



TELNET Basics

BUPT/QMUL

2021-04-08

Refer to Chapter 24, Textbook



北京邮电大学

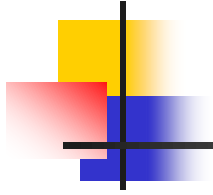
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

Electronic Engineering 



Agenda

- A brief introduction to TELNET
- Concept of remote/virtual terminal
- TELNET operations
- TELNET protocol
- TELNET options negotiation
- Other remote access technologies



A Brief Introduction to TELNET



Brief Introduction To TELNET

- Use of TELNET: BBS
- What is TELNET?
- History



BBS: Bulletin Board System

- A computer system running software that allows users to connect and log in to the system using a terminal program.
- Once logged in, a user can perform functions such as
 - uploading and downloading software and data;
 - reading news and bulletins;
 - and exchanging messages with other users, either through Email or in public message boards.

Traditional BBS example:

```
IVI Monochrome (1.101j 20-Dec-03) (Last on Mon Jun 21 20:50) IVI
HH9?&H[RHGHHGHHG[dBkSi&??Z?::+<:::'\ - -::--::^::d::ISd+L/rHk6Z?Z9&HHHSH9&H&S
&RH Did you know? <FS&::~#SI?::?!-::' . -':l-'?'b;>.,b\LH?>?1Lk/[H]HRRMHV\RH{MP
]pS
DZH Scanning makes it easy to find files that have been added to since
H&H you last read them. Simply press [SPACE] in a menu to find the next
6MH updated file. For more information, press [?][C][H] from this screen.
R,b
HRRk...HSHk/\&VH?HSS&S&/6pt?S?SH&v./\ - .':.+'--. ?b?/?/?>'H>HH9&...ZSH&HHZ&H?
monodoc

Menu [ESC] = Utilities (inc. Talker & EXIT)

Menu [I] = Help and Information on Monochrome

Welcome to
the new
version of
Monochrome!
(version 1.101j)

Menu [N] = News and Media
Menu [T] = Science, Technology and Medicine
Menu [E] = Entertainment
Menu [C] = Society and Culture
Menu [R] = Recreation

Menu [H] = Monochrome Users
Hello 'Guest User'. (guest2:2)
<< 5 other users at Tue Jun 22 03:36 GMT (You have new messages) >>
```

Example of BBS Today(1)



密码



当前总共**8498**人在线: 注册用户**5171**人, 访客**3327**人
powered by BYR-Team©2009-2020.
all rights reserved

Example of BBS Today(2)

全部讨论区

本站站务

北邮校园

学术科技

信息社会

人文艺术

生活时尚

休闲娱乐

体育健身

游戏对战

乡亲乡爱

我的收藏夹

控制面板

北邮人论坛微博

优秀版主评选

投票系统

竞猜系统

积分系统

手机客户端

手机版

北邮人设计

精华区

Telnet登录

搜索讨论区

家庭生活

公告

个人转租房子

地点: 回龙观龙锦苑东二区

学为人师, 行为世范

只招男生

推销与购买的脑机制

50分钟50-70元

飞跃重洋

Ph.D. Position

犹他大学秋季博士招生

安居乐业

求合租

西二旗金域华府一期两居室, 2500出租次卧

创业交流

承接网站、小程序开发、SEO搜索优化

信息产业

实习/社招

广告算法和推荐算法工程师!!!

近期热点活动

公告

我校组织寒假留校学生共度新春, 一起来参加吧!

Momenta北邮站火热来袭~~听大牛给你讲CNN网络SENet的那些事情

思科公司《我的SDN之路》讲座北邮站来啦~

北京邮电大学第二届研究生创新创业成果展参观邀请函

第五期后勤服务学生座谈会要开始啦~

爱邮, 你今天表白了么?

公告

2018考研经验交流会来啦

这一世 你是我唯一的心事

招新

北邮人团队六大组系欢迎你的加入

公告

2018考研经验交流会——政策性问题征集

北邮校园

热门话题

版面列表

分区暂不存在热门话题

生活时尚

热门话题

版面列表

情感的天空 176

谈天说地

如何委婉地告诉室友 味道确实很重?

缘来如此

五一放假第一天征个人去看五月天天津演唱会, 不收票钱

美容护肤

求问

化妆品的淘宝旗舰店水深吗?

绝色可餐

老三的烤鸡饭了解一下~

欢迎2019级保研生选择FNL实验室(31)

4.18日晚学校超市购买茶叶, 有很多小黑虫, 如何维权?(28)

林俊杰北京演唱会, 有没有组队抢票的啊(22)

邀请大家加入“北邮易飞榜”!(18)

晚安前小唱《追光者》(15)

学术科技

热门话题

版面列表

机器学习与数据挖掘

大数据实习

笔记本电脑

8k内游戏本求推荐~

Python

求助

pycharm的社区版不能debug 是设置的问题吗?

算法与程序设计竞赛

问题

百度笔试, 排队问题

科研与论文

讨论

有偿请同学“指导”一篇在职研究生软件工具类论文

电子电路

有没有人用过ioio开发板? 网上买不到了

软件开发

承接网站、小程序开发、SEO搜索优化

信息安全

问题

信安专业英语的学习用书?

电脑硬件与维修

研究生想在宿舍攒个主机, 求建议

人文艺术

热门话题

版面列表

英语吧

如何提高雅思口语???

