网络运维管理

第3讲：园区网设备的远程管理

河南中医药大学信息技术学院
《网络运维管理》课程教学组

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查看，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

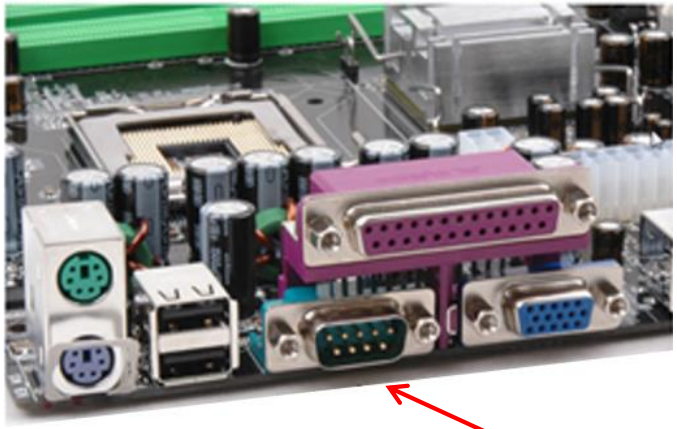
- 在配置通过Console口登录设备之前，需要完成以下任务：
  - 设备正常上电。
  - 准备好Console通信电缆。
  - 准备好PC终端仿真软件。PC操作系统自带的终端仿真软件（如Windows 2000系统的超级终端），或第三方终端仿真软件

Console口

DB-9格式的Console口

电脑上的COM口

Console口与Console线

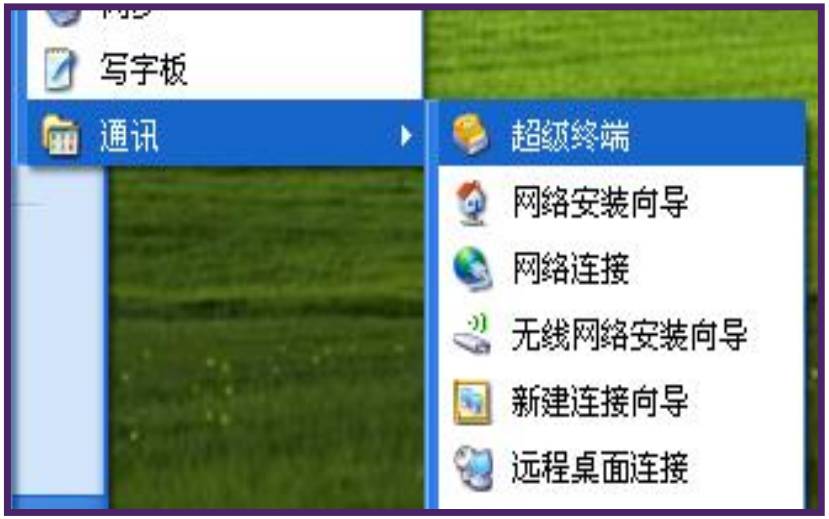


COM口

Console线

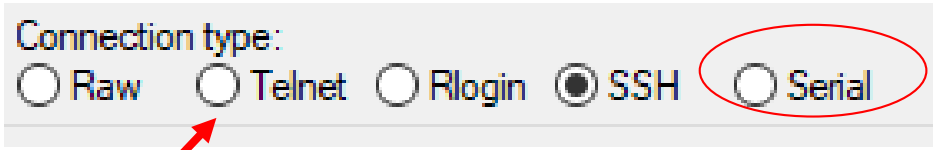
console口

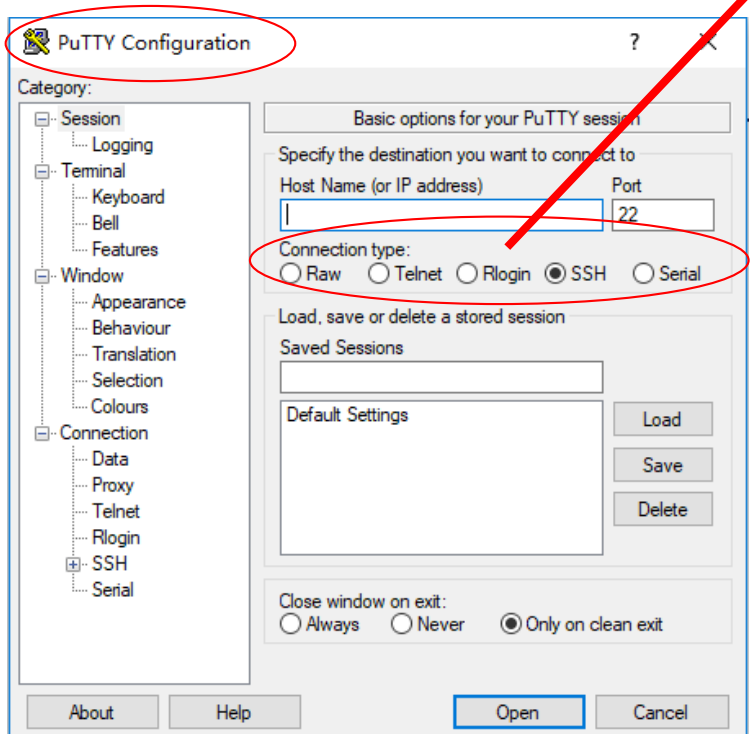
终端仿真软件——超级终端

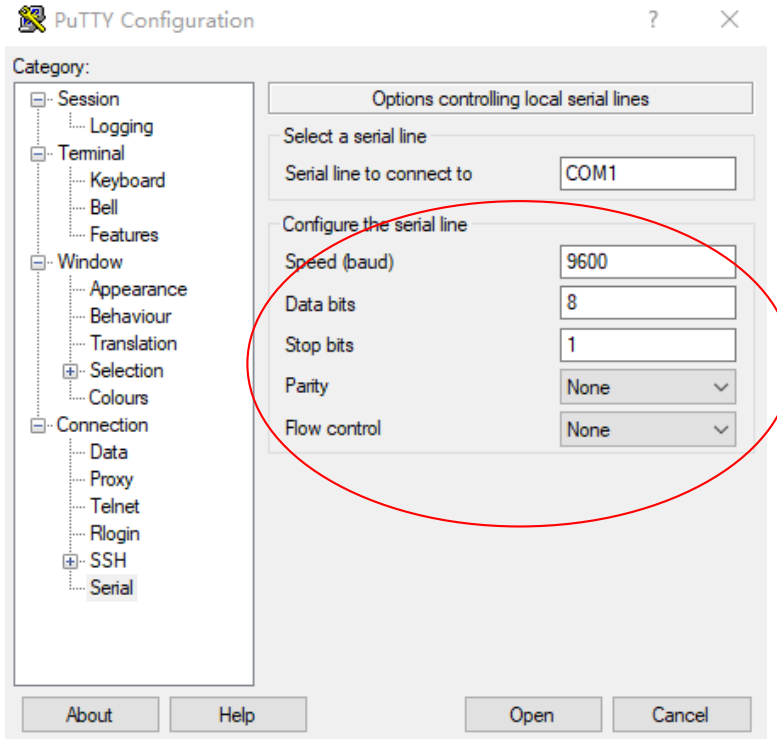


Windows2000自带的超级终端软件

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

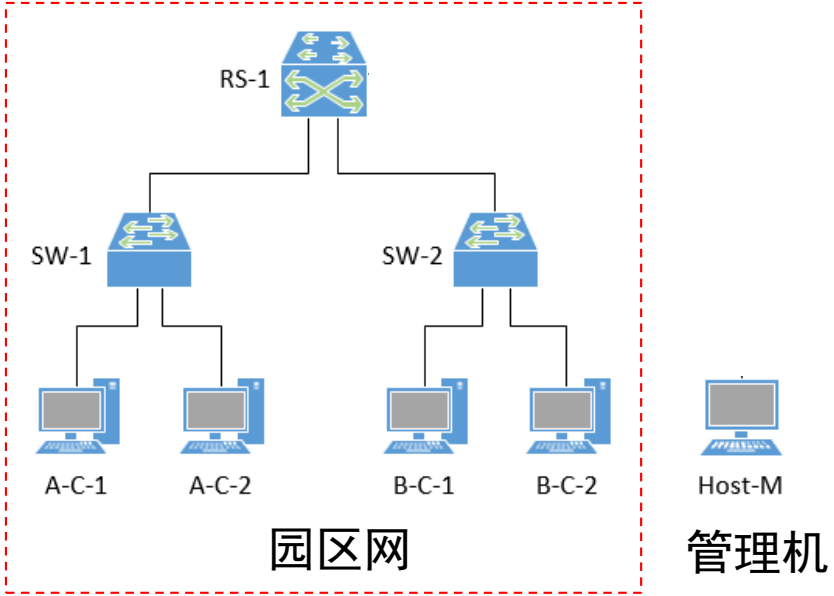
应用场景

- 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

案例

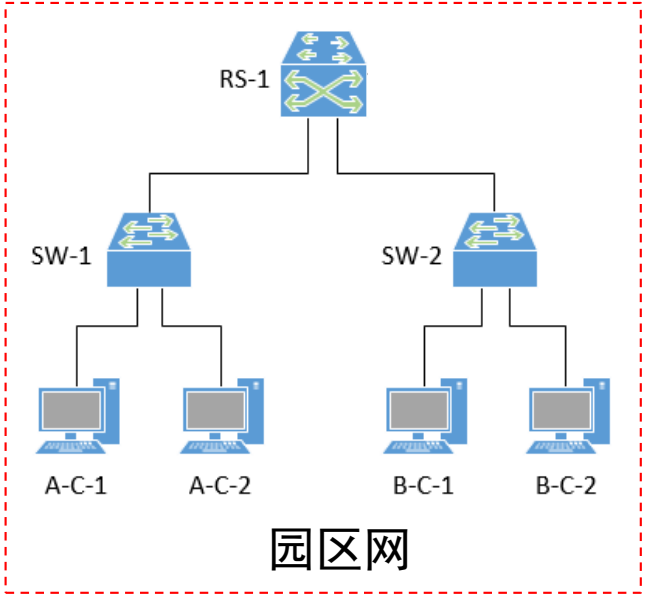
- 一个由路由交换机RS-1构建的园区网，其中的网络设备包含RS-1、SW-1、SW-2。
- 管理员想通过办公室内部的一台计算机Host-M，远程管理配置上述网络设备。



Telnet方式登录网络设备

案例分析1

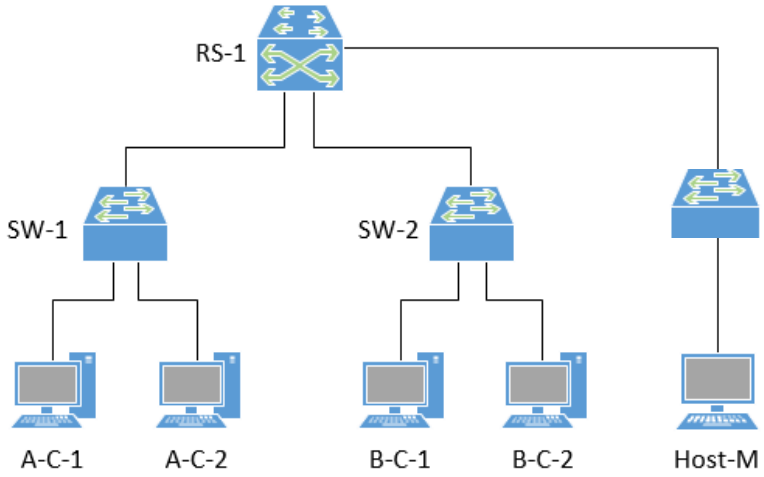
- “远程管理”，通常指管理机可通过网络（使用TCP/IP），登录被管理设备，然后实施配置操作的行为。
- 要想“通过网络登录”，需要具备哪些前提条件？



Telnet方式登录网络设备

案例分析2

- “通过网络登录”的前提条件
  - ① Host-M要接入园区网
  - ② 能访问到被管理的设备（简单说，就是ping通）
  - ③ 符合“登录”的要求



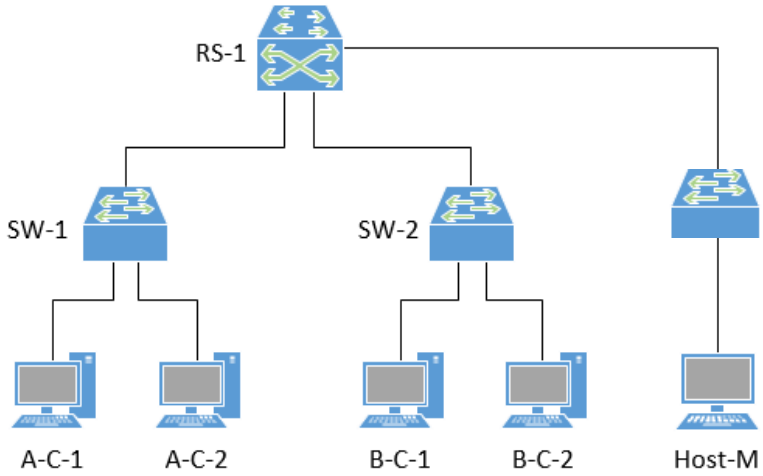
Telnet方式登录网络设备

案例分析3

- 远程登录前提条件的引申分析

① 物理上有接入(无线或有线)

