MSR 系列路由器 L2TP 使用 Shiva 进行认证及地址分配功能的典型配置举例

目 录

1 简介

本文档介绍 L2TP 用户端进行 Shiva 认证及地址分配的典型案例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 L2TP 和 RADIUS 服务器的特性。

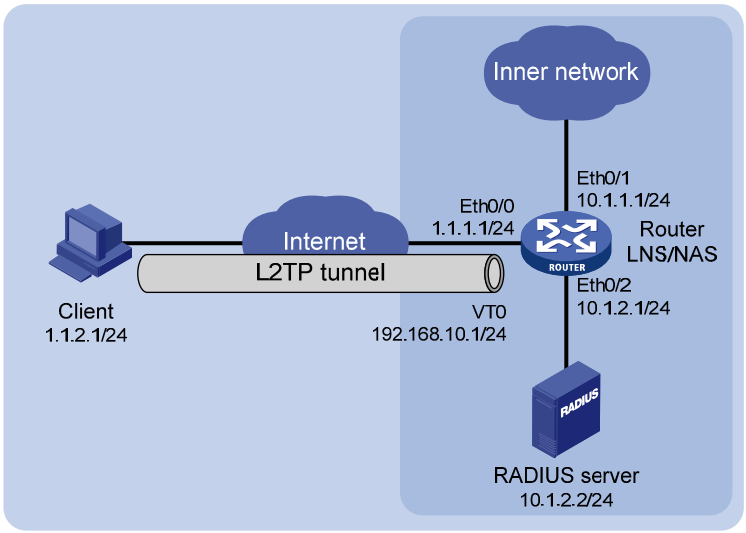
3 配置举例

3.1 组网需求

如 图 1 所示，客户端主机通过MSR路由器连接内部局域网，MSR路由器与RADIUS服务器相连，现要求：

- RADIUS 服务器对登录内部局域网的客户端进行认证授权并分配地址。
- 客户端主机与 MSR 路由器建立 L2TP 连接。

图1 MSR 系列路由器 L2TP 使用 Shiva 进行认证及地址分配功能组网图



3.2 配置思路

为了使 RADIUS 服务器正常认证授权客户端，需要在路由器上建立 RADIUS 方案，并且配置与 RADIUS 服务器一致的接口地址和端口号。

3.3 使用版本

本举例是在 Release 2311 版本上进行配置和验证的。

3.4 配置注意事项

在 LNS 设备上配置时，先要全局开启 L2TP 功能，再建立虚模模板，否则可能会导致虚拟模板不断自动开启和关闭。

3.5 配置步骤

3.5.1 Router配置

配置接口 IP 地址。

```
<Router> system-view
[Router] interface ethernet 0/0
[Router-Ethernet0/0] port link-mode route
[Router-Ethernet0/0] ip address 1.1.1.1 255.255.255.0
[Router-Ethernet0/0] quit
[Router] interface ethernet 0/1
[Router-Ethernet0/1] port link-mode route
[Router-Ethernet0/1] ip address 10.1.1.1 255.255.255.0
[Router-Ethernet0/1] quit
[Router] interface ethernet 0/2
[Router-Ethernet0/2] port link-mode route
[Router-Ethernet0/2] ip address 10.1.2.1 255.255.255.0
[Router-Ethernet0/2] quit
```

创建 RADIUS 方案 shiva。

```
[Router] radius scheme shiva
```

配置服务器类型。

```
[Router-radius-shiva] server-type standard
```

配置认证和计费服务器地址和端口号。

```
[Router-radius-shiva] primary authentication 10.1.2.2 1645
[Router-radius-shiva] primary accounting 10.1.2.2 1646
```

配置认证和计费密码。

```
[Router-radius-shiva] key authentication cipher h3c
[Router-radius-shiva] key accounting cipher h3c
```

配置认证用户名不带 ISP 域名。

```
[Router-radius-shiva] user-name-format without-domain
[Router-radius-shiva] quit
```

创建 ISP 域 h3c.com。

```
[Router] domain h3c.com
```

配置 PPP 认证，授权和计费方案 shiva。

```
[Router-isp-h3c.com] authentication ppp radius-scheme shiva
```

```
[Router-isp-h3c.com] authorization ppp radius-scheme shiva
[Router-isp-h3c.com] accounting ppp radius-scheme shiva
[Router-isp-h3c.com] quit
```

设置本地用户名、密码及服务类型。

```
[Router] local-user user1
[Router-luser-user1] password simple hello
[Router-luser-user1] service-type ppp
```

配置域 h3c.com，配置 IP 地址池 0，地址范围为 192.168.10.2 到 192.168.10.254。

```
[Router] domain h3c.com
[Router-isp-h3c.com] ip pool 0 192.168.10.2 192.168.10.254
[Router-isp-h3c.com] quit
```

启用 L2TP 服务。

```
[Router] l2tp enable
```

创建虚模模板 Virtual-Template 0，并配置模板地址。

```
[Router] interface virtual-template 0
[Router-Virtual-Template0] ip address 192.168.10.1 255.255.255.0
```

配置 PPP 认证方式为 PAP 验证。

```
[Router-Virtual-Template0] ppp authentication-mode pap domain h3c.com
[Router-Virtual-Template0] remote address pool 0
[Router-Virtual-Template0] quit
```