音乐交流区

生气的时候听什么歌

吉他

在哪里可以练吉他? 坐标沙河

摄影

就是想分享一下.....随拍

休闲娱乐

热门话题

版面列表

海天游踪

有人想夜爬泰山吗

电视剧

《夫妻那些事》简直毁三观啊

宠物家园

好久没来了, 晒猫

telnet BBS of BYR



```
Telnet bbs.byrcn

-----== 本日十大热门话题 ==-----

第 1 名 信区 : Food          【Apr  7 16:54:23 】 42 人      w2017
标题 : 物美的菠萝可太香了啊

第 2 名 信区 : Picture       【Apr  7 16:31:42 】 20 人      a10859241999
标题 : 晚上的花

第 3 名 信区 : Talking       【Apr  7 13:04:07 】 20 人      xzq2016
标题 : 有没有五一想一起去东北或者废弃工厂之类地方的?

第 4 名 信区 : AimGraduate   【Apr  7 16:52:22 】 15 人      Boron
标题 : 21计算机考研 初试404上岸经验

第 5 名 信区 : WorkLife      【Apr  7 15:52:21 】 15 人      zz931213
标题 : 要不要签服务期承诺书啊

第 6 名 信区 : Pet           【Apr  7 14:54:25 】 13 人      miaow
标题 : 求大橘近照

第 7 名 信区 : Constellations 【Apr  7 16:45:45 】 13 人      yinyi
标题 : 【转】超神准! 星座小王子独创的新型占卜、來一起试玩一下!

第 8 名 信区 : Job           【Apr  7 16:35:33 】 11 人      YogurtM
标题 : 【暑期实习offer比较】转正压价问题讨论

第 9 名 信区 : Feeling       【Apr  7 14:24:25 】 10 人      shuidi
标题 : 柳絮抚着那条街

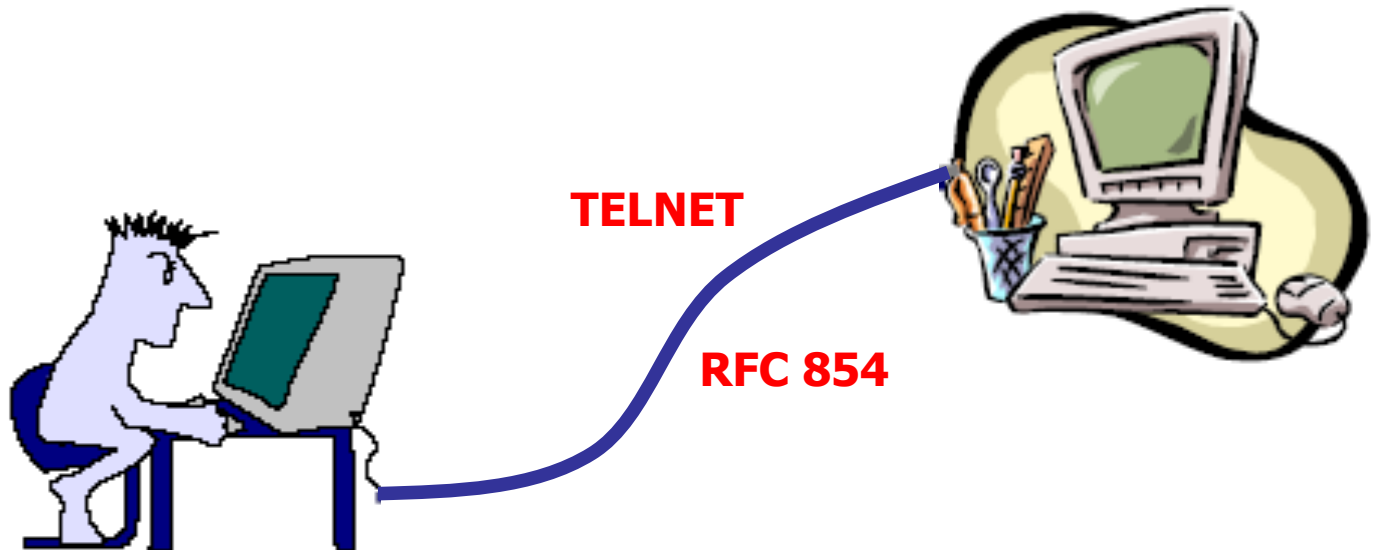
第 10 名 信区 : DigiLife     【Apr  7 15:13:15 】  8 人      A1025718635
标题 : 【收】大疆手机云台

☆ 这是您第 1075 次上站, 上次您是从 10.38.13.126 连往本站。
☆ 上次连线时间为 Wed Apr  7 16:17:03 2021
```

You can also type in: *telnet bbs.byrcn*

What Is TELNET? (1)

- A **protocol** used to establish a **dumb terminal** session to another computer on the Internet
- An important Internet **application** for remote access





What Is TELNET? (2)

- Definition in RFC854
 - The purpose of the TELNET Protocol is to provide a **general, bi-directional, byte oriented** communications facility.
 - Its primary goal is to allow a **standard** method of interfacing **terminal devices and terminal-oriented processes** to each other.
 - It is envisioned that the protocol may also be used for **terminal-terminal** communication ("linking") and **process-process** communication (distributed computation).



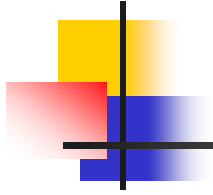
TELNET vs. telnet

- **TELNET** is a *protocol* that provides “a general, bi-directional, eight-bit byte oriented communications facility”
- **telnet** is a *program* that supports the TELNET protocol over **TCP**
- Many application protocols are built upon the TELNET protocol



The History Of Telnet

- Telnet is simple
 - Total pages of RFC 854 is 15
 - HTTP (we will see later) is 176 pages
- The idea of **option negotiation** was a very good design feature
 - Enables telnet to evolve to meet new demands without endless new versions of basic protocol
- Currently over 100 RFCs on telnet and its options



Concept Of Remote / Virtual Terminal

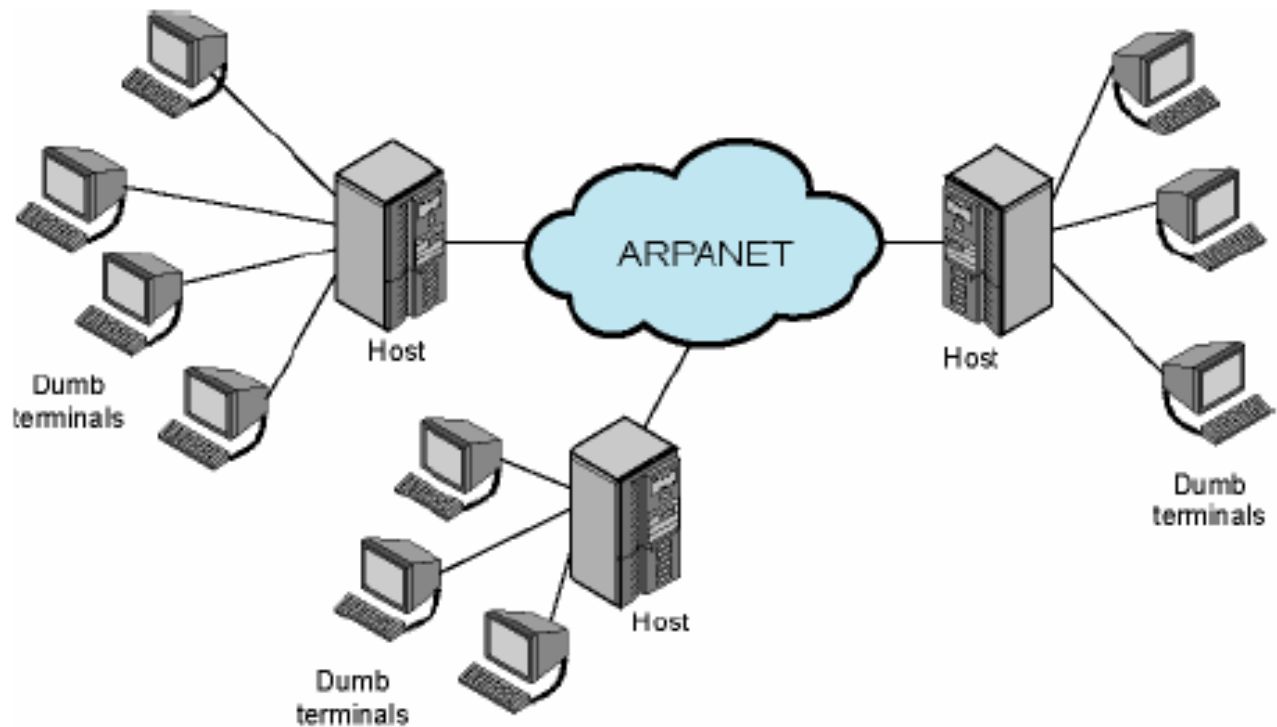


Remote Terminal Access

- Early motivation for networks was remote access to interactive systems
- Dumb terminals (see figure on the next slide)
 - Keyboard and screen with primitive communication hardware
 - Local host computer establish connection to remote host
- The challenge is that terminals and host systems were not standardized
 - local terminal was not speaking the same language as the remote host

