

# 网络运维管理

## 第3讲：园区网设备的远程管理

许成刚

---

## 一、网络设备管理的概念

# 网络设备管理的概念

---

## □ 概念

- 对于**可网管型**的网络设备，例如交换机、路由器、防火墙等，网管人员可以通过一定的方式，**登录进设备的系统**，对该设备的运行状况进行检查，并对各种参数进行配置，从而满足网络通信的需求。
- 各种网络设备的详细配置过程比较复杂，命令繁多，而且具体的配置方法会因不同种类的设备、同种设备的不同品牌、不同系列而有所不同。具体的管理过程和管理命令可以参考设备的官方文档。

---

## 二、首次登录网络设备

# 首次登录网络设备

---

## □ 首次登录

- 对于一台新出厂的设备，如果希望进入它的命令行界面完成基本业务配置，必须先完成首次登录（第一次上电）。
- 首次登录时的**特点？以交换机为例**
  - 无IP地址，无法通过TCP/IP协议访问

# 首次登录网络设备

---

## □ Console口登录应用场景

- 当对设备进行第一次配置时，可以通过Console口登录设备进行配置。
  - 网络设备中的一块主控板提供一个Console口。用户终端的串行口可以与设备Console口直接连接，实现对设备的本地配置。
- 当用户无法进行远程登录设备时，可通过Console口进行本地登录。

# 首次登录网络设备

---

## □ 通过Console口登录设备

- 在配置通过Console口登录设备之前，需要完成以下任务：
  - 设备正常上电。
  - 准备好Console通信电缆。
  - 准备好PC终端仿真软件。PC操作系统自带的终端仿真软件（如Windows 2000系统的超级终端），或第三方终端仿真软件

# Console口

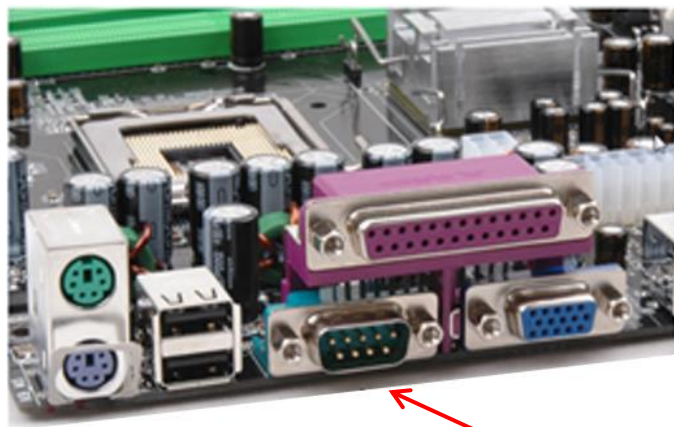


DB-9格式的Console口





# Console口与Console线



COM口



Console线



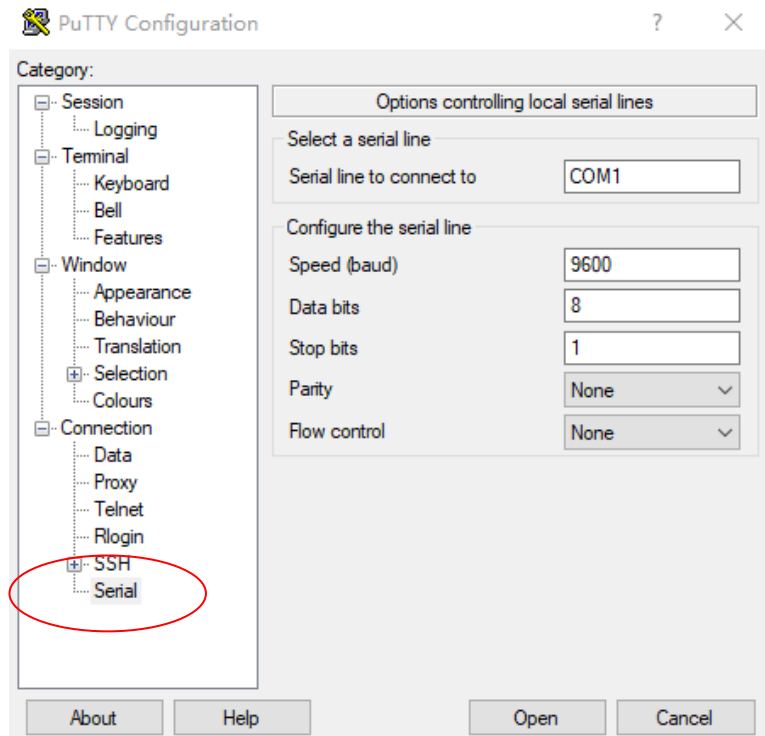
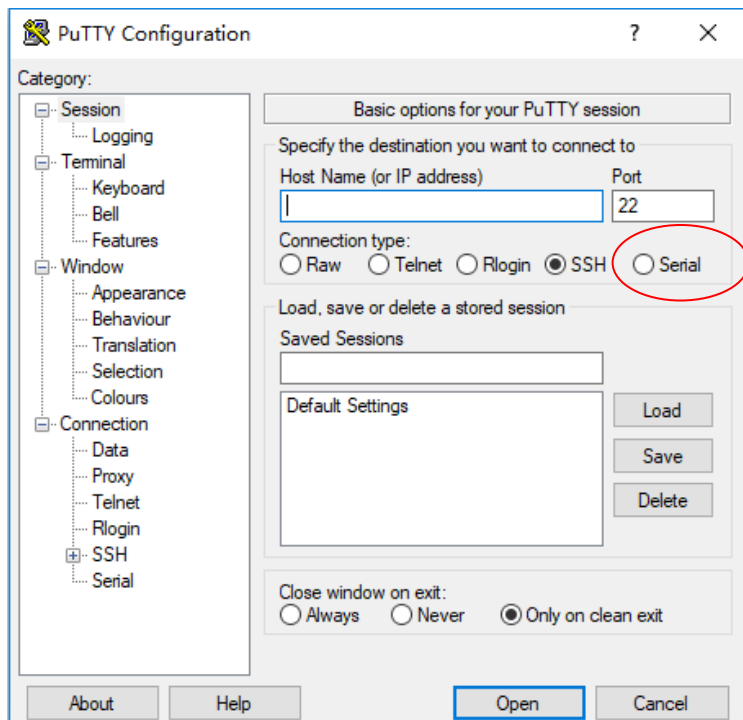
console口