设置 L2TP 组 1，指定接收呼叫的虚拟模板接口。

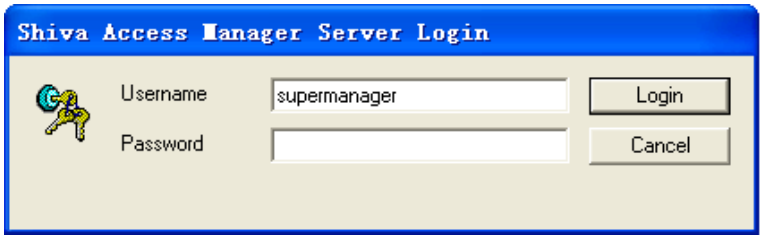
```
[Router] l2tp-group 1
[Router-l2tp1] allow l2tp virtual-template 0
```

不启用 L2TP 的隧道验证。

```
[Router-l2tp1] undo tunnel authentication
[Router-l2tp1] quit
```

3.5.2 服务器配置

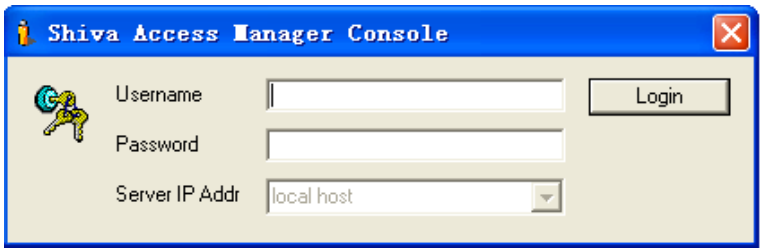
点击 Shiva Access Manager 图标，出现如下界面：



在“Username”一栏中输入“supermanager”，“Password”为空。

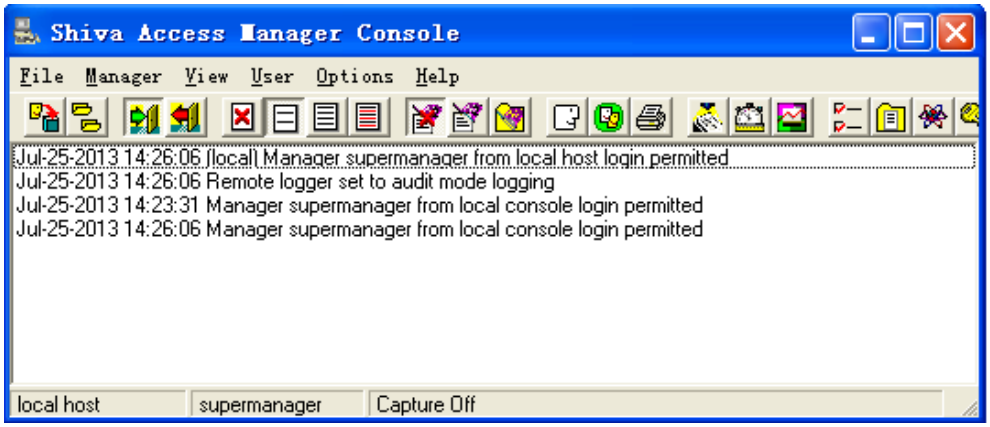
点击“Login”按钮,出现界面：

点击“Start Console Now”按钮,出现如下界面：

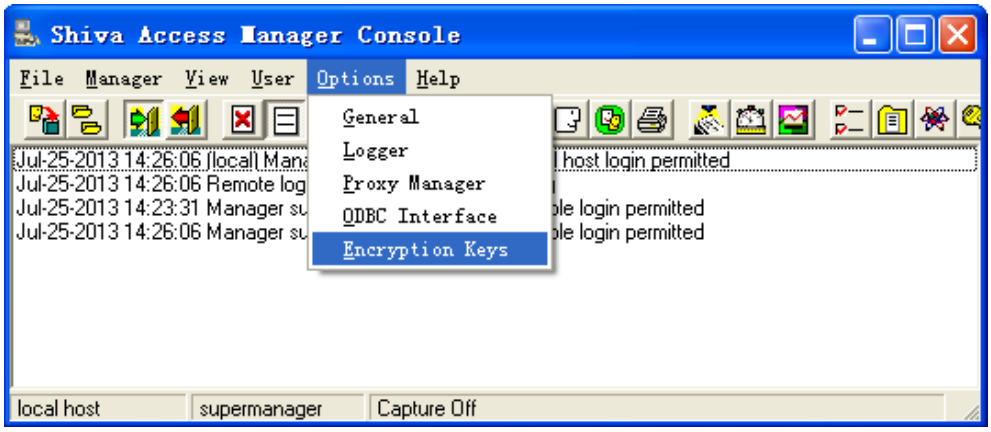


在“Username”一栏中输入“supermanager”，“Password”为空。

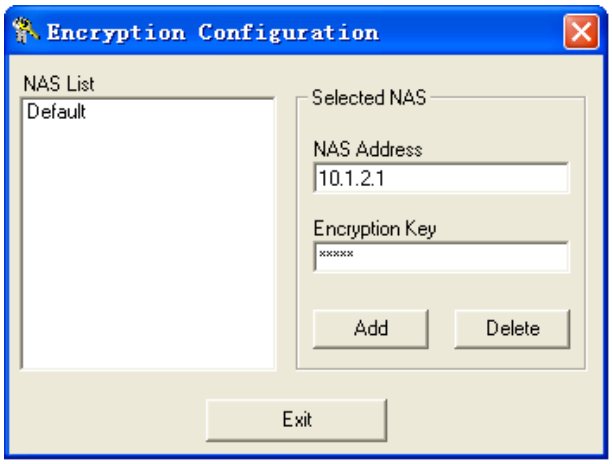
点击“Login”按钮,出现 Shiva Access Manager 主界面：