② 由于通过TCP/IP网络访问，因此双方都要配置IP地址，且互联互通；



③ Host-M要安装telnet软件(例Putty)，被管理设备要启用telnet服务；

④ 由于是远程登录，出于安全需求，要在被管理设备上进行登录配置，包括添加允许登录的用户名和密码，设置用户认证的方式等。

Telnet方式登录网络设备

案例分析4

- 具体操作过程分析（1）

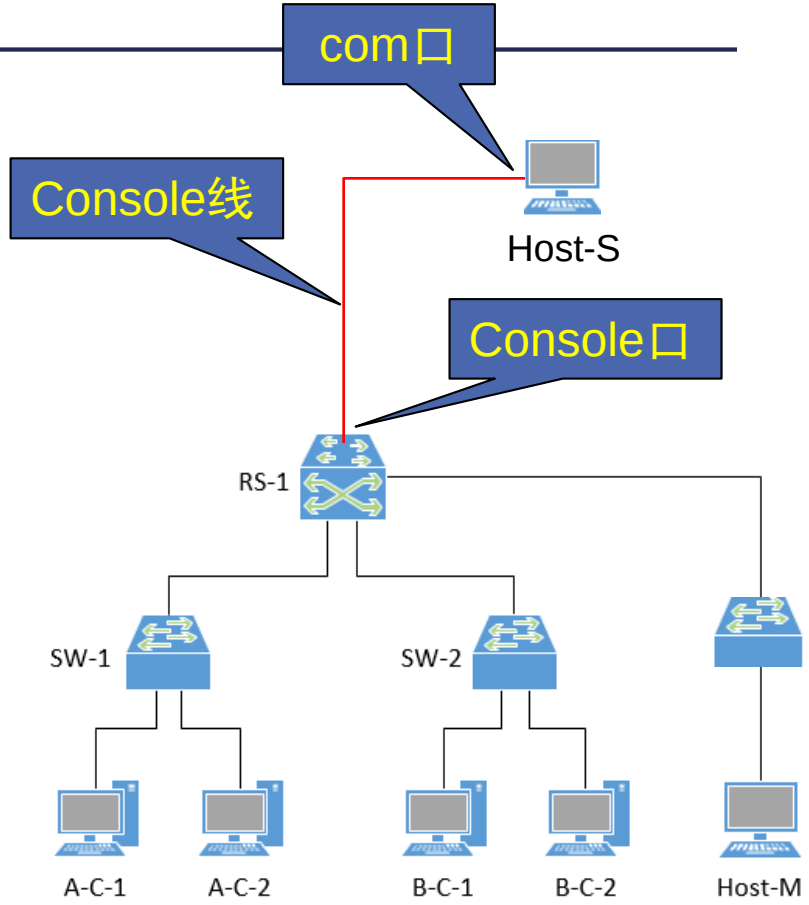
① 首先，通过Console方式登录网络设备（例如RS-1）；

② 给该设备配置IP地址，即管理IP；

③ 启用该设备的Telnet服务

④ 添加该设备允许登录的用户名和密码，设置用户认证的方式等；

⑤ 同理，配置其他网络设备；



Telnet方式登录网络设备

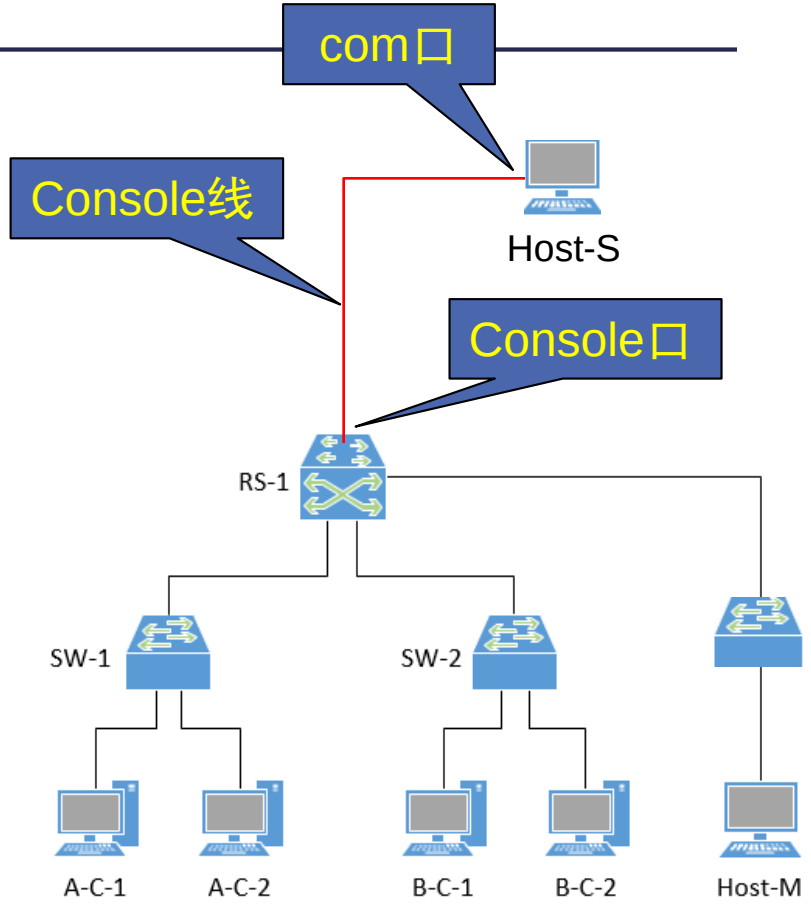
案例分析4

- 具体操作过程分析（2）

⑥ 仍然以console配置方式，配置全网的路由、VLAN等，使得Host-M可以ping通各网络设备；

⑦ 在Host-M上安装Putty；

⑧ 通过telnet登录网络设备；



Telnet方式登录网络设备

总结

- 缺省情况下，用户不能通过Telnet方式直接登录设备；
- 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：
  - 配置网络设备的管理IP（缺省情况下，设备上没有配置IP地址）；
  - 确保管理机和网络设备之间路由可达；
  - 在网络设备上，配置Telnet服务器功能及认证方式；
  - 在网络设备上，配置Telnet用户登录的用户界面（含用户名、密码等）。

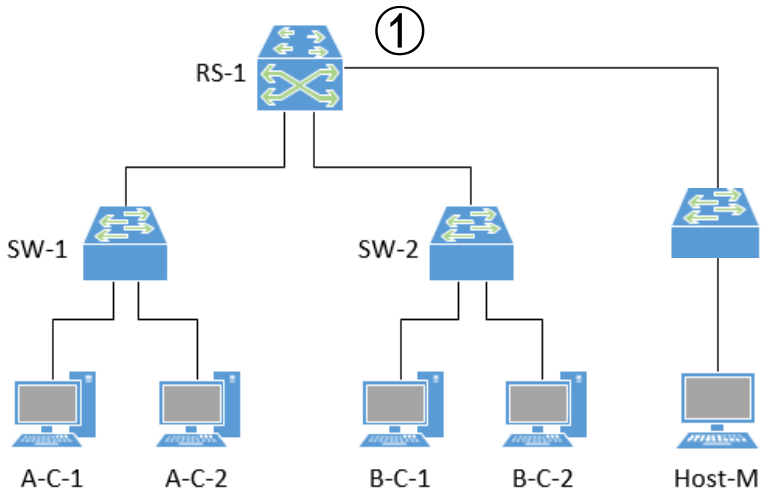
Telnet方式登录网络设备

- 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。

案例分析：Telnet方式采用明文传输

基本思路：

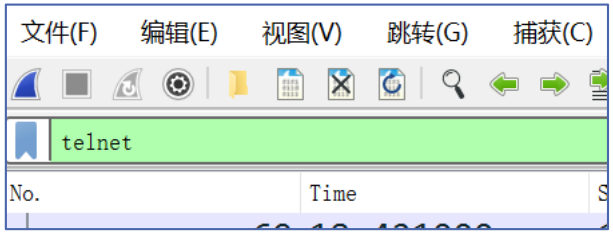
1. Host-M以telnet方式远程登录SW-1
2. 对整个登录过程进行分析，并且在①处进行抓包，分析一下telnet协议的报文内容。

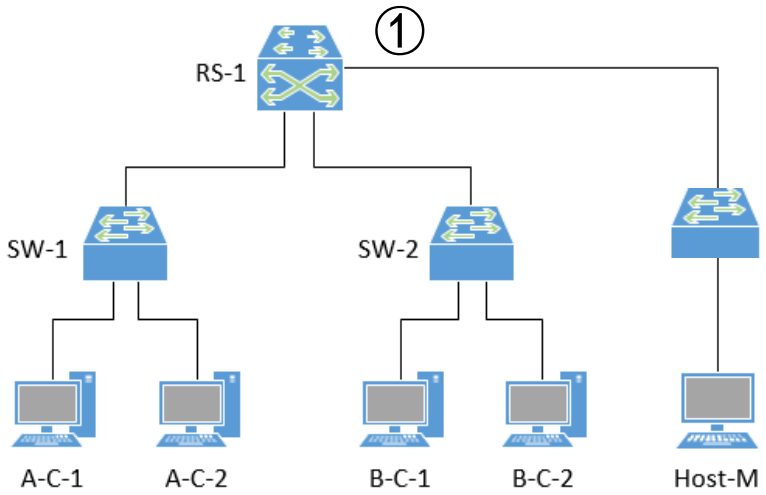


案例分析：Telnet方式采用明文传输

步骤1：

- 在①处启动抓包程序。

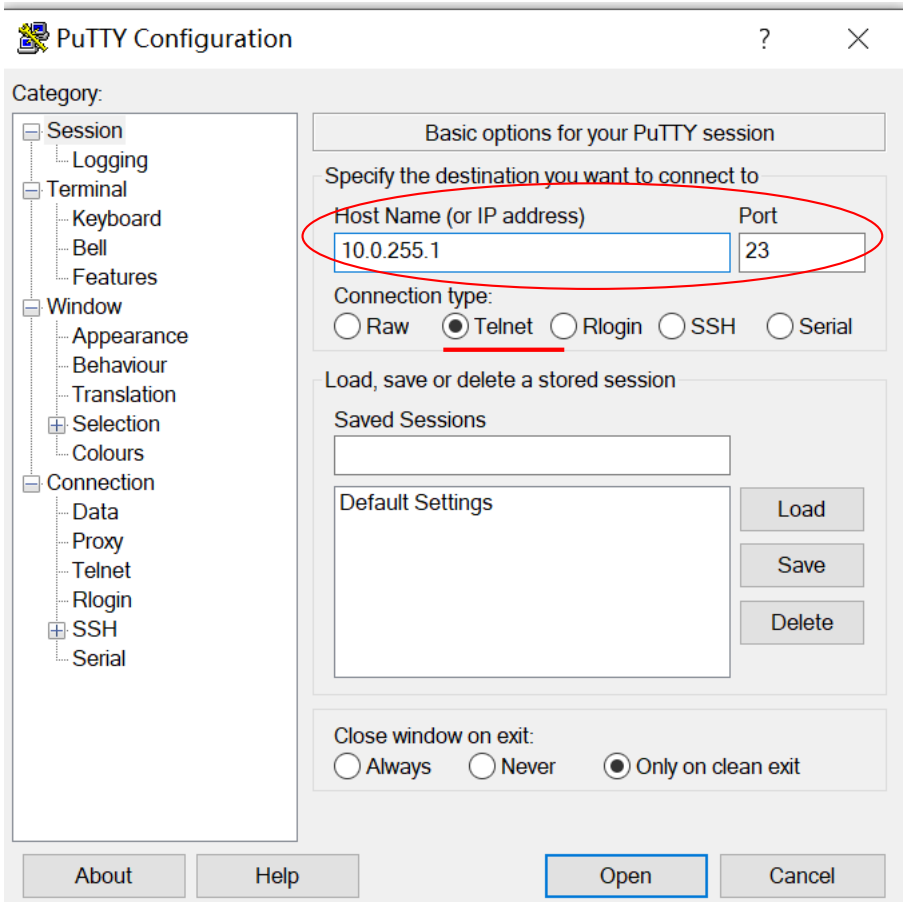




案例分析：Telnet方式采用明文传输

步骤2：

- 在Host-M上启动Putty程序，并以telnet方式登录交换机SW-1。
- 假设此处的SW-1的管理IP是10.0.255.1



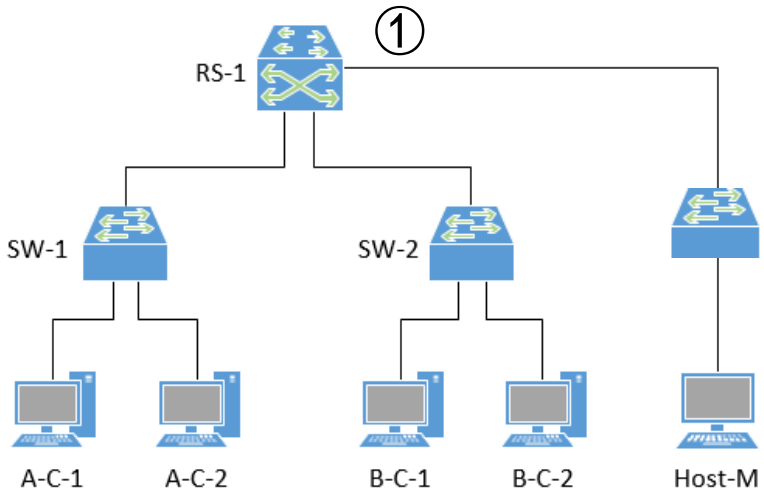
案例分析：Telnet方式采用明文传输

步骤3：

- 出现登录界面，输入前期在SW-1上配置好的用户名和密码。

  用户名：　user_tel

  密码：　　abc@123




10.0.255.1 - PuTTY
Login authentication
Username:
1. 提示输入用户名


10.0.255.1 - PuTTY
Login authentication
Username:user_tel
2. 输入用户名user_tel

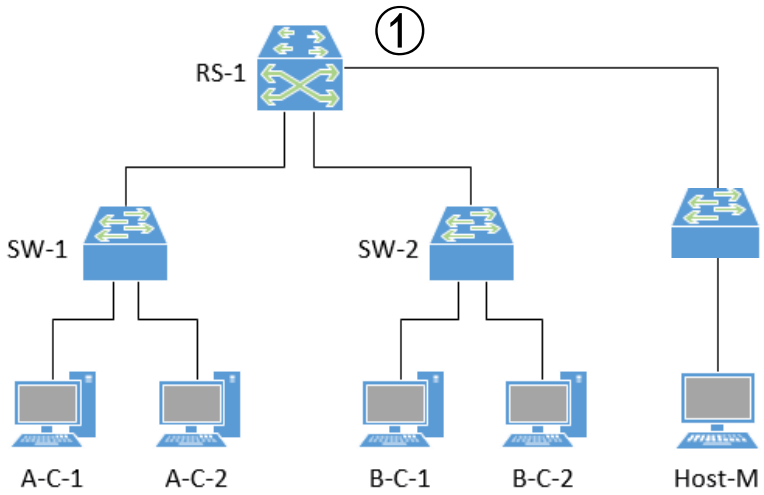

10.0.255.1 - PuTTY
Login authentication
Username:user_tel
Password:
3. 提示输入密码


10.0.255.1 - PuTTY
Login authentication
Username:user_tel
Password:
Info: The max number of VTY users is 5, a
nd the number
of current VTY users on line is 1.
The current login time is 2024-02-0
3 18:27:48.
<SW-1>
4. 输入密码并回车，登录成功