## 终端仿真软件



Windows2000自带的超级终端软件

# 终端仿真软件



第三方软件：Putty

# 首次登录网络设备

---

## □ 应用说明

- 通过Console口进行本地登录是登录设备最基本的方式，也是其他登录方式的基础。
- 缺省情况下，用户可以直接通过Console口本地登录设备，不需要IP地址

# 首次登录网络设备

---

## □ 优点

- 使用专门的Console通信线缆连接，保证可以对设备有效控制。

## □ 缺点

- 不能远程登录维护设备。

---

### 三、Telnet方式登录网络设备

# Telnet方式登录网络设备

---

## □ Telnet概念

- Telnet协议在TCP/IP协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。
- 以服务器/客户端（Server/Client）模式工作，Telnet客户端向Telnet服务器发起请求，Telnet服务器提供Telnet服务。网络设备支持Telnet客户端和Telnet服务器功能，既可以作为Telnet服务器，也提供Telnet客户端服务。

# Telnet方式登录网络设备

---

## □ 应用场景

- 可将用户终端（即管理机）连接到网络上，使用Telnet方式登录设备，进行本地或远程的配置。
- 应用在对安全性要求不高的网络。



# Telnet方式登录网络设备

---

## □ 应用说明

- 缺省情况下，用户不能通过Telnet方式直接登录设备，若需要通过Telnet方式登录，可先通过Console口本地登录设备，并完成以下配置：
  - 确保终端和登录的设备之间路由可达（缺省情况下，设备上没有配置IP地址）。
  - 配置Telnet服务器功能及参数。
  - 配置Telnet用户登录的用户界面。

# Telnet方式登录网络设备

---

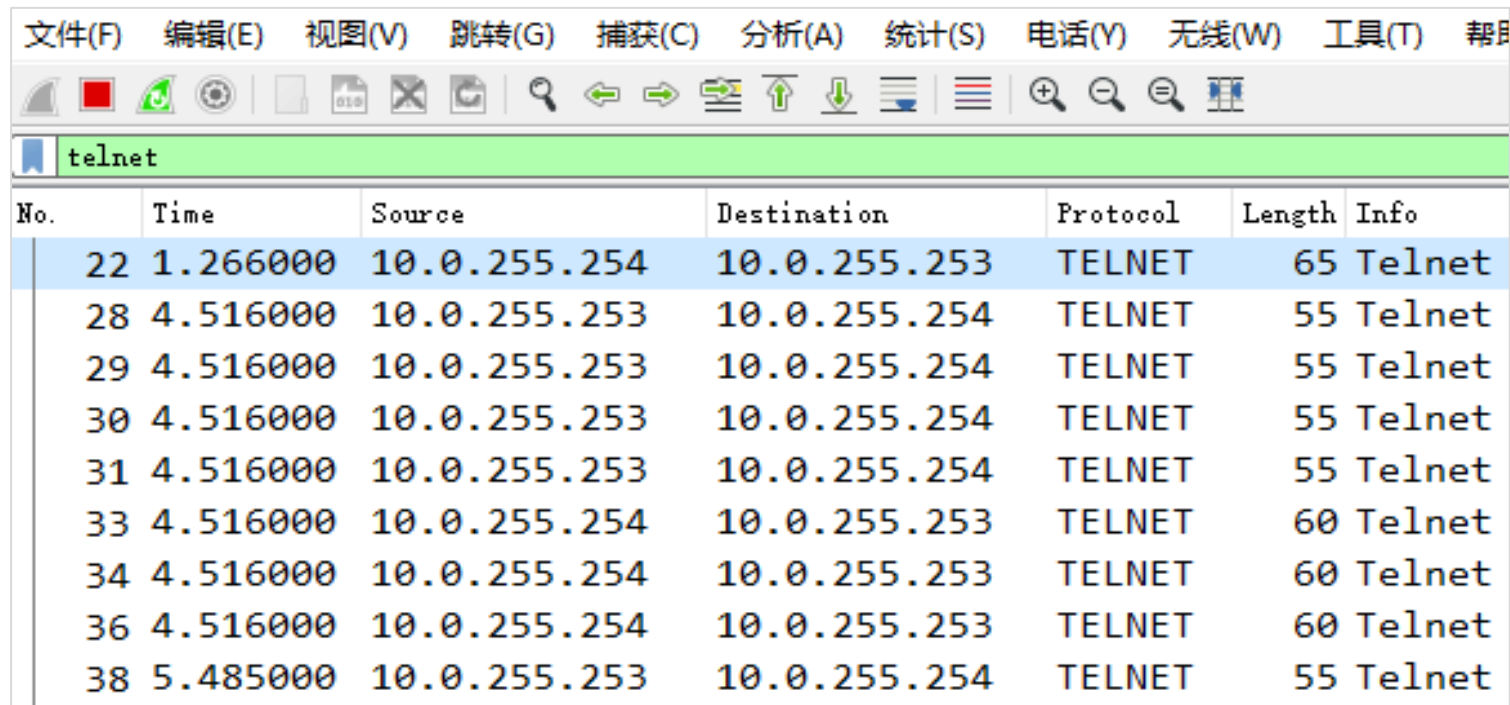
## □ 优点

- 便于对设备进行远程管理和维护，不需要为每一台设备都连接一个管理终端，方便了用户的操作。

## □ 缺点

- 由于Telnet缺少安全的认证方式，而且采用了TCP的明文传输，存在很大安全隐患，单纯提供Telnet服务容易导致主机IP地址欺骗、路由欺骗等恶意攻击，存在安全隐患。