在“Options”菜单下选择“Encryption Keys”，如下图所示：

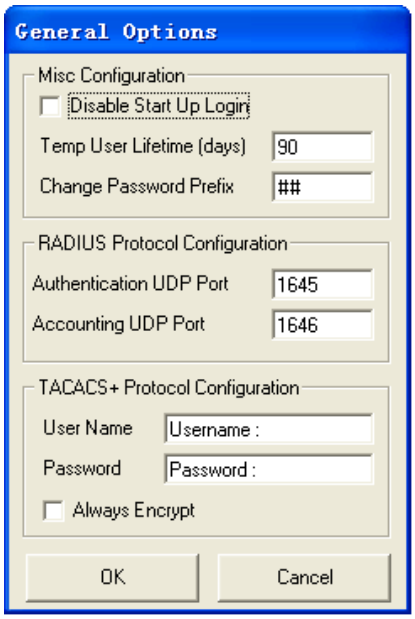


出现如下界面：



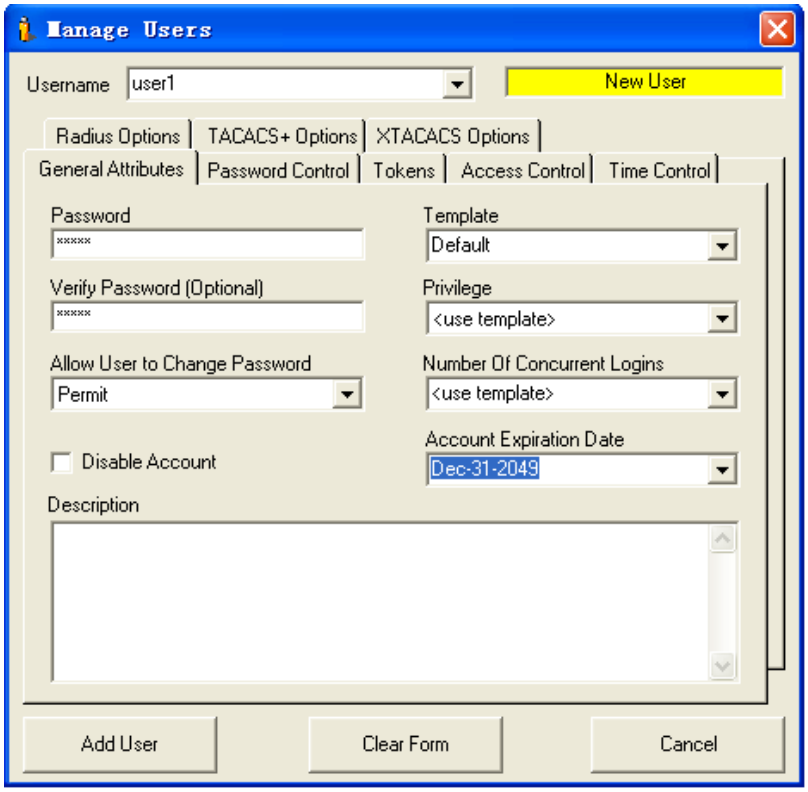
在“NAS Address”一栏填写与服务器相连的接口的 IP 地址 10.1.2.1，“Encryption Key”一栏填写密钥，要与路由器上已配置好的认证密钥保持一致，点击“Add”按钮即可。

在“Options”菜单下选择“General”，出现如下界面：



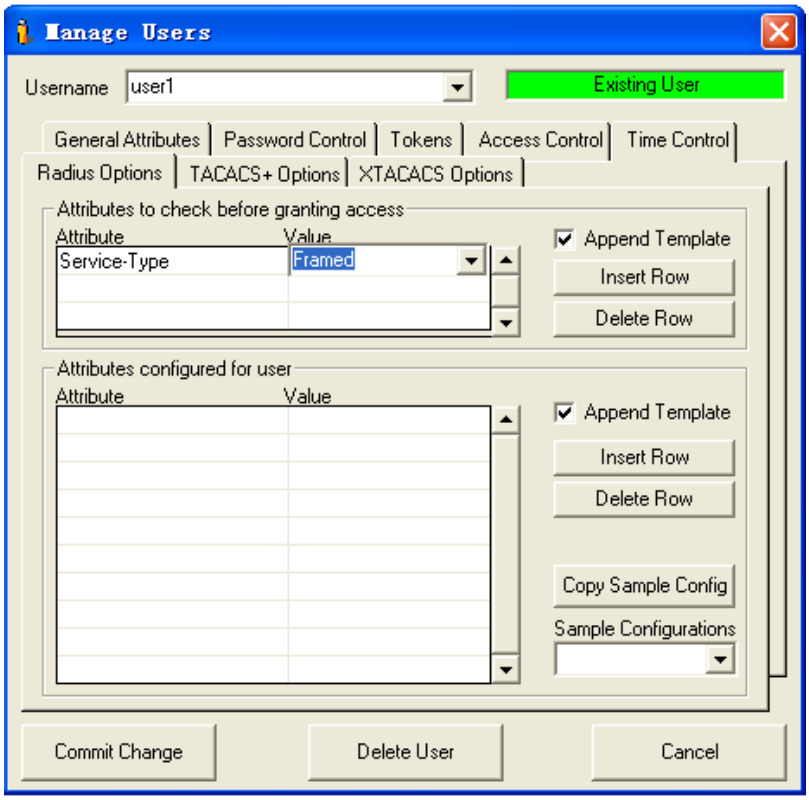
在“Authentication UDP Port”一栏填写认证端口号，“Accounting UDP Port”一栏填写计费端口号，点击“OK”按钮即可。（Shiva 默认端口号为 1645，1646）。

