

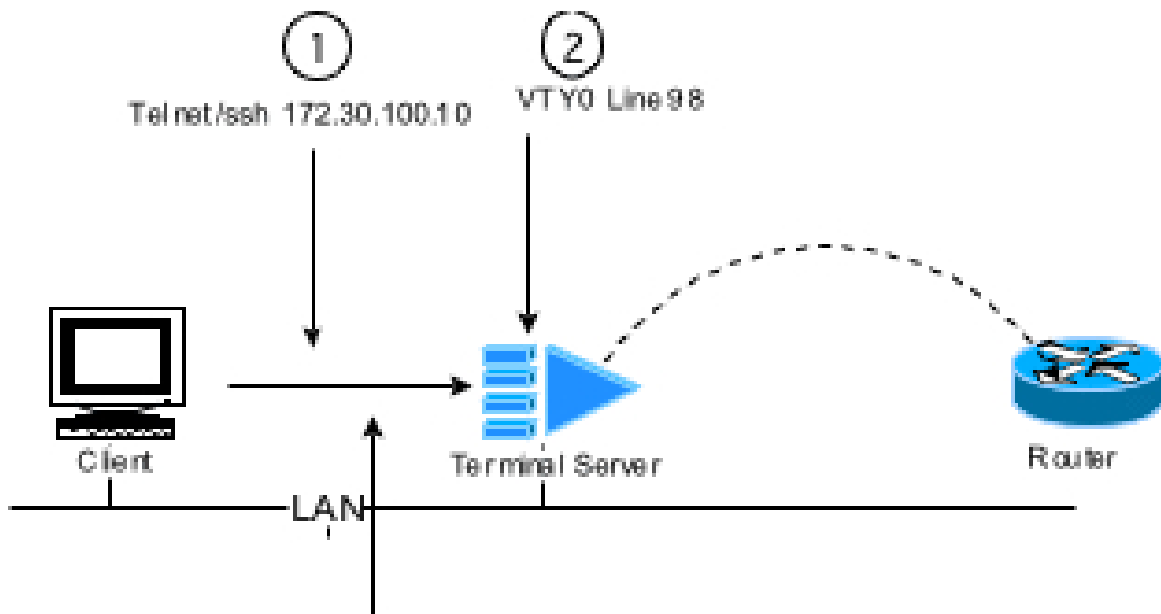
Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin

Configuring out-of-band (OOB) terminal services on a 26xx or 3xxx series routers is one of those tasks that on the face seems quite simple, but becomes far more involved once you start. The reason for this lies not in the configuration of the terminal server to support DTE to DTE connections between itself and the connected devices. Rather it is in the administrative elements (i.e., defining user access, user authentication, and device access control) of the configuration that make deploying an OOB terminal server a challenge. This article will focus on how users interact with the terminal server and its connected devices through the use of:

- Reverse telnet
- Line and group rotaries
- Terminal line interfaces

The easiest way to get your arms around the concept of reverse telnet is to start with the concept of forward telnet. Forward telnet is what's commonly referred to as "telnet." It is the process in which a line on the router accepts a connection on a terminal line interface. In other words, this is "normal" telnet. The client opens a telnet session, the server accepts the session, and client now has a virtual terminal on the server. The key idea here is that the session is accepted into the line. This same idea holds true when using SSH to open a session (so in these instances the term "forward SSH" would apply). Here is a simple illustration:

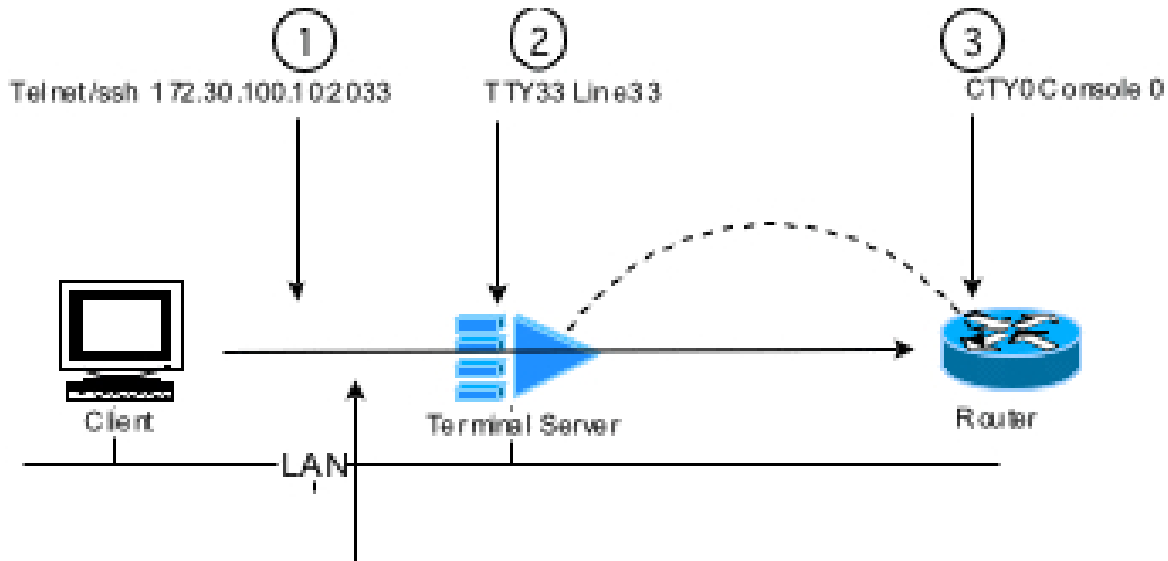


Client opens Telnet/ssh session to a Virtual Terminal Line 0, logical terminal line 98 on the Terminal Server. Upon successful authentication, the client has access to the Terminal Servers CLI.

The reverse telnet (and by extension reverse SSH) process is one in which a connection is established out of a terminal line, thus allowing communication to take place between a client and a directly connected upstream device. Here is another illustration:

Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin



Client opens Telnet/ssh session to service port 2033, Async Terminal Line 33, logical terminal line 33 on the Terminal Server. To connect to Console 0, logical terminal line 0 on the connected router. Upon successful authentication on the terminal server, the client has access to the routers Console port.

Along with the session path, the other critical difference between forward telnet and reverse telnet is authentication. In order for a forward session to be opened, the IOS requires authentication to be in place and successful for the session to be established. When a reverse session is opened, the IOS provides the capability, but does not require authentication for the session to be established. Reverse telnet/SSH is how users interact with the devices connected to the terminal server's async line or the auxiliary line. Reverse telnet/SSH support is enabled using the line configuration command `<transport input {telnet | ssh}>`. Here is a configuration example:

```
outland-ts(config)#line vty 15
outland-ts(config-line)#transport input telnet ssh
outland-ts(config-line)#exit
```

To connect using reverse telnet (SSH), you need to know the IP address of the terminal server hardware interface (or loopback interface) and the rotary group. The IOS uses rotaries to provide connectivity to line interfaces.

There are two types of rotaries: rotary groups and rotary lines. Rotary groups are used to provide connection access to one or more router line interfaces. The number of rotary groups a router can support depends on the hardware and IOS version. The base TCP port for group rotaries starts at 3000. To connect to a rotary group, a reverse telnet session is established to the TCP base port plus the rotary group number. For example, if the rotary group number is 47, the connection service port would be 3047. The most common use of rotary groups is for creating a dial-out modem pool. A group of async lines attached to modems are grouped to a single connection port. Users establish reverse telnet sessions to the rotary group. Then, once connected, the rotary group routes the session to a free group member.

Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin

Line rotaries behave the same way as group rotaries, except only a single line interface is associated with a line rotary. The TCP base port for line rotaries is 2000. To connect to a line rotary, a reverse telnet session is opened to the TCP base port 2000 plus the line number. So to connect to a device attached to async line 1, the line rotary port would be 2001. To connect to the device attached to line 1, a telnet connection to one of the router's IP interfaces at port 2001 needs to be opened.

```
Trinity:~ user$ telnet outlan-ts 2001
Trying 157.191.170.50...
Connected to outlan-ts01
Escape character is '^]'.