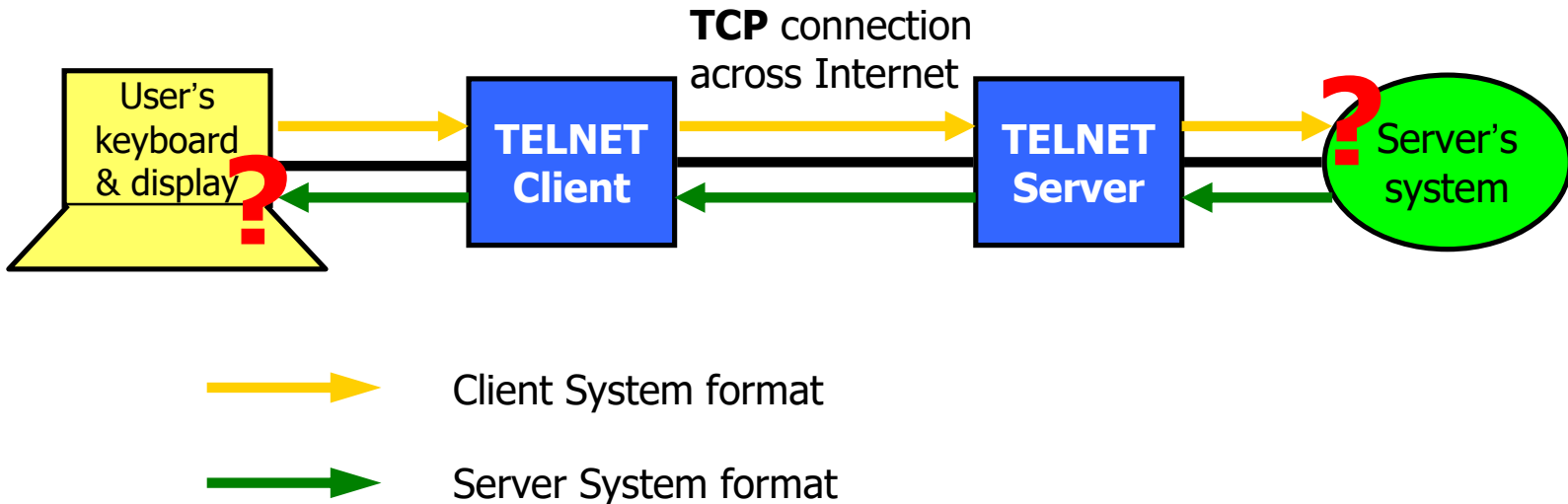


Telnet Operation Environment On Early Internet



Problem

- Lack of **common language** between the terminal and the remote host

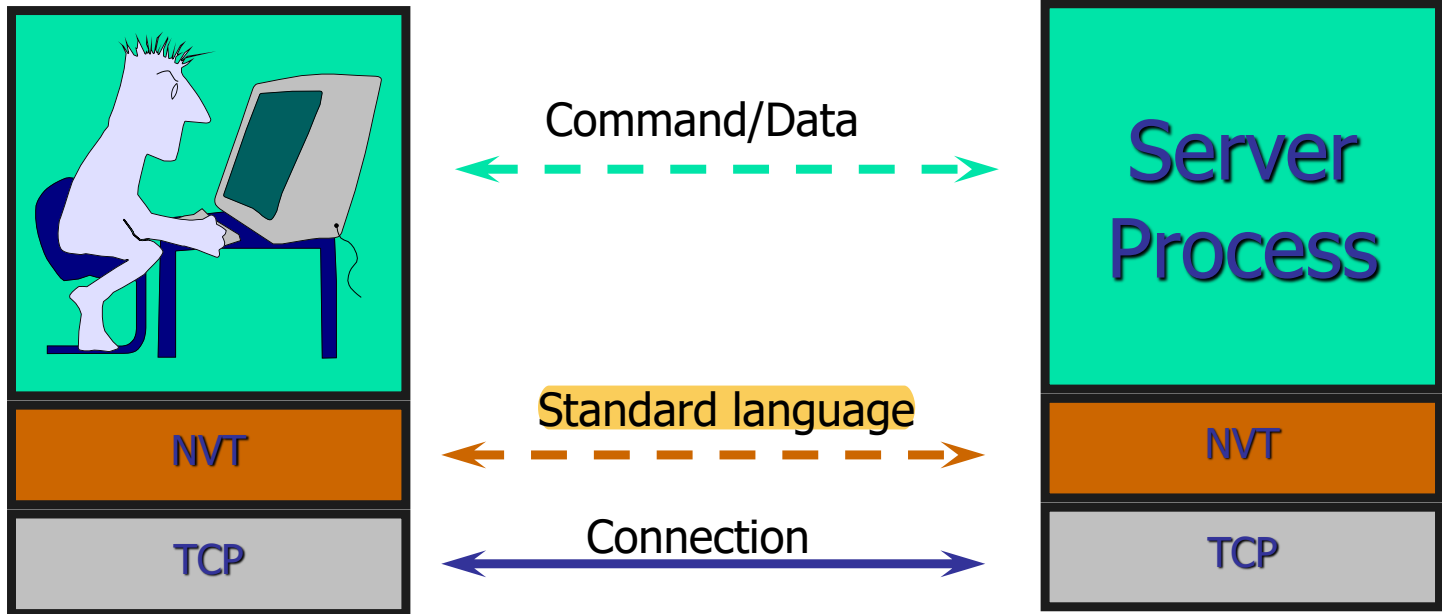




Network Virtual Terminal

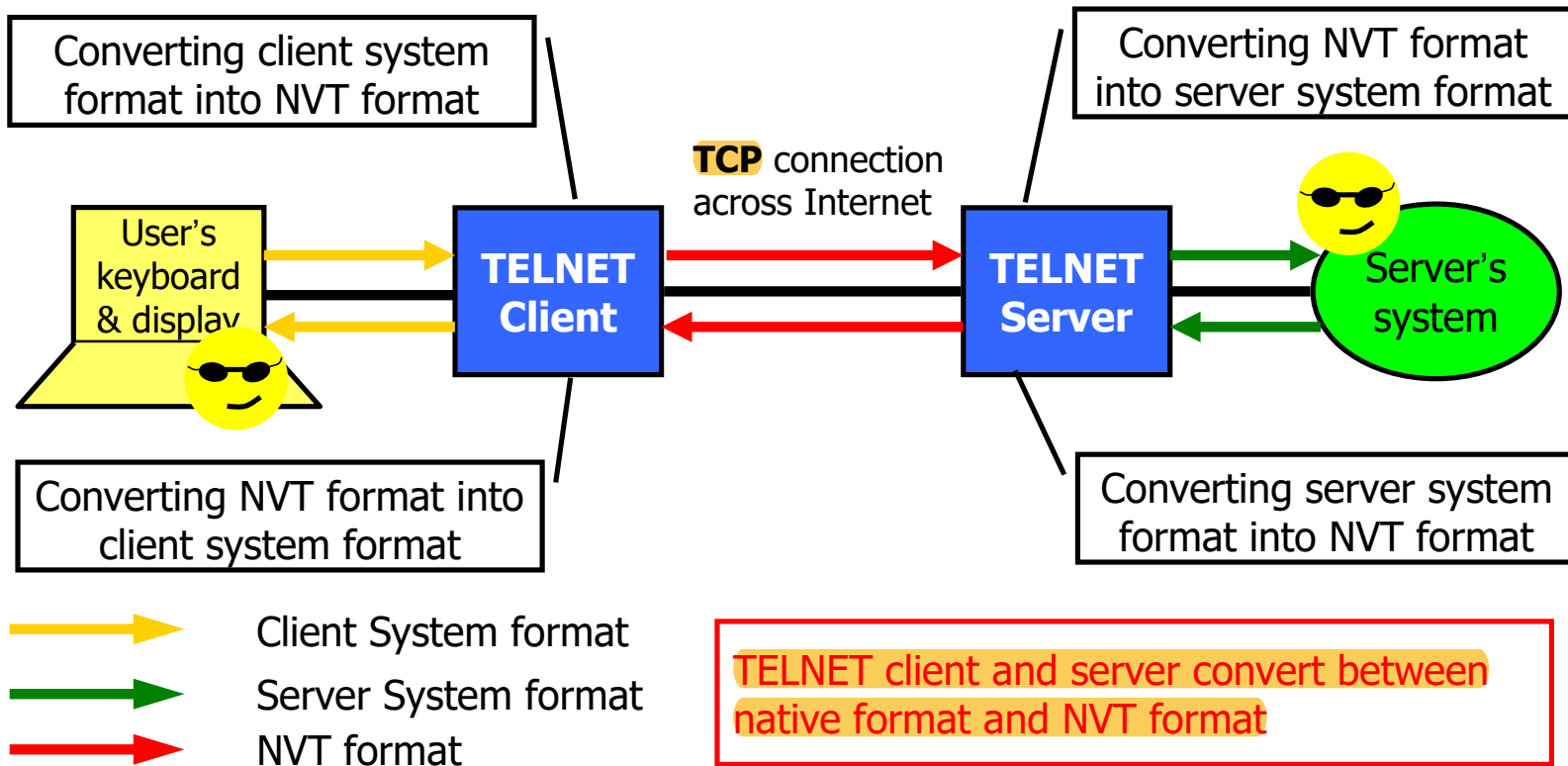
- Transform local characteristics into **standardized form**
 - Network virtual terminal (NVT)
- Imaginary device
 - Well defined set of characteristics
- Both sides generate data and control signals in native language but translates them to NVT form
 - The sending side translates native data and control signals into NVT form before sending out
 - The receiving side gets the NVT data and signals and translates into its native form

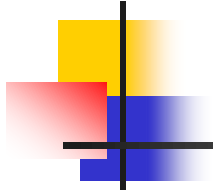
Network Virtual Terminal



NVT Operation

- Accommodating heterogeneity




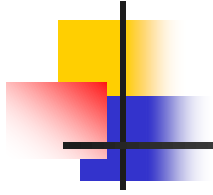


TELNET Operations



TELNET Operations

- Connection management
 - Connection request, establish and terminate
 - Telnet uses **TCP (port 23)** by default
- Option Negotiation
 - To determine **mutually agreeable** set of characteristics and options
- Exchange of **control information** (e.g. end of line), **commands** and **transfer of data** between two correspondents 
- A typical telnet session is to exchange of data between terminal and host
 - Multiple rounds
 - Not only for accessing remote accounts; was also used for interactive system
 - Try “telnet bbs.byr.cn”



TELNET Protocol



Related RFCs

- Basic protocol
 - RFC854: Telnet Protocol Specification
- Options
 - RFC855: Telnet Option Specifications
 - RFC856: Telnet Binary Transmission
 - RFC857: Telnet Echo Option
 - RFC858: Telnet Suppress Go Ahead Option
 - RFC859: Telnet Status Option
 - ...



Some Features

- **TCP connection**: directed toward **port 23** of the server being asked to perform a service
- Data and control **multiplexed** over the same connection
- **NVT** - representation of a **generic** terminal
- **Negotiated options** - Enabling Telnet to evolve to meet new demands without endless new versions of basic protocol
- A **symmetric view** of terminals and processes