在“User”菜单下选择“Manage Users”，出现如下界面：



在“Username”一栏填写要添加的用户名字如“user1”，系统中不存在该用户时右边会显示“New User”字样，选择“General Attributes”属性页，在“Password”一栏中输入认证密码，“Account Expiration Date”一栏选择“Dec-31-2049”。点击“Add User”按钮。

管理用户界面选择“Radius Options”属性页:

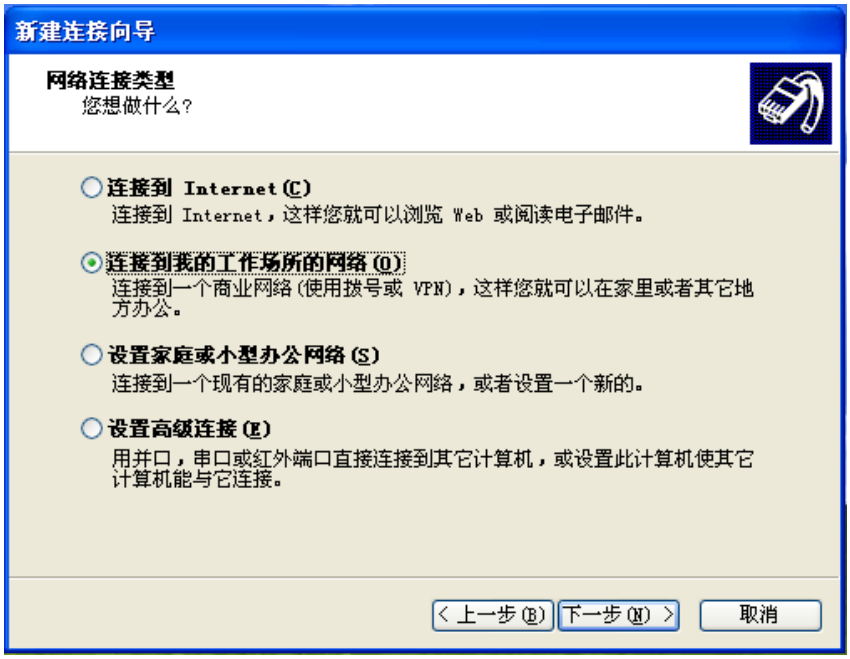


在“Attributes to check before granting access”框中添加属性“Service-Type”，属性值选“Framed”，点击“Commit Change”按钮即可完成配置。

