过 Console 口、Telnet、Web、SSH（Secure Shell，即安全外壳）方式进行登录。

1.2 配置文件管理
USG 文件系统的主要功能是管理存储设备，把文件保存在存储设备中。USG 目前支持的存储设备为 Flash。

1.3 配置信息中心
信息中心是 USG 主机软件中不可缺少的一部分，它作为 USG 的信息枢纽而存在。信息中心接管大多数的信息输出，并对信息进行有效的、细致的分类筛选。

1.4 配置 NTP
NTP 属于应用层协议（基于 UDP 传输，使用的端口号为 123），用来同步网络中分布式时间服务器和客户端之间的时间，使网络中的设备提供基于统一时间的应用成为可能。

1.5 配置网管软件
目前，计算机网络中用得最广泛的网络管理协议是简单网络管理协议 SNMP（Simple Network Management Protocol），它是被广泛接受并投入使用的工业标准。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

1.1 配置用户登录

用户可以通过 Console 口、Telnet、Web、SSH（Secure Shell，即安全外壳）方式进行登录。

1.1.1 配置通过 Console 口登录举例
USG 在任何情况下都能通过 Console 口搭建配置环境。

1.1.2 配置通过 Telnet 登录举例
用户可以通过 PC 等配置终端登录到其它网段上的 USG，进行远程维护。

1.1.3 配置通过 Web 登录举例
设备为用户提供了简单、易用的 Web 配置界面，使用户能够方便地对 USG 进行操作和维护。

1.1.4 配置 SSH 终端服务密码验证方式举例
SSH 是 Secure Shell（安全外壳）的简称。SSH 是一套标准的网络协议，具有强大的安全保障作用，能够在不安全的网络上建立安全通道。当对用户登录的安全性要求较高时，用户则需要通过 SSH 方式登录到 USG，对 USG 进行管理。

1.1.5 配置 SSH 终端服务 RSA 验证方式举例
当用户通过一个不能保证安全的网络远程登录到 USG 时，为更大限度地保证数据信息交换的安全性，采用 RSA 认证方式，使用 SSH 来实现此目的。

1.1.1 配置通过 Console 口登录举例

USG 在任何情况下都能通过 Console 口搭建配置环境。

组网需求

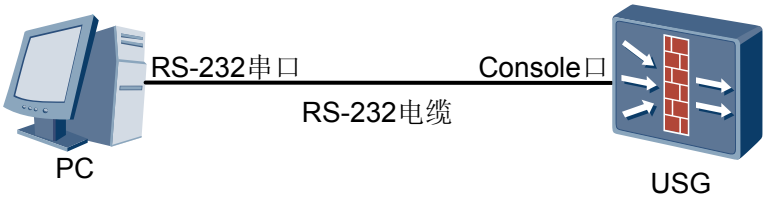
以下情况时只能通过 Console 口搭建配置环境：

- USG 第一次上电，需要通过串口对 USG 进行初始的配置。
- 无法通过 Telnet 或 SSH 方式搭建配置环境。

通过 Console 口搭建配置环境的连接如**图 1-1** 所示，PC（Personal Computer）终端的串口和 USG 的 Console 口通过标准 RS-232 电缆连接。

缺省情况下，USG 通过 Console 口登录时的认证方式为 AAA（Authorization，Authentication and Accounting），用户名为**admin**，口令为**Admin@123**。

图 1-1 通过 Console 口搭建配置环境



火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

配置思路

1. 通过 Console 口连接 PC 和 USG。
2. 在 PC 端进行登录的设置。
3. 登录 USG。

操作步骤

步骤 1 按照图 1-1 建立本地配置环境。

步骤 2 将所有设备上电，并且保证设备运行正常。

步骤 3 在 PC 上运行终端仿真程序（以 Windows XP 的超级终端为例），选择“开始 > 程序 > 附件 > 通讯 > 超级终端”，显示“连接描述”对话框。

步骤 4 在“名称”中输入 PC 与 USG 的连接名称，例如**COMM1**；并在“图标”中选择任一图标，如图 1-2 所示。

图 1-2 “连接描述”对话框（通过 Console 口登录）

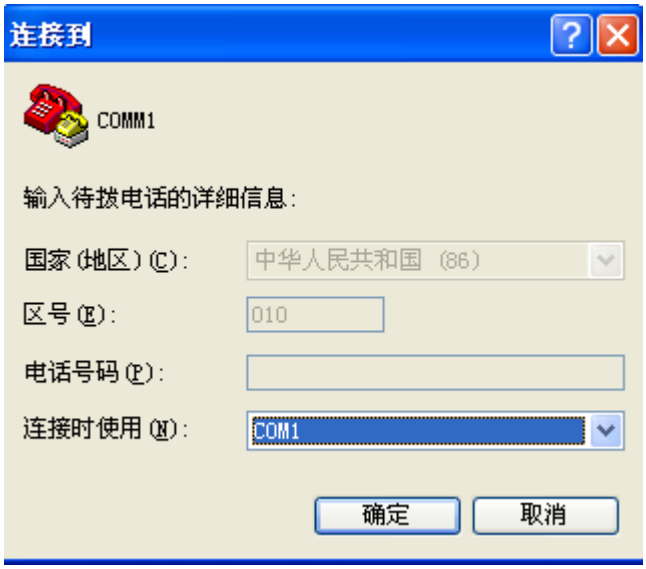
步骤 5 单击“确定”，显示“连接到”对话框。

步骤 6 在“连接时使用”中选择 PC 与 USG 连接时使用的串口，例如**COM1**，如图 1-3 所示。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-3 “连接到”对话框（通过 Console 口登录）



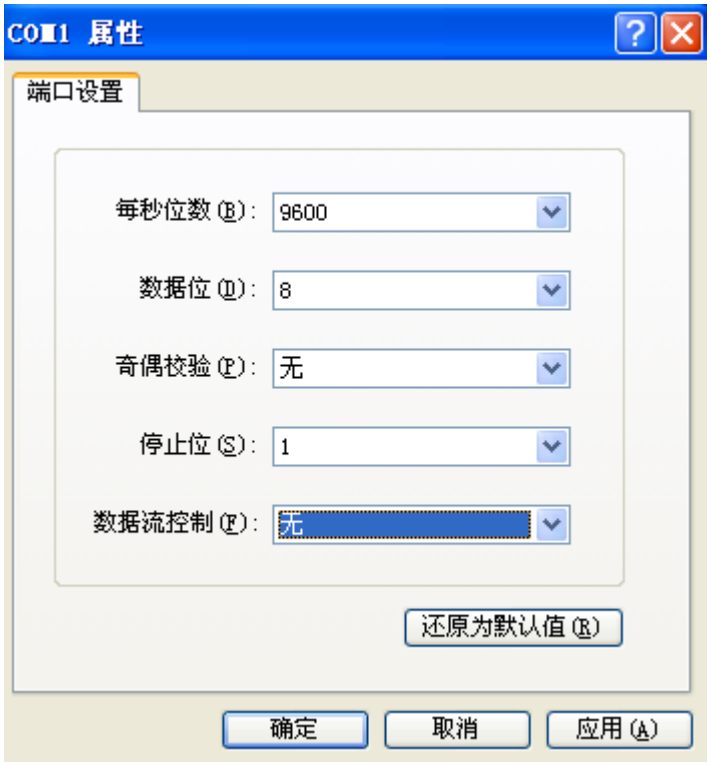
步骤 7 单击“确定”，显示“COM1 属性”对话框。

步骤 8 设置端口的通信参数，如图 1-4 所示。

说明

终端端口的通信参数必须和 USG Console 口的配置保持一致。

图 1-4 设置端口属性（通过 Console 口登录）



步骤 9 单击“确定”，完成配置。

----结束

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

结果验证

在 PC 仿真终端上，单击“Enter”，通过 USG 配置的认证方式后，即可进入用户视图，具体如下：

- 如果 USG 的认证方式为 AAA，输入正确的用户名和口令后，在终端上显示命令行提示符<USG>。
- 如果 USG 的认证方式为 Local，输入正确的用户名和口令后，在终端上显示命令行提示符<USG>。
- 如果 USG 的认证方式为 Password，输入正确的口令后，在终端上显示命令行提示符<USG>。
- 如果 USG 的认证方式为 None，则在终端上直接显示命令提示符<USG>。

1.1.2 配置通过 Telnet 登录举例

用户可以通过 PC 等配置终端登录到其它网段上的 USG，进行远程维护。

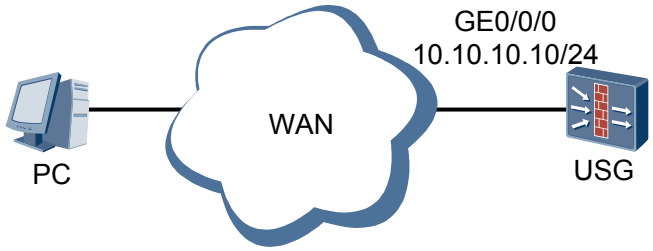
组网需求

如图 1-5 所示，USG 以太网接口 GigabitEthernet 0/0/0 的 IP 地址为 10.10.10.10/24。

只允许 192.168.1.0/24 网段的用户通过 Telnet 登录到 USG。

登录的用户名为 user1，密码为 password1，级别为 level3。

图 1-5 配置通过 Telnet 登录组网图



配置思路

1. 建立物理连接。
2. 配置用户登录参数。
3. 从客户端 Telnet 登录 USG。

操作步骤

步骤 1 按照图 1-5 建立物理连接，保证终端 PC 和 USG 路由可达。具体步骤略。

步骤 2 配置登录用户参数。

进入系统视图。

```
<USG> system-view
```

配置登录地址。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 10.10.10.10 24
[USG-GigabitEthernet0/0/0] quit
```

配置以太网接口 GigabitEthernet 0/0/0 加入 trust 安全区域。

```
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet 0/0/0
[USG-zone-trust] quit
```

配置域间包过滤规则。

```
[USG] firewall packet-filter default permit interzone local trust
```

配置 ACL 2000。

```
[USG] acl 2000
[USG-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[USG-acl-basic-2000] quit
```

进入用户界面视图。

```
[USG] user-interface vty 0 4
```

配置 AAA 认证方式。

```
[USG-ui-vty0-4] authentication-mode aaa
```

配置 VTY0 到 VTY4 的用户界面仅支持 Telnet 协议。

```
[USG-ui-vty0-4] protocol inbound telnet
[USG-ui-vty0-4] quit
```

配置只允许 192.168.1.0/24 网段的用户登录 USG。

```
[USG-ui-vty0-4] acl 2000 inbound
[USG-ui-vty0-4] quit
```

进入 AAA 视图。

```
[USG] aaa
```

添加一个用户 user1，验证口令为 password1，口令的存储方式为密文方式（cipher）。

```
[USG-aaa] local-user user1 password cipher password1
```

配置本地用户的服务类型为 Telnet。

```
[USG-aaa] local-user user1 service-type telnet
```

配置本地用户的优先级为 level 3。

```
[USG-aaa] local-user user1 level 3
```

----结束

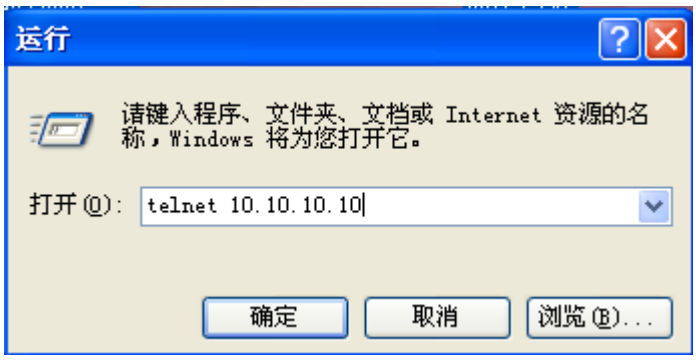
结果验证

1. （以 Windows 系统为例）在 192.168.1.0/24 网段的 PC 上选择“开始＞运行”，显示“运行”窗口，在“打开”中输入**telnet 10.10.10.10** 10.10.10.10 为例），如图 **1-6** 所示。

火龙果 - 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-6 运行 telnet



2. 单击“确定”，开始连接 USG。
3. 通过 USG 配置的认证方式后，即可进入用户视图，具体如下：
   - 如果 USG 的认证方式为 AAA，输入正确的用户名和口令后，在终端上显示命令行提示符<USG>。
   - 如果 USG 的认证方式为 Password，输入正确的口令后，在终端上显示命令行提示符<USG>。
   - 如果 USG 的认证方式为 None，则在终端上直接显示命令提示符<USG>。

配置脚本

USG 配置脚本：