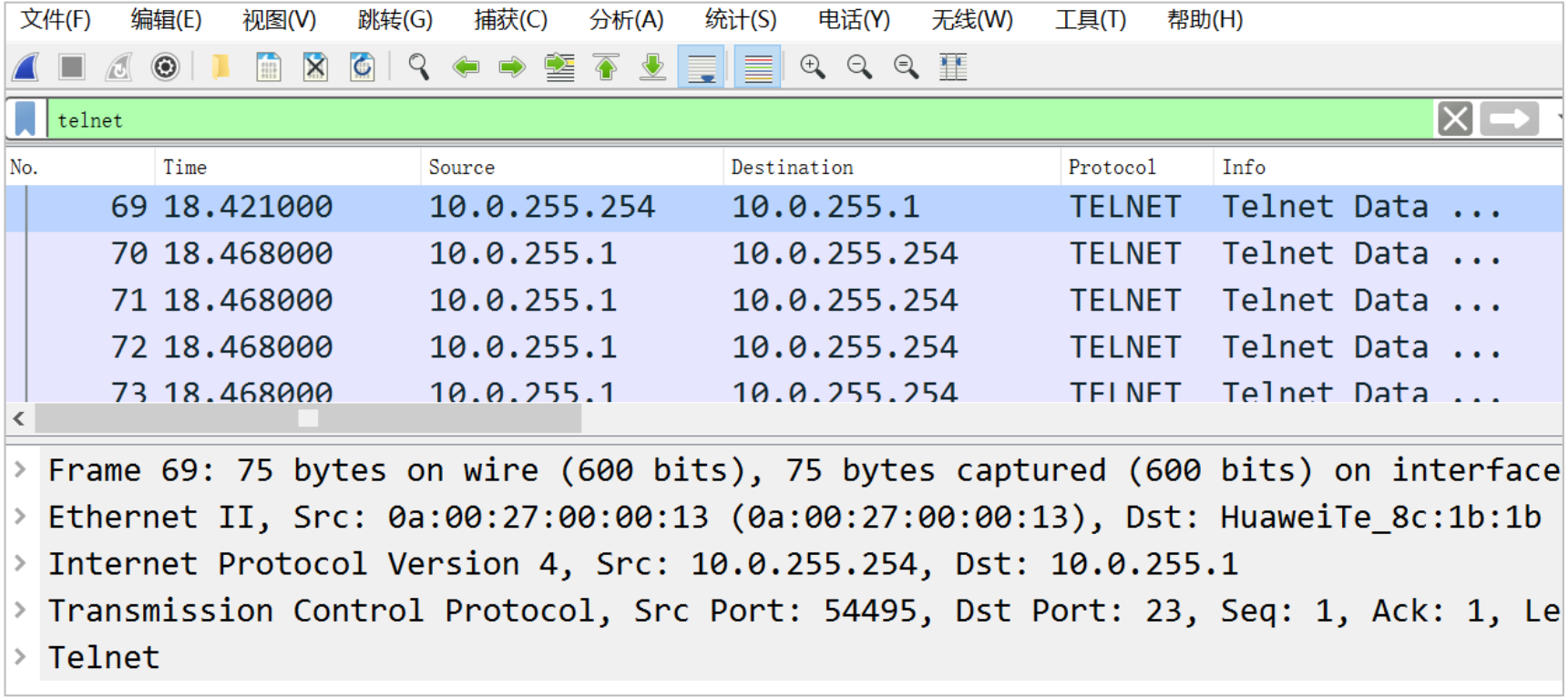
案例分析：Telnet方式采用明文传输

步骤4：

- 分析在①抓取的telnet协议报文

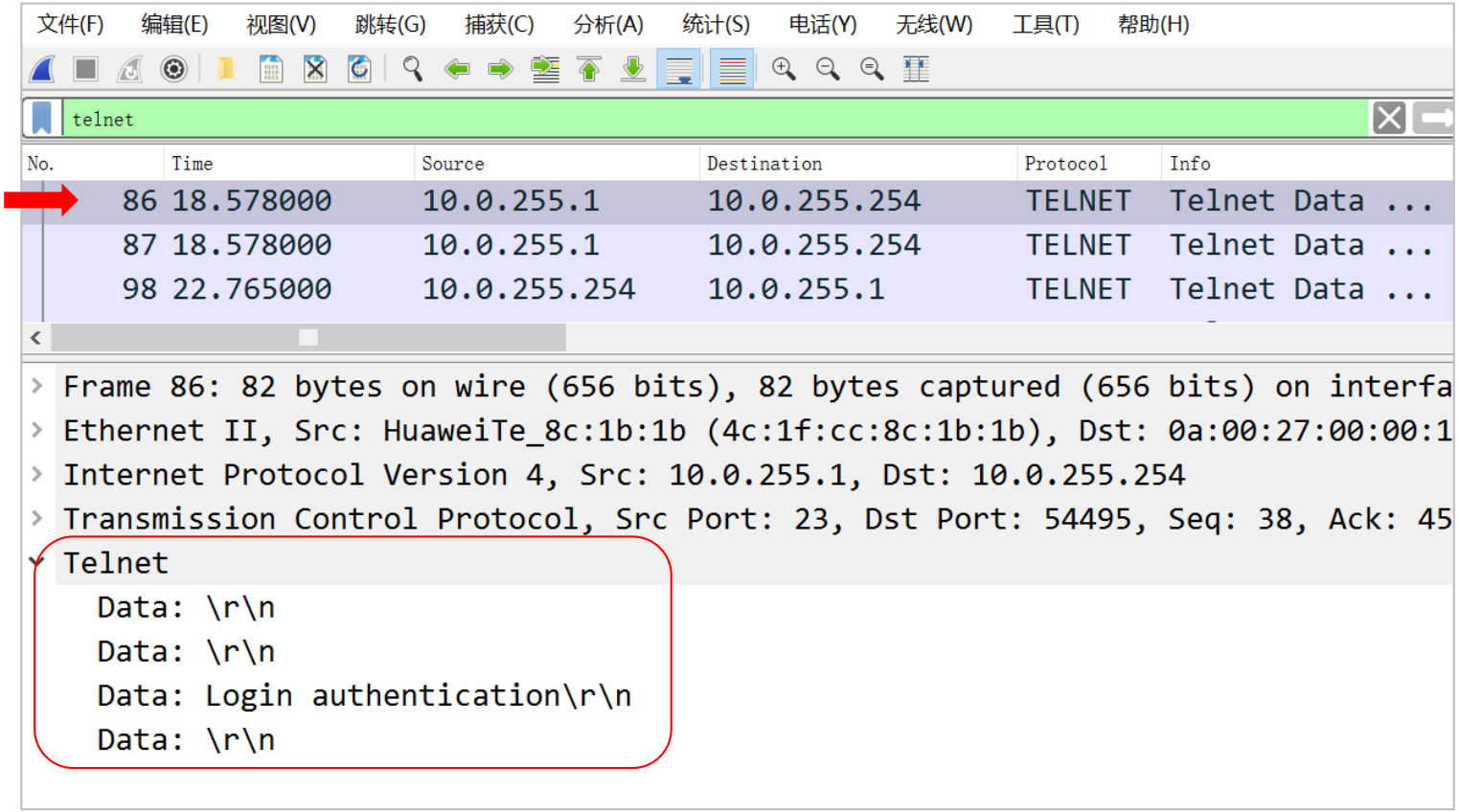


➢ 分析1：过滤后，可以看到Host-M和SW-1之间相互有telnet报文



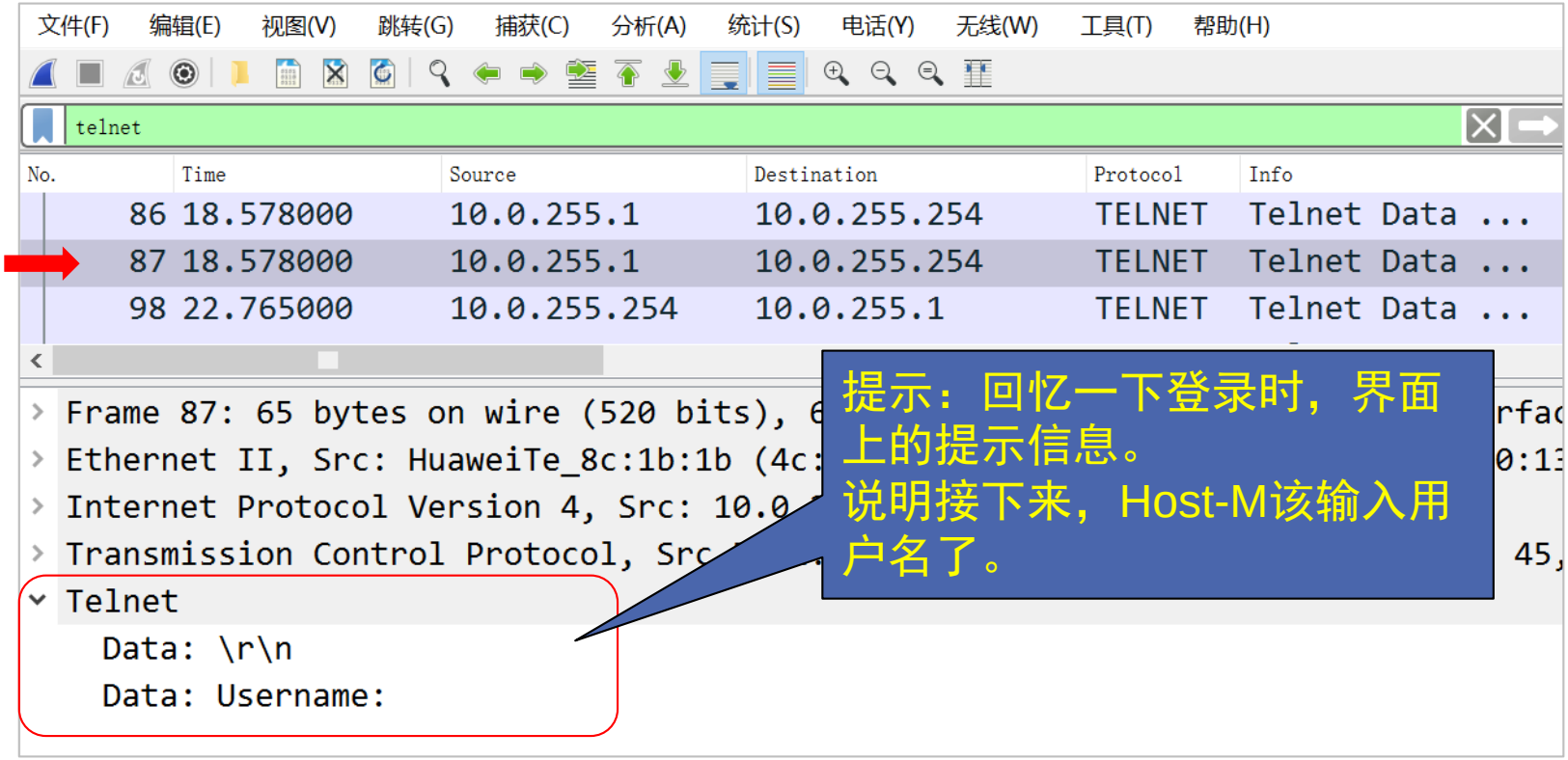
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析2：查看86号报文，可看到SW-1发给Host-M的信息如下



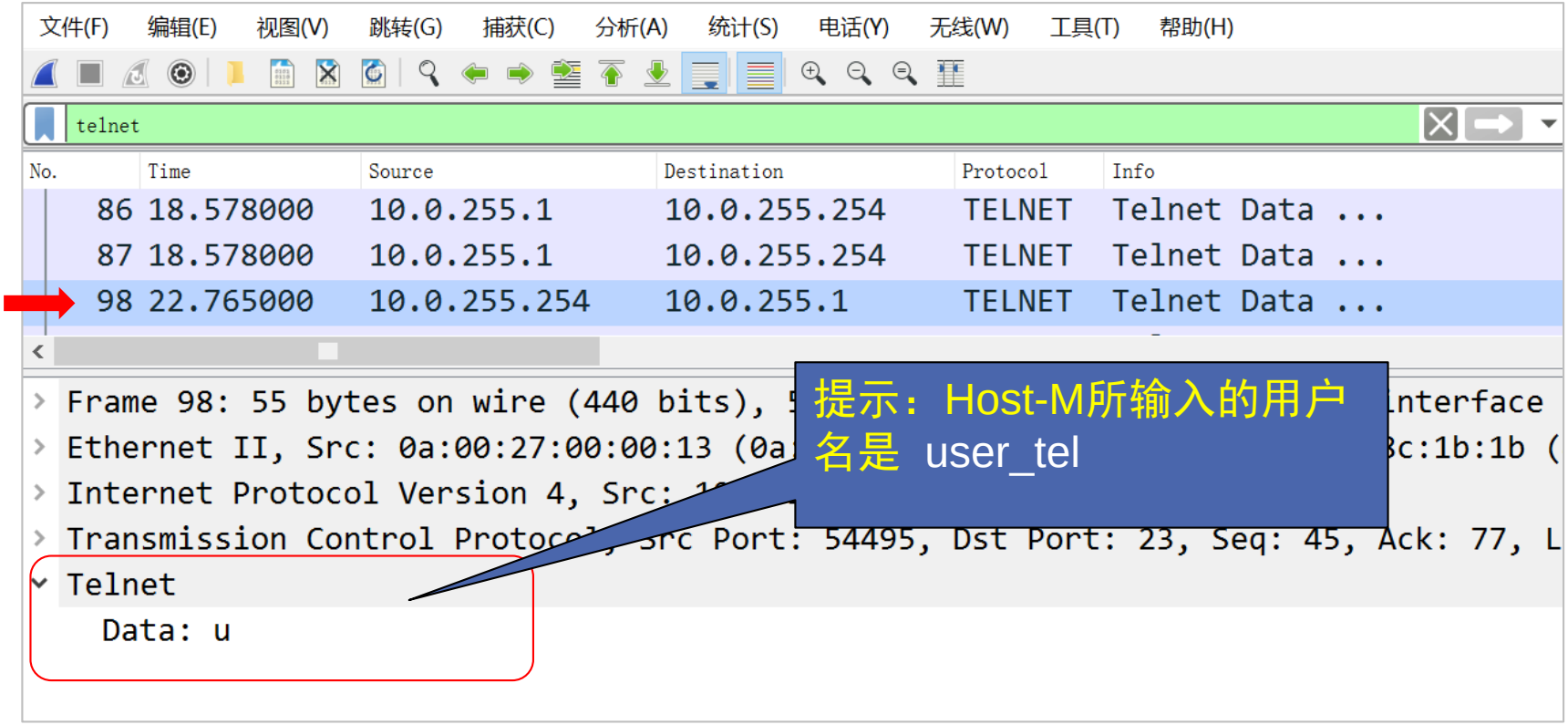
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析3：查看87号报文，可看到SW-1发给Host-M的信息如下