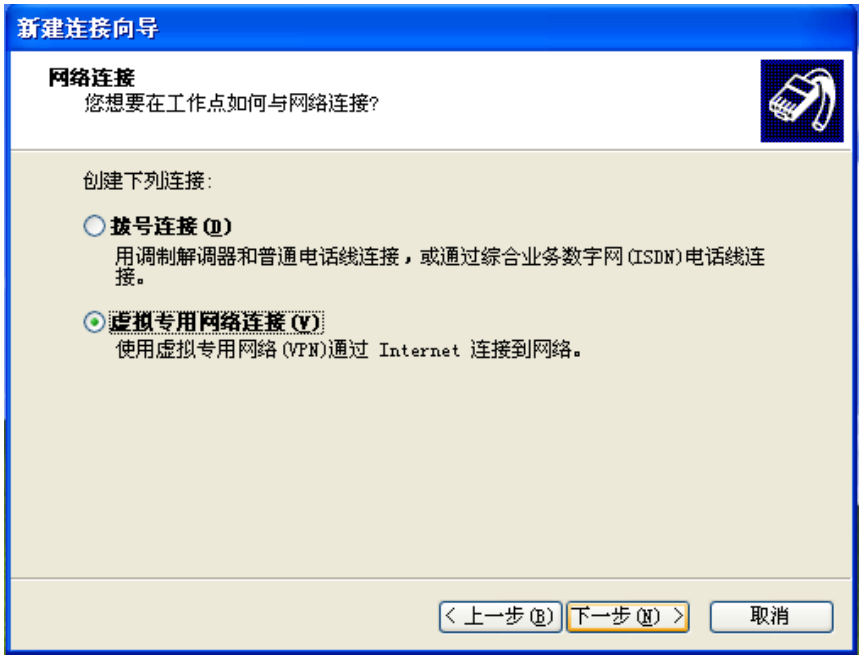
3.5.3 用户端配置

以 Windows xp 系统为例，创建一个新的连接，进入新建连接向导，点击“下一步”。

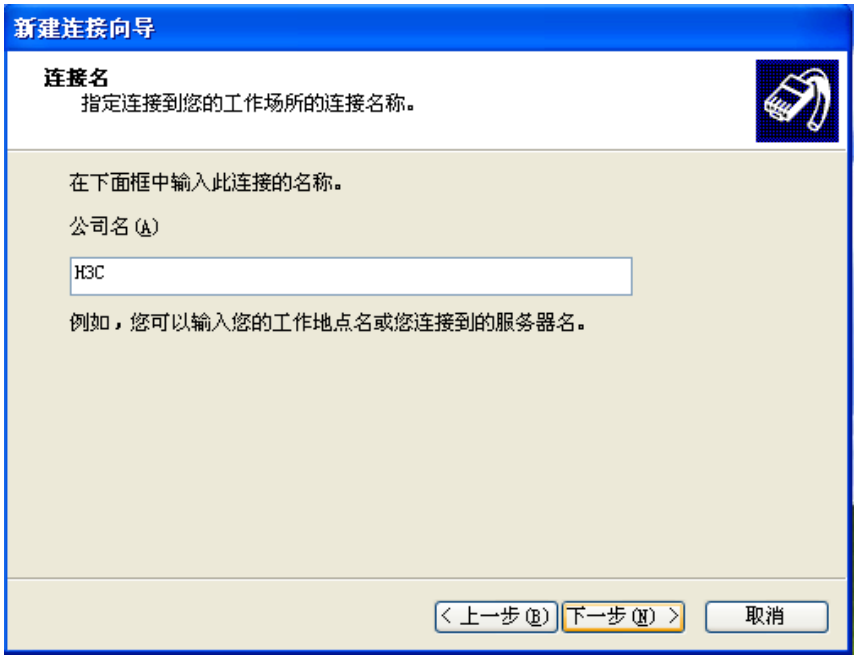
选择“连接到我的工作场所的网络”，点击“下一步”。



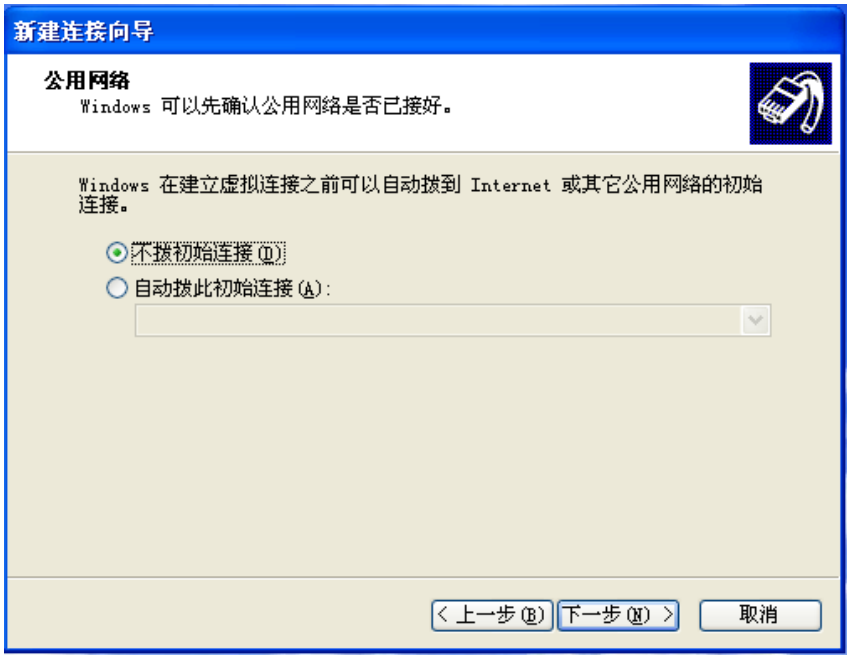
选择“虚拟专用网络连接”，然后点击“下一步”。



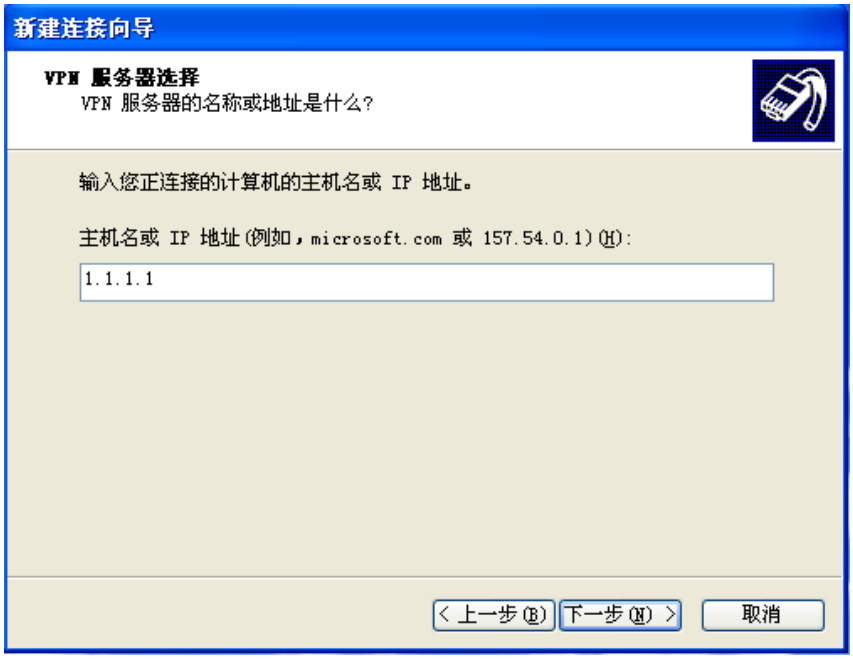
输入“连接名”，自定义即可。



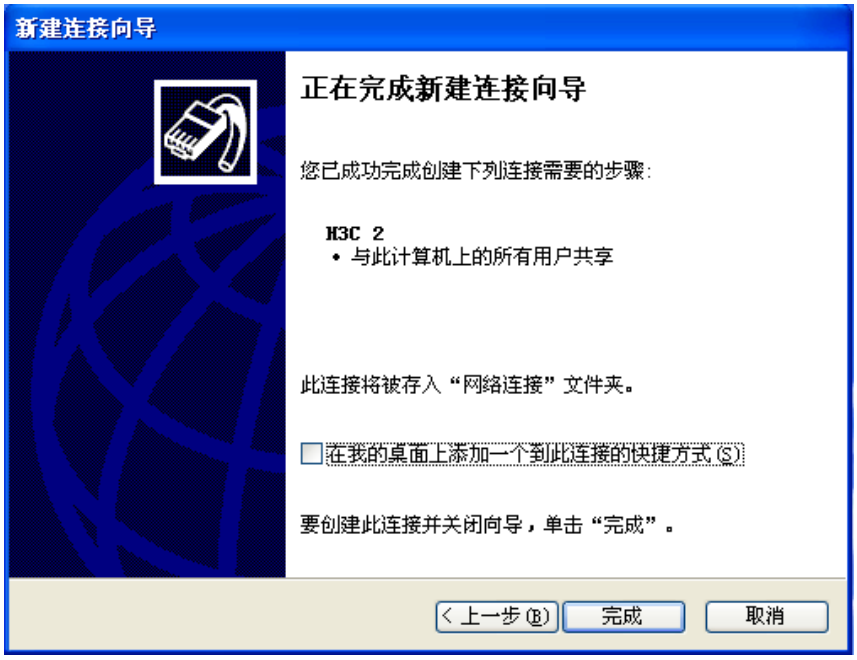
选择“不拨初始连接”。



VPN 服务器选择，输入路由器侧的 IP 地址 1.1.1.1，输入完毕后选择“下一步”。

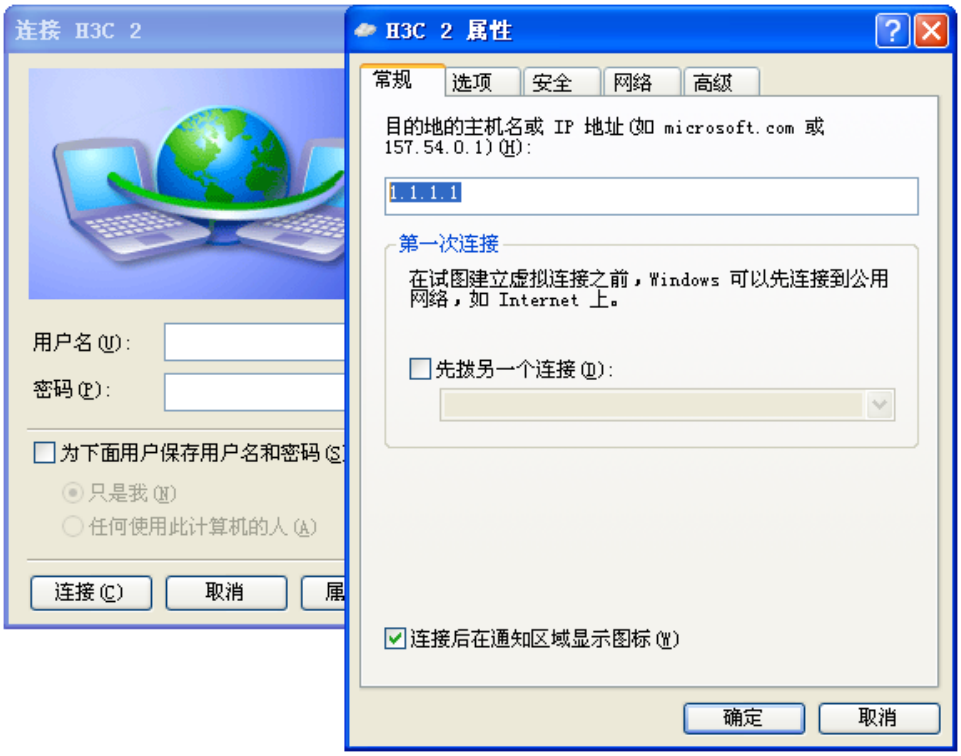


点击“完成”。可见成功创建了连接“H3C”，“H3C”正是刚才填写的连接名。

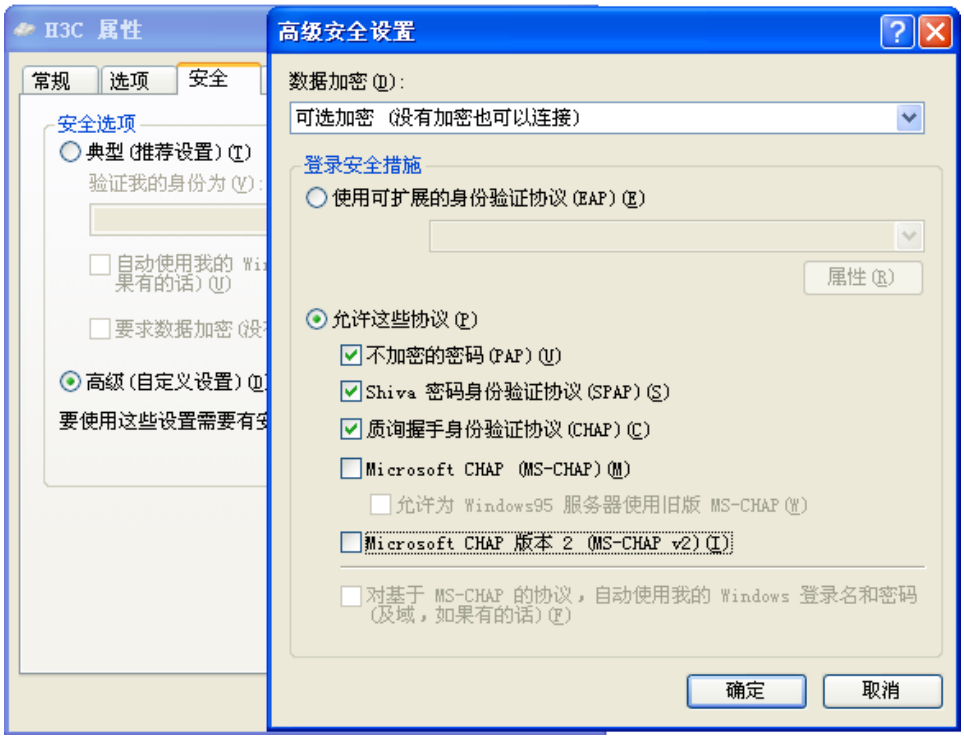


再次进入网络连接。发现新生成了一个网络连接“H3C”，双击之后会出现登陆窗口。

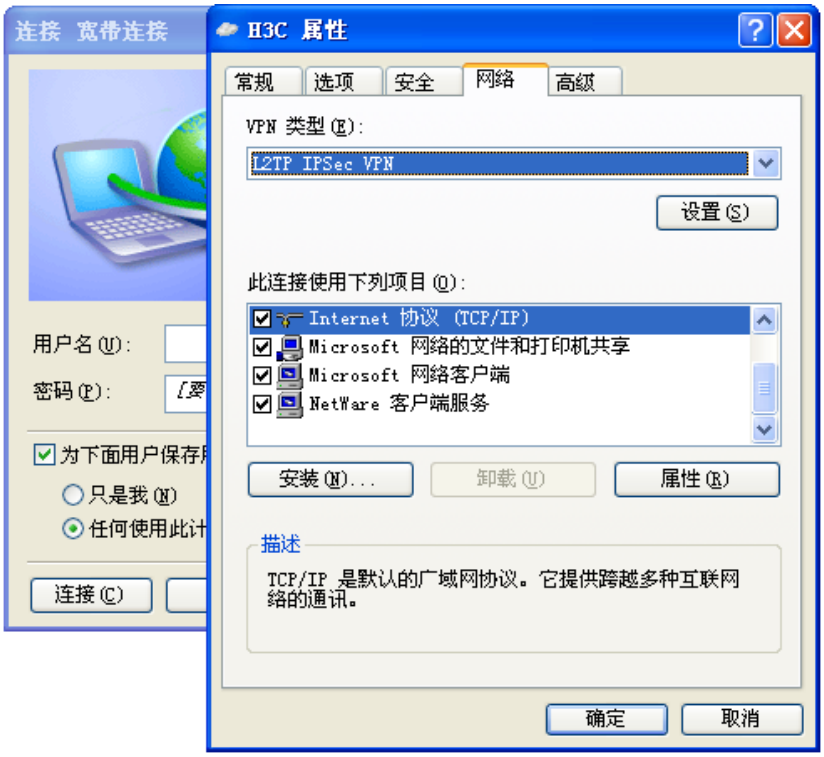
配置“属性”，点击“常规”选项。



配置“安全”，选择“高级（自定义设置）”，“IPSec 设置”暂时不用配置。