```
#
 sysname USG
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 10.10.10.10 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
aaa
 local-user user1 password cipher password1
 local-user user1 service-type telnet
 local-user user1 level 3
#
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode aaa
 protocol inbound telnet
#
return
```

1.1.3 配置通过 Web 登录举例

设备为用户提供了简单、易用的 Web 配置界面，使用户能
维护。

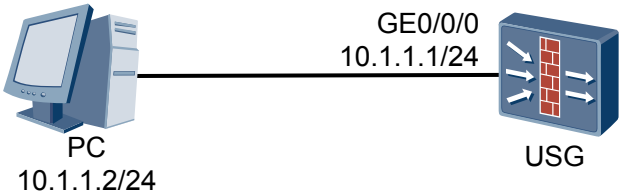
火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

组网需求

如图 1-7 所示，客户端与 USG 的以太网接口 GigabitEthernet 0/0/0 相连，用户可以在客户端通过 Web 浏览器访问 USG 的接口地址 10.1.1.1，进而控制和管理 USG。

图 1-7 Web 管理组网图



配置思路

1. 配置 Web 用户。
2. 开启 Web 管理功能。

操作步骤

步骤 1 配置 USG 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将该接口加入安全区域，并配置域间包过滤规则。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 10.1.1.1 24
[USG-GigabitEthernet0/0/0] quit
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet 0/0/0
[USG] firewall packet-filter default permit interzone local trust
```

步骤 2 配置 Web 用户。

```
[USG] aaa
[USG-aaa] local-user webuser password simple web12345
[USG-aaa] local-user webuser service-type web
[USG-aaa] local-user webuser level 3
```

步骤 3 开启 Web 管理功能。

```
[USG] web-manager enable
```

----结束

结果验证

1. 在 PC 端的 Web 浏览器中输入 http://10.1.1.1，出现管理登录页面。登录页面如图 1-8 所示。

图 1-8 Web 管理登录页面

2. 输入用户名 webuser 和密码 web12345，单击“提交”。如果能够进入 Web 管理系统则表示配置成功。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

配置脚本

USG 的配置脚本：

```
#
 sysname USG
#
 web-manager enable      // 开启Web管理功能
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
aaa
 local-user webuser password simple web12345
 local-user webuser service-type web
 local-user webuser level 3
#
return
```

1.1.4 配置 SSH 终端服务密码验证方式举例

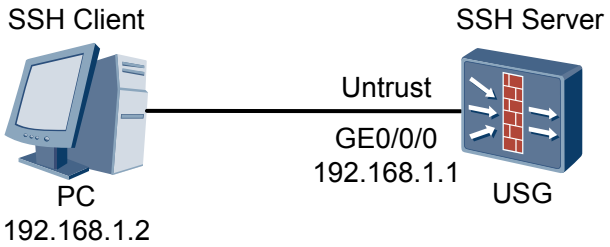
SSH 是 Secure Shell（安全外壳）的简称。SSH 是一套标准的网络协议，具有强大的安全保障作用，能够在不安全的网络上建立安全通道。当对用户登录的安全性要求较高时，用户则需要通过 SSH 方式登录到 USG，对 USG 进行管理。

组网需求

如图 1-9 所示，配置终端（SSH Client）与 USG（SSH Server）建立本地连接，终端上运行支持 SSH1.5 的客户端软件。

用户 sshuser 采用密码认证方式登录。密码为 password1，以明文形式显示。

图 1-9 SSH 密码验证方式组网图



配置思路

1. 配置 USG 以太网接口的 IP 地址，将接口加入安全区域，并配置域间包过滤，允许 SSH Client 访问 SSH Server。
2. 生成本地密钥对。
3. 创建 SSH 用户。
4. 在终端上运行支持 SSH1.5 的客户端软件，访问 USG

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

操作步骤

步骤 1 配置 USG 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将接口加入 Untrust 域，并配置 Untrust 与 Local 域间包过滤，允许 SSH Client 访问 SSH Server。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet 0/0/0] ip address 192.168.1.1 24
[USG-GigabitEthernet 0/0/0] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 0/0/0
[USG-zone-untrust] quit
[USG] acl 3001
[USG-acl-adv-3001] rule permit ip source 192.168.1.2 0
[USG-acl-adv-3001] quit
[USG] firewall interzone local untrust
[USG-local-untrust] packet-filter 3001 inbound
[USG-local-untrust] quit
```

步骤 2 生成本地密钥对

说明

如果此前已完成生成本地密钥对的配置，可以略过此项操作。

```
<USG> system-view
[USG] rsa local-key-pair create
The key name will be: USG_Host
Confirm to replace them? [yes/no]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.......................++++++++++++
.....++++++++++++
...............++++++++
....++++++++
```

步骤 3 创建 SSH 用户。

说明

如果 SSH 用户的认证方式为 password，必须配置同名的 local-user 用户。

配置 VTY 用户界面。

```
[USG] user-interface vty 0 4
[USG-ui-vty0-4] authentication-mode aaa
[USG-ui-vty0-4] protocol inbound ssh
[USG-ui-vty0-4] quit
```

新建用户名为 sshuser 的 SSH 用户，且认证方式为 password。

```
[USG] ssh user sshuser authentication-type password
```

为 SSH 用户 sshuser 配置密码为 password1。

```
[USG] aaa
[USG-aaa] local-user sshuser password simple password1
[USG-aaa] local-user sshuser service-type ssh
```

说明

SSH 的验证超时时间、重试次数以及服务器密钥更新时间可以采取系统默认值。这些配置完成以后，您就可以在其它与 USG 连接的终端上，运行支持 SSH1.5 密码 password1，访问 USG 了。

火龙果 · 整理
uml.org.cn

步骤 4 配置 SSH Client。

版权所有 © 成都市华为赛门铁克科技有限公司

配置 Client 主机 IP 地址与 USG 接口 GigabitEthernet 0/0/0 的 IP 地址在同一网段，这里设置为 192.168.1.2。

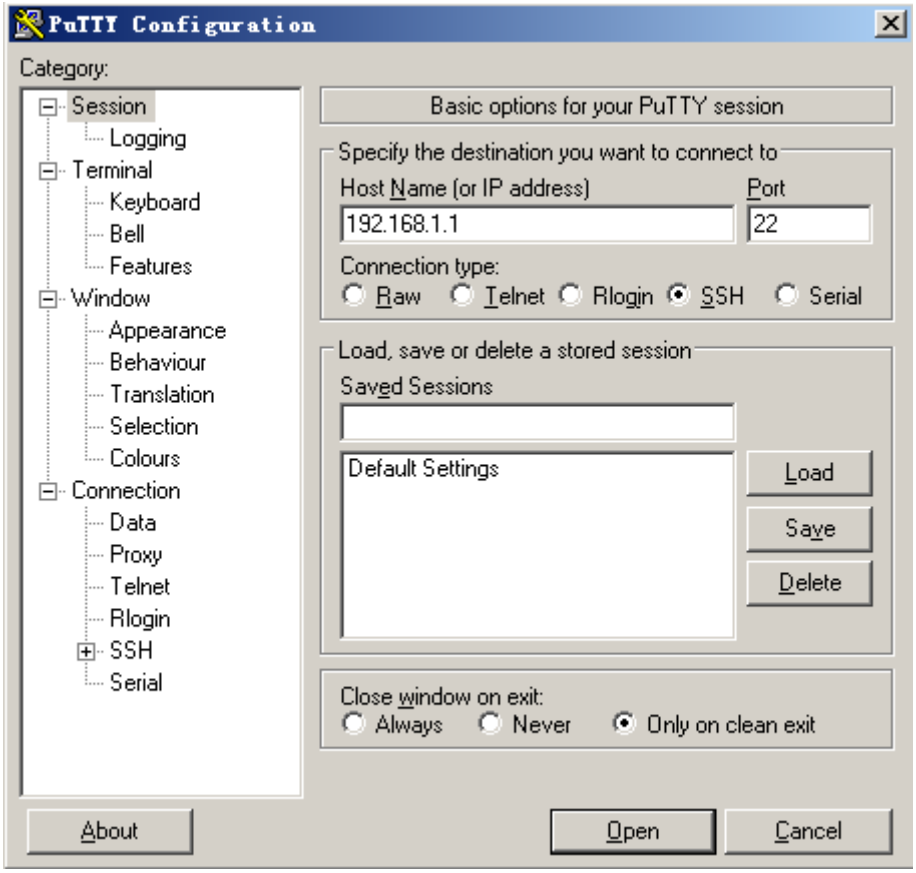
建立与 SSH Server 的连接。（下文中以 PuTTY0.60 为例。）

说明

客户端软件不同，具体配置步骤和界面可能与下述有所不同。

1. 打开 Putty.exe 程序，出现如图 1-10 所示客户端配置界面。在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址。

图 1-10 SSH 客户端配置界面

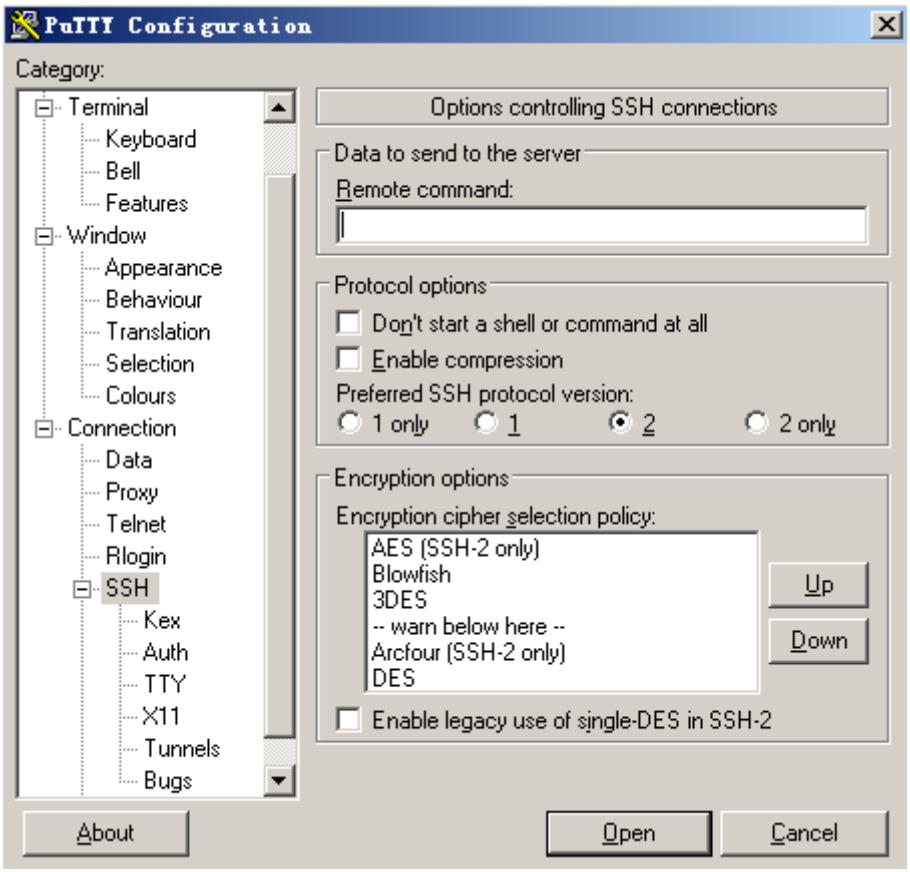


2. 单击 SSH 客户端配置界面左侧目录树（“Category”）中的连接协议（“Connection”）中的“SSH”，出现如图 1-11 界面。在“Protocol options”区域中，选择“Preferred SSH protocol version”参数的值为 2。

火龙果 · 整理
uml.org.cn

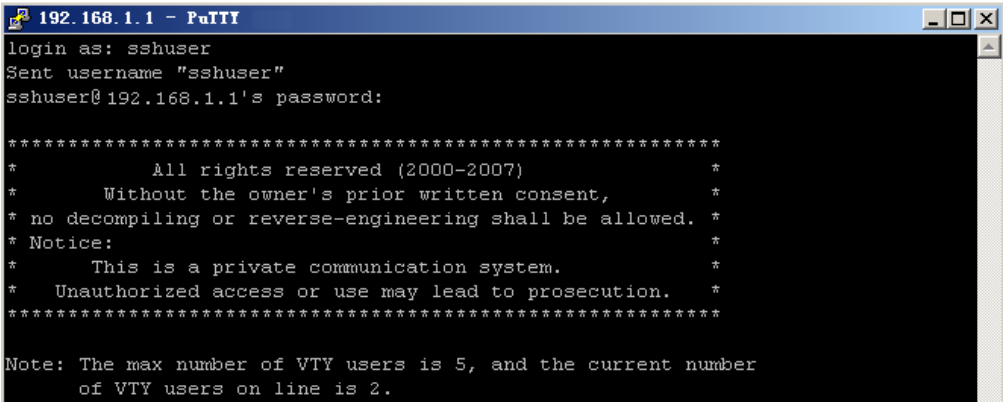
版权所有 © 成都市华为赛门铁克科技有限公司

图 1-11 SSH 客户端配置界面（2）



3. 在图 1-11 中，单击“Open”。如果连接正常则会提示用户输入用户名 sshuser，密码 Password1。如图 1-12 所示，认证成功后，即可登录到服务器端。

图 1-12 SSH 客户端认证成功登录界面



----结束

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

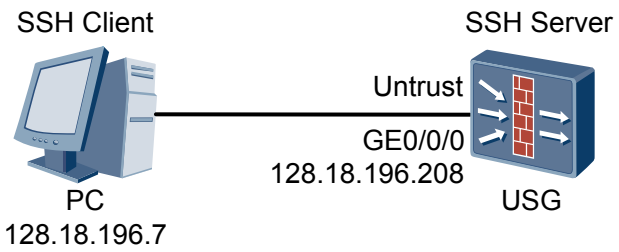
1.1.5 配置 SSH 终端服务 RSA 验证方式举例

当用户通过一个不能保证安全的网络远程登录到 USG 时，为更大限度地保证数据信息交换的安全性，采用 RSA 认证方式，使用 SSH 来实现此目的。

组网需求

如图 1-13 所示，PC 终端（SSH Client）上运行支持 SSH1.5 的客户端软件，与 USG（SSH Server）建立本地连接。

图 1-13 配置 SSH 终端服务组网图



配置思路

1. 配置 USG 以太网接口的 IP 地址，将接口加入安全区域，并配置域间包过滤，允许 SSH Client 访问 SSH Server。
2. 生成本地密钥对。
3. 创建用户，并设置登录验证方式为 RSA。
4. 配置 RSA 公共密钥。
5. 配置 SSH Client。

操作步骤

步骤 1 配置 USG 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将接口加入 Untrust 域，并配置 Untrust 与 Local 域间包过滤，允许 SSH Client 访问 SSH Server。

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet 0/0/0] ip address 128.18.196.208 24
[USG-GigabitEthernet 0/0/0] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet 0/0/0
[USG-zone-untrust] quit
[USG] acl 3001
[USG-acl-adv-3001] rule permit ip source 128.18.196.7 0
[USG-acl-adv-3001] quit
[USG] firewall interzone local untrust
[USG-local-untrust] packet-filter 3001 inbound
[USG-local-untrust] quit
```