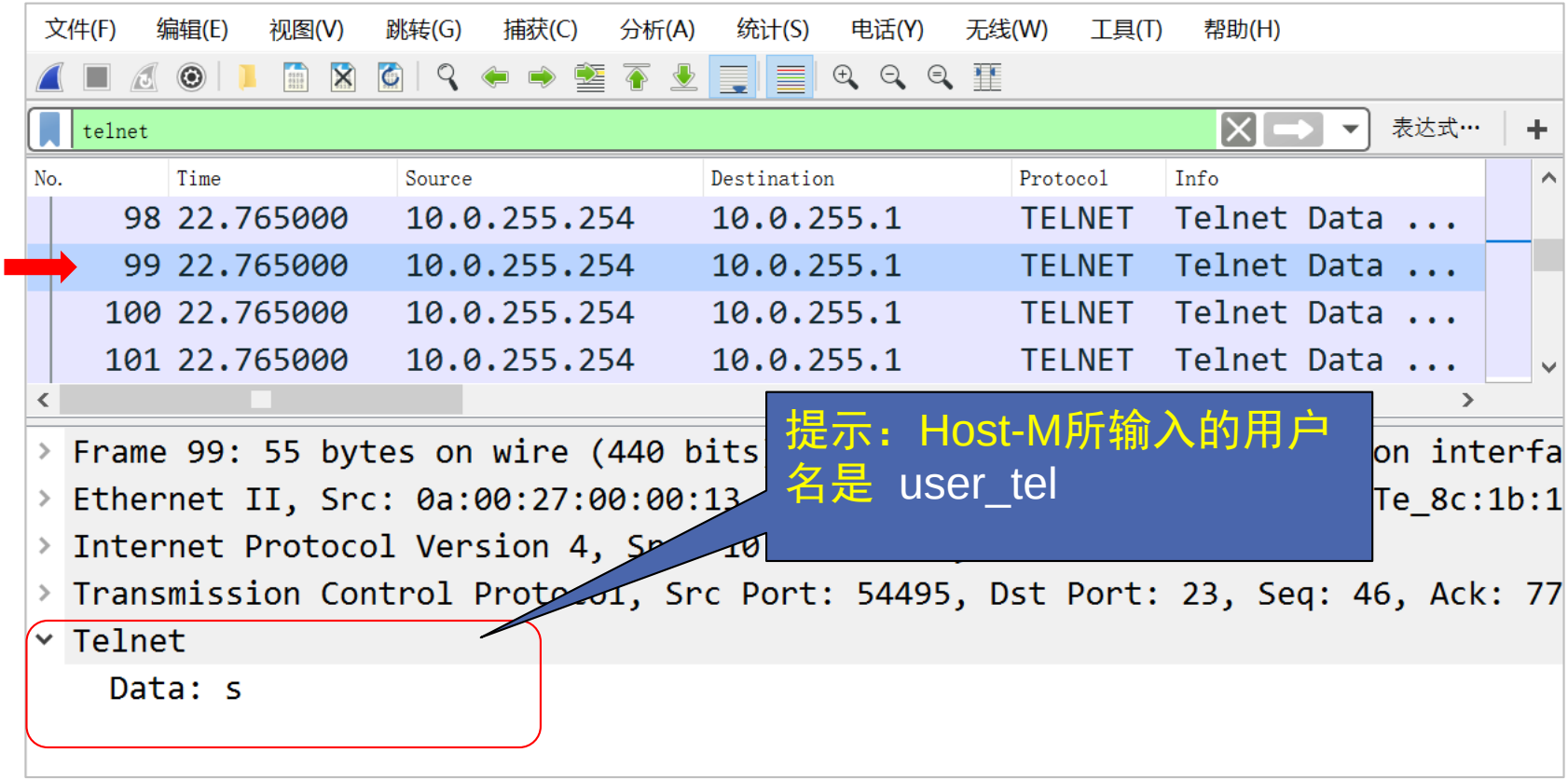
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析4：查看98号报文，可看到Host-M发给SW-1的信息如下



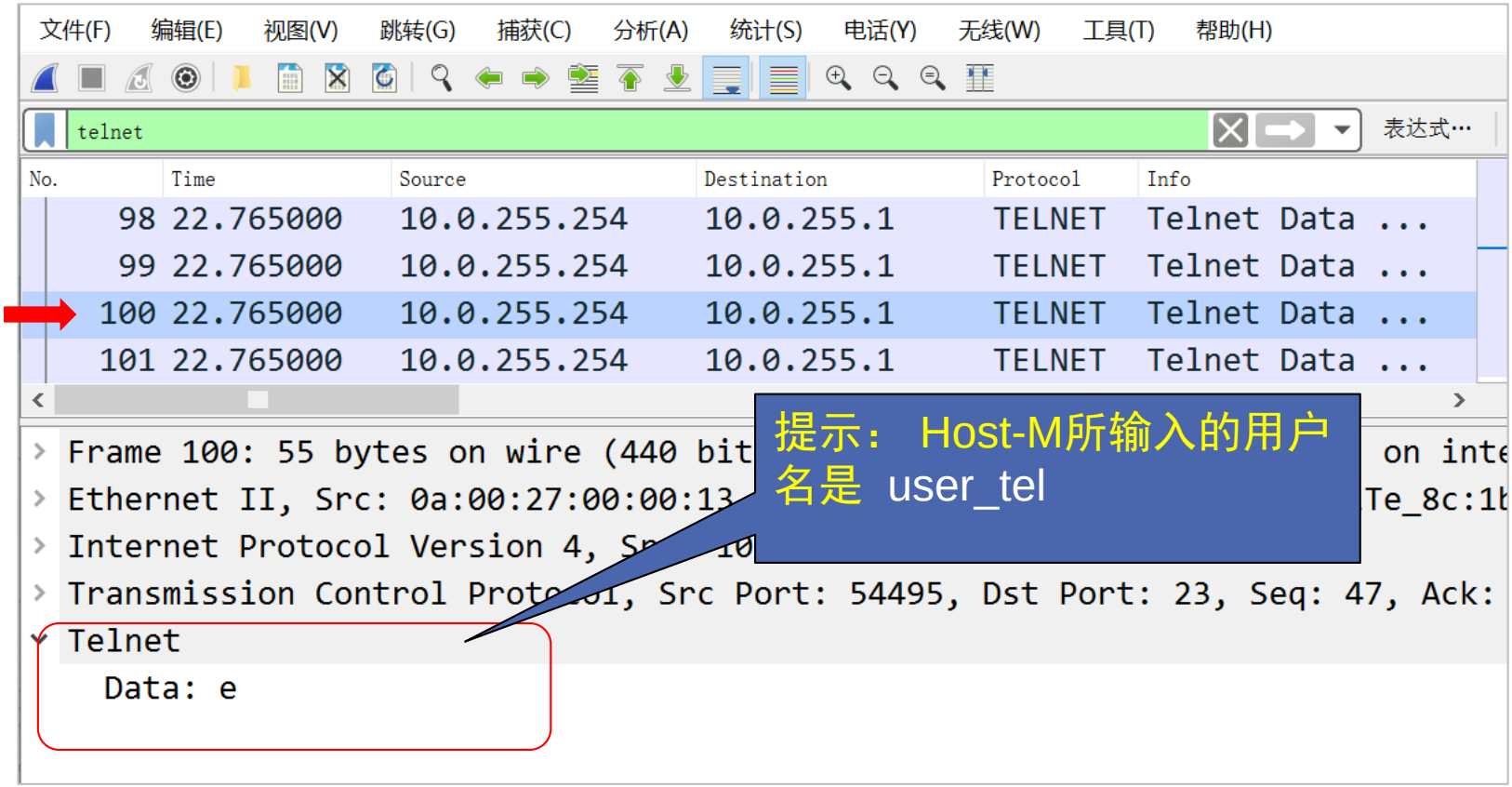
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析5：查看99号报文，可看到Host-M发给SW-1的信息如下



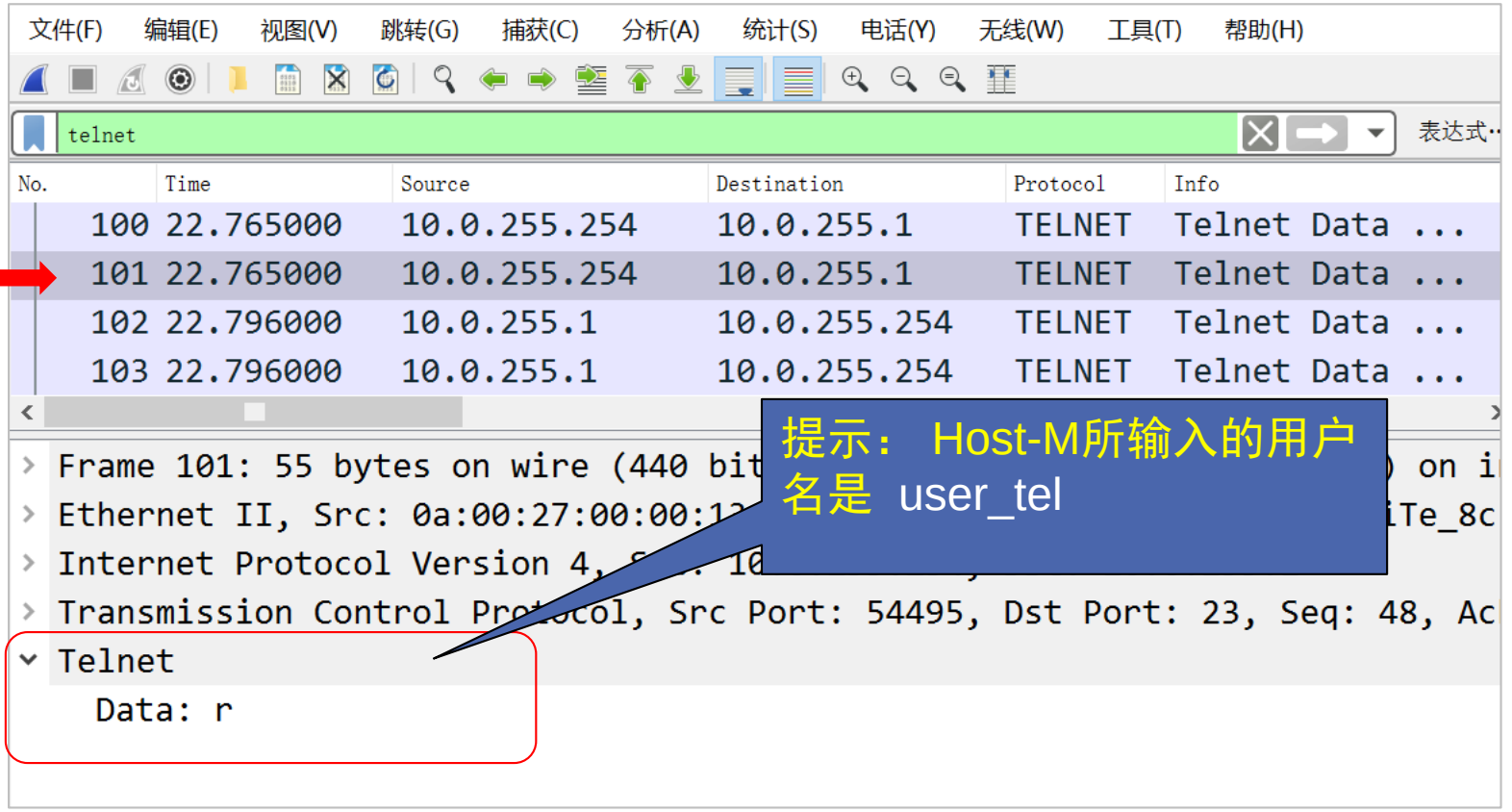
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析6：查看100号报文，可看到Host-M发给SW-1的信息如下



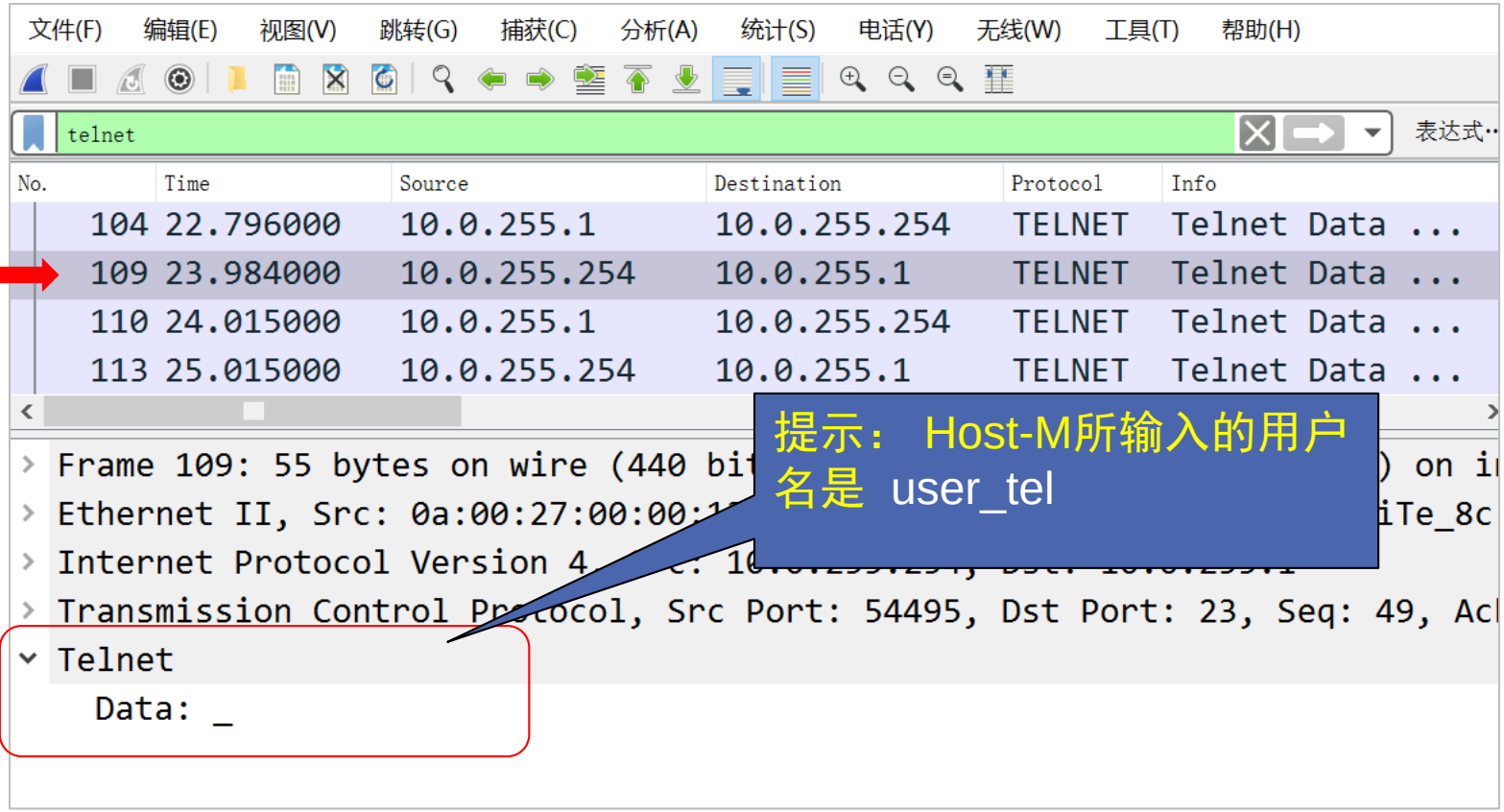
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析7：查看101号报文，可看到Host-M发给SW-1的信息如下