# Telnet方式登录网络设备



The image shows a Wireshark network traffic capture window. The title bar includes menu items: 文件(F), 编辑(E), 视图(V), 跳转(G), 捕获(C), 分析(A), 统计(S), 电话(Y), 无线(W), 工具(T), 帮助(H). The toolbar contains various icons for file operations, search, and display. The active tab is labeled 'telnet'. The main display area shows a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
22	1.266000	10.0.255.254	10.0.255.253	TELNET	65	Telnet
28	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet
29	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet
30	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet
31	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet
33	4.516000	10.0.255.254	10.0.255.253	TELNET	60	Telnet
34	4.516000	10.0.255.254	10.0.255.253	TELNET	60	Telnet
36	4.516000	10.0.255.254	10.0.255.253	TELNET	60	Telnet
38	5.485000	10.0.255.253	10.0.255.254	TELNET	55	Telnet

# Telnet方式登录网络设备

No.	Time	Source	Destination	Protocol	Length	Info
22	1.266000	10.0.255.254	10.0.255.253	TELNET	65	Telnet
28	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet

```

> Internet Protocol Version 4, Src: 10.0.255.254, Dst: 10.0.255.
> Transmission Control Protocol, Src Port: 23, Dst Port: 58496,
v Telnet
  Data: \r\n
  Data: Username:
  
```

← 表示从该报文开始输入用户名

No.	Time	Source	Destination	Protocol	Length	Info
28	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet
29	4.516000	10.0.255.253	10.0.255.254	TELNET	55	Telnet

```

> Internet Protocol Version 4, Src: 10.0.255.253, Dst: 10.0.255.
> Transmission Control Protocol, Src Port: 58496, Dst Port: 23,
v Telnet
  Data: u
  
```

← 明文显示用户名的第1个字母“u”

---

## 四、STelnet方式 (SSH) 登录网络设备

# STelnet方式 (SSH) 登录网络设备

---

## □ 概念

- STelnet是Secure Telnet的简称。在一个传统不安全的网络环境中，服务器通过对用户**登录认证**及**双向的数据加密**，为终端用户提供安全的Telnet服务。
- 相对于Telnet，STelnet基于SSH协议，客户端和服务端之间经过协商，建立安全连接，客户端可以像操作Telnet一样登录服务器端。

# STelnet方式 (SSH) 登录网络设备

---

## □ SSH协议

- SSH提供了两种登录验证方法：
  - 基于口令的安全验证：Password验证。
  - 基于密钥的安全验证：RSA、DSA认证。

# STelnet方式 (SSH) 登录网络设备

---

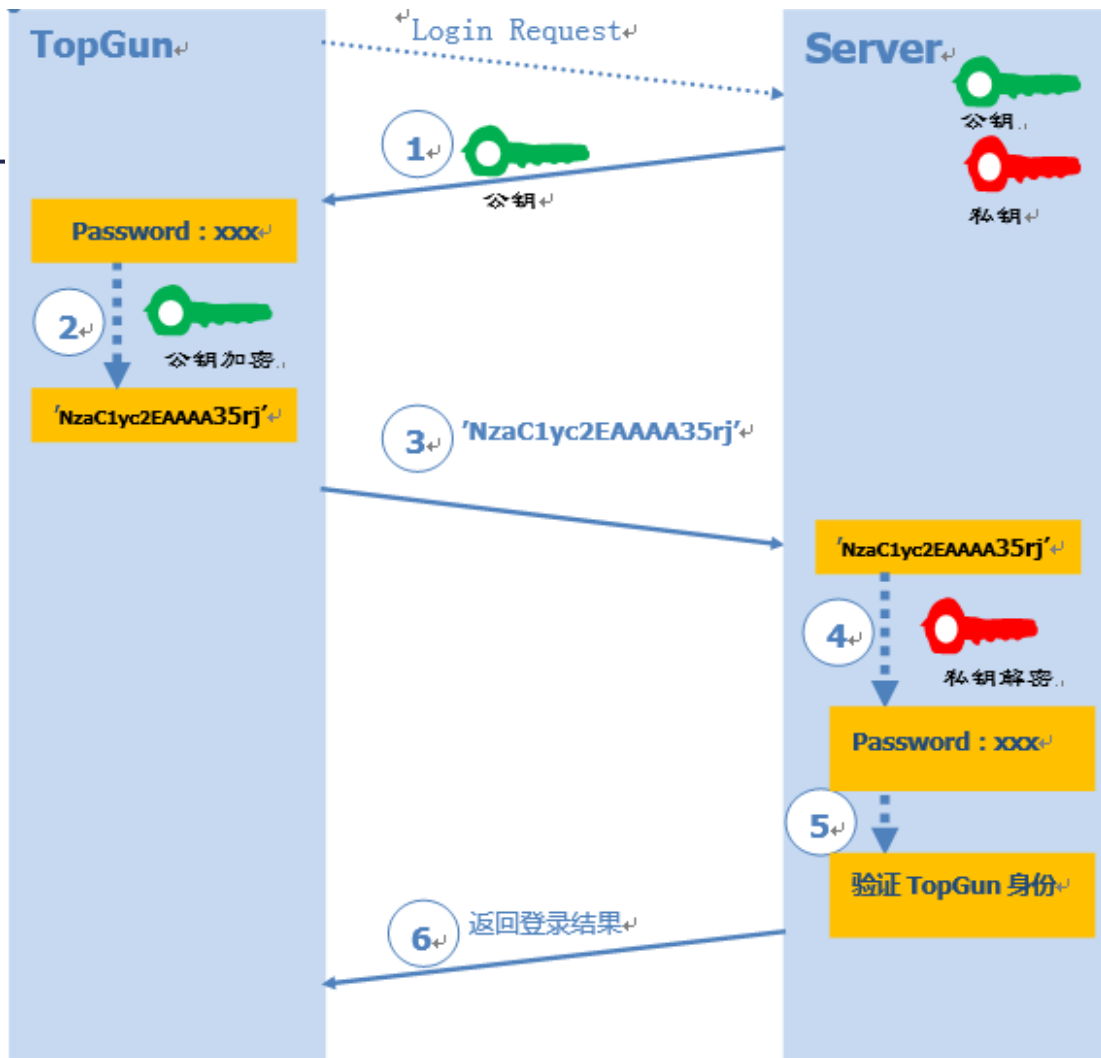
## □ Password验证

- 通过帐号和口令，登录到远程设备（主机）。所有传输的数据都会被加密：
  - 远程设备生产本地密钥对，公钥和私钥；
  - 远程设备收到用户的登录请求，把自己的公钥发给用户。
  - 用户使用这个公钥，将登录密码加密后，发送回来。
  - 远程设备用自己的私钥，解密登录密码，然后与自己保存的账号密码对比，如果密码正确，就同意用户登录。



