作者：豆豆老师

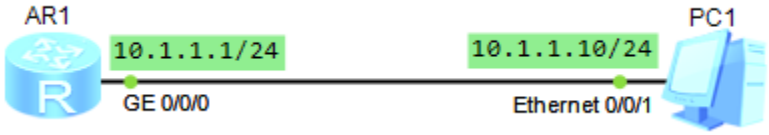
实验 3　配置通过 SSH 登陆设备

实验目的

- ✧ 理解 SSH 协议原理及功能
- ✧ 掌握配置通过 SSH 登录设备方法
- ✧ 掌握利用终端仿真软件 SSH 远程登陆到路由器的方法
- ✧ 掌握使用 Wireshark 捕获报文的方法

实验步骤

1 使用 eNSP 搭建如下拓扑图



2 基本配置（接口 IP 地址、路由器主机名等）

3 在 AR1 上配置 SSH，允许远程用户使用 SSH 远程管理设备

第 1 步：在路由器上开启 SSH 服务

第 2 步：配置用于 SSH 认证的用户名和密码

第 3 步：开启 SSH 认证服务

4 测试检查

5 利用 wireshark 抓包分析 SSH 协议

实验总结

作者：豆豆老师

实验配置详解

1 使用 eNSP 搭建拓扑图

2 基本配置（接口 IP 地址、路由器主机名等）

注意：测试路由器和主机的连通性

3 在 AR1 上配置 SSH，允许远程用户使用 SSH 远程管理设备

第 1 步：在路由器上开启 SSH 服务

[AR1]stelnet server enable

第 2 步：配置用于 SSH 认证的用户名和密码

[AR1]aaa

[AR1-aaa]local-user sshuser password cipher huawei123

[AR1-aaa]local-user sshuser privilege level 3

[AR1-aaa]local-user sshuser service-type ssh

[AR1-aaa]quit

第 3 步：开启 SSH 认证服务

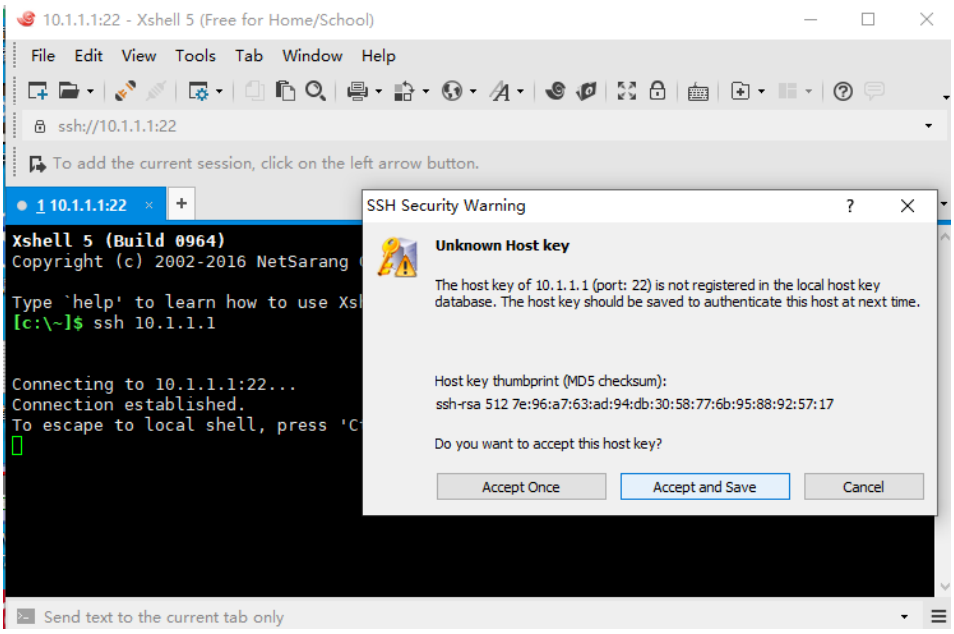
[AR1]user-interface vty 0 4

[AR1-ui-vty0-4]authentication-mode aaa

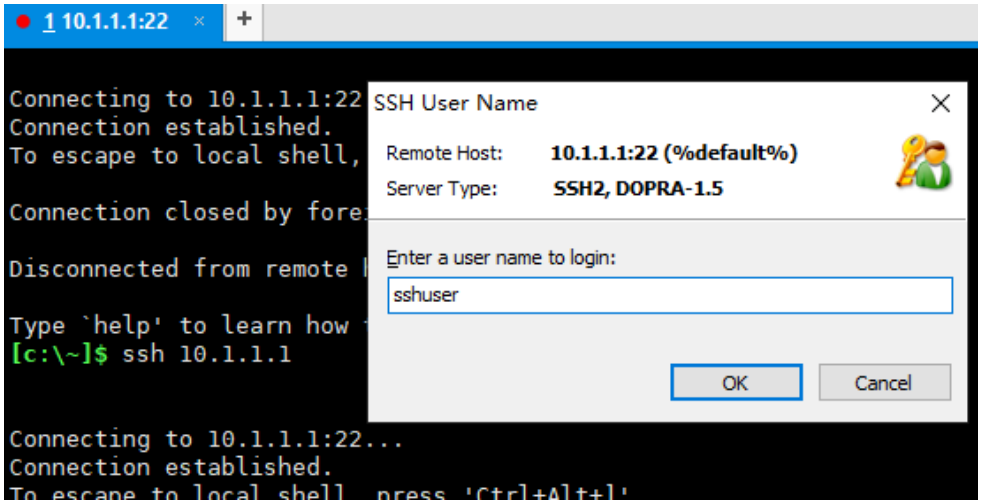
[AR1-ui-vty0-4]protocol inbound ssh

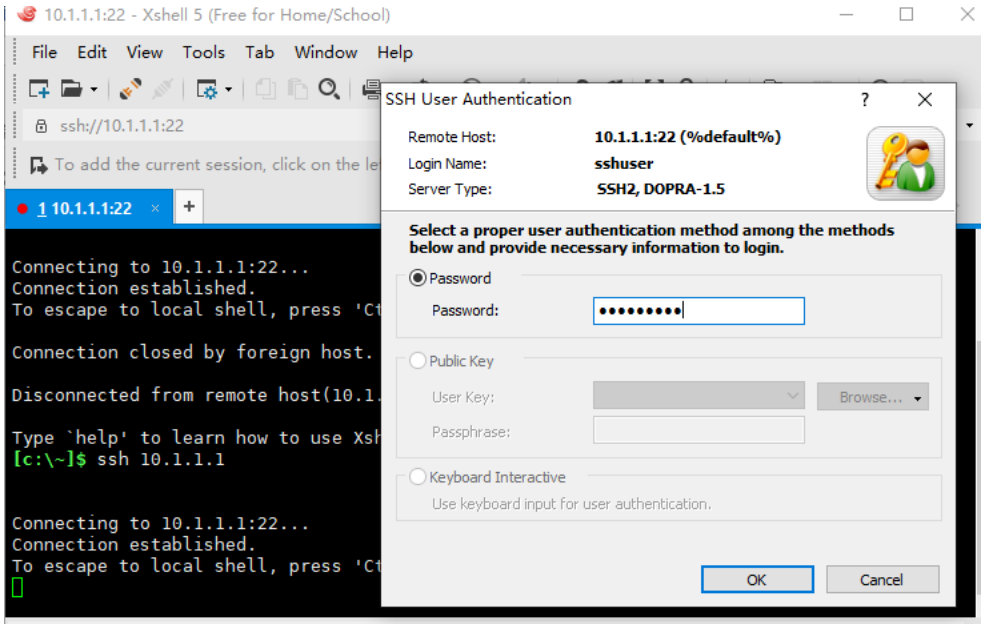
[AR1-ui-vty0-4]quit

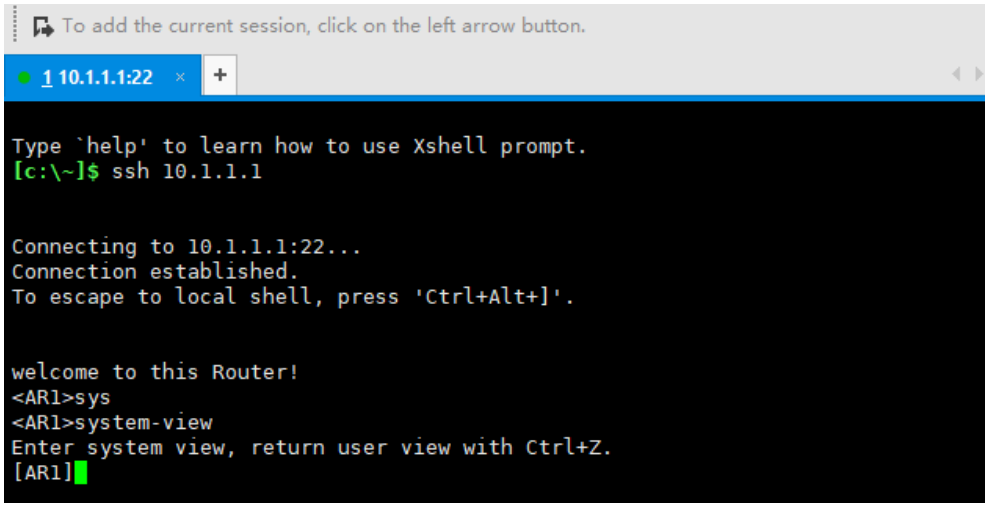
4 测试检查，在主机上使用 Xshell 终端软件 SSH 远程登陆到路由器上



作者：豆豆老师

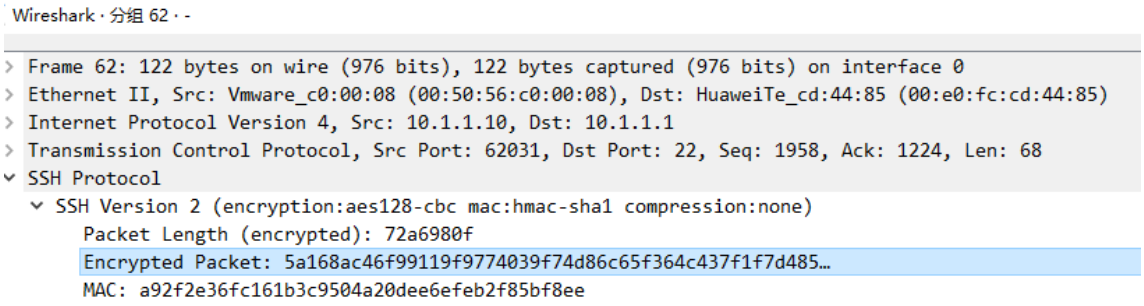