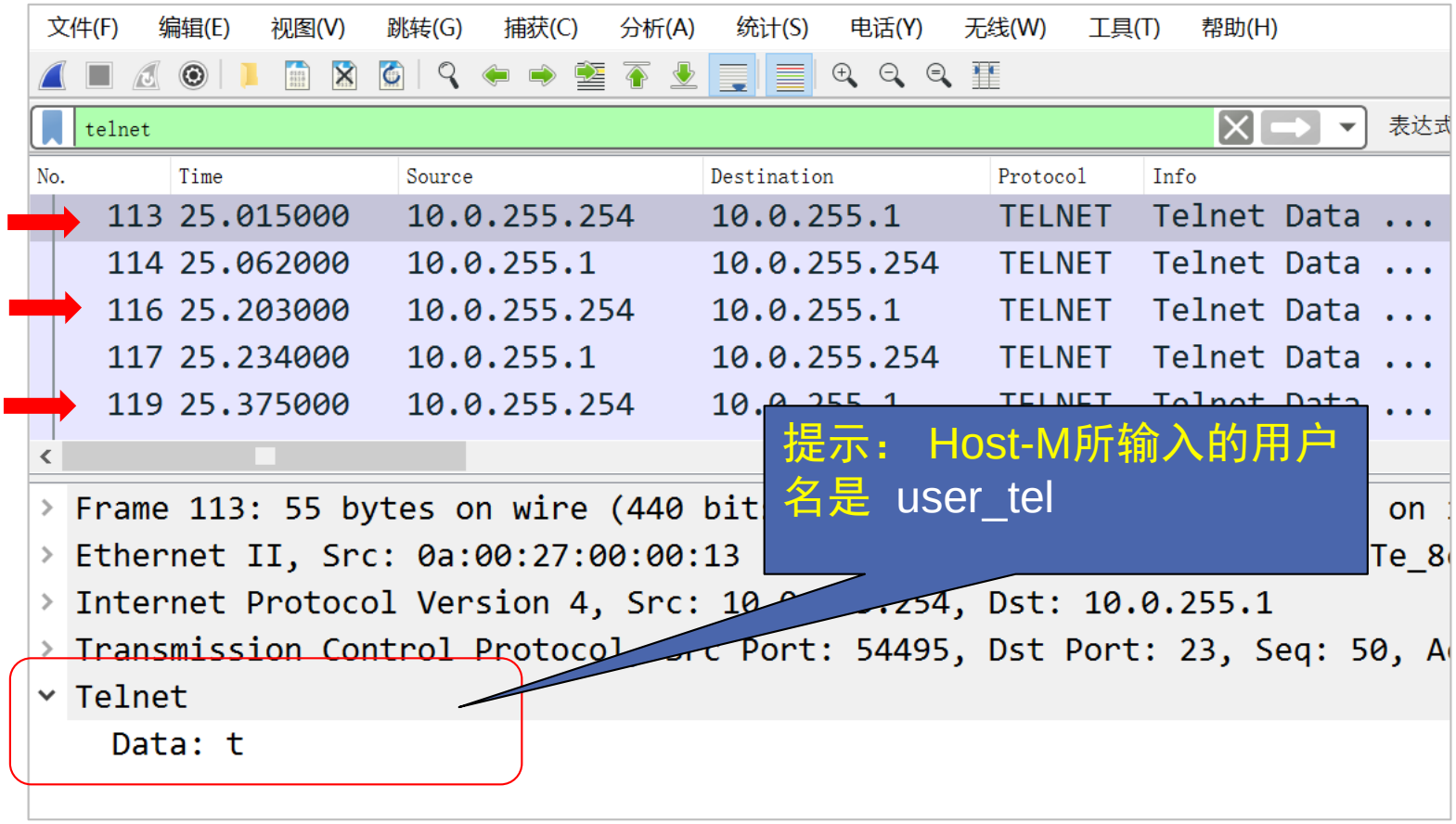
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析8：查看109号报文，可看到Host-M发给SW-1的信息如下