## Password验证

客户端



网络设备

## Password验证登录方式——抓包分析（登录交换机SW-2, 10.0.255.2）

No.	Time	Source	Destination	Protocol	Length	Info
42	13.188000	10.0.255.253	10.0.255.2	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.72)
43	13.235000	10.0.255.2	10.0.255.253	SSHv2	65	Server: Protocol (SSH-1.99--)
44	13.235000	10.0.255.2	10.0.255.253	SSHv2	366	Server: Key Exchange Init
46	13.235000	10.0.255.253	10.0.255.2	TCP	590	62046 → 22 [ACK] Seq=29 Ack=324 Win=65069 Len=536 [.
48	13.235000	10.0.255.253	10.0.255.2	SSHv2	150	Client: Key Exchange Init
49	13.235000	10.0.255.253	10.0.255.2	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
52	13.281000	10.0.255.2	10.0.255.253	SSHv2	206	Server: Diffie-Hellman Group Exchange Group
53	13.281000	10.0.255.253	10.0.255.2	SSHv2	198	Client: Diffie-Hellman Group Exchange Init
56	13.703000	10.0.255.2	10.0.255.253	SSHv2	374	Server: Diffie-Hellman Group Exchange Reply
57	13.703000	10.0.255.2	10.0.255.253	SSHv2	70	Server: New Keys
65	15.922000	10.0.255.253	10.0.255.2	SSHv2	106	Client: New Keys, Encrypted packet (len=36)
66	15.922000	10.0.255.253	10.0.255.2	SSHv2	142	Client: Encrypted packet (len=88)
67	15.953000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
102	26.281000	10.0.255.253	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)
103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
121	35.610000	10.0.255.253	10.0.255.2	SSHv2	354	Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)
123	35.672000	10.0.255.253	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)
124	35.719000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
125	35.719000	10.0.255.253	10.0.255.2	SSHv2	242	Client: Encrypted packet (len=188)
127	35.766000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)
128	35.766000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)
130	35.875000	10.0.255.2	10.0.255.253	SSHv2	250	Server: Encrypted packet (len=196)
131	35.875000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)

# Password验证登录方式——抓包分析 (1) —— 传递公钥

No.	Time	Source	Destination	Protocol	Length	Info
42	13.188000	10.0.255.253	10.0.255.2	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.72)
43	13.235000	10.0.255.2	10.0.255.253	SSHv2	65	Server: Protocol (SSH-1.99--)
44	13.235000	10.0.255.2	10.0.255.253	SSHv2	366	Server: Key Exchange Init
46	13.235000	10.0.255.253	10.0.255.2	TCP	590	62046 → 22 [ACK] Seq=29 Ack=324 Win=65069 Len=536 [.
48	13.235000	10.0.255.253	10.0.255.2	SSHv2	150	Client: Key Exchange Init
49	13.235000	10.0.255.253	10.0.255.2	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
52	13.281000	10.0.255.2	10.0.255.253	SSHv2	206	Server: Diffie-Hellman Group Exchange Group
53	13.281000	10.0.255.253	10.0.255.2	SSHv2	198	Client: Diffie-Hellman Group Exchange Init
56	13.703000	10.0.255.2	10.0.255.253	SSHv2	374	Server: Diffie-Hellman Group Exchange Reply
57	13.703000	10.0.255.2	10.0.255.253	SSHv2	70	Server: New Keys
65	15.922000	10.0.255.253	10.0.255.2	SSHv2	106	Client: New Keys, Encrypted packet (len=36)
66	15.922000	10.0.255.253	10.0.255.2	SSHv2	142	Client: Encrypted packet (len=88)
67	15.953000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)

## 操作:

通过PuTTY输入网络设备的IP地址并点击“open”

## 效果:

- 1、建立连接
- 2、把网络设备的公钥发给客户端

Diffie-Hellman密钥协商  
算法主要解决秘钥配送  
问题

ssh-rsa 2048 36:8c:e4:0c:19:7d:a7:d4:c3:6d:5f:c2:cf:64:b9:3e  
If you trust this host, hit Yes to add the key to  
PuTTY's cache and carry on connecting.  
If you want to carry on connecting just once, without  
adding the key to the cache, hit No.  
If you do not trust this host, hit Cancel to abandon the  
connection.

 是(Y)

 否(N)

 取消

 帮助

## Password验证登录方式——抓包分析 (2) —— 验证用户名

66	15.922000	10.0.255.253	10.0.255.2	SSHv2	142	Client: Encrypted packet (len=88)
67	15.953000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
102	26.281000	10.0.255.253	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)
103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
121	35.610000	10.0.255.2	10.0.255.2	SSHv2	354	Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)

客户端输入用户名，  
网络设备返回结果

操作：

输入用户名 “user\_ssh”