步骤 2 生成本地密钥对。

说明

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，务必完成 **rsa local-key-pair create** 配置，生成本地密钥对后不必再次执行。

火龙果 · 整理
uml.org.cn

```
<USG> system-view
[USG] rsa local-key-pair create
```


版权所有 © 成都市华为赛门铁克科技有限公司

```
The key name will be: USG_Host
Confirm to replace them? [yes/no]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
.......................++++++++++++
.....++++++++++++
...............++++++++
....++++++++
```

步骤 3 配置用户 sshuser，并设置其登录验证方式为 RSA。

配置用户界面的认证模式为 AAA，并且仅支持 SSH 协议。

```
[USG] user-interface vty 0 4
[USG-ui-vty0-4] authentication-mode aaa
[USG-ui-vty0-4] protocol inbound ssh
[USG-ui-vty0-4] quit
```

创建 AAA 用户 sshuser，设置密码为 Password2、登录协议为 SSH、用户级别为 3。

```
[USG] aaa
[USG-aaa] local-user sshuser password simple Password2
[USG-aaa] local-user sshuser service-type ssh
[USG-aaa] local-user sshuser level 3
[USG-aaa] quit
```

指定用户 sshuser 的登录验证方式为 RSA。

```
[USG] ssh user sshuser authentication-type rsa
```

步骤 4 配置 RSA 公共密钥。

配置公共密钥前需要在 SSH 客户端使用 SSH 客户端软件（下文中以 PuTTYGen.exe 为例进行说明）生成 RSA 密钥对，请参见如下**步骤 4.1**-**步骤 4.4**。

说明

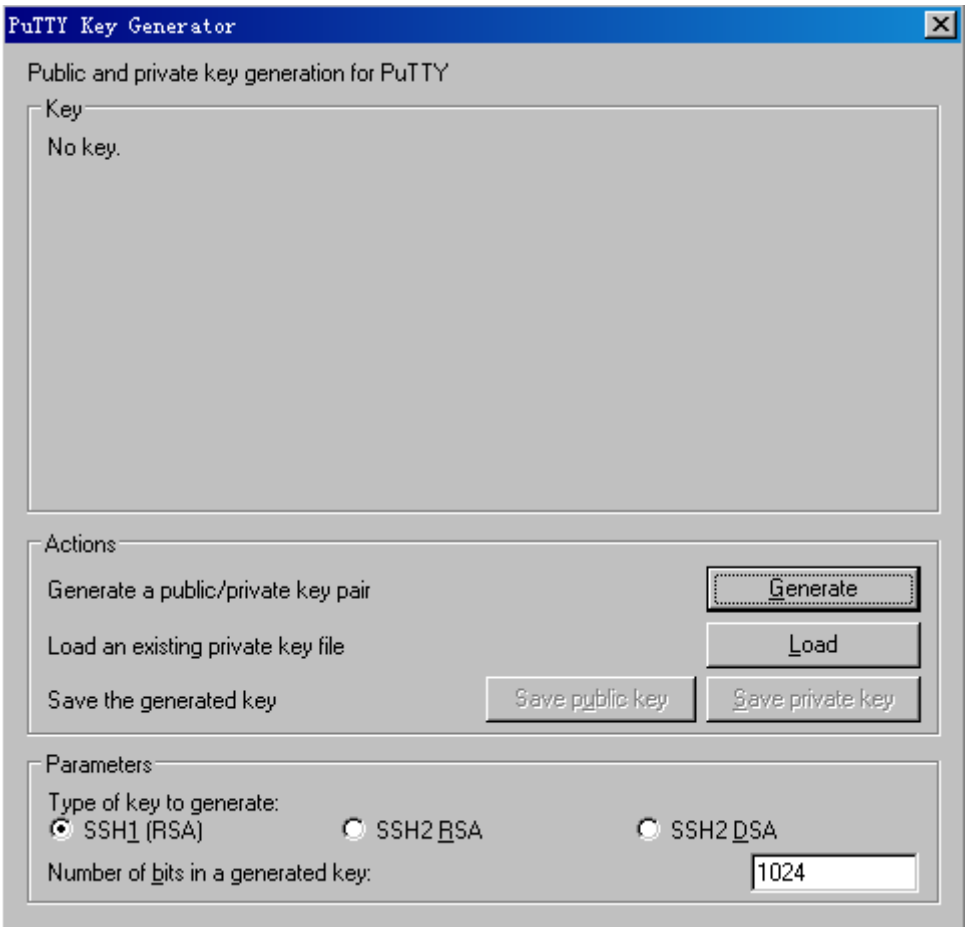
客户端软件不同，具体配置步骤和界面可能与下述有所不同。

1. 在 SSH 客户端 PC 上运行 PuTTYGen.exe，选择要生成的密钥对。单击“Generate”，产生密钥对。参数配置如**图 1-14** 所示。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-14 生成客户端密钥对

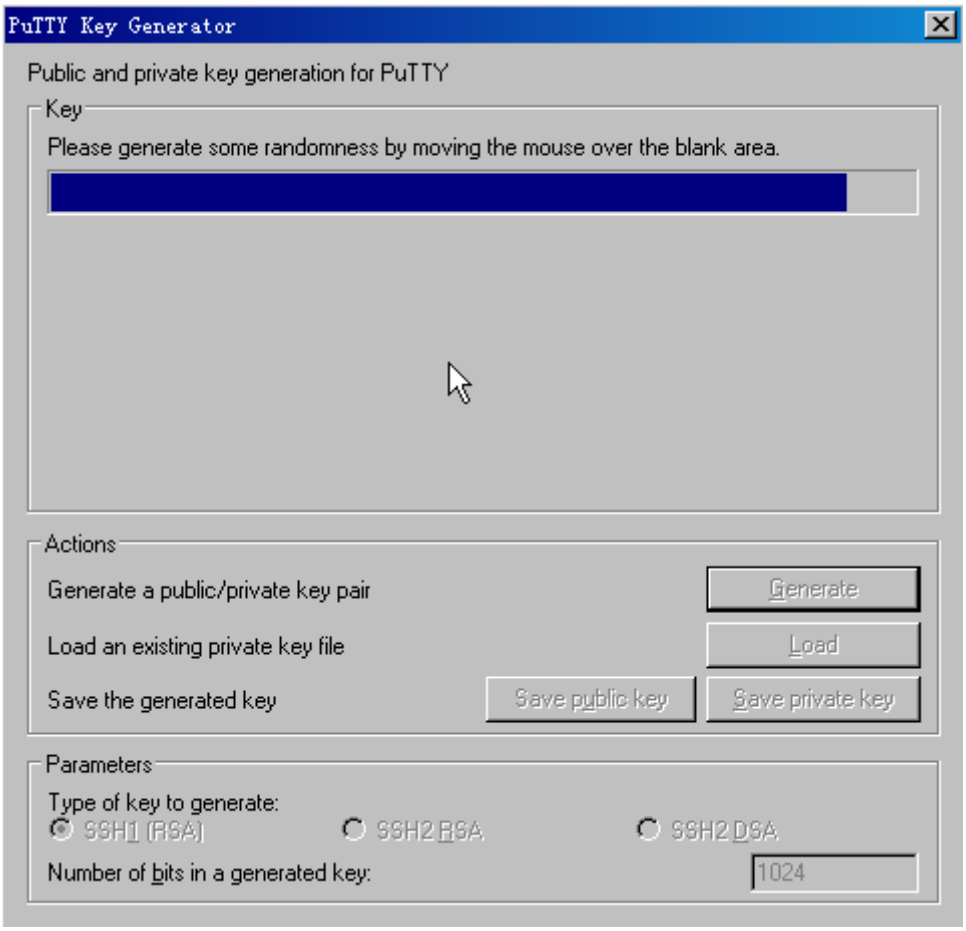


2. 在产生密钥对的过程中需不停的移动鼠标，鼠标移动仅限于窗口中除蓝色标记进程条外的地方。否则进程条的显示会不动，密钥对将停止产生，如图 **1-15** 所示。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-15 生成客户端密钥对（2）

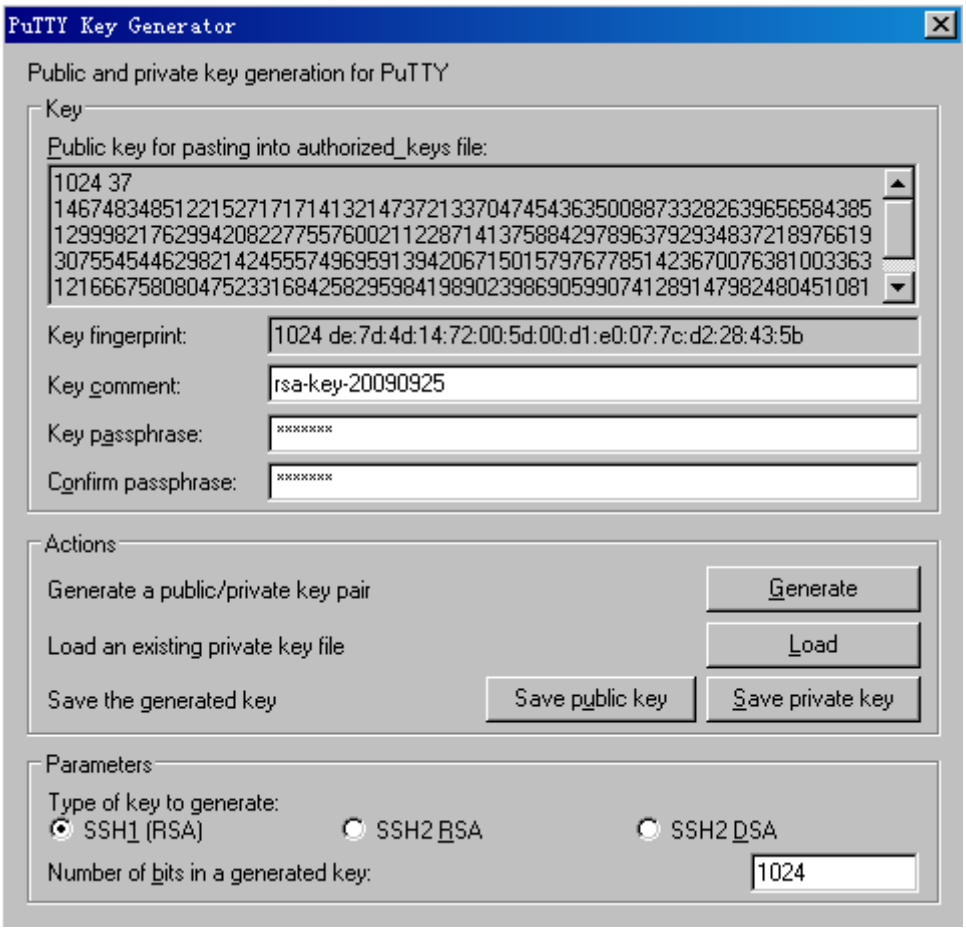


3. 密钥对产生后，在“Key passphrase”文本框中输入密码，并在“Confirm passphrase”文本框中再次输入该密码，作为 SSH 终端用户登录 USG 的密码。单击“Save public key”，输入存储公钥的文件名 public，单击“保存”。单击“Save private key”，输入存储私钥的文件名 private，单击保存。如图 **1-16** 所示。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-16 生成客户端密钥对（3）