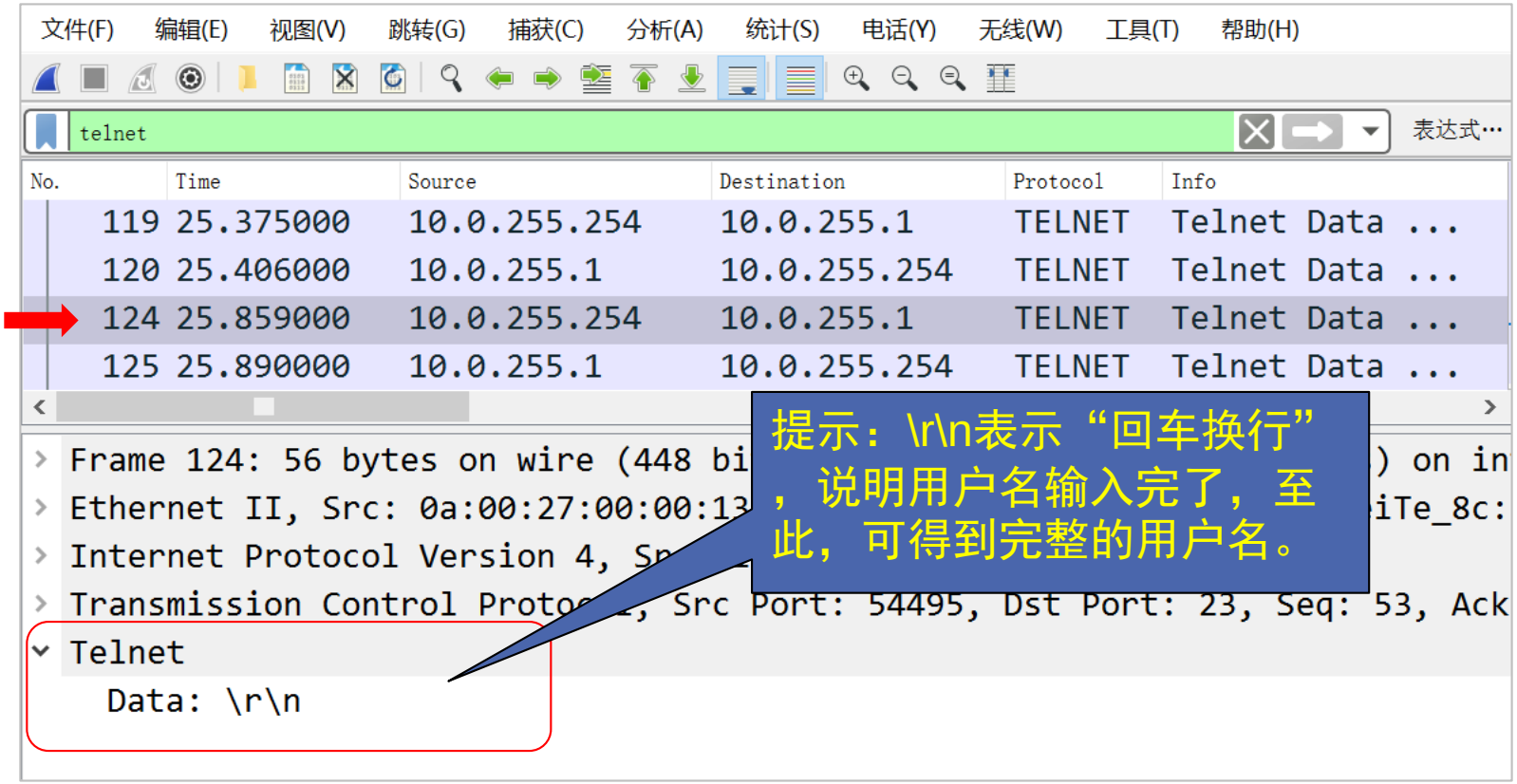
Host-M：10.0.255.254　　SW-1：10.0.25.1

➢ 分析9：查看113、116、119号报文，可看到Host-M发给SW-1的信息分别是t、e、l



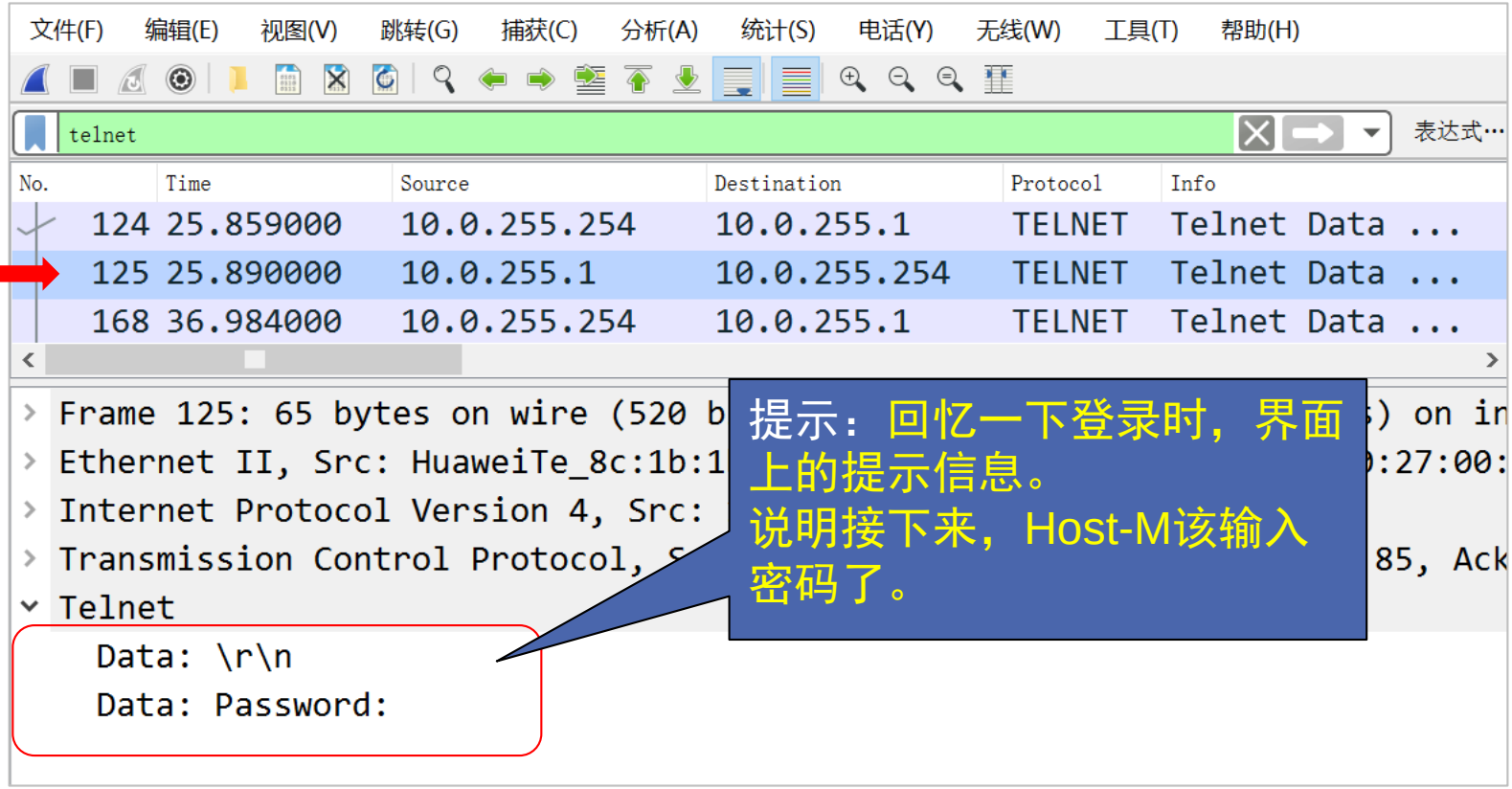
Host-M：10.0.255.254　　SW-1：10.0.25.1

- 分析10：查看下一个Host-M发给SW-1的报文（124号），可看到发的是\r\n



Host-M：10.0.255.254　　SW-1：10.0.25.1

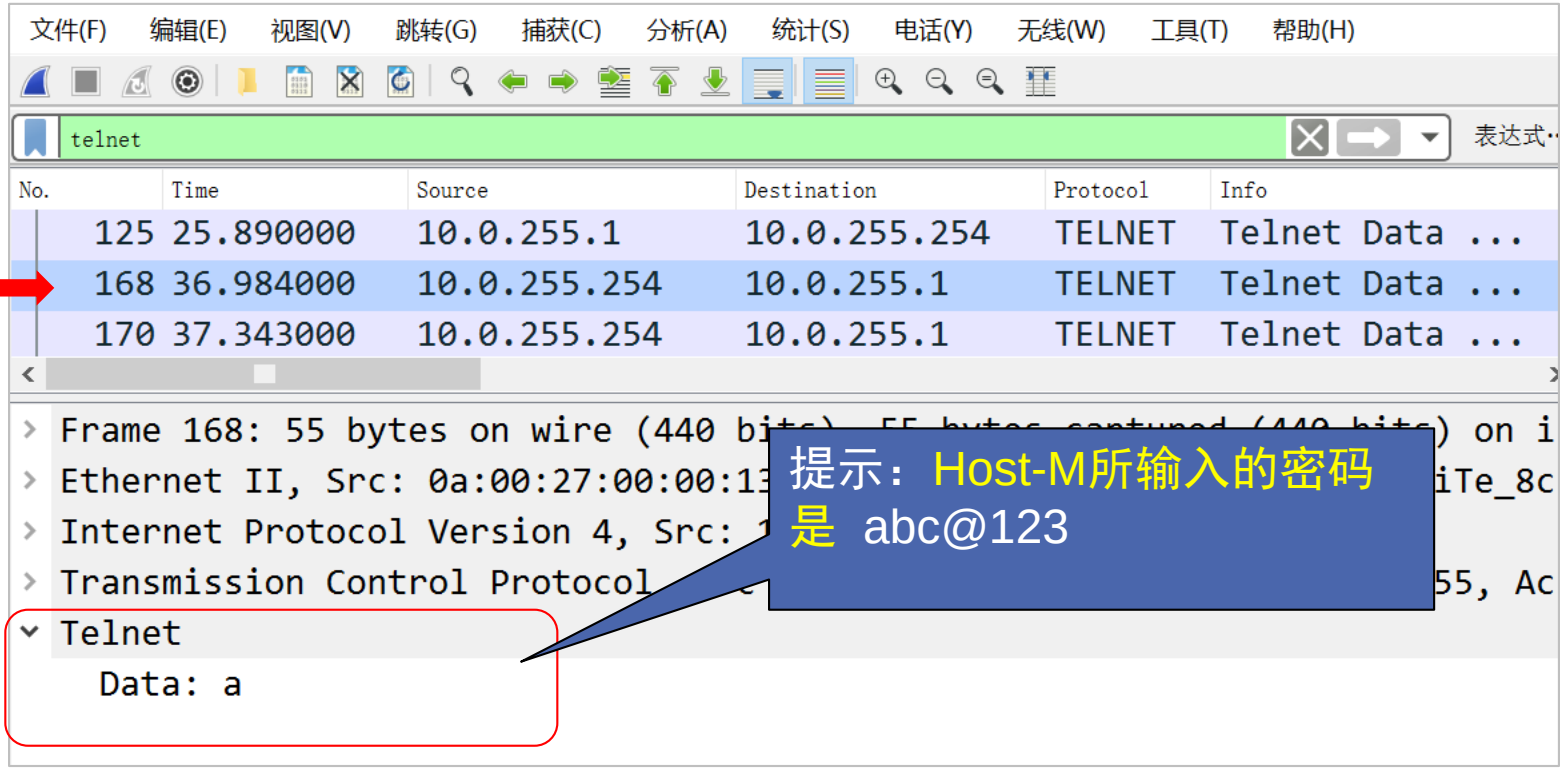
➢ 分析11：查看125号报文，可看到SW-1发给Host-M的信息如下



Host-M：10.0.255.254

SW-1：10.0.25.1

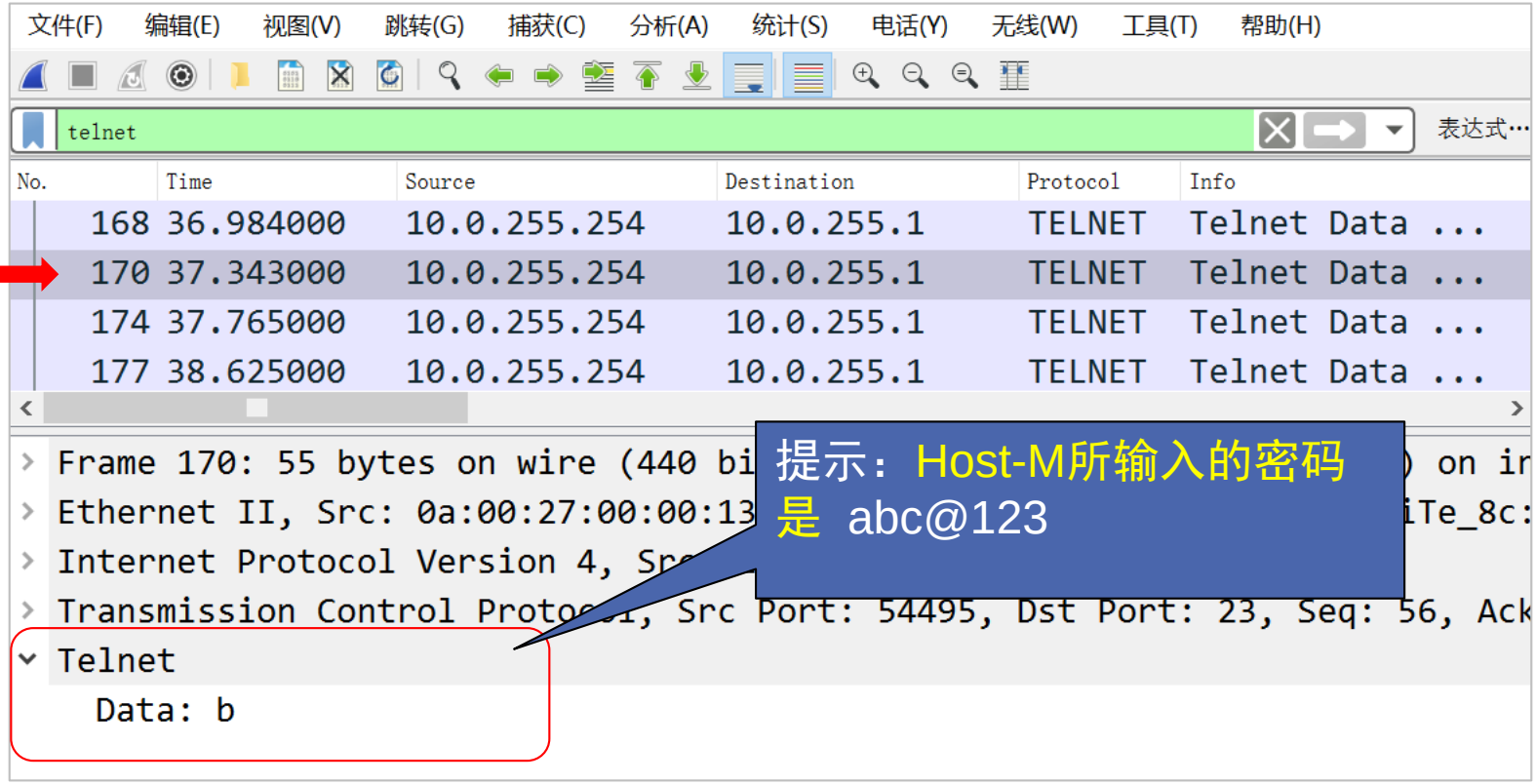
- 分析12：查看下一个Host-M发给SW-1的报文（168号），可看到发的是字符a



Host-M：10.0.255.254

SW-1：10.0.25.1

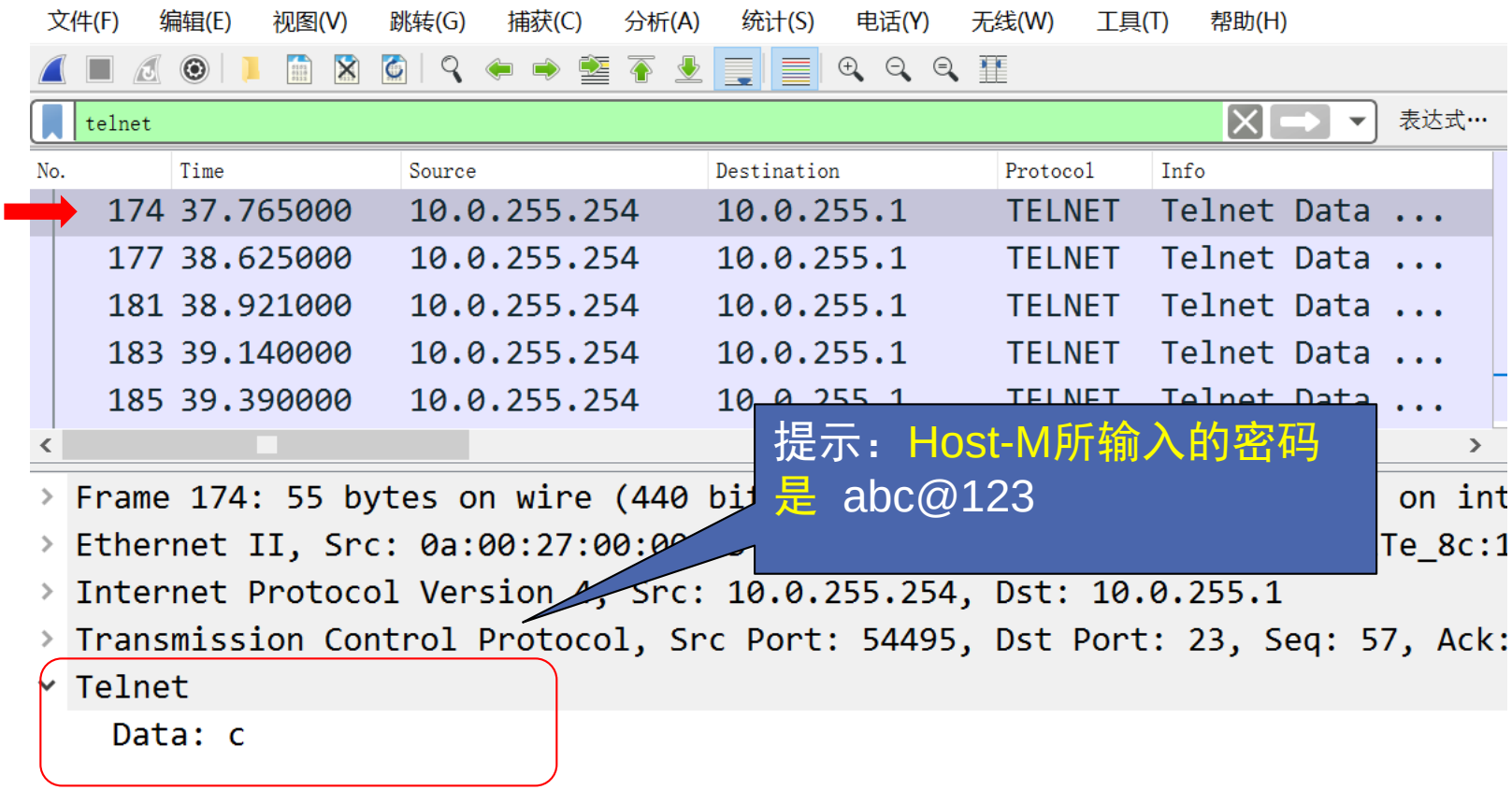
- 分析13：查看下一个Host-M发给SW-1的报文（170号），可看到发的是字符b



Host-M：10.0.255.254

SW-1：10.0.25.1

➢ 分析14：查看174、177、181、183、185号报文，可看到Host-M发给SW-1的信息分别是c、@、1、2、3



Host-M：10.0.255.254　　SW-1：10.0.25.1

- 分析15：查看下一个Host-M发给SW-1的报文（187号），可看到发的信息是\r\n

Host-M：10.0.255.254　　SW-1：10.0.25.1

Telnet方式登录网络设备

总结

- 由于Telnet采用了TCP的明文传输（双向都是明文），存在很大安全隐患，因此，为了保证通信的安全性，通常在进行远程登录设备时，不使用telnet方式，而是采用安全性更好的SSH方式。

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，客户端和服务器端之间经过协商，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

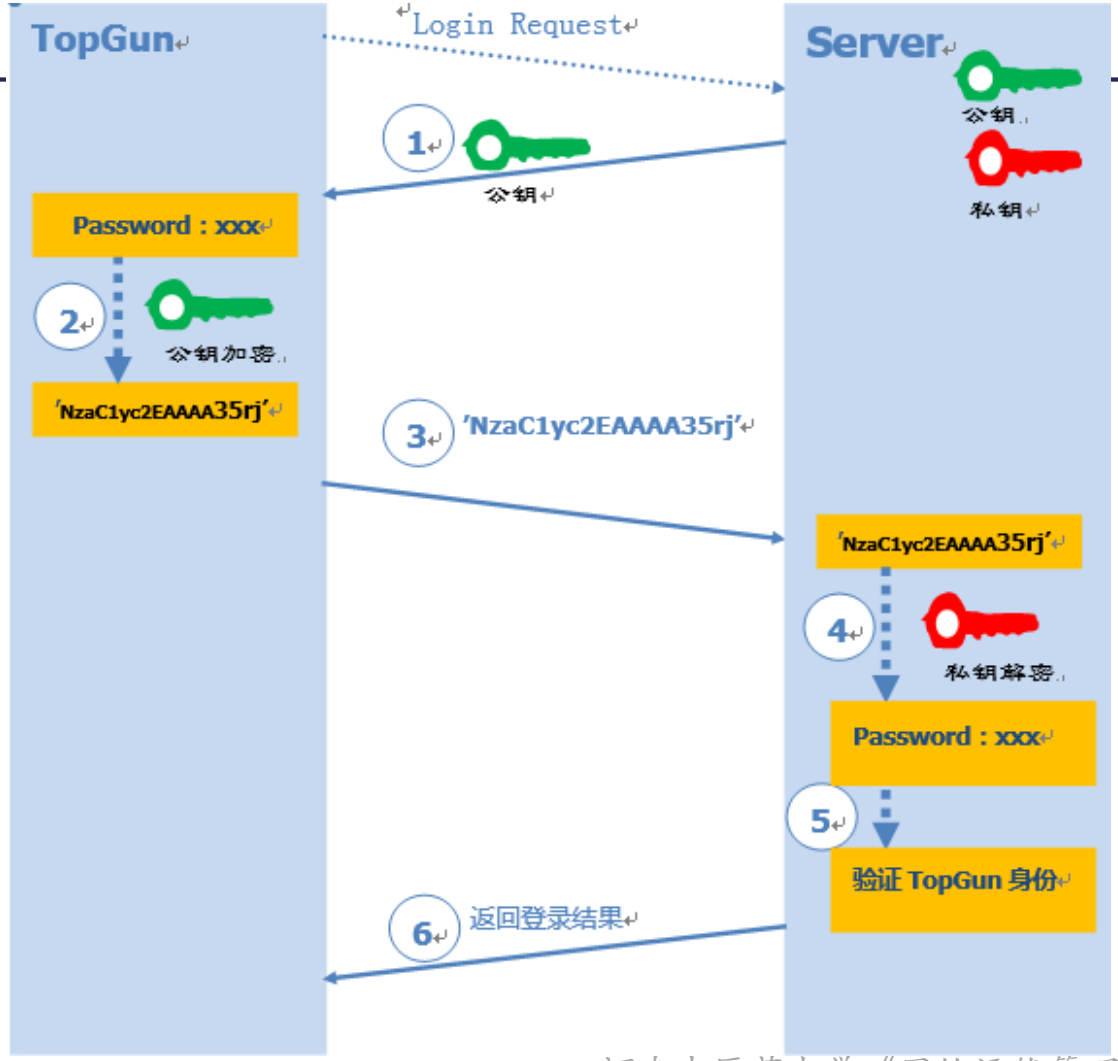
Password验证

- 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）

ssh 表达式…

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

ssh 表达式…

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)