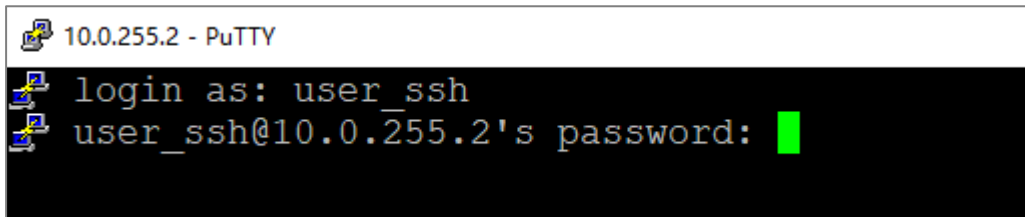


图1

效果：

- 1、若正确，则网络设备返回图1；
- 2、若不正确，则网络设备返回图2；

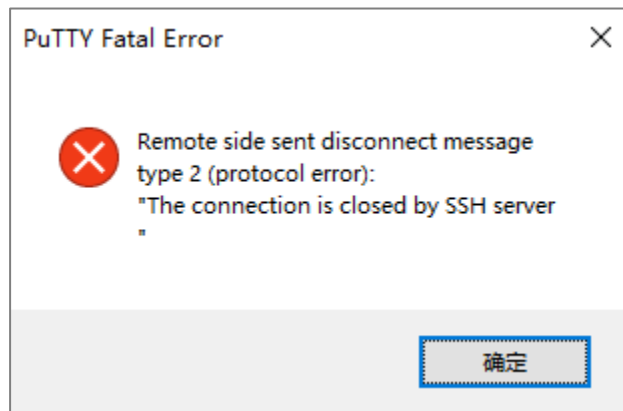


图2

# Password验证登录方式——抓包分析 (2) —— 验证用户名

No.	Time	Source	Destination	Protocol	Length	Info
67	15.953000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
102	26.281000	10.0.255.253	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)
103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
121	35.610000	10.0.255.253	10.0.255.2	SSHv2	354	Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)

Internet Protocol Version 4, Src: 10.0.255.253, Dst: 10.0.255.2

Transmission Control Protocol, Src Port: 62046, Dst Port: 22, Seq: 1500000000, Len: 104

SSH Protocol

SSH Version 2 (encryption:aes128-cbc mac:hmac-sha1 compression:none)

Packet Length (encrypted): b0b6e972

Encrypted Packet: b2b0e112780e1b178de762b81a121363f2e0f79d40486992...

MAC: 09e647ed9a1aedcf421059e88d6035034c9cc8ba

```

0000  4c 1f cc 8c 1b 1b 0a 00 27 00 00 11 08 00 45 00  L.....'.....E.
0010  00 90 65 8f 00 00 80 06 c1 d8 0a 00 ff fd 0a 00  ..e.....
0020  ff 02 f2 5e 00 16 50 9d 29 45 9f 78 42 cd 50 18  ...^..P.)E.xB.P.
0030  ff 3c c8 8c 00 00 b0 b6 e9 72 b2 b0 e1 12 78 0e  .<.....r....x.
0040  1b 17 8d e7 62 b8 1a 12 13 63 f2 e0 f7 9d 40 48  ...b...c....@H
0050  69 92 e3 48 a3 4f 03 53 bf 4d 88 e9 cc 40 2a ab  i..H.O.S.M...@*
0060  e7 e1 95 f6 14 a0 81 1b 25 7a 63 71 94 79 fa df  ....%zcq.y..
0070  13 75 3e 0f 40 51 e8 ee 8e b0 30 24 ad ca 9f 2c  .u>.@Q..0$...
0080  3b ed 22 2a b4 8f 3e bc f8 2e 09 e6 47 ed 9a 1a  ;"*...>....G...
0090  ed cf 42 10 59 e8 8d 60 35 03 4c 9c c8 ba      ..B.Y..`5.L...

```

客户端发往网络设备

Encrypted Packet:  
b2b0e112780e1.....

加密的报文

## Password验证登录方式——抓包分析 (2) —— 验证用户名

ssh

No.	Time	Source	Destination	Protocol	Length	Info
67	15.953000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
102	26.281000	10.0.255.253	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)
103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
121	35.610000	10.0.255.253	10.0.255.2	SSHv2	354	Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)

网络设备发往客户端

Encrypted Packet:  
fe3982b8194e.....

Internet Protocol Version 4, Src: 10.0.255.2, Dst: 10.0.255.253  
 Transmission Control Protocol, Src Port: 22, Dst Port: 62046  
 SSH Protocol  
 SSH Version 2 (encryption:aes128-cbc mac:hmac-sha1 compression:none)  
 Packet Length (encrypted): b75b5a48  
 Encrypted Packet: fe3982b8194e2fc520e732d103e1c61d715210a544aa340c...  
 MAC: 61f49117172eee7065dca5084019db71b66fb8a0

```

0000  0a 00 27 00 00 11 4c 1f  cc 8c 1b 1b 08 00 45 c0  ..'...L. ....E.
0010  00 5c 00 0b 00 00 fe 06  a8 d0 0a 00 ff 02 0a 00  .\.....
0020  ff fd 00 16 f2 5e 9f 78  42 cd 50 9d 29 ad 50 18  .....^x B.P.)P.
0030  a0 00 a2 20 00 00 b7 5b  5a 48 fe 39 82 b8 19 4e  ... ..[ ZH.9...N
0040  2f c5 20 e7 32 d1 03 e1  c6 1d 71 52 10 a5 44 aa  /. .2... ..qR..D.
0050  34 0c 98 66 f0 d0 61 f4  91 17 17 2e ee 70 65 dc  4..f..a. ....pe.
0060  a5 08 40 19 db 71 b6 6f  b8 a0  ..@..q.o ..
  
```

也是加密的报文

## Password验证登录方式——抓包分析 (3) —— 验证密码

103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106 Server: Encrypted packet (len=52)
121	35.610000	10.0.255.253	10.0.255.2	SSHv2	354 Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90 Server: Encrypted packet (len=36)
123	35.672000	10.0.255.253	10.0.255.2	SSHv2	158 Client: Encrypted packet (len=104)
124	35.719000	10.0.255.2	10.0.255.253	SSHv2	106 Server: Encrypted packet (len=52)
125	35.719000	10.0.255.253	10.0.255.2	SSHv2	242 Client: Encrypted packet (len=188)
127	35.766000	10.0.255.2	10.0.255.253	SSHv2	90 Server: Encrypted packet (len=36)
128	35.766000	10.0.255.2	10.0.255.253	SSHv2	90 Server: Encrypted packet (len=36)
130	35.875000	10.0.255.2	10.0.255.253	SSHv2	250 Server: Encrypted packet (len=196)
131	35.875000	10.0.255.2	10.0.255.253	SSHv2	106 Server: Encrypted packet (len=52)