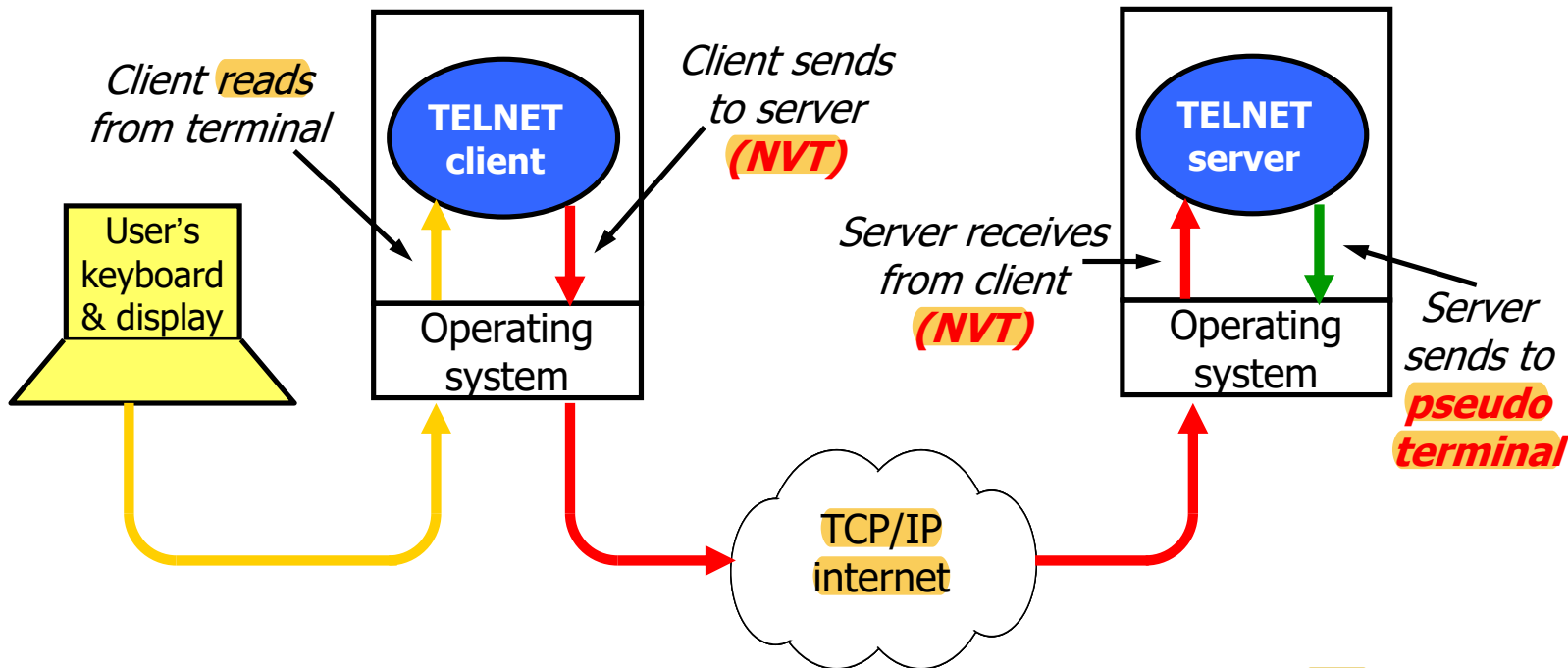


TELNET Protocol

- Transmission of data
- Standard representation of control functions

Transmission Of Data (1)

- Data path from the user's keyboard to the remote system





Transmission Of Data (2)

- Underlying TCP full duplex
 - The underlying network is intrinsically full duplex
- Data sent half duplex
 - The communication between terminal and process is one direction at a time.
- Data sent as stream of 8-bit bytes
 - No other formatting
- Control signals and other non-data information sent as Telnet commands
 - Byte strings embedded in data stream
 - User control signals, commands between Telnet processes as part of protocol and option negotiation and subnegotiation



Control Functions (1)

- TELNET includes support for a series of **control functions** commonly supported by servers
- This provides a uniform mechanism for communication of (the supported) control functions
- You can imagine them as some extra virtual keys in the NVT keyboard



Control Functions (2)

- Interrupt Process (IP)
 - suspend/interrupt/abort/terminate process
- Abort Output (AO)
 - allow a process, which is generating output, to run to completion **but without sending the output to the user's terminal**
- Are You There (AYT)
 - check to see **if system is still running**
- Erase Character (EC)
 - delete last character sent
 - typically used to **edit keyboard input**
- Erase Line (EL)
 - delete all input in current line
 - typically used to edit keyboard input





Control Functions (3) – delivery

Command	Decimal Codes	Description
IAC	255	Interpret next octet as command
DONT	254	Denial of request to perform specific option
DO	253	Approval to allow specific option
WONT	252	Refusal to perform specific option
WILL	251	Agreement to perform specific option
SB	250	Start of option subnegotiation
GA	249	Go ahead
EL	248	Erase line
EC	247	Erase character
AYT	246	Are you there
AO	245	Abort output
IP	244	Interrupt process
BRK	243	Break
DMARK	242	Data mark
NOP	241	No operation
SE	240	End of subnegotiation
EOR	239	End of record



Control Functions (4) – IAC

- TELNET command structure
 - at least a **two byte** sequence: the **IAC** (Interpret as Command) **escape character** followed by **the code for the command**
- The IAC code is **255**  
 - If a 255 is sent as data - it must be followed by another 255
- **Looking for a command**
 - Each receiver must look at each byte that arrives and look for an **IAC**
 - If IAC is found and the next byte is “IAC” - **a single data byte (value 255)** is presented to the application/ terminal
 - If IAC is followed by any other code - the TELNET layer interprets this as **a command**



Control Functions (5)

– DO, DONT, WILL, WONT

- Used for options negotiation
- Examples

Sender	Receiver	Meaning
WILL →	← DO	Sender wants to active a option, and receiver agrees
WILL →	← DON'T	Sender wants to active a option, and receiver refuses
DO →	← WILL	Sender wants receiver to active a option, and receiver agrees
DO →	← WONT	Sender wants receiver to active a option, and receiver refuses



TELNET Options Negotiation



Motivations

- All NVTs support a minimal set of capabilities
- Some terminals have more capabilities than the minimal set
- The two endpoints negotiate a set of mutually acceptable options (character set, echo mode, etc.)
- The set of options is not part of the TELNET protocol, so that new terminal features can be incorporated without changing the TELNET protocol



Option Examples

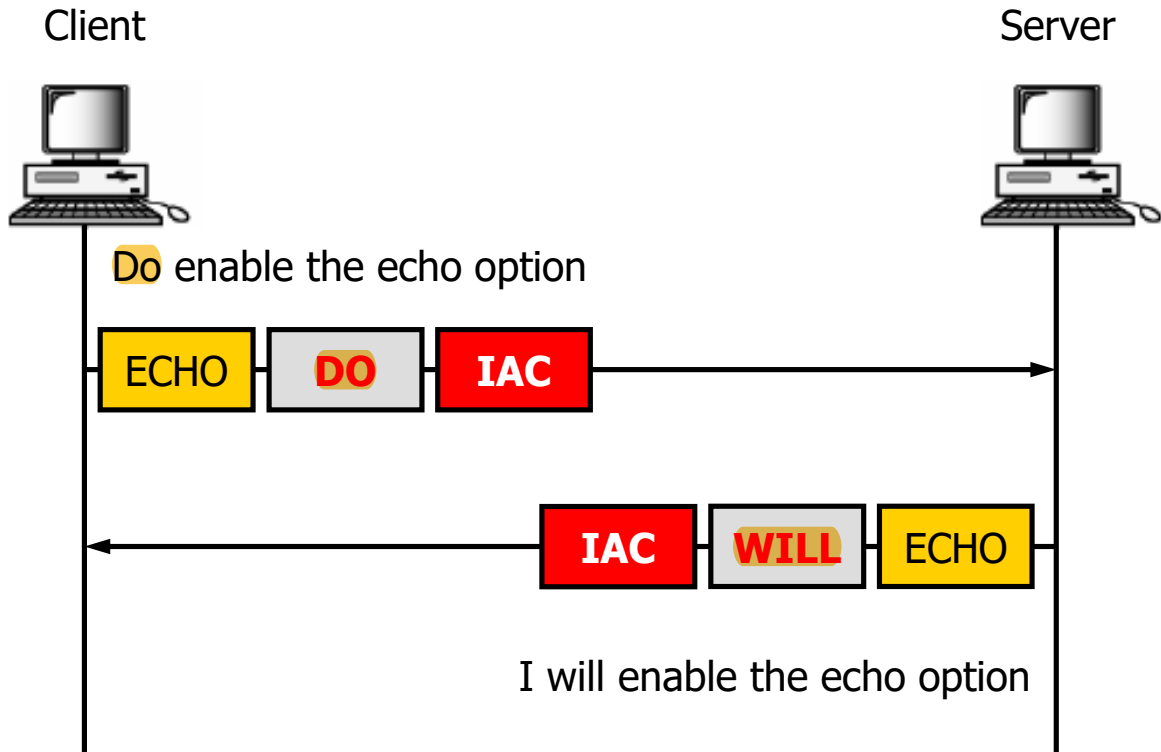
- echo modes
 - Keyboard input be echoed on the terminal side or not
- Line mode vs. character mode
 - One line or one character per transmission
- character set (EBCDIC vs. ASCII)
 - EBCDIC - Extended Binary-Coded Decimal Interchange Code
 - ASCII - American Standard Code for Information Interchange