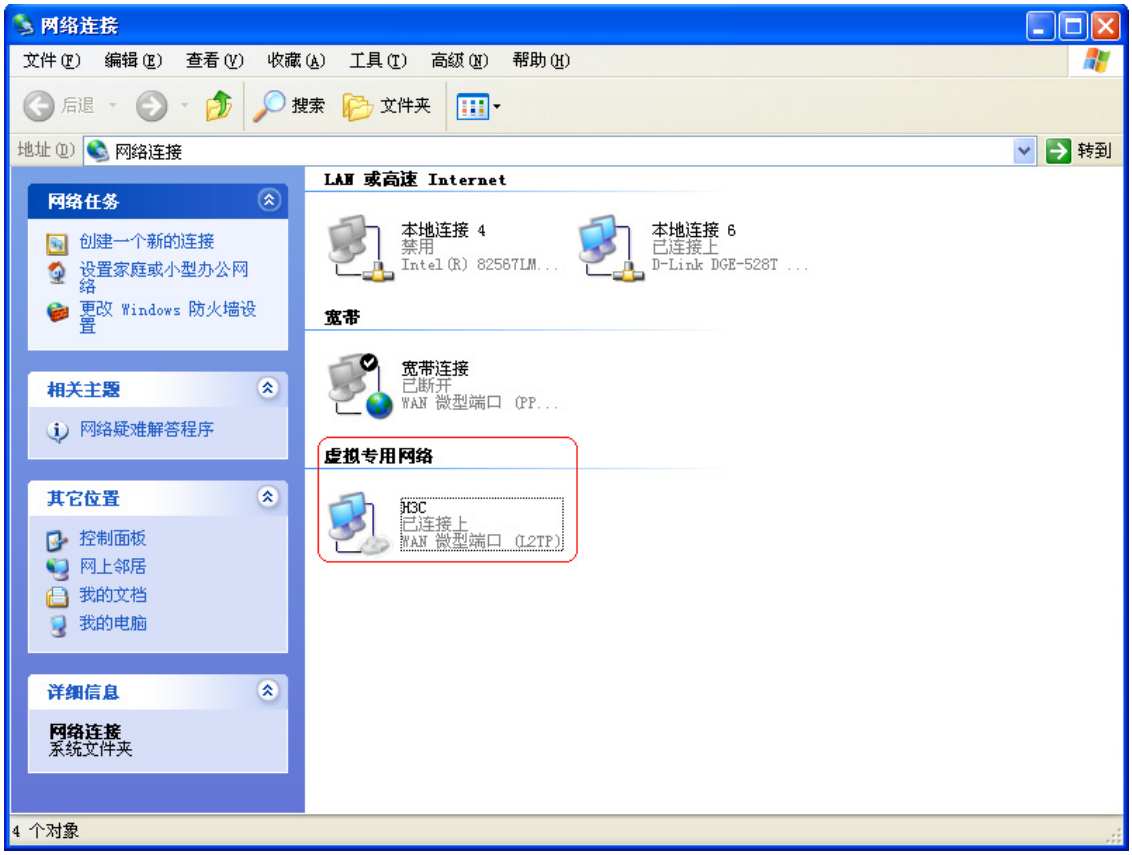


配置“高级安全设置”，选择 VPN 类型是“L2TP IPSec VPN”，“允许这些协议（U）”选择对应的多选框，配置完毕，返回登录窗口。



在登录窗口中输入在路由器设备上配置的用户名和密码：user1 和 hello，点击“连接”。

连接成功。



3.6 验证配置

在客户端上虚拟专用网络远程拨号，连接 L2TP 隧道，MSR 路由器显示如下：

```
<Router>
%Jul 25 20:04:06:807 2013 Router E IFNET/3/LINK_UPDOWN: Virtual-Template0:0 link
 status is UP.
%Jul 25 20:04:09:801 2013 Router E IFNET/5/LINEPROTO_UPDOWN: Line protocol on th
e interface Virtual-Template0:0 is UP.
%Jul 25 20:04:09:803 2013 Router E IFNET/5/PROTOCOL_UPDOWN: Protocol PPP IPCP on
 the interface Virtual-Template0:0 is UP.
<Router>
```

在 MSR 路由器上查看建立的 L2TP 隧道。

```