4. 上述生成的为 SSH 格式的密钥对，需转换成 RSA 密钥。使用 ssh key convert.exe 工具，将保存的 public 文件导入，单击“转换”，将 SSH 格式的密钥对转换成 RSA 密钥。如图 **1-17** 所示。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-17 转换成 RSA 密钥

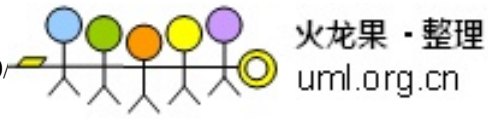
在 USG 上继续操作，进入公共密钥编辑视图，将在客户端上产生的 RSA 公共密钥拷贝到 USG 上。

```
[USG] rsa peer-public-key public
Enter "RSA public key" view, return system view with "peer-public-key end"
[USG-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[USG-rsa-key-code]30818602 8180D0FA 01796464 FC499055 A929BAEE 3E446115
[USG-rsa-key-code]32CB4D60 C7BE63E9 7A529060 D40F0CE8 C12A1757 4BED9756
[USG-rsa-key-code]FD966BA7 152A7F13 DC9204BE 525850E9 34786797 0B77A1F4
[USG-rsa-key-code]9A7DDFE4 27CCADD6 02164F52 186EB477 F5BBEA10 95AAD5A9
[USG-rsa-key-code]9E834A50 F2E4F4AE 27176FB2 76750192 95BB9E0A B4ED548A
[USG-rsa-key-code]662C5ABF 9CDAF349 82F82A3D 4A7D0201 25
[USG-rsa-key-code] public-key-code end
[USG-rsa-public-key] peer-public-key end
```

为用户 sshuser 分配公共密钥 public。

```
[USG] ssh user sshuser assign rsa-key public
```

步骤 5 配置 SSH Client。



配置 Client 主机 IP 地址与 USG 接口 GigabitEthernet 0/0/ 设置为 128.18.196.7。

版权所有 © 成都市华为赛门铁克科技有限公司

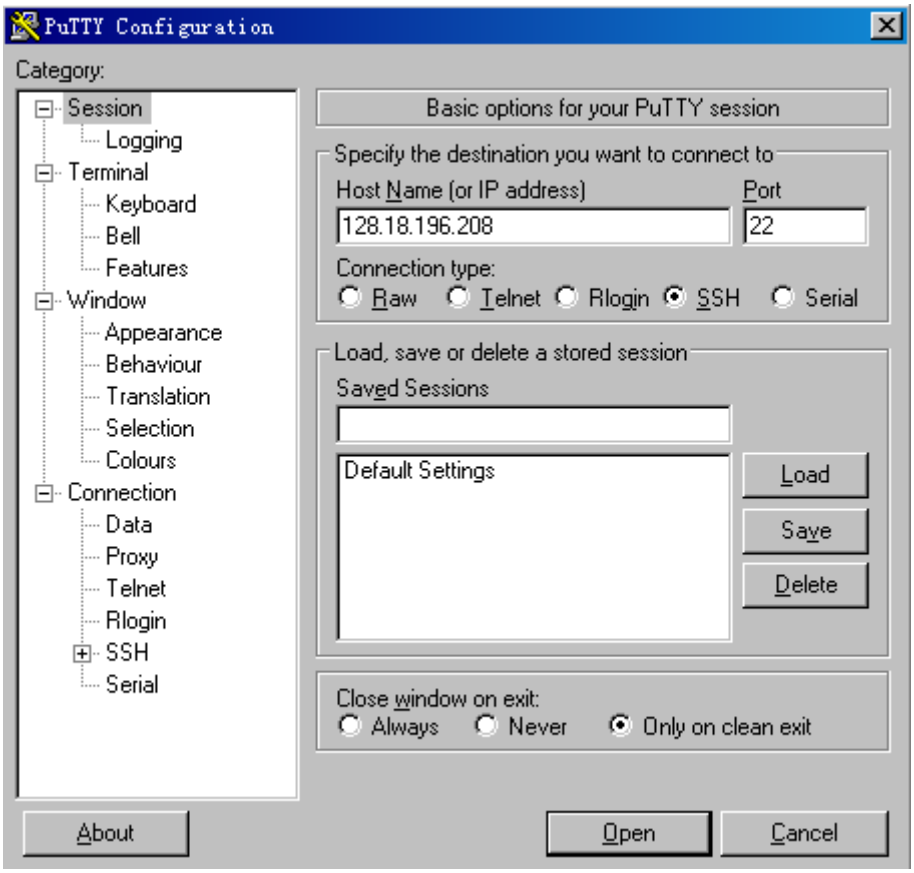
建立与 SSH Server 的连接。（下文中以 PuTTY0.60 为例。）

说明

客户端软件不同，具体配置步骤和界面可能与下述有所不同。

1. 打开 Putty.exe 程序，出现如图 1-18 所示客户端配置界面。在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址。

图 1-18 SSH 客户端配置界面

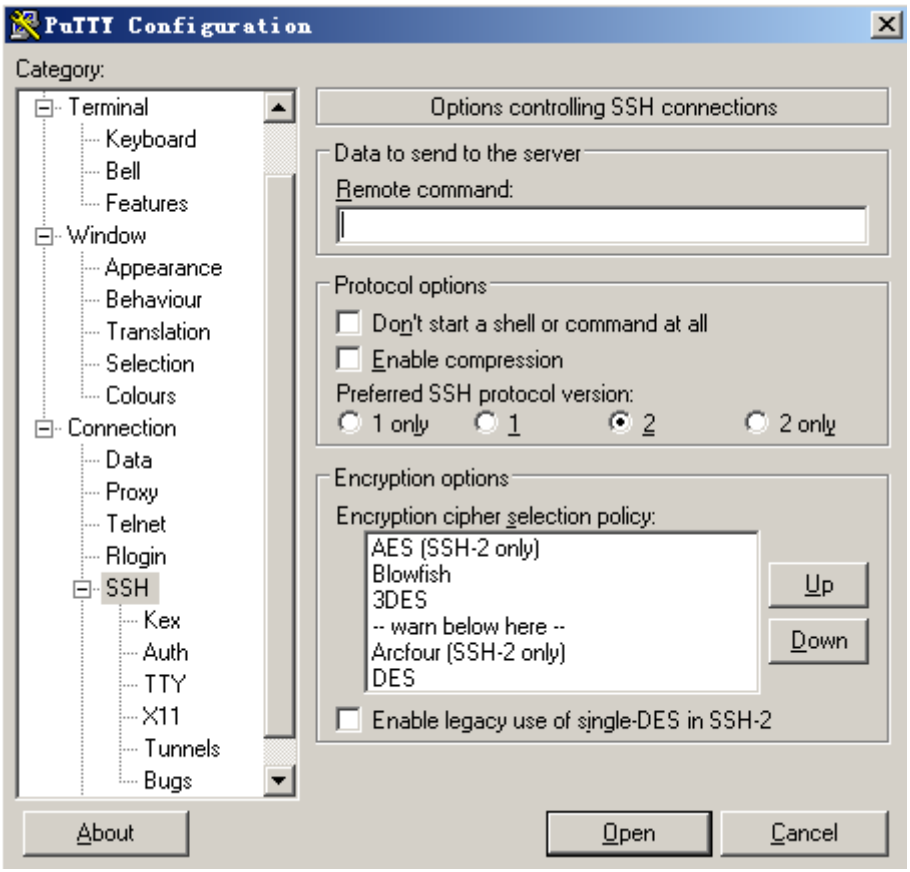


2. 选择 SSH 客户端配置界面左侧目录树（“Category”）中的连接协议（“Connection”）中的“SSH”，出现如图 1-19 界面。在“Protocol options”区域中，选择“Preferred SSH protocol version”参数的值为 2。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-19 SSH 客户端配置界面（2）

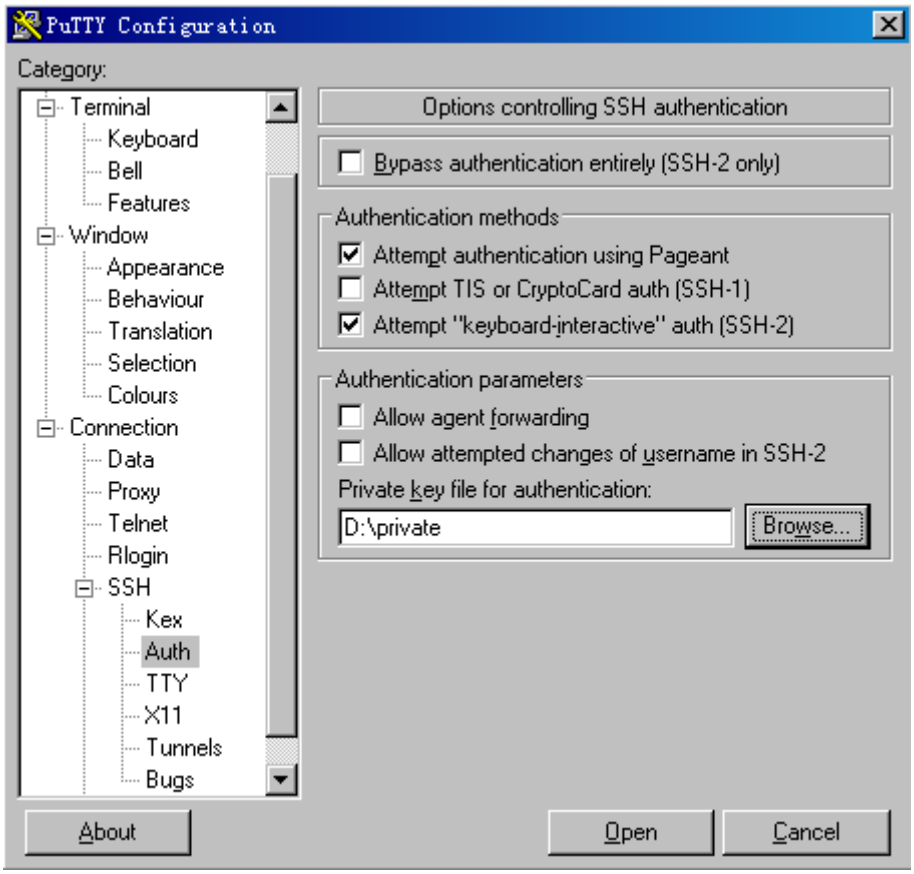


3. 继续选择“SSH”下的“Auth”，出现如图 **1-20** 所示界面。单击“Browse”，导入存储的私钥文件 private。

火龙果 · 整理
uml.org.cn

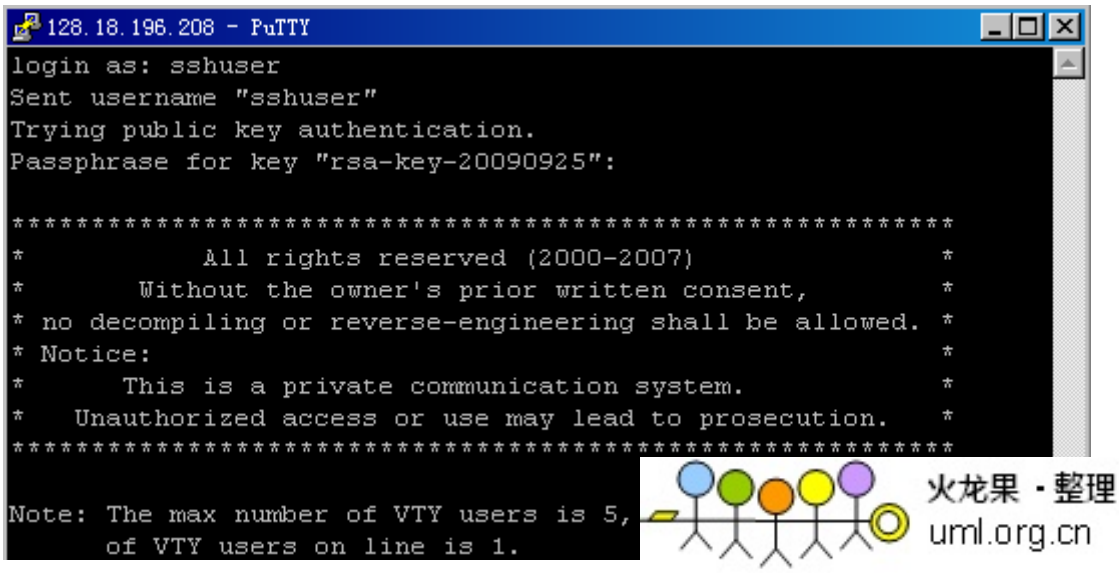
版权所有 © 成都市华为赛门铁克科技有限公司

图 1-20 SSH 客户端配置界面（3）



4. 单击“Open”。如果连接正常则会提示用户输入用户名和密码（本例中用户名为sshuser，密码为步骤 4.3 设定的密码）。如图 1-21 所示，认证成功后，即可登录到服务器端。