**操作:**

输入密码 "abc@123"

**效果:**

- 1、若正确，则网络设备返回图1，已登录；
- 2、若不正确，则禁止登录；

```
10.0.255.2 - PuTTY
login as: user_ssh
user_ssh@10.0.255.2's password:

Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
The current login time is 2020-10-18 12:18:16.
<SW-2>
```

图1



# Password验证登录方式——抓包分析 (3) —— 验证密码

No.	Time	Source	Destination	Protocol	Length	Info
103	26.328000	10.0.255.2	10.0.255.253	SSHv2	106	Server: Encrypted packet (len=52)
121	35.610000	10.0.255.253	10.0.255.2	SSHv2	354	Client: Encrypted packet (len=300)
122	35.672000	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)
123	35.672000	10.0.255.2	10.0.255.2	SSHv2	158	Client: Encrypted packet (len=104)

Frame 121: 354 bytes captured on interface (2832 bits), 354 bytes captured (2832 bits) on interface 0:11 (0a:00:27:00:00:11), Dst: HuaweiTe\_8c...: 10.0.255.253, Dst: 10.0.255.2, Src Port: 62046, Dst Port: 22, Seq: 1609, Len: 354

SSH Version 2 (encryption:aes128-cbc mac:hmac-sha1 compression:none)  
 Packet Length (encrypted): e4c2874c  
 Encrypted Packet: 1acb330bea4cecee0aa7eb921a5643446c96c09b0b0da7de...  
 MAC: 50c7164be09cd90e5da40213948a52cfd9d320

```

0000  4c 1f cc 8c 1b 1b 0a 00 27 00 00 11 08 00 45 00  L.....'......E.
0010  01 54 65 91 00 00 80 06 c1 12 0a 00 ff fd 0a 00  .Te.....
0020  ff 02 f2 5e 00 16 50 9d 29 ad 9f 78 43 01 50 18  ...^..P.)..xC.P.
0030  ff 08 3d 7e 00 00 e4 c2 87 4c 1a cb 33 0b ea 4c  ..=~....L...3..L
0040  ec ee 0a a7 eb 92 1a 56 43 44 6c 96 c0 9b 0b 0d  ....V CD1....
0050  a7 de f7 89 97 15 26 d3 d7 0f 99 3d 6d 44 cc 55  ....&...=mD.U
0060  53 e8 11 62 1c c4 6a 60 bc 5a 52 ea 40 c7 8a 16  S..b..j`..ZR.@...
0070  03 0b 37 c8 9a 28 ac 5e 9f de 12 29 d3 19 ad e3  ..7..(^...)...
0080  b7 cf 1b 71 db 1c 91 0f 6e b8 4e 18 90 4b cb 0e  ...q....n.N..K..
0090  0b 29 d7 bb db f9 e2 da 24 8c e5 9c 78 f6 45 6e  .).....$....x.En
00a0  86 b4 85 c9 2c 98 a4 f9 db f7 4a 49 31 6e de 77  ....JIn.w
00b0  ea 8f 54 0b 42 bd c9 5f 44 65 21 c4 e2 92 a7 98  ..T.B...De!....
00c0  47 53 22 ec 67 c6 87 a9 03 1b c1 92 fb 31 2a f4  GS".g... ..1*.
00d0  dc 04 36 89 64 30 17 87 e6 75 03 2d ee a7 b6 03  ..6.d0...u-....
00e0  fb fc 9c e7 1b b7 0e 2a de 00 d0 63 3d a7 97 64  ....*...c=..d
00f0  72 88 f2 cd e1 49 cd c0 dd ae 7e 8c 33 71 36 46  r...I...~.3q6F
0100  d1 47 07 e8 f3 0b fc 6e 77 dd b7 a4 46 c9 ae 3c  .G....n w...F.<
0110  50 0d 08 77 27 7c dd bb 10 82 dd f8 b9 b7 4d ab  P..w'|... ..M.
0120  15 ba 70 de 41 32 93 02 e7 26 ab ed ba fc 62 90  ..p.A2...&....b.
0130  cc bc 8b bd f6 fa b5 65 fa 07 d2 c6 f5 3f 13 8b  ....e.....?.
0140  31 90 2b 96 1a eb cb 24 6c d9 02 6d ef 22 50 c7  1.+...$ l..m."P.
0150  16 4b e0 9c d9 0e 5d a4 02 13 94 8a 52 cf da 79  .K....]. ....R..y
0160  d3 20
  
```

客户端发往网络设备

Encrypted Packet:  
1acb330bea4c.....

也是加密的报文



# STelnet方式 (SSH) 登录网络设备

---

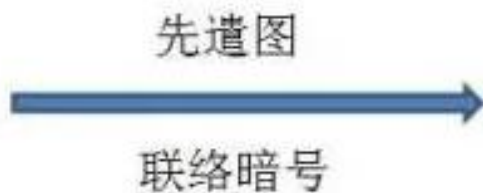
## □ Password验证

### ■ 中间人攻击:

- Password验证实施的时候存在一个风险：如果有人截获了用户的登录请求，然后冒充远程主机，将伪造的公钥发给用户，那么用户很难辨别真伪。
- 可以设想，如果攻击者插在用户与远程主机之间（比如在公共的wifi区域），用伪造的公钥，获取用户的登录密码。再用这个密码登录远程主机，那么SSH的安全机制就荡然无存了。这种风险就是著名的"中间人攻击" (Man-in-the-middle attack)。