<Router> display l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        32        1.1.1.2          1701   1        h3c
```

在 MSR 路由器上查看建立的 L2TP 会话。

```
<Router> display l2tp session
 Total session = 1
```

```
 LocalSID  RemoteSID  LocalTID
  22581     1          1
```

3.7 配置文件

```
#
 l2tp enable
#
radius scheme shiva
 primary authentication 10.1.2.2 1645
 primary accounting 10.1.2.2 1646
 key authentication cipher $c$3$K0N41MIy1AUGIcNyqZbUHrPkaisbww==
 key accounting cipher $c$3$kwfSO/QLFf8dq0yoSWJNrwv15D4NiQ==
 user-name-format without-domain
#
domain h3c.com
 authentication ppp radius-scheme shiva
 authorization ppp radius-scheme shiva
 accounting ppp radius-scheme shiva
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 0 192.168.10.2 192.168.10.254
#
local-user user1
 password cipher $c$3$N30dbnObEXDlLX5gml/XwEx83KNUqIew
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 0
#
interface Virtual-Template0
 ppp authentication-mode pap domain h3c.com
 remote address pool 0
 ip address 192.168.10.1 255.255.255.0
#
interface ethernet0/0
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface ethernet0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
interface ethernet0/2
 port link-mode route
```

```
 ip address 10.1.2.1 255.255.255.0
#
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311