Diffie-Hellman密钥协商算法主要解决秘钥配送问题

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

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”

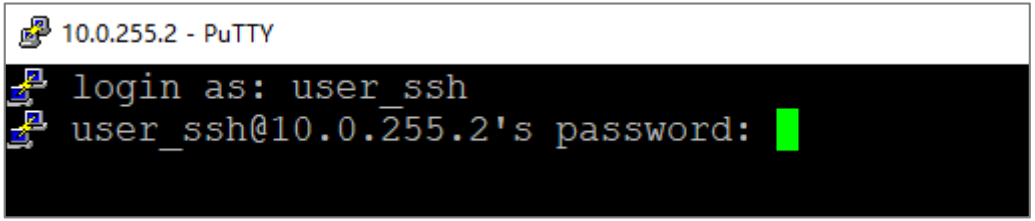


图1

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；

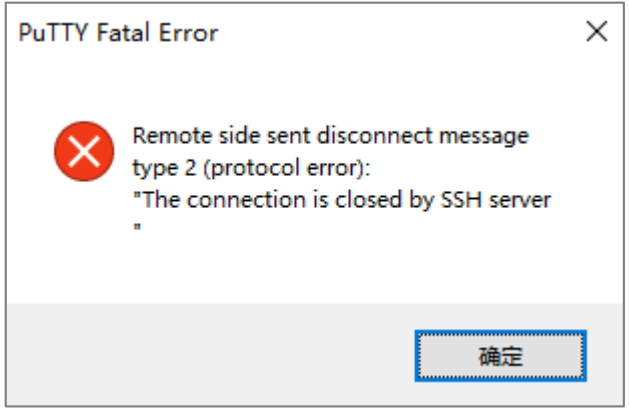


图2

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	35.672...	10.0.255.2	10.0.255.253	SSHv2	90	Server: Encrypted packet (len=36)

客户端发往网络设备

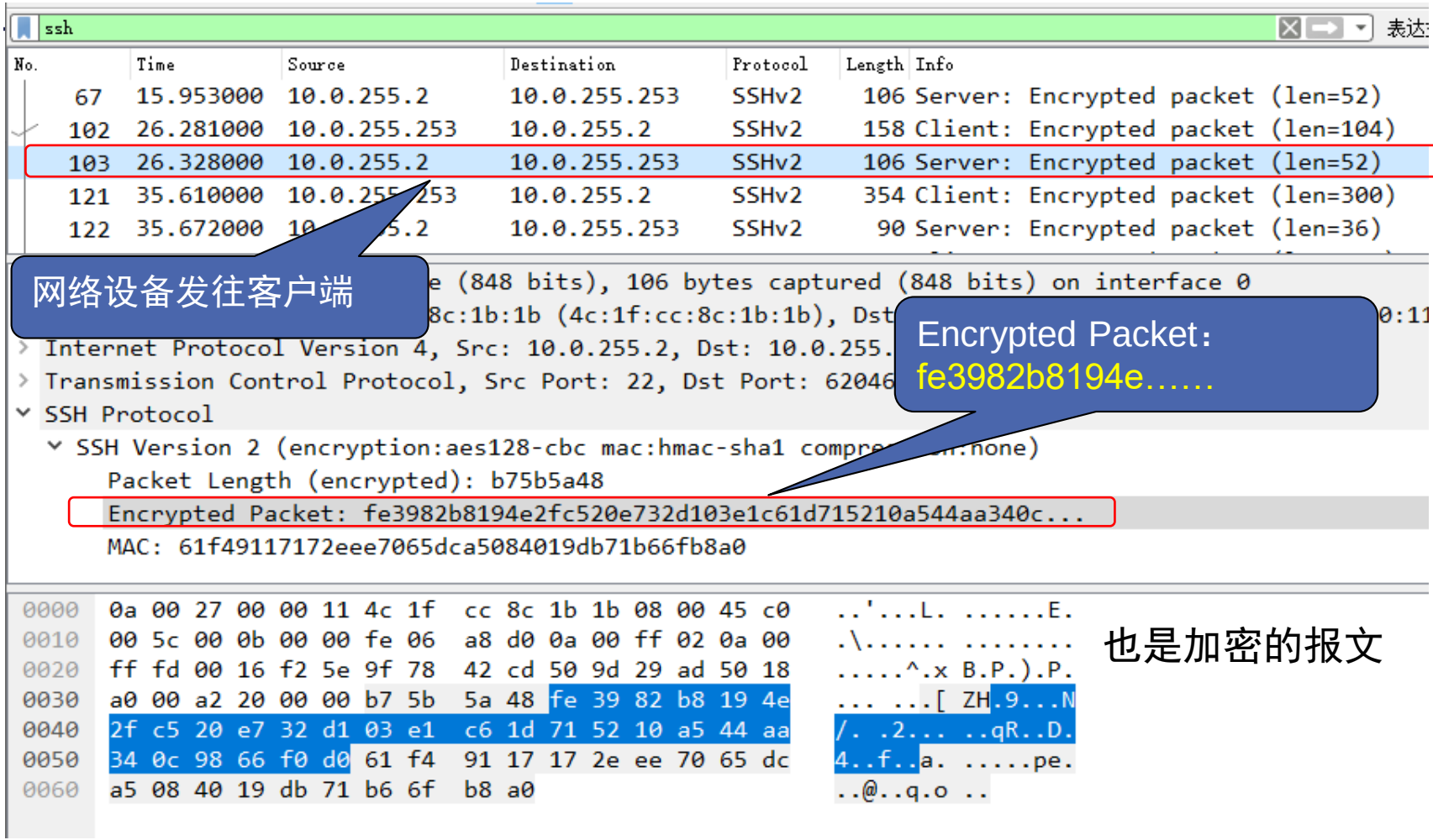
Encrypted Packet:
b2b0e112780e1……

```
> Internet Protocol Version 4, Src: 10.0.255.253, Dst: 10.0.255.2
> Transmission Control Protocol, Src Port: 62046, Dst Port: 22, Seq:
v SSH Protocol
  v SSH Version 2 (encryption:aes128-cbc mac:hmac-sha1 compressi
      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...
```

加密的报文

Password验证登录方式——抓包分析（2）—— 验证用户名



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；

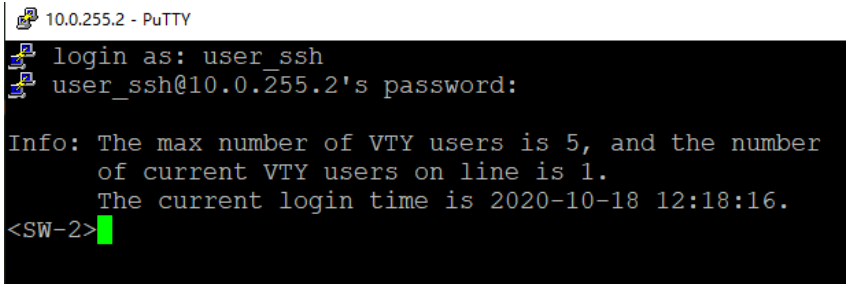
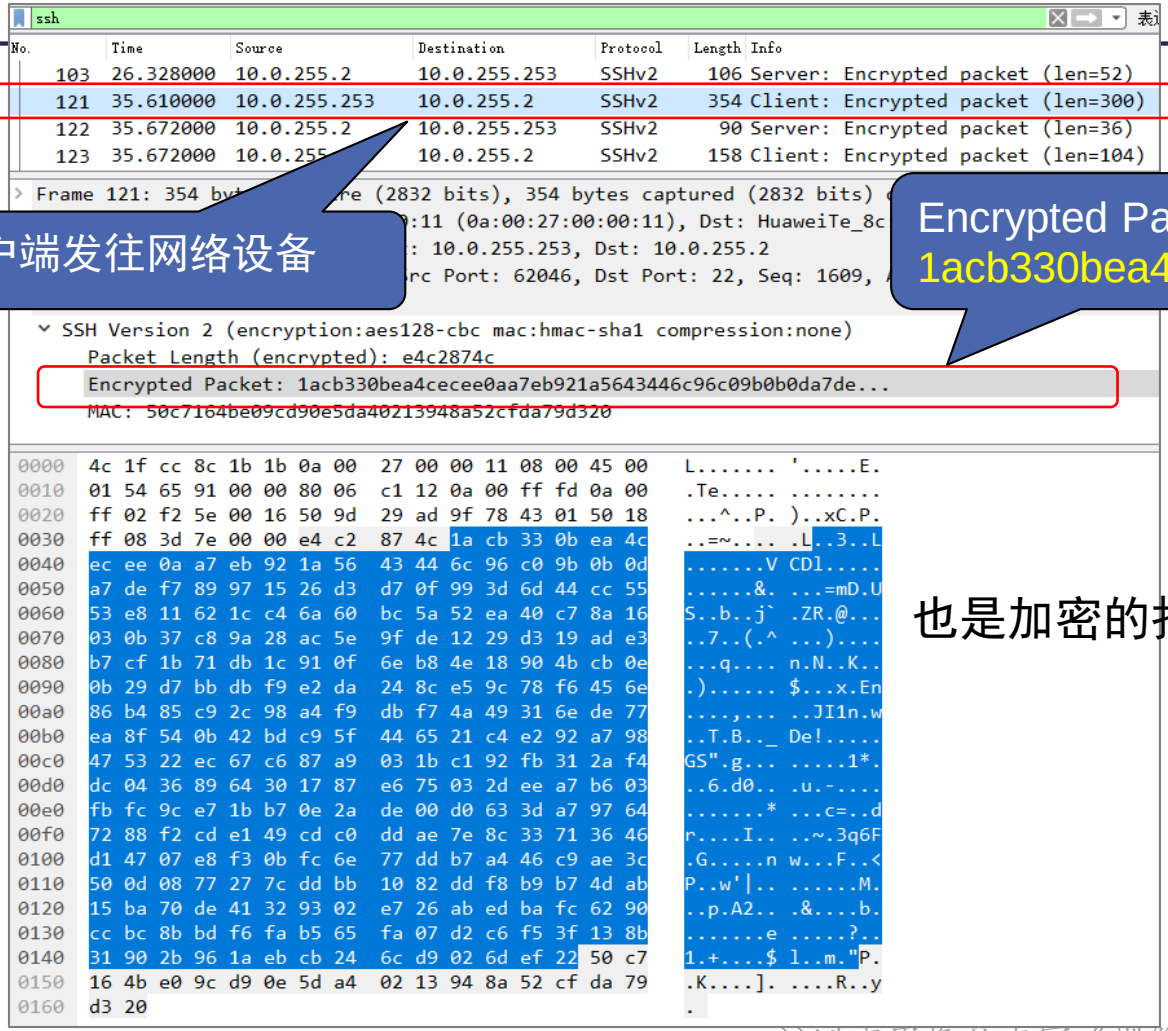