## STelnet方式 (SSH) 登录网络设备

- 中间人攻击 (Man-in-the-middle attack) 。

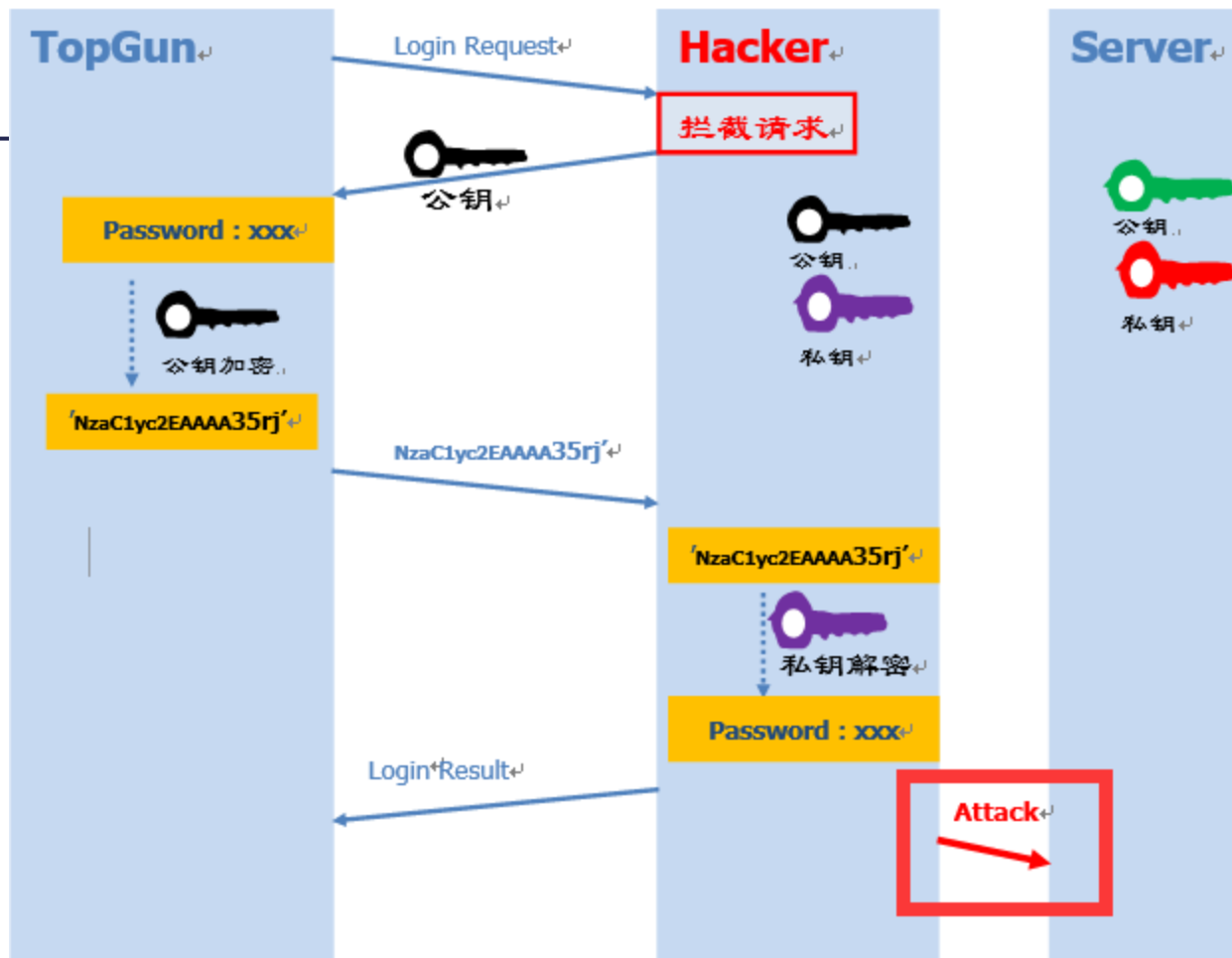


## STelnet方式 (SSH) 登录网络设备

- 中间人攻击 (Man-in-the-middle attack) 。

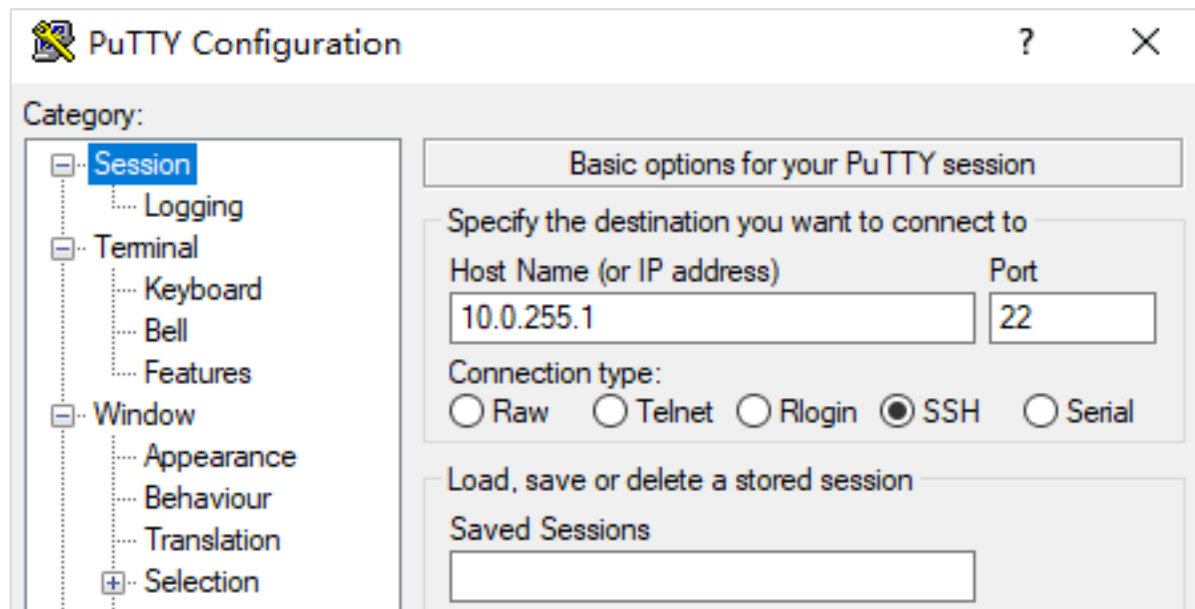


# 中间人攻击



# STelnet方式 (SSH) 登录网络设备

## □ Password验证



## ➤ Password验证：第一次登录远程设备时

“服务器的主机密钥未缓存在本地主机的注册表中，你不能保证该服务器就是你认为的计算机。该服务器的rsa2密钥指纹是：`ssh-rsa 2048 36:8c:e4:0c:19:7d:a7:d4:c3:6d:5f:c2:cf:64:b9:3e`。