Options Negotiation

- Each option is assigned a **byte value**
- The **DO, DONT, WILL, and WONT** commands are used to negotiate options
- Options negotiation is **symmetric**
- Steps must be taken to avoid option processing loops
- **Subnegotiations** are used when more information is needed, such as when negotiating terminal type, window size, etc

Example: Negotiation of Echo Option





TELNET Options List (1)

Options	Name	References
0	Binary Transmission	[RFC856]
1	Echo	[RFC857]
2	Reconnection	[NIC50005]
3	Suppress Go Ahead	[RFC858]
4	Approx Message Size Negotiation	[ETHERNET]
5	Status	[RFC859]
6	Timing Mark	[RFC860]
7	Remote Controlled Trans and Echo	[RFC726]
8	Output Line Width	[NIC50005]
9	Output Page Size	[NIC50005]
10	Output Carriage-Return Disposition	[RFC652]
11	Output Horizontal Tab Stops	[RFC653]
12	Output Horizontal Tab Disposition	[RFC654]
13	Output Formfeed Disposition	[RFC655]
14	Output Vertical Tabstops	[RFC656]
15	Output Vertical Tab Disposition	[RFC657]
16	Output Linefeed Disposition	[RFC657]
17	Extended ASCII	[RFC698]
18	Logout	[RFC727]
19	Byte Macro	[RFC735]



TELNET Options List (2)


20	Data Entry Terminal	[RFC1043, RFC732]
21	SUPDUP	[RFC736, RFC734]
22	SUPDUP Output	[RFC749]
23	Send Location	[RFC779]
24	Terminal Type	[RFC1091]
25	End of Record	[RFC885]
26	TACACS User Identification	[RFC927]
27	Output Marking	[RFC933]
28	Terminal Location Number	[RFC946]
29	Telnet 3270 Regime	[RFC1041]
30	X.3 PAD	[RFC1053]
31	Negotiate About Window Size	[RFC1073, DW183]
32	Terminal Speed	[RFC1079]
33	Remote Flow Control	[RFC1372]
34	Linemode	[RFC1184]
35	X Display Location	[RFC1096]
36	Environment Option	[RFC1408]
37	Authentication Option	[RFC1416]
38	Encryption Option	[Borman]
39	New Environment Option	[RFC1572]
40	TN3270E	[RFC1647]
41	XAUTH	[Earhart]
255	Extended-Options-List	[RFC861]



A Telnet Session Example (1)

```
C:\Documents and Settings\Administrator> telnet 192.168.1.253
Red Hat Enterprise Linux AS release 4 <Nahant Update 1>
Kernel 2.6.9-11.Elsmg on an i686
Login: shiyan
Password:
Last login: Sun Nov 11 17:48:30 from 192.168.1.168
[shiyan@localhost ~]$
```

Using Wireshark to know what are sent and received

- 
- **Wireshark**: A network protocol analyzer (packet sniffer)
 - Renamed from Ethereal in 2006
 - Able to **capture packets** transferred on the network and **display packet fields** and their **meanings**
 - Used for network troubleshooting, analysis, software and communications protocol development, and education.

telnet-server-253.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: telnet Expression... Clear Apply

Packet List pane

No.	Time	Source	Destination	Protocol	Info
1402	137.197041	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1403	137.197253	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1405	137.197411	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1406	137.197419	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1408	137.237354	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1409	137.237477	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1410	137.237584	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1412	137.277498	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1414	137.278074	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1415	137.286710	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1417	137.326588	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1419	137.331700	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1420	137.333410	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1421	137.333564	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Packet Details pane

- Frame 1402 (66 bytes on wire, 66 bytes captured)
- Ethernet II, Src: Dell_4f:9d:3a (00:13:72:4f:9d:3a), Dst: AsustekC_14:99:f4 (00:15:f4:99:f4:14)
- Internet Protocol, Src: 192.168.1.253 (192.168.1.253), Dst: 192.168.1.168 (192.168.1.168)
- Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1229 (1229), Seq: 1, Ack: 1, Len: 12
- Telnet
 - Command: Do Terminal Type
 - Command: Do Terminal Speed
 - Command: Do X Display Location
 - Command: Do New Environment Option

Packet Bytes pane

0000	00 15 f2 14 99 f4 00 13 72 4f 9d 3a 08 00 45 10 rO...E.
0010	00 34 17 b2 40 00 40 06 9e 0c c0 a8 01 fd c0 a8	.4..@.
0020	01 a8 00 17 04 cd 64 98 79 f1 8d 0c b3 11 50 18d. y....P.
0030	05 b4 ca 47 00 00 ff fd 18 ff fd 20 ff fd 23 ff	...G... ..#.
0040	fd 27	.

telnet-server-253.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Apply

Some options negotiated firstly

No. .	Time	Source	Destination	Protocol	Info
1402	137.197041	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1403	137.197253	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1405	137.197411	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1406	137.197419	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1408	137.237354	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1409	137.237477	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1410	137.237584	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1412	137.277498	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1414	137.278074	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1415	137.286710	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1417	137.326588	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1419	137.331700	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1420	137.333410	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1421	137.333564	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Frame 1402 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: Dell_4f:9d:3a (00:13:72:4f:9d:3a), Dst: AsustekC_14:99:f4 (00:15:f2:14:99:f4)

Internet Protocol, Src: 192.168.1.253 (192.168.1.253), Dst: 192.168.1.168 (192.168.1.168)

Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1229 (1229), Seq: 1, Ack: 1, Len: 12

Telnet

Command: Do Terminal Type

Command: Do Terminal Speed

Command: Do X Display Location

Command: Do New Environment Option

IAC

DO

Terminal Type

255

253

24

ff

fd

18

0000 00 15 f2 14 99 f4 00 13 72 4f 9d 3a 08 00 15 10 rO...E.

0010 00 34 17 b2 40 00 40 06 9e 0c c0 a8 11 fd c0 a8 .4..@.@.

0020 01 a8 00 17 04 cd 64 98 79 fd 0c b3 11 50 18d. y....P.

0030 05 b4 ca 47 00 00 ff fd 18 11 fd 20 ff fd 23 ff ...G.. ..#.

0040 fd 27

telnet-server-253.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: telnet Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1402	137.197041	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1403	137.197253	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1405	137.197411	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1406	137.197419	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1408	137.237354	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1409	137.237477	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1410	137.237584	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1412	137.277498	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1414	137.278074	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1415	137.286710	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1417	137.326588	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1419	137.331700	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1420	137.333410	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1421	137.333564	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Frame 1412 (64 bytes on wire, 64 bytes captured)

Ethernet II, Src: AsustekC_14:99:f4 (00:15:f2:14:99:f4), Dst: Dell_4f:9d:3a (00:13:72:4f:9d:3a)

Internet Protocol, Src: 192.168.1.168 (192.168.1.168), Dst: 192.168.1.253 (192.168.1.253)

Transmission Control Protocol, Src Port: 1229 (1229), Dst Port: telnet (23), Seq: 31, Ack: 28, Len: 10

Telnet

Suboption Begin: Terminal Type
Here's my Terminal Type
Value: ANSI
Command: Suboption End

Suboption about the terminal type
ANSI / DEC / IBM3270 / ...