图 1-21 SSH 客户端认证成功登录界面



版权所有 © 成都市华为赛门铁克科技有限公司

----结束

1.2 配置文件管理

USG 文件系统的主要功能是管理存储设备，把文件保存在存储设备中。USG 目前支持的存储设备为 Flash。

1.2.1 配置文件拷贝举例
文件系统可以对 USG 存储设备中的目录进行创建、删除、修改，对文件进行拷贝、移动、删除，以及文件名更改。

1.2.2 配置 FTP 举例
FTP 协议在 TCP/IP 协议族中属于应用层协议，主要向用户提供与远程主机之间的文件传输。

1.2.3 配置 TFTP 举例
TFTP 是一种简单文件传输协议，适用于客户机和服务器之间交互不复杂的环境。

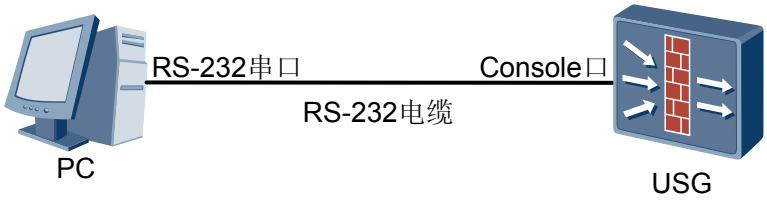
1.2.1 配置文件拷贝举例

文件系统可以对 USG 存储设备中的目录进行创建、删除、修改，对文件进行拷贝、移动、删除，以及文件名更改。

组网需求

如图 1-22 所示，用户通过 Console 口登录 USG，创建指定目录 flash:/test，拷贝 USG 中的文件到指定目录下。

图 1-22 配置文件系统组网图



配置思路

1. 创建指定目录。
2. 拷贝文件到指定目录。

操作步骤

步骤 1 创建指定目录。

```
<USG> mkdir flash:/test
%Create directory flash:/test......Done.
```

步骤 2 显示当前目录下的文件信息。

```
<USG> dir
Directory of flash:/
```

火龙果 · 整理
uml.org.cn

```
  0   -rw-  20143323  Jul 01 2009 00:11:15   sup.bin
  1   -rw-        16  Jul 10 2009 22:08:46   private-data.txt
  2   -rw-      3697  Jul 10 2009 22:08:55   ssl_vpn_cfg.zip
  3   -rw-      7760  Jul 10 2009 22:09:14   cfg123.cfg
  4   -rw-      4462  Jul 07 2009 21:23:17   on1029252_20vfw200vpn.dat
  5   drw-         -  Jul 15 2009 12:37:20   test

57277 KB total (37581 KB free)
```

步骤 3 拷贝文件 private-data.txt 从 flash:/到 flash:/test/。

```
<USG> copy flash:/private-data.txt flash:/test/private-data.txt
Copy flash:/private-data.txt to flash:/test/private-data.txt?[Y/N]:y
100%  complete
%Copied file flash:/private-data.txt to flash:/test/private-data.txt...Done
```

----结束

结果验证

显示当前目录下的文件信息，可以看到文件已经被拷贝至指定目录下。

```
<USG> cd flash:/test
<USG> dir
Directory of flash:/test/

  0   -rw-        16  Jul 15 2009 12:38:02   private-data.txt

57277 KB total (37580 KB free)
```

1.2.2 配置 FTP 举例

FTP 协议在 TCP/IP 协议族中属于应用层协议，主要向用户提供与远程主机之间的文件传输。

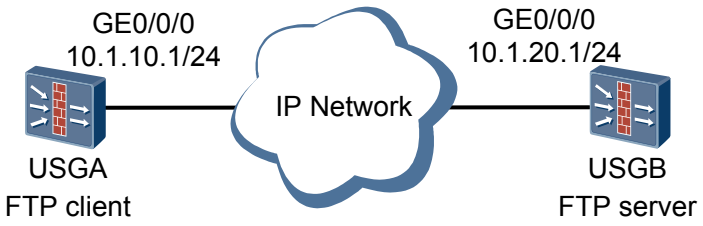
组网需求

如图 1-23 所示，作为 FTP 客户端的 USGA 和作为 FTP 服务器的 USGB 路由可达。

在 USGB 端设置 FTP 用户名为 user，密码为 password1。

USGA 从 USGB 中下载 sup.bin 文件，并存放于 flash:目录下。

图 1-23 配置 FTP 服务器组网图



配置思路

1. 配置 FTP 服务器。
2. 配置 FTP 客户端。
3. 从 FTP 客户端登录到 FTP 客户端下载文件。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

注意事项

进行下述配置前请保证 USGA 和 USGB 路由可达。

操作步骤

步骤 1 配置 FTP 服务器。

配置 USGB 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将接口加入 Untrust 域，并配置 Untrust 与 Local 域间包过滤，允许 FTP client 访问 FTP server。

```
<USGB> system-view
[USGB] interface GigabitEthernet 0/0/0
[USGB-GigabitEthernet 0/0/0] ip address 10.1.20.1 24
[USGB-GigabitEthernet 0/0/0] quit
[USGB] firewall zone untrust
[USGB-zone-untrust] add interface GigabitEthernet 0/0/0
[USGB-zone-untrust] quit
[USGB] acl 3001
[USGB-acl-adv-3001] rule permit ip source 10.1.10.1 0
[USGB-acl-adv-3001] quit
[USGB] firewall interzone local untrust
[USGB-local-untrust] packet-filter 3001 inbound
[USGB-local-untrust] quit
```

在 USGB 上开启 FTP，配置连接空闲时间为 30 分钟。

```
[USGB] ftp server enable
[USGB] ftp timeout 30
```

配置 FTP 用户的验证信息，授权方式和授权目录。

```
[USGB] aaa
[USGB-aaa] local-user user password simple password1
[USGB-aaa] local-user user service-type ftp
[USGB-aaa] local-user user ftp-directory flash:
[USGB-aaa] quit
```

步骤 2 配置 FTP 客户端。

配置 USGA 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将接口加入 Trust 域，并配置 Trust 与 Local 域间包过滤。

```
<USGA> system-view
[USGA] interface GigabitEthernet 0/0/0
[USGA-GigabitEthernet 0/0/0] ip address 10.1.10.1 24
[USGA-GigabitEthernet 0/0/0] quit
[USGA] firewall zone trust
[USGA-zone-trust] add interface GigabitEthernet 0/0/0
[USGA-zone-trust] quit
[USGA] firewall packet-filter default permit interzone local trust
```

修改 USG 当前工作路径为 flash:。

```
<USGA> cd flash:
<USGA> pwd
flash:
```

从 USGA 登录到 FTP 服务器 USGB。

```
<USGA> ftp 10.1.20.1
Trying 10.1.20.1 ...
Press CTRL+K to abort
Connected to 10.1.20.1.
220 FTP Server ready.
User(10.1.20.1:(none)):user
331 Password required for user.
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
Password:
230 User logged in.
```

设置文件传输类型为二进制模式。

```
[ftp] binary
```

从 USGB 上下载软件。

```
[ftp] get sup.bin
200 Port command successful.
150 Opening data connection for file.cc.
226 File sent ok
FTP: 20133443 byte(s) received in 69.012 second(s) 291.74Kbyte(s)/sec.
```

----结束

结果验证

在 USGA 上执行 **dir** 命令查看：下载的目标文件是否存在于 USGA 的指定目录下。

```
<USGA> dir
Directory of flash:/

  0   -rw-        16  Apr 02 2000 06:44:46   private-data.txt
  1   -rw-      1736  Apr 02 2000 06:44:57   ssl_vpn_cfg.zip
  2   drw-         -  Apr 02 2000 01:16:53   test
  3   -rw-      1638  Apr 02 2000 06:45:18   vrpcfg.zip
  4   -rw-  27270484  Apr 02 2000 00:07:30   sup1.bin
  5   -rw-  20133443  Apr 02 2000 00:10:52   sup.bin
```

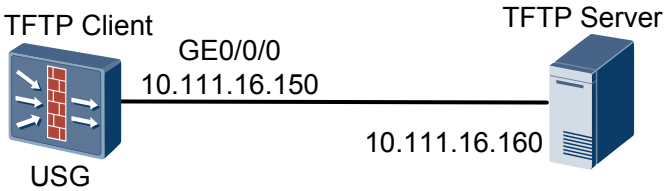
1.2.3 配置 TFTP 举例

TFTP 是一种简单文件传输协议，适用于客户机和服务器之间交互不复杂的环境。

组网需求

如图 1-24 所示，TFTP 服务器与 USG 的以太网接口 GigabitEthernet 0/0/0 相连。TFTP 服务器端 IP 地址为 10.111.16.160/24，接口 GigabitEthernet 0/0/0 的 IP 地址为 10.111.16.150/24。通过 PC 的超级终端登录到 USG，从 TFTP 服务器下载文件 sup1.bin，并存放于 flash:目录下。

图 1-24 配置 TFTP 组网图



配置思路

1. 在 TFTP 服务器端运行 TFTP 软件，并设置源文件在服务器中的位置。
2. 在 USG 上使用 TFTP 命令下载文件。

操作步骤

步骤 1 配置 USG 以太网接口 GigabitEthernet 0/0/0 的 IP 地址，将域间包过滤规则。

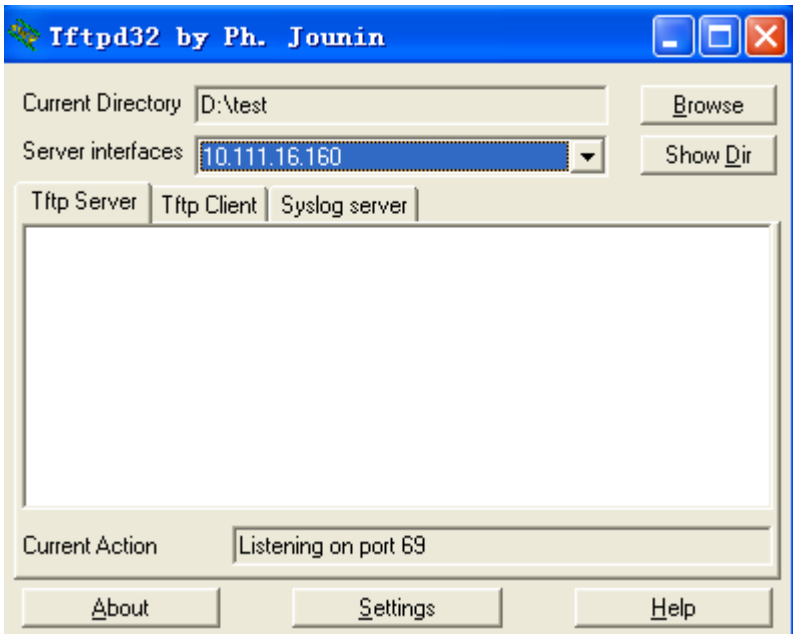
火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
<USG> system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 10.111.16.150 24
[USG-GigabitEthernet0/0/0] quit
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet 0/0/0
[USG] firewall packet-filter default permit interzone local trust
```

步骤 2 启动 TFTP 服务器，设置 TFTP 服务器的“Current Directory”为文件 sup1.bin 所在的目录；“Server interfaces”为 TFTP 服务器的 IP 地址。参数配置如图 1-25。

图 1-25 设置 TFTP 服务器基础目录



步骤 3 通过计算机超级终端登录到 USG，输入以下命令下载文件。