1 10.1.1.1:22
Connecting to 10.1.1.1:22
Connection established.
To escape to local shell,
Connection closed by fore
Disconnected from remote
Type `help' to learn how
[c:\~]$ ssh 10.1.1.1
SSH User Name
Remote Host: 10.1.1.1:22 (%default%)
Server Type: SSH2, DOPRA-1.5
Enter a user name to login:
sshuser
OK
Cancel
Connecting to 10.1.1.1:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'


10.1.1.1:22 - Xshell 5 (Free for Home/School)
File Edit View Tools Tab Window Help
ssh://10.1.1.1:22
To add the current session, click on the le
1 10.1.1.1:22
Connecting to 10.1.1.1:22...
Connection established.
To escape to local shell, press 'Ct
Connection closed by foreign host.
Disconnected from remote host(10.1.
Type `help' to learn how to use Xsh
[c:\~]$ ssh 10.1.1.1
Connecting to 10.1.1.1:22...
Connection established.
To escape to local shell, press 'Ct
SSH User Authentication
Remote Host: 10.1.1.1:22 (%default%)
Login Name: sshuser
Server Type: SSH2, DOPRA-1.5
Select a proper user authentication method among the methods below and provide necessary information to login.
Password
Password:
Public Key
User Key:
Browse...
Passphrase:
Keyboard Interactive
Use keyboard input for user authentication.
OK
Cancel


To add the current session, click on the left arrow button.
1 10.1.1.1:22
Type `help' to learn how to use Xshell prompt.
[c:\~]$ ssh 10.1.1.1
Connecting to 10.1.1.1:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
welcome to this Router!
<AR1>sys
<AR1>system-view
Enter system view, return user view with Ctrl+Z.
[AR1]

作者：豆豆老师

5 利用 wireshark 抓包分析 SSH 协议



重要知识点

SSH 协议的概述

SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组 (Network Working Group) 所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台。SSH 在正确使用时可弥补网络中的漏洞。SSH 客户端适用于多种平台。几乎所有 UNIX 平台—包括 HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix，以及其他平台—都可运行 SSH。

传统的网络服务程序，如：ftp、pop 和 telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的， 就是很容易受到“中间人”（man-in-the-middle）这种方式的攻击。所谓“中间人”的攻击方式， 就是“中间人”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。 服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。 通过使用 SSH，你可以把所有传输的数据进行加密，这样"中间人"这种攻击方式就不可能实现了，而且也能够防止 DNS 欺骗和 IP 欺骗。使用 SSH，还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、PoP、甚至为 PPP 提供一个安全的"通道"。