IAC SB Terminal Type IAC SE

0000 00 13 72 4f 9d 3a 00 15 f2 14 99 f4 08 00 45 00 ..rO:... ..E.
0010 00 32 0a 40 40 00 80 06 6b 14 c0 a8 01 a8 c0 a8 .2.@@... k.....
0020 01 fd 04 cd 00 17 8d 0c b3 2f 64 98 7a 0c 50 18/d z p.
0030 fa e9 5f 9a 00 00 ff fa 18 00 41 4e 53 49 ff f0ANSI..

telnet-server-253.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: telnet Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1402	137.197041	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1403	137.197253	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1405	137.197411	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1406	137.197419	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1408	137.237354	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1409	137.237477	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1410	137.237584	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1412	137.277498	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1414	137.278074	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1415	137.286710	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1417	137.326588	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1419	137.331700	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1420	137.333410	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1421	137.333564	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Frame 1419 (151 bytes on wire, 151 bytes captured)

Ethernet II, Src: Dell_4f:9d:3a (00:13:72:4f:9d:3a), Dst: AsustekC_14:99:f4 (00:15:f2:14:99:f4)

Internet Protocol, Src: 192.168.1.253 (192.168.1.253), Dst: 192.168.1.168 (192.168.1.168)

Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1229 (1229), Seq: 40, Ack: 53, Len: 97

Telnet

Command: Don't Echo

Command: Will Echo

Data: Red Hat Enterprise Linux AS release 4 (Nahant update 1)\r\n

Data: Kernel 2.6.9-11.ELsmp on an i686\r\n

Some prompt information given by the server

Data and control multiplexed over the same connection

```

0000  00 15 f2 14 99 f4 00 13 72 4f 9d 3a 08 00 45 10  ....rO...E.
0010  00 89 17 c6 40 00 40 06 9d a3 c0 a8 01 fd c0 a8  ....@.@. ....
0020  01 a8 00 17 04 cd 64 98 7a 18 8d 0c b3 45 50 18  ....d. z.....EP.
0030  05 b4 d0 1e 00 00 ff fe 01 ff fb 01 52 65 64 20  ....Red
0040  48 61 74 20 45 6e 74 65 72 70 72 69 73 65 20 4c  Hat Ente rprise L
0050  69 6e 75 78 20 41 53 20 72 65 6c 65 61 73 65 20  inux AS release
0060  34 20 28 4e 61 68 61 6e 74 20 55 70 64 61 74 65  4 (Nahan t update
0070  20 31 29 0d 0a 4b 65 72 6e 65 6c 20 32 2e 36 2e  1)..Ker nel 2.6.
0080  39 2d 31 31 2e 45 4c 73 6d 70 20 6f 6e 20 61 6e  9-11.ELs mp on an
0090  20 69 36 38 36 0d 0a                                i686..
  
```

When I typed in login ID "shiyan"

No.	Time	Source	Destination	Protocol	Info
1417	137.320388	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1419	137.331700	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1420	137.333410	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1421	137.333564	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1422	137.333649	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1427	139.346597	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1429	139.346849	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1430	139.439606	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1431	139.439869	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1432	139.523179	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1433	139.523454	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1434	139.608721	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1435	139.608871	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1437	139.841050	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1438	139.841236	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1439	139.937124	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1440	139.937312	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1443	140.255423	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1444	140.255631	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1446	140.391176	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1449	141.033455	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1451	141.154705	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1453	141.225313	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1456	141.336550	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1458	141.528760	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1460	141.685240	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1464	142.028721	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1466	142.029022	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1468	142.201615	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Character 's' sent to server

Echo character 's' to client

Character 'h' sent to server

Echo character 'h' to client

...

Character mode

Ethernet II, Src: AsustekC_14:99:f4 (00:15:f2:14:99:f4), Dst: Dell_4f:9d:3a (00:13:72:4f:9d:3a)
 Internet Protocol, Src: 192.168.1.168 (192.168.1.168), Dst: 192.168.1.253 (192.168.1.253)
 Transmission Control Protocol, Src Port: 1229 (1229), Dst Port: telnet (23), Seq: 59, Ack: 144, Len: 1
 Telnet

```

0000  00 13 72 4f 9d 3a 00 15 f2 14 99 f4 08 00 45 00  ..rO... ..E.
0010  00 29 0a 46 40 00 80 06 6b 93 c0 a8 01 a8 c0 a8  .).F@... k.....
0020  01 fd 04 cd 00 17 8d 0c b3 4b 64 98 7a 80 50 18  .... .kd.z.P.
0030  fa cc 98 b3 00 00 73  ....S
  
```


telnet-server-253.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

When I pressed ENTER

No.	Time	Source	Destination	Protocol	Info
1440	139.937312	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1443	140.255423	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1444	140.255631	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1446	140.391176	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1449	141.033455	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1451	141.154705	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1453	141.225313	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1456	141.336550	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1458	141.528760	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1460	141.685240	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1464	142.028721	192.168.1.168	192.168.1.253	TELNET	Telnet Data ...
1466	142.029022	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...
1468	142.201615	192.168.1.253	192.168.1.168	TELNET	Telnet Data ...

Frame 1466 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: Dell_4f:9d:3a (00:13:72:4f:9d:3a), Dst: AsustekC_14:99:f4 (00:15:f2:14:99:f4)

Internet Protocol, Src: 192.168.1.253 (192.168.1.253), Dst: 192.168.1.168 (192.168.1.168)

Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1229 (1229), Seq: 162, Ack: 75, Len: 2

Telnet

Data: \r\n

CR LF

13 10

0d 0a

0000 00 15 f2 14 99 f4 00 13 72 4f 9d 3a 08 00 45 10 rO...E.
0010 00 2a 17 ec 40 00 40 06 9d 3a c0 a8 01 fd c0 a8 *..@.@.
0020 01 a8 00 17 04 cd 64 98 92 8d 0c b3 5b 50 18d. z....[P.
0030 05 b4 f3 9f 00 00 0d 0a 00 00 00 00



Summary (1) – usages of telnet

- Use Internet accounts you may have on remote computers
 - you need an account (login ID) and password on the remote computer to permit access
- Use free services accessible with telnet, e.g.
 - library catalogues
 - databases
 - BBS (Bulletin Board System)
 - Router/switch configuration



Summary (2) – Disadvantages of telnet

- Poor user interface
 - Based on dumb terminal
 - Text-only display
 - Monochrome
 - One color for text, one for background
 - Have to type command-line commands
 - Often have complex syntax
 - Not very secure, SSH made enhancement
 - TELNET does not encrypt any data sent over the connection (**including passwords**)