```
<USG> tftp 10.111.16.160 get sup1.bin flash:/sup1.bin
Transfer file in binary mode.
  Now begin to download file from remote tftp server, please wait for a while...
 \
  TFTP:       20133443 bytes received in 42734 second.
  File downloaded successfully.
```

----结束

结果验证

执行 **dir** 命令查看：下载的目标文件是否存在于 USG 的指定目录下。

```
<USG> dir
Directory of flash:/

  0   -rw-        16  Apr 02 2000 06:44:46   private-data.txt
  1   -rw-      1736  Apr 02 2000 06:44:57   ssl_vpn_cfg.zip
  2   drw-         -  Apr 02 2000 01:16:53   test
  3   -rw-      1638  Apr 02 2000 06:45:18   vrpcfg.zip
  4   -rw-  27270484  Apr 02 2000 00:07:30   sup.bin
  5   -rw-  20133443  Apr 02 2000 00:10:52   sup1.bin
```

火龙果 · 整理
uml.org.cn

1.3 配置信息中心

信息中心是 USG 主机软件中不可缺少的一部分，它作为 USG 的信息枢纽而存在。信息中心接管大多数的信息输出，并对信息进行有效的、细致的分类筛选。

1.3.1 配置向日志服务器输出 syslog 日志举例
在 USG 中，攻击防范、流量监控、黑名单和地址绑定产生的日志信息量小，因此采用 syslog 方式以文本格式进行输出。

1.3.2 配置向日志主机输出二进制流日志举例
对于信息量很大的日志，如 NAT/ASPF 日志，USG 提供了一种“二进制”输出方式。二进制流日志直接输出到日志主机上，无需信息中心模块的参与。

1.3.3 配置向控制台输出调试信息举例
打开需要调试的软件模块的 Debugging 开关后，该软件模块会产生 Debug 信息。通过调试信息可以跟踪业务的运行过程，查找故障的原因。USG 的调试信息可以通过 0 号 console 信息通道输出到本地控制台。

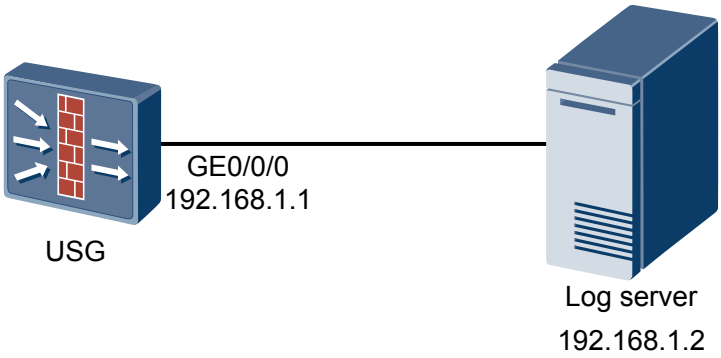
1.3.1 配置向日志服务器输出 syslog 日志举例

在 USG 中，攻击防范、流量监控、黑名单和地址绑定产生的日志信息量小，因此采用 syslog 方式以文本格式进行输出。

组网需求

如图 1-26 所示，USG 向日志主机（UNIX 工作站）发送由 PPP 模块和 IP 模块产生、严重等级为 notifications 的日志信息。

图 1-26 配置向日志服务器输出 syslog 日志组网图



配置思路

1. 开启信息中心。
2. 配置日志主机类型
3. 指定日志主机的 IP 地址。
4. 配置严重等级和允许输出信息的模块。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

操作步骤

步骤 1 按照图 1-26 配置 USG 相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 配置将由 PPP 模块和 IP 模块产生、严重等级为 notification 的 syslog 日志发送到日志主机（UNIX 工作站）。

开启信息中心。

```
<USG> system-view
[USG] info-center enable
```

配置日志主机类型为 UNIX。

```
[USG] info-center loghost type unix
```

配置日志主机的 IP 地址为 192.168.1.2，日志主机记录工具使用 local4，日志记录的语言为英文。

```
[USG] info-center loghost 192.168.1.2 facility local4 language english
```

配置严重等级为 notificationl，允许输出信息的模块为 PPP 和 IP。

```
[USG] info-center source ppp channel loghost log level notifications
[USG] info-center source ip channel loghost log level notifications
```

----结束

结果验证

在 USG 上执行 **display info-center** 命令，查看已经配置的日志主机。

```
<USG> display info-center
Information Center:enabled
Log host:
        192.168.1.2, channel number 2, channel name loghost,
                                        language english , host facility local4
Console:
        channel number : 0, channel name : console
Monitor:
        channel number : 1, channel name : monitor
SNMP Agent:
        channel number : 5, channel name : snmpagent
Log buffer:
        enabled,max buffer size 1024, current buffer size 512,
current messages 256, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 156
Trap buffer:
        enabled,max buffer size 1024, current buffer size 256,
current messages 12, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
logfile:
        channel number : 9, channel name : channel9, language : english
Information timestamp setting:
        log   - date
        trap  - date
        debug - boot

 Sent messages = 431, Received messages = 430
```

配置脚本

```
#
 sysname USG
#
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
 info-center source PPP channel 2 log level notification
 info-center source IP channel 2 log level notification
 info-center loghost type unix
 info-center loghost 192.168.1.2 facility local4
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

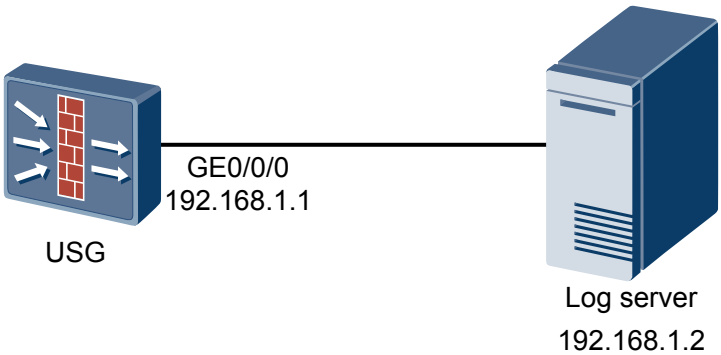
1.3.2 配置向日志主机输出二进制流日志举例

对于信息量很大的日志，如 NAT/ASPF 日志，USG 提供了一种“二进制”输出方式。二进制流日志直接输出到日志主机上，无需信息中心模块的参与。

组网需求

如图 1-27 所示，USG 上产生的二进制日志信息，实时的传送到日志主机中。用户或维护人员通过日志解析工具对日志进行解析，通过查看日志信息，为故障定位提供依据。

图 1-27 配置向日志主机输出二进制流日志组网图



配置思路

1. 开启信息中心。
2. 指定日志主机的 IP 地址。
3. 配置二进制日志发送到日志主机。

操作步骤

步骤 1 按照图 1-27 配置 USG 相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 配置将二进制日志发送到日志主机。

开启信息中心。

```
<USG> system-view
[USG] info-center enable
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

配置日志主机的 IP 地址为 192.168.1.2，日志记录的语言为英文。

```
[USG] info-center loghost 192.168.1.2 language english
```

配置日志输出格式为二进制，并配置日志主机的 IP 地址和接收日志端口。

```
[USG] firewall session log-type binary host 192.168.1.2 9002
```

----结束

结果验证

在 USG 上执行 **display info-center** 命令，查看已经配置的日志主机。

```
<USG> display info-center
Information Center:enabled
Log host:
        192.168.1.2, channel number 2, channel name loghost,
                                        language english , host facility local7
Console:
        channel number : 0, channel name : console
Monitor:
        channel number : 1, channel name : monitor
SNMP Agent:
        channel number : 5, channel name : snmpagent
Log buffer:
        enabled,max buffer size 1024, current buffer size 512,
current messages 54, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 0
Trap buffer:
        enabled,max buffer size 1024, current buffer size 256,
current messages 4, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 0
logfile:
        channel number : 0, channel name : console, language : english
Information timestamp setting:
        log   - date
        trap  - date
        debug - date

 Sent messages = 58, Received messages = 57
```

配置脚本

USG 配置脚本：

```
#
 sysname USG
#
 info-center loghost 192.168.1.2
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
 firewall session log-type binary host 192.168.1.2 9002
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

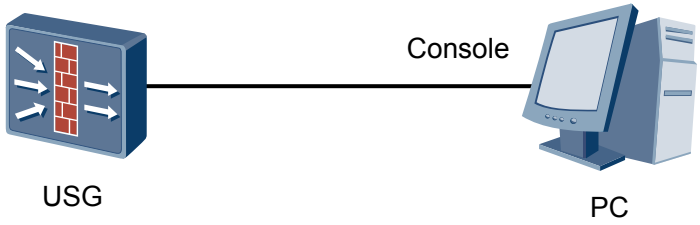
1.3.3 配置向控制台输出调试信息举例

打开需要调试的软件模块的 Debugging 开关后，该软件模块会产生 Debug 信息。通过调试信息可以跟踪业务的运行过程，查找故障的原因。USG 的调试信息可以通过 0 号 console 信息通道输出到本地控制台。

组网需求

如图 1-28 所示，PC 机与 USG 的 Console 口相连。要求配置 USG 向控制台输出 PPP 模块的调试信息。

图 1-28 配置向控制台输出调试信息组网图



配置思路

1. 开启信息中心。
2. 配置向控制台输出信息以及信息通道。
3. 配置允许调试信息输出的模块。
4. 打开相关模块的调试开关。

操作步骤

步骤 1 开启信息中心。

```
<USG> system-view
[USG] info-center enable
```

步骤 2 配置向控制台输出信息，信息通道名为 console。

```
[USG] info-center console channel console
```

步骤 3 配置允许通过通道 console 向控制台输出 ARP 模块的调试信息，并且严重等级限制为 debugging。

```
[USG] info-center source arp channel console debug level debugging
```

步骤 4 打开 ARP 模块的调试开关。

```
<USG> debugging arp packet
```

----结束

结果验证

在 USG 上执行 **display channel 0** 命令，查看配置的通道信息。

```
<USG> display channel 0
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABL
ffff0000 default  Y      warning       Y      debugging     Y
810000   ARP      Y      informational Y      informational Y
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

1.4 配置 NTP

NTP 属于应用层协议（基于 UDP 传输，使用的端口号为 123），用来同步网络中分布式时间服务器和客户端之间的时间，使网络中的设备提供基于统一时间的应用成为可能。

1.4.1 配置 NTP 对等体模式举例
NTP 主要应用于需要网络中所有主机或设备时钟保持一致的场合。

1.4.2 配置 NTP 广播模式举例
在局域网中，NTP 广播服务器从指定接口周期性地向广播地址 255.255.255.255 发送时钟同步报文。NTP 广播客户端从指定接口侦听服务器发来的 NTP 广播消息包，并对本地时钟同步。

1.4.3 配置 NTP 组播模式举例
在局域网中，NTP 组播服务器从指定接口周期性地向组播地址 224.0.1.1 发送时钟同步报文。NTP 组播客户端从指定接口侦听服务器发来的 NTP 组播消息包，并对本地时钟同步。

1.4.4 配置带验证的 NTP 服务器/客户端模式举例
在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。本节介绍了带验证的 NTP 服务器/客户端模式。

1.4.5 配置带验证的 NTP 广播模式举例
在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。本节介绍了带验证的 NTP 广播模式。

1.4.1 配置 NTP 对等体模式举例

NTP 主要应用于需要网络中所有主机或设备时钟保持一致的场合。

组网需求

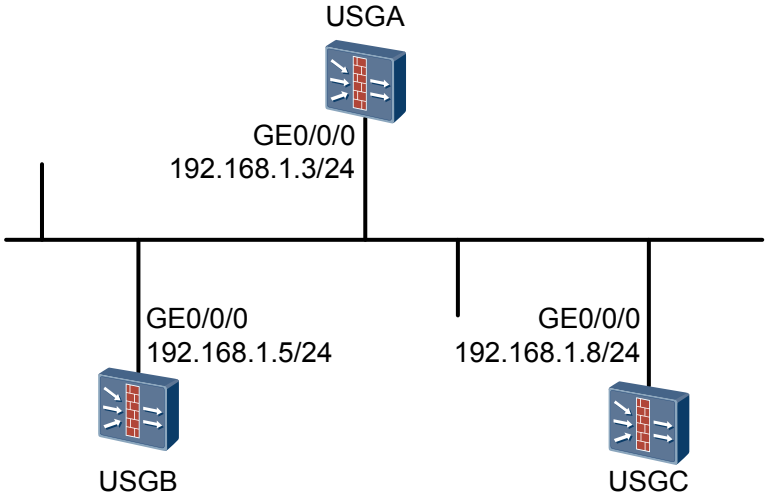
如**图 1-29** 所示，在同一个局域网中有三台 USG，要求以 USGA 的本地时钟为主时钟进行时钟同步。

- USGA 将自己的本地时钟设为 NTP 主时钟，层数为 2。
- USGB 将 USGA 设为自己的 NTP 服务器，即 USGB 作为 NTP 客户端。
- USGC 将 USGB 设为自己的被动对等体，即 USGC 作为 NTP 主动对等体。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-29 配置 NTP 对等体模式组网图



配置思路

1. 配置 NTP 主时钟，NTP 客户端向 NTP 服务器请求时钟同步。
2. 在 NTP 主动对等体上指定被动对等体，主动对等体向被动对等体请求时钟同步。

操作步骤

步骤 1 按照图 1-29 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 配置 NTP 单播服务器/客户端模式。

在 USGA 上指定使用自己的本地时钟作为参考时钟，层数为 2。