```

Your connected to outlan-ts01

User Access Verification

Username:

If SSH support has been configured, the same holds true. An SSH client connection to port 2001 must be opened:

```
Trinity:~ martin$ ssh -l martin outlan-ts -p 2001
Password:

```

Understanding IOS Terminal (Tty) Lines

Once you understand how rotaries work, it becomes immediately apparent why understanding IOS terminal lines is important. The IOS supports four types of terminal lines: console, async, auxiliary and virtual. Each IOS line type has its own unique function, personality and purpose. The IOS uses line interfaces to provide asynchronous communication for IOS command-line interface (CLI) access and protocol-based data transmission. The IOS supports four types of terminal lines, but every line type is not supported in every hardware family. To see the terminal lines available on any given router, use the command <show line>. Here is the command output from a 2600 router with a NM-16A installed:

```
outland-ts#sh line
  Tty Typ      Tx/Rx      A Modem  Roty  AccO  AccI  Uses  Noise  Overruns  Int
   0 CTY
  33 TTY    9600/9600  - -      1 - -    48   104    0/0      -
  34 TTY    9600/9600  - -      2 - -     6     0    0/0      -
  35 TTY    9600/9600  - -      - - -     0     0    0/0      -
 * 36 TTY    9600/9600  - -      - - -     7   293    0/0      -
  37 TTY    9600/9600  - -      - - -     1    10    0/0      -
  38 TTY    9600/9600  - -      - - -     1   129    0/0      -
  39 TTY    9600/9600  - -      - - -     0     0    0/0      -
  40 TTY 115200/115200- inout  - - -     6     0    0/0      -
  41 TTY    9600/9600  - -      - - -     0     0    0/0      -
  42 TTY    9600/9600  - -      - - -     0     0    0/0      -
  43 TTY    9600/9600  - -      - - -     0     0    0/0      -
  44 TTY    9600/9600  - -      - - -     0     0    0/0      -
  45 TTY    9600/9600  - -      - - -     0     0    0/0      -
  46 TTY    9600/9600  - -      - - -     0     0    0/0      -
  47 TTY    9600/9600  - -      - - -     0     0    0/0      -
  48 TTY    9600/9600  - -      - - -     0     0    0/0      -
  65 AUX    9600/9600  - -      - - -     0     0    0/0      -
 * 66 VTY
 * 67 VTY
  68 VTY
      - -      - - -    1143  0    0/0      -
      - -      - - -     89   0    0/0      -
      - -      - - -     20   0    0/0      -

```

Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin

```
69 VTY          -   -   -   -   -   0       0       0/0       -  
70 VTY          -   -   -   -   -   0       0       0/0       -
```

Line(s) not in async mode -or- with no hardware support:
1-32, 49-64

outlan-ts#

The <show line> command lists the available (and non-available) Tty lines by number, type, speed, and rotary, and provides stats on usage and operational state. (The * indicates the line is active.) The 2600 family is one of the three hardware lines (along with the 25xx and 3x00 series) that supports all four line types:

- CTY: The console line provides hardware level CLI access. Wired as a DTE line without any handshaking support, it supports speeds up to 9600 baud. The CTY port is always Tty 0. The console port does not support reverse connections.
- AUX : The auxiliary port provides a DTE asynchronous line for dial-in/dial-out support. The Aux line supports DTE to DCE handshaking and is capable of connection rates up to 115,200 baud (36,600 on lower end hardware). The AUX line Tty line number differs depending on whether the router hardware supports asynchronous serial lines, but the AUX line is always numbered as the last physical Tty port.