Other Remote Access Technologies



Other Remote Access Technologies

- **Remote login** in text-based system
 - telnet
 - SSH
 - Rlogin
- **Remote desktop** in windowing system
 - VNC (Virtual Network Computing)
 - RDP (Remote Desktop Protocol)



SSH (1) – brief information

- Secure Shell
- Command line terminal connection tool
- All traffic **encrypted**
- Both ends **authenticate** themselves to the other end
- Ability to carry and encrypt non-terminal traffic
- Private key kept on client, public key stored on server
- Now, it is an IETF standard
 - **RFC4251**, The Secure Shell (SSH) Protocol Architecture



SSH (2) – two enhancements of telnet

- Providing secure communications
- Providing users with the ability to perform additional, independent data transfer over the same connection that is used for remote login

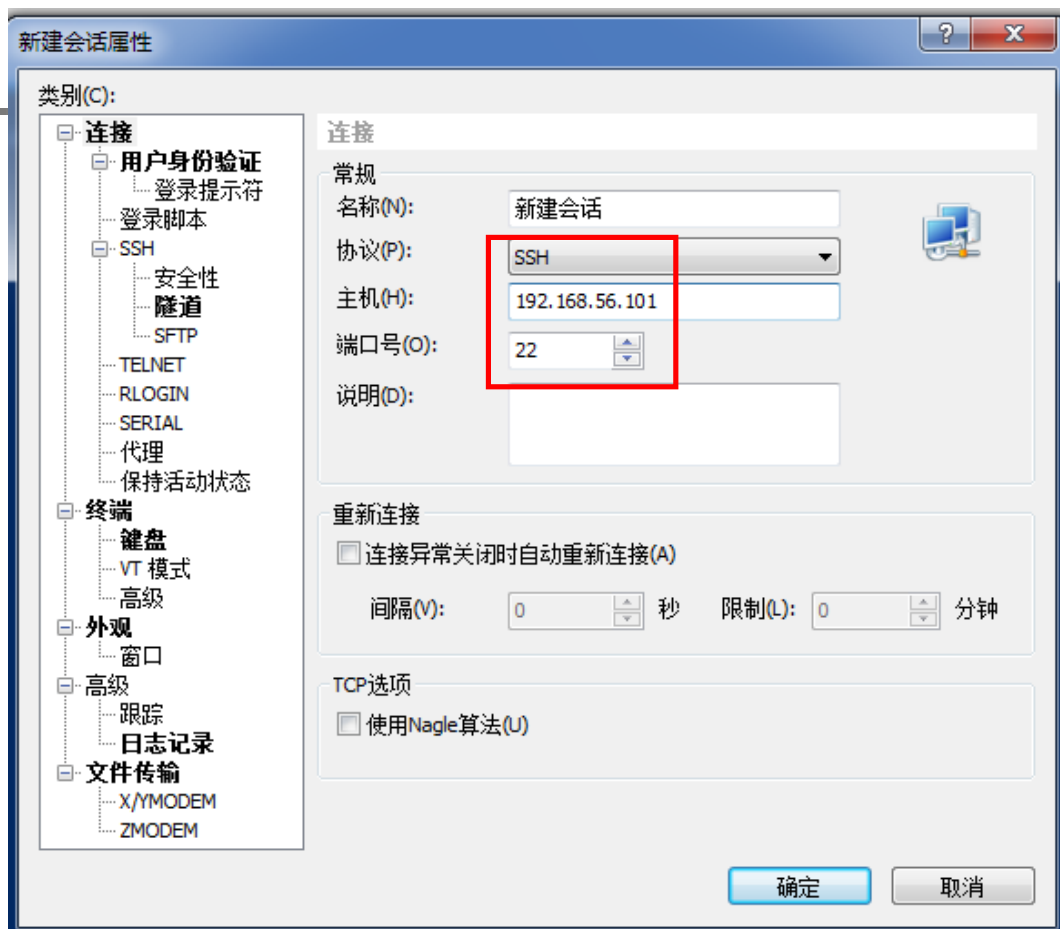


SSH (3) – three major mechanisms

- A transport layer protocol that provides sever authentication, data confidentiality, and data integrity with perfect forward secrecy
- A user authentication protocol that authenticates the user to the server
- A connection protocol that multiplexes multiple logical communications channels over a single underlying SSH connection

SSH (4) – tools

■ Xshell5





Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.101	192.168.56.1	SSH	1434	Encrypted response packet len=1380
2	0.011157000	192.168.56.1	192.168.56.101	SSH	170	Encrypted request packet len=116
3	0.014711000	192.168.56.101	192.168.56.1	SSH	14654	Encrypted response packet len=14600
4	0.016350000	192.168.56.1	192.168.56.101	TCP	60	50771 > ssh [ACK] Seq=117 Ack=4301 Win=256 Len=0
5	0.016377000	192.168.56.101	192.168.56.1	SSH	1890	Encrypted response packet len=1836
6	0.016402000	192.168.56.1	192.168.56.101	TCP	60	50771 > ssh [ACK] Seq=117 Ack=7221 Win=256 Len=0

▶ Frame 2: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
▶ Ethernet II, Src: 0a:00:27:00:00:13 (0a:00:27:00:00:13), Dst: CadmusCo_d3:fd:ae (08:00:27:d3:fd:ae)
▶ Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 192.168.56.101 (192.168.56.101)
▶ Transmission Control Protocol, Src Port: 50771 (50771), Dst Port: ssh (22), Seq: 1, Ack: 1381, Len: 116

SSH Protocol

Encrypted Packet: 0000005001e1ce6bd9dafd74f6bc1869991d1219ea29089f...

0000	08 00 27 d3 fd ae 0a 00 27 00 00 13 08 00 45 00	..'. '.....E.
0010	00 9c 4a 01 40 00 80 06 be a3 c0 a8 38 01 c0 a8	..J.@...8...
0020	38 65 c6 53 00 16 3f 66 ee 0e 58 5e f9 8e 50 18	8e.S..?f ..X^..P.
0030	01 00 b1 f5 00 00 00 00 00 50 01 e1 ce 6b d9 daP...k..
0040	fd 74 f6 bc 18 69 99 1d 12 19 ea 29 08 9f c3 6e	.t...i.. ...)...n
0050	47 3d 78 7c c9 b7 2a 7d e5 14 59 ae bc b1 c2 1b	G=x ..*} ..Y.....
0060	16 a9 a6 f0 a8 21 90 d2 67 97 fe cd ab a1 5c 7a!.. g.....\z
0070	48 60 e9 a1 40 64 65 8a 3d ba dc c2 c0 33 55 c9	H`..@de. =....3U.
0080	81 e7 f2 a8 2b 02 6a 27 12 86 6d 80 80 fe 58 e7	..i7 ..m..Y



Helpful URLs

- RFCs
 - <http://www.ietf.org/>
- Useful utilities
 - <http://winfiles.search.com/search?cat=316&tag=ex.sa.fd.srch.wf&q=TELNET>
- About telnet
 - <http://en.wikipedia.org/wiki/Telnet>
 - <http://baike.baidu.com/item/Telnet>
- About SSH
 - <http://www.ssh.com>
- About realVNC
 - <http://www.realvnc.com/>