```
<USGA> system-view
[USGA] ntp-service refclock-master 2
```

在 USGB 上指定 USGA 作为自己的 NTP 服务器。

```
<USGB> system-view
[USGB] ntp-service unicast-server 192.168.1.3
```

配置完成后，USGB 的时钟同步到 USGA。

查看 USGB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 USGA 低 1 级。

```
[USGB] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 192.168.1.3
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 29.24 ms
 root dispersion: 15.30 ms
 peer dispersion: 10.00 ms
 reference time: 02:04:48.984 UTC Oct 16 2009(CE825340.FBECEDD4)
```

步骤 3 配置 NTP 单播对等体模式

火龙果 · 整理
uml.org.cn

在 USGC 上指定 USGB 作为自己的被动对等体。

版权所有 © 成都市华为赛门铁克科技有限公司

```
<USGC> system-view
[USGC] ntp-service unicast-peer 192.168.1.5
```

USGC 没有配置主时钟，层数低于 USGB，所以 USGC 向 USGB 同步。

----结束

结果验证

在 USGC 上执行 **display ntp-service status** 命令，查看 USGC 的 NTP 状态。

```
[USGC] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 192.168.1.5
 nominal frequency: 100.0000 Hz
 actual frequency: 100.0000 Hz
 clock precision: 2^16
 clock offset: 13.5770 ms
 root delay: 34.06 ms
 root dispersion: 7.49 ms
 peer dispersion: 14.45 ms
 reference time: 02:04:19.393 UTC Oct 16 2009(CE825323.64AAEAFA)
```

可以看到 USGC 的时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比对等体 USGB 低 1 级。

配置脚本

USGA 配置脚本：

```
#
 sysname USGA
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.3 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
ntp-service refclock-master 2
#
return
```

USGB 配置脚本：

```
#
 sysname USGB
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.5 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
ntp-service unicast-server 192.168.1.3
#
return
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

USGC 配置脚本：

```
#
 sysname USGC
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.8 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
ntp-service unicast-peer 192.168.1.5
#
return
```

1.4.2 配置 NTP 广播模式举例

在局域网中，NTP 广播服务器从指定接口周期性地向广播地址 255.255.255.255 发送时钟同步报文。NTP 广播客户端从指定接口侦听服务器发来的 NTP 广播消息包，并对本地时钟同步。

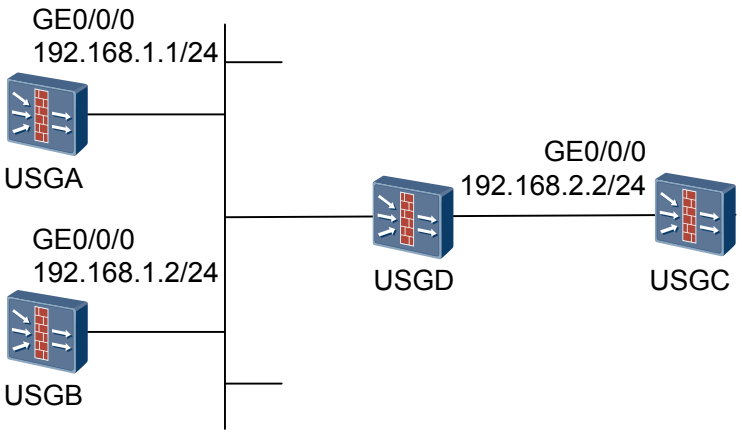
组网需求

如图 1-30 所示，USGA 和 USGB 在同一个网段，USGC 在另一个网段，USGD 连接这两个网段。

USGA 作为 NTP 广播服务器，使用本地时钟作为 NTP 主时钟，层数为 2，从接口 GigabitEthernet 0/0/0 外发送广播消息包。

配置 USGD 和 USGA 分别从各自的接口 GigabitEthernet 0/0/0 监听广播消息。

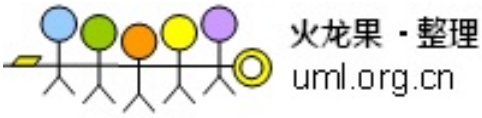
图 1-30 配置 NTP 广播模式组网图



配置思路

1. 在接口视图下配置 NTP 广播服务器。
2. 在接口视图下配置广播客户端。

注意事项



进行下述配置前请保证各 USG 之间路由可达。

版权所有 © 成都市华为赛门铁克科技有限公司

操作步骤

步骤 1 按照图 1-30 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 在 USGA 上配置 NTP 广播服务器。

配置 USGA 使用本地时钟作为 NTP 主时钟，层数为 2。

```
<USGA> system-view
[USGA] ntp-service refclock-master 2
```

在 USGA 的接口上配置 NTP 广播服务器。

```
[USGA] interface GigabitEthernet 0/0/0
[USGA-GigabitEthernet0/0/0] ntp-service broadcast-server
```

步骤 3 配置与服务器在同一网段的 NTP 广播客户端 USGB。

```
<USGB> system-view
[USGB] interface GigabitEthernet 0/0/0
[USGB-GigabitEthernet0/0/0] ntp-service broadcast-client
```

步骤 4 配置与服务器在不同网段的 NTP 广播客户端 USGC。

```
<USGC> system-view
[USGC] interface GigabitEthernet 0/0/0
[USGC-GigabitEthernet0/0/0] ntp-service broadcast-client
```

----结束

结果验证

- 在 USGB 执行 **display ntp-service status** 命令，查看 USGB 的 NTP 状态。

```
[USGB] display ntp-service status
clock status: synchronized
 clock stratum: 3
 reference clock ID: 192.168.1.1
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 29.24 ms
 root dispersion: 15.30 ms
 peer dispersion: 10.00 ms
 reference time: 02:04:48.984 UTC Oct 16 2009(CE825340.FBECEDD4)
```

可以看到时钟状态为“synchronized”，即，USGB 能够同步到 USGA。时钟的层数为 3，比服务器 USGA 低 1 级。

- 在 USGC 行 **display ntp-service status** 命令，查看 USGC 的 NTP 状态。

```
[USGC] display ntp-service status
 clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 0.00 ms
 reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000
```

可以看到时钟状态为“unsynchronized”，即，USGC

火龙果 · 整理
uml.org.cn

这是因为 USGC 和 USGA 不在同一个网段，收不到 USGA 发出的广播包；而 USGB 和 USGA 在同一个网段，能够收到 USGA 发出的广播包。

配置脚本

USGA 配置脚本：

```
#
 sysname USGA
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ntp-service broadcast-server      // 在接口上配置NTP广播服务器
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
ntp-service refclock-master 2
#
return
```

USGB 配置脚本：

```
#
 sysname USGB
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
 ntp-service broadcast-client      // 在同一网段的USG接口上配置NTP广播客户端
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

USGC 配置脚本：

```
#
 sysname USGC
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
 ntp-service broadcast-client      // 在不同网段的USG接口上配置NTP广播客户端
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

1.4.3 配置 NTP 组播模式举例

在局域网中，NTP 组播服务器从指定接口周期性地向组播
报文。NTP 组播客户端从指定接口侦听服务器发来的 NT
同步。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

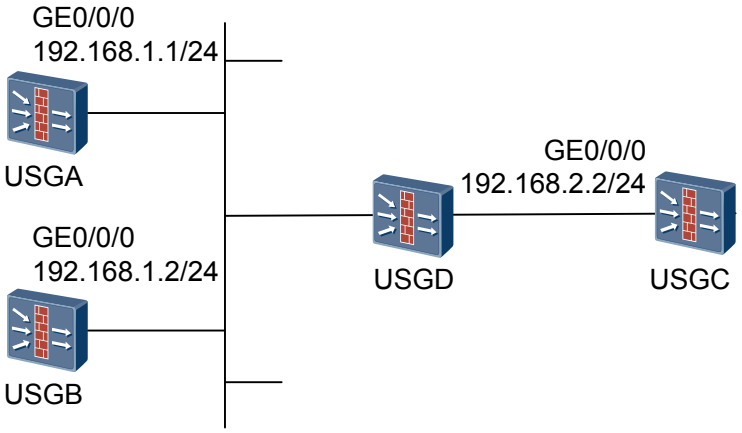
组网需求

如图 1-31 所示，USGA 和 USGB 在同一个网段，USGC 在另一个网段，USGD 连接这两个网段。

USGA 作为 NTP 组播服务器，使用本地时钟作为 NTP 主时钟，层数为 2，从接口 GigabitEthernet 0/0/0 外发送组播消息包。

配置 USGD 和 USGA 分别从各自的接口 GigabitEthernet 0/0/0 监听组播消息。

图 1-31 配置 NTP 组播模式组网图



配置思路

1. 在接口视图下配置 NTP 组播服务器。
2. 在接口视图下配置组播客户端。

注意事项

进行下述配置前请保证各 USG 之间路由可达。

操作步骤

步骤 1 按照图 1-31 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 在 USGA 上配置 NTP 组播服务器。

配置 USGA 使用本地时钟作为 NTP 主时钟，层数为 2。

```
<USGA> system-view
[USGA] ntp-service refclock-master 2
```

在 USGA 的接口上配置 NTP 组播服务器。

```
[USGA] interface GigabitEthernet 0/0/0
[USGA-GigabitEthernet0/0/0] ntp-service multicast-server
```

步骤 3 配置与服务器在同一网段的 NTP 组播客户端 USGB。

```
<USGB> system-view
[USGB] interface GigabitEthernet 0/0/0
[USGB-GigabitEthernet0/0/0] ntp-service multicast-client
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

步骤 4 配置与服务器在不同网段的 NTP 组播客户端 USGC。

```
<USGC> system-view
[USGC] interface GigabitEthernet 0/0/0
[USGC-GigabitEthernet0/0/0] ntp-service multicast-client
```

----结束

结果验证

- 在 USGB 执行 **display ntp-service status** 命令，查看 USGB 的 NTP 状态。

```
[USGB] display ntp-service status
clock status: synchronized
 clock stratum: 3
 reference clock ID: 192.168.1.1
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 29.24 ms
 root dispersion: 15.30 ms
 peer dispersion: 10.00 ms
 reference time: 02:04:48.984 UTC Oct 16 2009(CE825340.FBECEDD4)
```

  可以看到时钟状态为“synchronized”，即 USGB 能够同步到 USGA。时钟的层数为 3，比服务器 USGA 低 1 级。

- 在 USGC 行 **display ntp-service status** 命令，查看 USGC 的 NTP 状态。

```
[USGC] display ntp-service status
 clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 0.00 ms
 reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

  可以看到时钟状态为“unsynchronized”，即 USGC 不能够同步到 USGA。

  这是因为 USGC 和 USGA 不在同一个网段，收不到 USGA 发出的组播包；而 USGB 和 USGA 在同一个网段，能够收到 USGA 发出的组播包。

配置脚本

USGA 配置脚本：

```
#
 sysname USGA
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ntp-service multicast-server      // 在接口上配置NTP组播服务器
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
ntp-service refclock-master 2
#
return
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

USGB 配置脚本：

```
#
 sysname USGB
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
 ntp-service multicast-client      // 在同一网段的USG接口上配置NTP组播客户端
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

USGC 配置脚本：

```
#
 sysname USGC
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
 ntp-service multicast-client      // 在不同网段的USG接口上配置NTP组播客户端
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
return
```