The AUX line supports reverse connections through a line rotary with a base TCP port of 2000. This table list AUX line rotaries for the different hardware platforms:

Hardware platform	Tty line and line rotary
7x00, 25x0, 17x0	Tty 1 = 2001
26xx	Tty 65 = 2065
3620	Tty 65 = 2065
3640	Tty 129 = 2129
3660	Tty 193 = 2093
3725	Tty 97 = 2097
3745	Tty 129 = 2129

VTY: Virtual terminal lines provide CLI access to the router. Most platforms can support up to 15 VTY interfaces. VTY lines listen on the default service ports for the protocols for which they are configured to support inbound connections. These are defined using the line configuration command <transport input {all | ssh | telnet | rlogin | v120 | none}>. VTY lines can also be members of rotary groups starting at the base TCP port of 3000, but only support forward connections.

TTY: Asynchronous DTE lines have full handshaking support capable of data rates up to 115,200 baud. When enabled, TTY lines support reverse connections through line (base port 2000 + Tty line number) and group rotaries (base port 3000 + rotary group number).

As I mentioned earlier, TTY line interfaces are only supported on certain hardware platforms, either as fixed ports or through the use of modular interface cards with fixed line densities. Here is a list of all the Cisco supported hardware platforms and supported TTY line densities:

Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin

Cisco 2509 (eight hardwired async ports -- discontinued)
Cisco 2511 (16 hardwired async ports -- discontinued)
Cisco 26XX (support for up to 32 ports NM-16A or NM-32A)
Cisco 3620 (support for 16 or 32 ports NM-16A or NM-32A)
Cisco 3640 (support for up to 96 ports 3 x NM-32A)
Cisco 3660 (support for up to 96 ports 6 x NM32A)
Cisco 3725 (support for 64 ports 2 x NM-32A)
Cisco 3745 (support for up to 96 ports 3 x NM-32A)

Now, it would seem logical that the Tty line number would correspond to the physical line interface number, and that each router with asynchronous serial hardware installed would start its Tty line numbering at port 1, so to connect to serial port 1, you would telnet to port 2001. Well, with the exception of the fixed-line configurations based on the 2500 series platform (which has been discontinued), things sadly do not work that way with Cisco routers.

Each IOS modular router reserves 32 asynchronous lines for each available slot on the router. In the command output example for the <show line> EXEC command you may have noticed this statement at the end:

```
70 VTY          -   -   -   -   -   -   0   0   0/0   -
```

```
Line(s) not in async mode -or- with no hardware support:  
1-32, 49-64
```

```
outlan-ts#
```

Although a pool of 32 asynchronous lines are reserved for each slot on the router, not all router slots are available to actually support TTY async lines. So Tty/TTY line numbers for the available port's start point are not determined by the actual number of TTY lines the router supports. Rather, the numbers are according to the line-pool allocation afforded to the slot on which the NM-16A or NM-32A is installed. In the case of our example 2600 router, the TTY line pool for slot 0 (lines 1 through 32) is unavailable, because slot 0 is used for the router's fixed LAN interfaces and WIC slots. To abate some of the confusion, here is a table that lists the line pool for each router that supports TTY lines (including the 25x0 routers that allocate the line numbers properly):

Router	Slot	Line number
2509	Slot 0	1 through 8
2511	Slot 0	1 through 16
.	.	.
2600	Slot 0	Reserved
	Slot 1	33 through 48
.	.	.
3620 – 3640	Slot 0	1 through 32
3620 – 3640	Slot 1	33 through 64
3640	Slot 2	65 through 96
3640	Slot 3	97 through 128
3660	Slot 4	129 through 160
3660	Slot 5	161 through 192

Understanding Reverse Telnet and IOS Terminal Lines

Michael J. Martin

.	.	.
3725 – 3745	Slot 0	1 through 32
3725 – 3745	Slot 1	33 through 48
3725 – 3745	Slot 2	65 through 96
3745	Slot 3	97 through 128

Although this is confusing, after a while you'll get used to it. As with all things that Cisco does that makes no real sense, your mind adjusts ;). What actual impact will this have on your deployment? That is the topic for the next article in this series.