如果你信任此主机，请点击【是】将其密钥添加到PuTTY的缓存中（记录在注册表中）并继续连接。如果你仅仅想连接一次并且不将密钥添加到PuTTY缓存中，请点击【否】。如果你不信任此主机，请按【取消】放弃连接。”



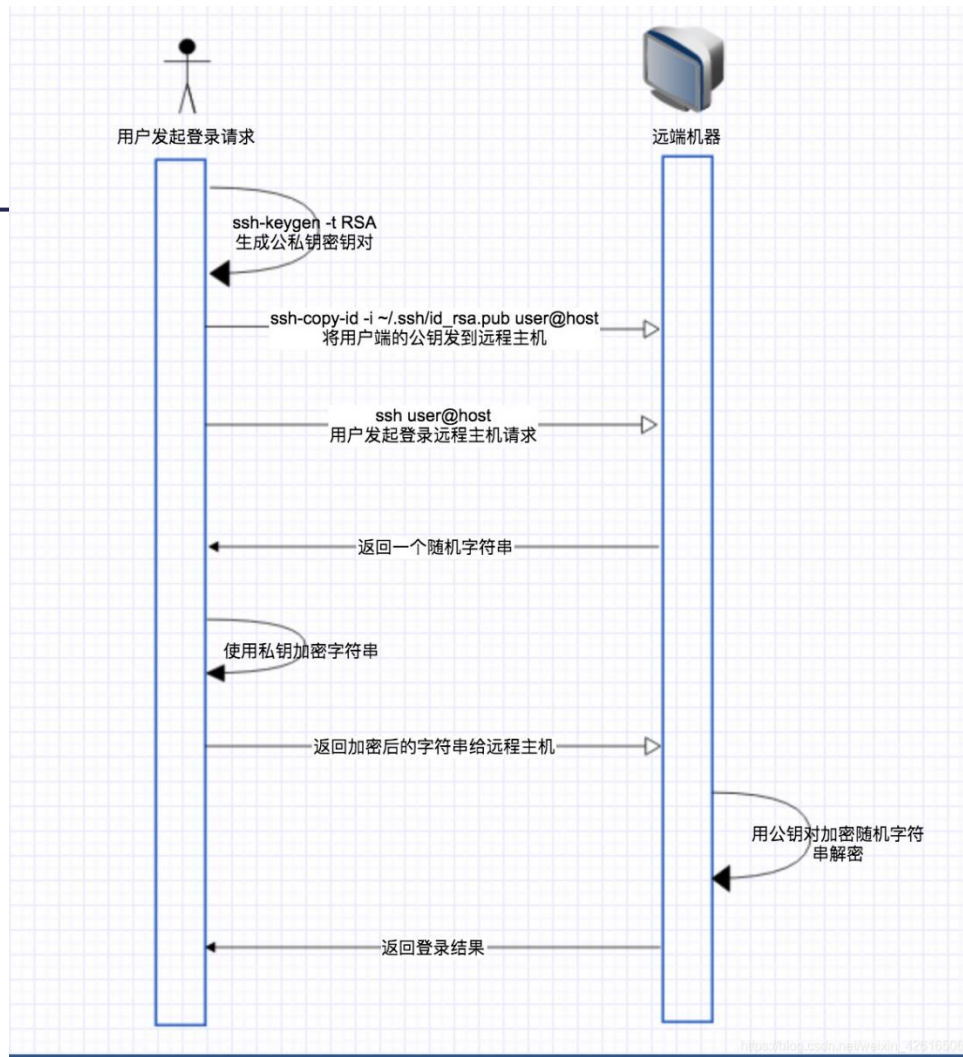
**基本含义：无法确认远程设备（Server）的真实性，只知道它的公钥指纹，问你还想继续连接吗？**

# STelnet方式 (SSH) 登录网络设备

## □ 密钥验证

- SSH还提供了公钥登录验证，可以省去输入密码的步骤。
  - 客户端生成密钥对（公钥和密钥），并把公钥存储在远程设备上；
  - 登录的时候，客户端软件向远程设备发出连接请求，远程设备收到请求之后，在本设备上寻找到该客户端的公钥，然后把它和客户端发送过来的公钥进行比较。
  - 如果两个密钥一致，远程设备就用公钥加密“质询”（一段随机字符），并把它发送给客户端。客户端收到“质询”之后就可以用自己的私钥解密。然后再用私钥加密“质询”，再把它发送给远程设备。
  - 远程设备再次用事先储存的客户端公钥解密，如果成功，就证明用户是可信的，直接允许登录，不再要求密码。

# 基于密钥验证





# STelnet方式 (SSH) 登录网络设备

---

## □ 说明

- 缺省情况下，用户不能通过STelnet方式直接登录设备。若需要通过STelnet方式登录设备，可以先通过Console口本地登录或Telnet远程登录设备，并完成以下配置：
  - 确保终端和登录的设备之间路由可达（缺省情况下，设备上没有配置IP地址）。
  - 配置STelnet服务器功能及参数。
  - 配置SSH用户登录的用户界面。
  - 配置SSH用户。

## STelnet方式 (SSH) 登录网络设备

---

### □ 优点

- 实现在不安全网络上提供安全的远程登录，保证了数据的完整性和可靠性，保证了数据的安全传输。

### □ 缺点

- 配置较为复杂

---

## 五、Web方式登录网络设备

# Web方式登录网络设备

---

## □ 概念

- 为了方便用户对设备的维护和使用，网络设备通常支持Web网管功能。设备内置一个Web服务器，与设备相连的终端（即管理机）可以通过Web浏览器访问设备。

# Web方式登录网络设备

---

## □ 说明

- (1) 确保网络设备已加载了Web网页文件。
- (2) 配置使能HTTP/HTTPS服务（缺省情况下，HTTP及HTTPS服务功能未使能）。
- (3) 配置HTTP用户（华为设备提供默认的HTTP用户，用户名：admin，密码：admin@huawei.com）。

Thanks.