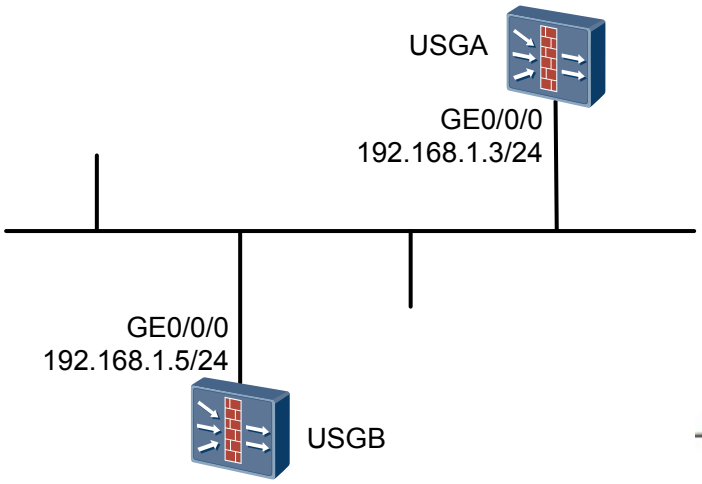
1.4.4 配置带验证的 NTP 服务器/客户端模式举例

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。本节介绍了带验证的 NTP 服务器/客户端模式。

组网需求

如图 1-32 所示，USGA 设置本地时钟作为 NTP 主时钟，层数为 2，USGB 以 USGA 作为时间服务器，同时两端配置 NTP 验证。

图 1-32 配置带验证的 NTP 服务器/客户端模式组网图



火龙果 · 整理
uml.org.cn

配置思路

1. 配置 NTP 服务器，在服务器上配置 NTP 验证。
2. 配置 NTP 客户端，在客户端上配置 NTP 验证。

操作步骤

步骤 1 按照图 1-32 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 在 USGA 上配置 NTP 服务器，并启用验证。

设置本地时钟作为 NTP 主时钟，层数为 2。

```
<USGA> system-view
[USGA] ntp-service refclock-master 2
```

启动 NTP 身份验证功能。

```
[USGA] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 42，密钥为 aNiceKey。

```
[USGA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥是可信的。

```
[USGA] ntp-service reliable authentication-keyid 42
```

步骤 3 在 USGB 上配置 NTP 客户端，并启用验证。

将 USGA 作为时间服务器并指定验证 ID。

```
<USGB> system-view
[USGB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

启动 NTP 身份验证功能。

```
[USGB] ntp-service authentication enable
```

设置 MD5 身份验证密钥，密钥 ID 号为 42，密钥为 aNiceKey。

```
[USGB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥是可信的。

```
[USGB] ntp-service reliable authentication-keyid 42
```

----结束

结果验证

在 USGB 上执行 **display ntp-service status** 命令，查看 USGB 的 NTP 状态。

```
<USGB> display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: 192.168.1.3
nominal frequence: 250.0000 Hz
actual frequence: 249.9992 Hz
clock precision: 2^19
clock offset: 0.66 ms
root delay: 27.47 ms
root dispersion: 208.39 ms
peer dispersion: 9.63 ms
reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

可以看到时钟状态为“synchronized”，即，USGB 能够同步到 USGA。时钟的层数为 3，比服务器 USGA 低 1 级。

配置脚本

USGA 配置脚本：

```
#
 sysname USGA
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.3 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 <-+XYME-P$WQ=^Q`MAF
4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service refclock-master  2
#
return
```

USGB 配置脚本：

```
#
 sysname USGB
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.5 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 <-+XYME-P$WQ=^Q`MAF
4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 192.168.1.3 authentication-keyid 42
#
return
```

1.4.5 配置带验证的 NTP 广播模式举例

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。本节介绍了带验证的 NTP 广播模式。

组网需求

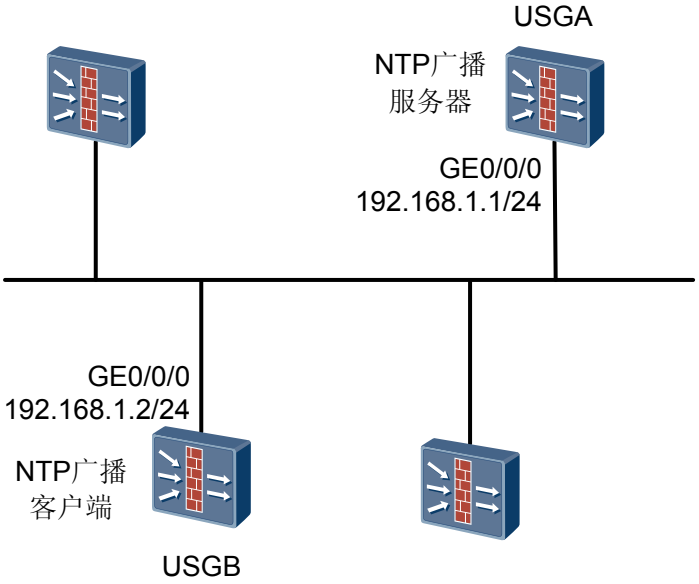
如图 1-33 所示，USGA 作为 NTP 广播服务器，使用本地时钟作为 NTP 主时钟，层数为 2，从接口 GigabitEthernet 0/0/0 外发送广播消息包。USG
监听广播消息。

本网络对安全性要求较高，要求运行 NTP 协议时启用验

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

图 1-33 配置带验证的 NTP 广播模式组网图



配置思路

1. 在接口视图下配置 NTP 广播服务器。
2. 在接口视图下配置广播客户端。
3. 在 NTP 广播服务器和客户端上分别配置 NTP 验证。

操作步骤

步骤 1 按照图 1-33 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 在 USGA 上配置 NTP 广播服务器，并启用验证。

配置 USGA 使用本地时钟作为 NTP 主时钟，层数为 2。

```
<USGA> system-view
[USGA] ntp-service refclock-master 2
```

启用 NTP 验证。

```
[USGA] ntp-service authentication enable
[USGA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
[USGA] ntp-service reliable authentication-keyid 42
```

配置 USGA 为 NTP 广播服务器，从接口 GigabitEthernet 0/0/0 发送 NTP 广播消息包，并指定使用密钥 ID 42 加密。

```
[USGA] interface GigabitEthernet 0/0/0
[USGA-GigabitEthernet0/0/0] ntp-service broadcast-server authentication-keyid 42
[USGB-GigabitEthernet0/0/0] quit
```

步骤 3 在 USGB 上配置 NTP 广播客户端，并启用验证。

启用 NTP 验证。

```
<USGB> system-view
USGB] ntp-service authentication enable
[USGB] ntp-service authentication-keyid 42 authentication-mode md
[USGB] ntp-service reliable authentication-keyid 42
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

配置 USGB 为 NTP 广播客户端，从接口 GigabitEthernet 0/0/0 侦听 NTP 广播消息包。

```
[USGB] interface GigabitEthernet 0/0/0
[USGB-GigabitEthernet0/0/0] ntp-service broadcast-client
[USGB-GigabitEthernet0/0/0] quit
```

----结束

结果验证

- 在 USGB 执行 **display ntp-service status** 命令，查看 USGB 的 NTP 状态。

```
[USGB] display ntp-service status
clock status: synchronized
 clock stratum: 3
 reference clock ID: 192.168.1.1
 nominal frequency: 60.2384 Hz
 actual frequency: 60.2384 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 29.24 ms
 root dispersion: 15.30 ms
 peer dispersion: 10.00 ms
 reference time: 02:04:48.984 UTC Oct 16 2009(CE825340.FBECEDD4)
```

  可以看到时钟状态为“synchronized”，即，USGB 能够同步到 USGA。时钟的层数为 3，比服务器 USGA 低 1 级。

配置脚本

USGA 配置脚本：

```
#
 sysname USGA
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ntp-service broadcast-server authentication-keyid 42      // 在接口上配置NTP广播服务器并指定使用密
钥ID 42加密
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 <-+XYME-P$WQ=^Q`MAF
4<1!!
 ntp-service reliable authentication-keyid 42
 ntp-service refclock-master  2
#
return
```

USGB 配置脚本：

```
#
 sysname USGB
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
 ntp-service broadcast-client      // 在接口上配置NTP广播客户端
#
firewall zone trust
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
 set priority 85
 add interface GigabitEthernet0/0/0
#
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 <-+XYME-P$WQ=^Q`MAF
4<1!!
 ntp-service reliable authentication-keyid 42
#
return
```

1.5 配置网管软件

目前，计算机网络中用得最广泛的网络管理协议是简单网络管理协议 SNMP（Simple Network Management Protocol），它是被广泛接受并投入使用的工业标准。

1.5.1 配置 SNMP 举例
配置 USG 作为 SNMP Agent，处理 NMS 发来的查询报文并返回响应报文。

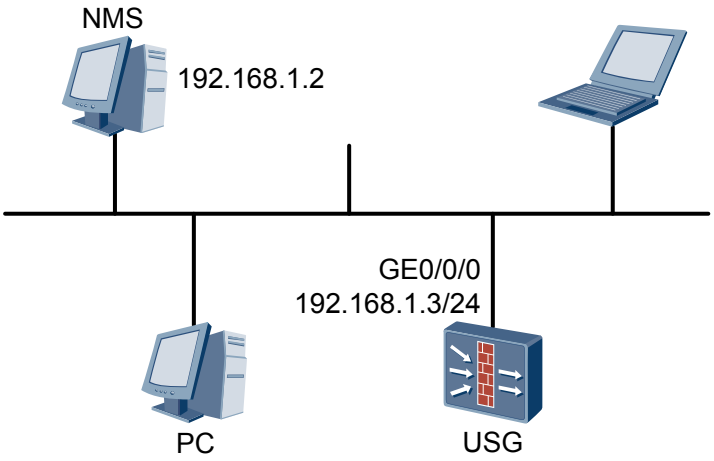
1.5.1 配置 SNMP 举例

配置 USG 作为 SNMP Agent，处理 NMS 发来的查询报文并返回响应报文。

组网需求

如图 1-34 所示，网管工作站（NMS）与 USG 通过以太网相连，网管工作站 IP 地址为 192.168.1.2，USG 以太网接口的 IP 地址为 192.168.1.3。

图 1-34 SNMP 配置举例组网图



配置思路

1. 配置 USG 基本信息。
2. USG 上配置 SNMP。
3. 配置 NMS。

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

操作步骤

步骤 1 按照图 1-34 配置相关接口的 IP 地址，把接口加入安全区域，并配置域间包过滤规则。具体配置过程略。

步骤 2 在 USG 上配置 SNMP。

配置 trap 报文的出接口。

```
<USG> system-view
[USG] snmp-agent trap source GigabitEthernet0/0/0
```

启动 SNMP Agent，配置版本为 SNMPv1。

```
[USG] snmp-agent sys-info version v1
```

配置团体名和访问权限。

```
[USG] snmp-agent community read public
[USG] snmp-agent community write private
```

配置管理员联系方法。

```
[USG] snmp-agent sys-info contact Mr.Wang-Tel:3306
```

配置 USG 物理位置。

```
[USG] snmp-agent sys-info location telephone-closet,3rd-floor
```

配置允许设备发送 TRAP 报文。

```
[USG] snmp-agent trap enable
```

配置接收 SNMP 通知的网管工作站的 IP 地址、端口号、团体名称。

该配置需与 NMS 接收 Trap 端口的配置保持一致。

```
[USG] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port 5000 params
securityname public
```

步骤 3 配置 NMS，具体配置请参见相关网管产品的用户手册。

说明

配置 NMS 的 SNMP 版本号为 SNMPv1。

----结束

配置脚本

USG 配置脚本：

```
#
 sysname USG
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.3 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100000FC3
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

```
 snmp-agent community read  public
 snmp-agent community write  private
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v1
 snmp-agent target-host trap address udp-domain 192.168.1.2 udp-port 5000 par
ams securityname public
 snmp-agent trap enable ldp
 snmp-agent trap enable ipsec
 snmp-agent trap enable configuration
 snmp-agent trap enable system
 snmp-agent trap enable standard
 snmp-agent trap enable lsp
 snmp-agent trap enable vrrp
 snmp-agent trap enable ospf 2
 snmp-agent trap enable ospf 1
 snmp-agent trap enable bgp
 snmp-agent trap enable flash
 snmp-agent trap enable srm
 snmp-agent trap source GigabitEthernet0/0/0
#
return
```

火龙果 · 整理
uml.org.cn

版权所有 © 成都市华为赛门铁克科技有限公司

火龙果 • 整理
uml.org.cn