图1

Password验证登录方式——抓包分析（3）—— 验证密码



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）。

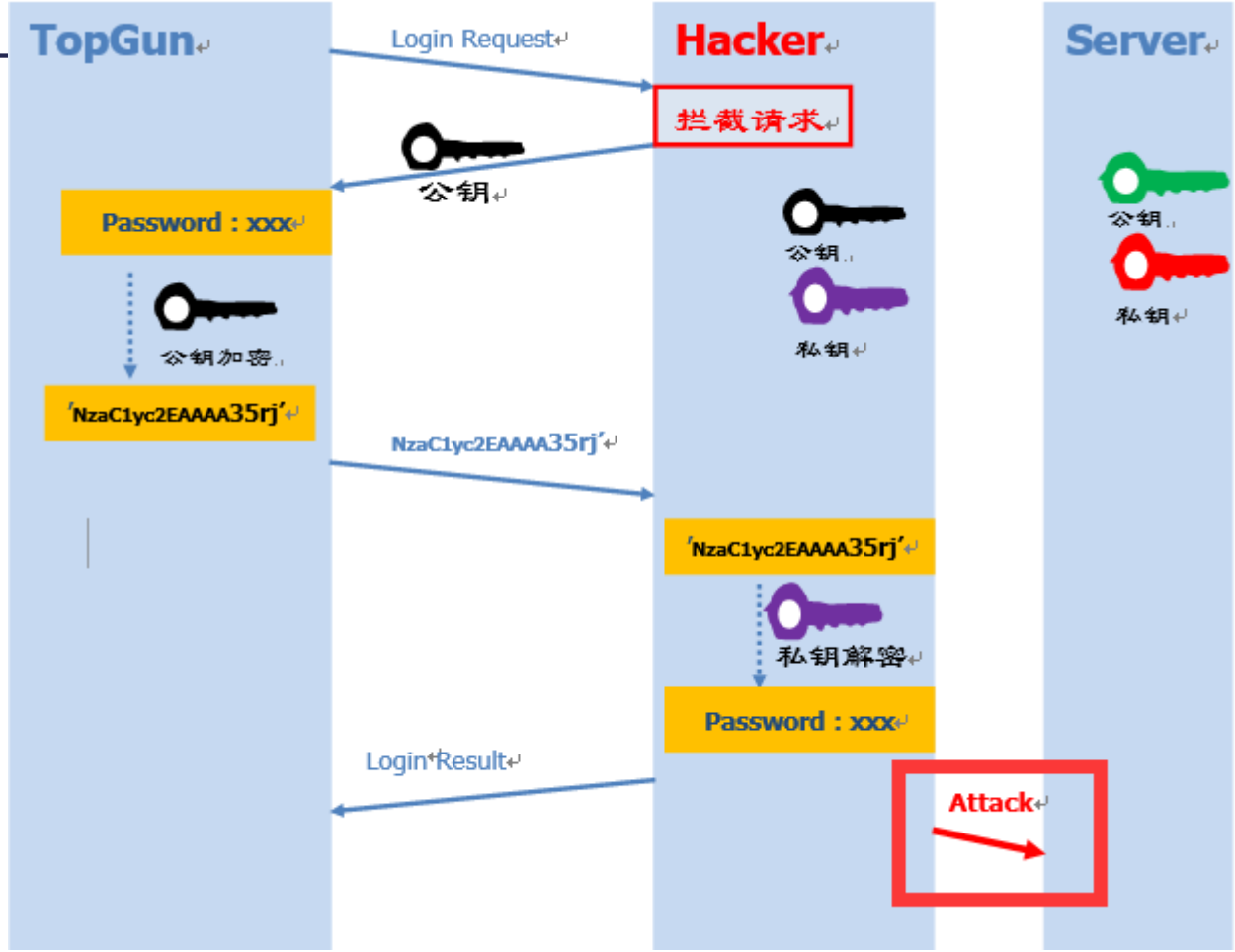
STelnet方式（SSH）登录网络设备

- 中间人攻击（Man-in-the-middle attack）。

STelnet方式（SSH）登录网络设备

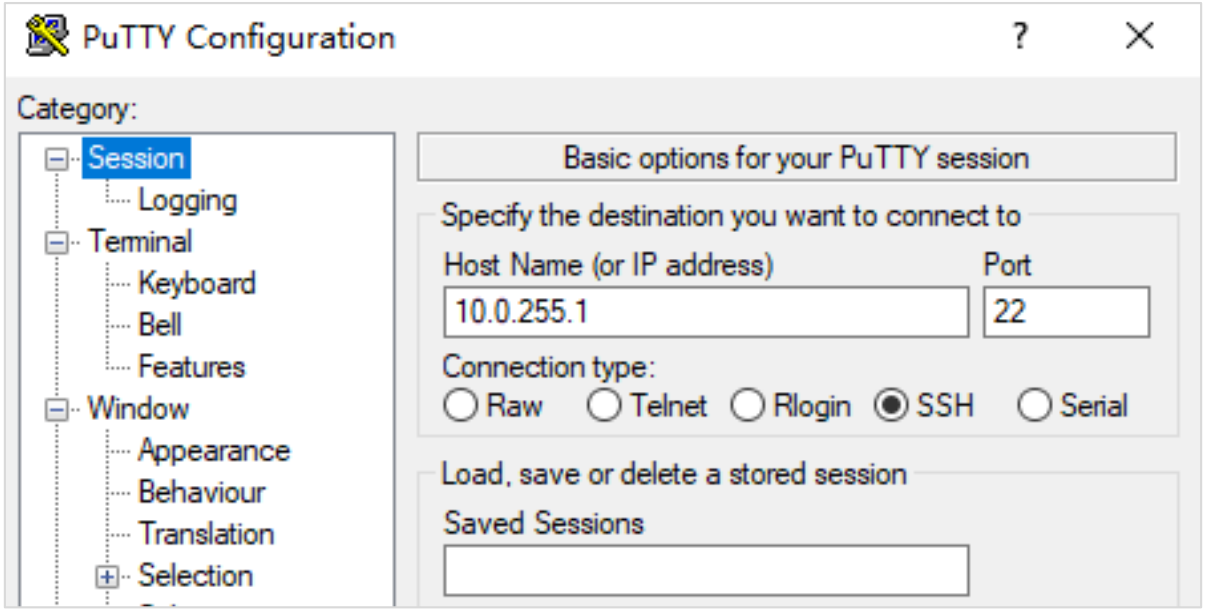
- 中间人攻击（Man-in-the-middle attack）。

中间人攻击


TopGun
Login Request
Hacker
Server
拦截请求
公钥
Password : xxx
公钥
公钥
私钥
公钥加密
'NzaC1yc2EAAAA35rj'
NzaC1yc2EAAAA35rj'
'NzaC1yc2EAAAA35rj'
私钥解密
Password : xxx
Login Result
Attack

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。”

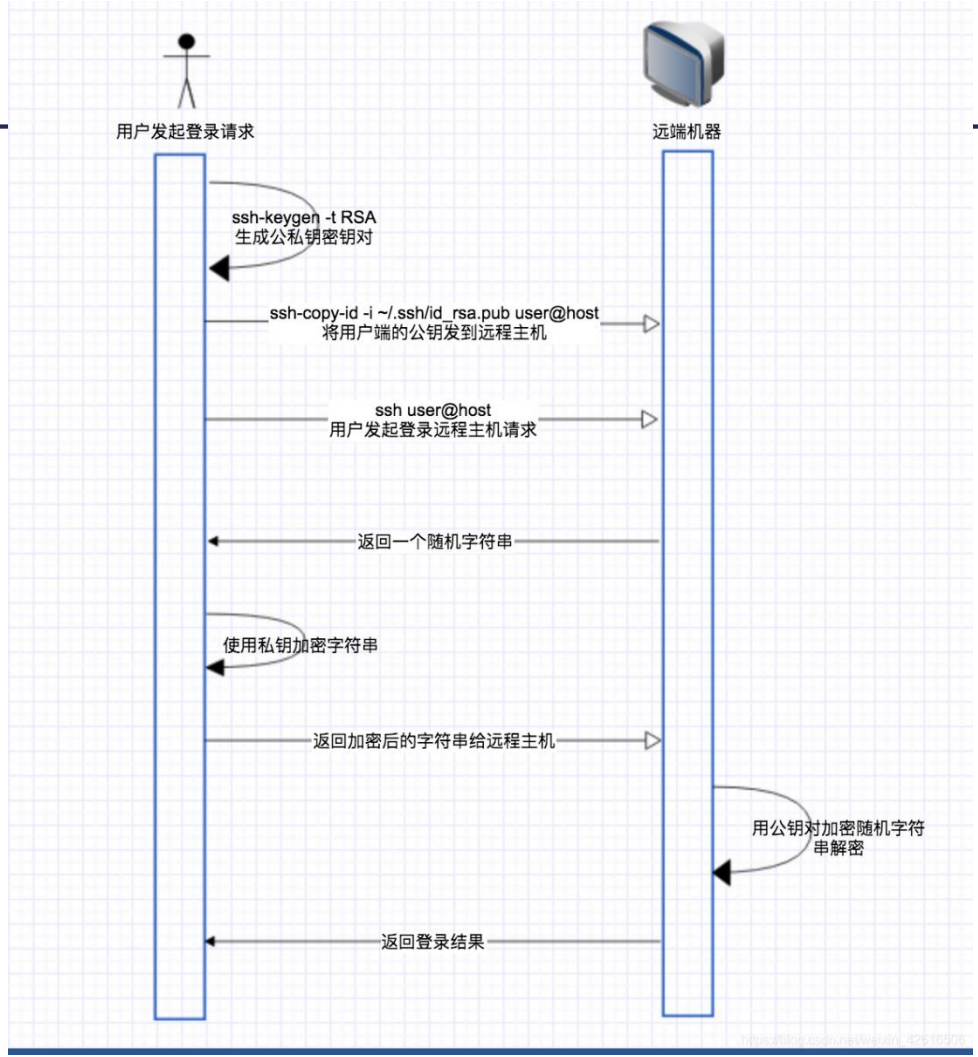
基本含义：无法确认远程设备（Server）的真实性，只知道它的公钥指纹，问你还想继续连接吗？

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


用户发起登录请求
远端机器
ssh-keygen -t RSA
生成公私钥密钥对
ssh-copy-id -i ~/.ssh/id_rsa.pub user@host
将用户端的公钥发到远程主机
ssh user@host
用户发起登录远程主机请求
返回一个随机字符串
使用私钥加密字符串
返回加密后的字符串给远程主机
用公钥对加密随机字符串解密
返回登录结果

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（创建用户名和密码）。

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）。

Web方式登录网络设备

Web方式登录网络设备

Web方式登录网络设备

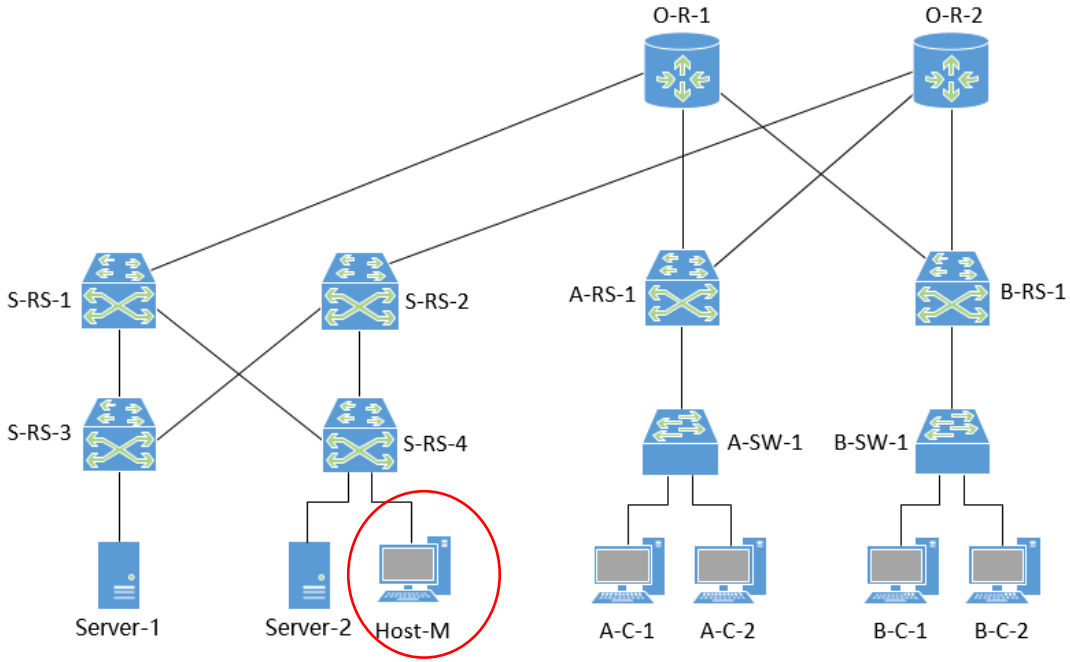
Web方式登录网络设备

六、案例分析：园区网设备的集中远程管理

6.案例分析：园区网设备的集中远程管理

要求

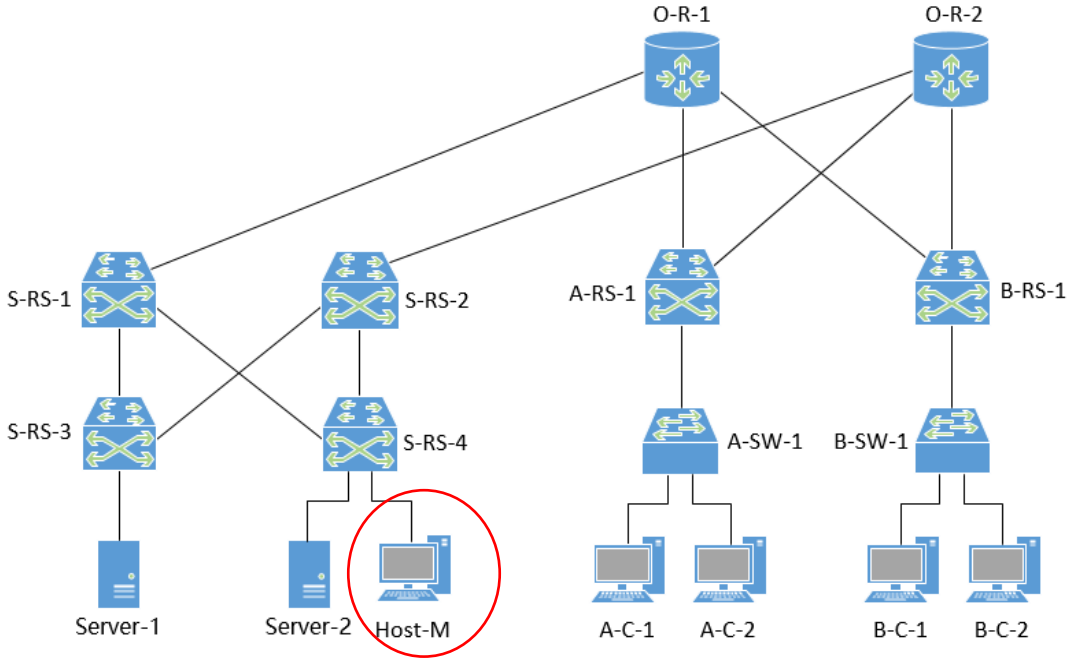
- 在实验一的基础上，添加一台管理机，分别通过Telnet方式和SSH方式实现对园区网网络设备（本实验指路由器、三层交换机）的远程登录管理。。



6.案例分析：园区网设备的集中远程管理

分析1

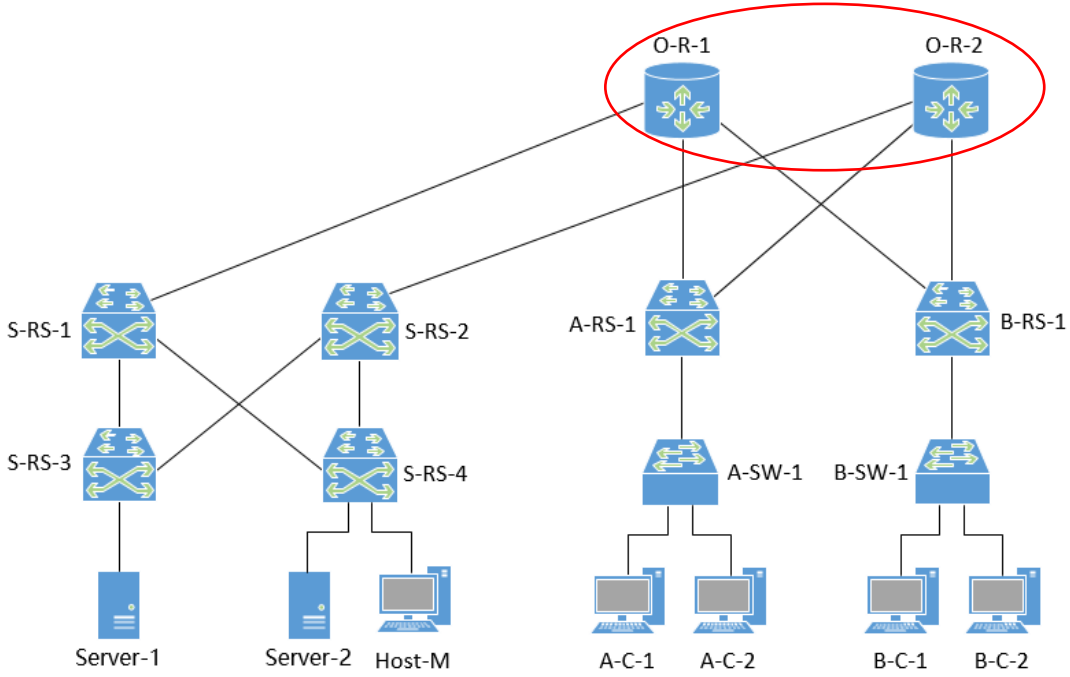
- 管理机采用什么设备？
  如何接入园区网？



6.案例分析：园区网设备的集中远程管理

分析2

- 园区网中的设备需要进行什么配置？



Thanks.