Telecommuting Service Connections

This chapter describes how to connect devices across telephone lines using SLIP, PPP, or XRemote (the NCD X Windows terminal protocol). Specifically, this chapter contains the following sections:

- SLIP Connections
- PPP Connections
- XRemote Connections

SLIP Connections

You can make a serial connection to a remote host using the Serial Line Internet Protocol (SLIP). Your system administrator can configure SLIP to expect a specific address or to provide one for you. It is also possible to set up SLIP in a mode that compresses packets for more efficient use of the line.

To make a SLIP connection, enter the following command at the EXEC prompt:

slip {**/default** | {*remote-ip-address* | *remote-name*} [@*tacacs-server*] [**/routing**]} [**/compressed**]

Syntax Description

/default	(Optional) Makes a SLIP connection when a default address has been configured.
remote-ip-address	IP address of the client workstation or PC.
remote-name	Name of the client workstation or PC.
@*tacacs-server*	(Optional) The IP address or IP host name of the TACACS server product to which your TACACS authentication request is sent.
/routing	(Optional) Indicates that the remote system is a router. Line must be configured for asynchronous routing using SLIP encapsulation.
/compressed	(Optional) Indicates that IP header compression should be negotiated. Your system administrator must have configured the system with the **ip tcp header-compression passive** command for this command to be valid in EXEC mode. The command **ip tcp header-compression** forces header compression on or off. The default is to not compress the packets. The configuration file must have header compression on and the **slip /compressed** EXEC command must be entered for header compression to occur.

If you specify an address for the TACACS server product using **default** or *tacacs-server*, the address must be the first parameter in the command after you type **slip**. If you do not specify an address or enter **default**, you are prompted for an IP address or host name. You can enter **default** at this point.

If you do not use the *tacacs-server* argument to specify a TACACS server product for SLIP address authentication, the TACACS server specified at login (if any) is used for the SLIP address query.

To optimize bandwidth on a line, SLIP allows compression of the SLIP packets using Van Jacobson TCP header compression as defined in RFC 1144.

You can issue any of the following commands to terminate an active SLIP session:

exit
quit
logout

Examples

The following example illustrates how to make a connection when a default IP address is assigned. Once a correct password is entered, you are placed in SLIP mode, and the IP address is displayed.

```
cs> slip
Password:
Entering SLIP mode.
Your IP address is 192.31.7.28, MTU is 1524 bytes
```

The following example illustrates the prompts displayed and the response required when dynamic addressing is used to assign the SLIP address:

```
cs> slip
IP address or hostname? 192.31.6.15
Password:
Entering SLIP mode
Your IP address is 192.31.6.15, MTU is 1524 bytes
```

In the preceding example, the address 192.31.6.15 has been assigned as the default. Password verification is still required before SLIP mode can be enabled.

```
cs> slip default
Password:
Entering SLIP mode
Your IP address is 192.31.6.15, MTU is 1524 bytes
```

The following example illustrates the implementation of header compression on the interface with the IP address 128.66.2.1:

```
cs> slip 128.66.2.1 /compressed
Password:
Entering SLIP mode.
Interface IP address is 128.66.2.1, MTU is 1500 bytes.
Header compression will match your system.
```

In the preceding example, the interface is configured for **ip tcp header-compression passive**, which permitted the user to enter the **/compressed** keyword at the EXEC mode prompt. The message "Header compression will match your system" indicates that the user specified compression. If the line was configured for **ip tcp header-compression on**, this line would read "Header compression is On."

The following example specifies a TACACS server product named "parlance" for address authentication:

```
cs> slip 1.0.0.1@parlance
Password:
Entering SLIP mode.
Interface IP address is 1.0.0.1, MTU is 1500 bytes
Header compression will match your system.
```

PPP Connections

You can make asynchronous connections using the Point-to-Point Protocol (PPP). To start a PPP connection, enter the following command at the EXEC prompt:

ppp {**/default** | {*remote-ip-address* | *remote-name*} [**@***tacacs-server*]} [**/routing**]

Syntax Description

/default	(Optional) Makes a PPP connection when a default address has been configured.
remote-ip-address	IP address of the client workstation or PC. This parameter can only be specified if the line is set for dynamic addresses using the line configuration command **async address dynamic**.
remote-name	Name of the client workstation or PC. This parameter can only be specified if the line is set for dynamic addresses using the line configuration command **async address dynamic**.
@*tacacs-server*	(Optional) Specifies an IP address or IP host name of the TACACS server to which the user's TACACS authentication request is sent.
/routing	(Optional) Indicates that the remote system is a router and that routing messages should be exchanged over the link. The line must be configured for asynchronous routing using PPP encapsulation.

If you specify an address for the TACACS server product, either **default** or *tacacs-server*, the address must be the first parameter in the command after you type **ppp**. If you do not specify an address or enter **default**, you will be prompted for an IP address or host name. You can enter **default** at this point.

Any of the following commands will terminate a PPP session:

exit
quit
logout

Example

The following example shows a line that is in asynchronous mode using PPP encapsulation (see Figure 4-1). The PC's name is "ntpc" (assuming that the name "ntpc" is in the domain name system [DNS] so that it can be resolved to a real IP address). The PC must be running a terminal emulator program.

```
cs> ppp ntpc@server1
```

Figure 4-1   Using the PPP EXEC Command
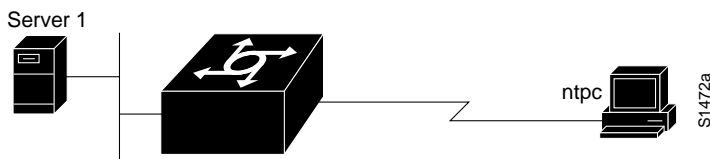
XRemote Connections

You use the XRemote protocol with an X display station and a modem to connect to remote hosts via TCP/IP and LAT. You make connections in one of the following ways:

- Automatically, using the X Display Manager Control Protocol (XDMCP) for TCP/IP networks

- Automatically, using DECwindows login for LAT networks

- Manually, using a step-by-step access process

The following sections outline the steps for starting up XRemote in several typical environments. When possible, use the automated processes. Make sure your system administrator has already configured a path for loading fonts.

Automatic Session Startup—XDMCP Server

If your host computer supports a server product for XDMCP (such as the *xdm* program included in X11R4 or later), you can use automatic session startup to make an XRemote session connection. To do so, enter the following command:

xremote xdm [*hostname*]

Syntax Description

hostname   (Optional) Host computer name.

This command sends an XDMCP session startup request to the host computer. If you do not specify a host name, a broadcast message is sent to all hosts. The first host to respond by starting up a session is used.

The server and X terminal stay in XRemote mode until either the display manager terminates the session or a reset request is received from the X terminal.

Example

The following example starts a session with a remote host named "star":

```
cs> xremote xdm star
```

Automatic Session Startup—DECwindows Login via LAT

If your host computer supports DECwindows login sessions, you can use automatic session startup to make an XRemote session connection. Once the system administrator at the remote host configures support for DECwindows over LAT, you can use the EXEC command **xremote lat** to initiate the connection. The command has the following syntax:

xremote lat *service*

Syntax Description

service   Name of the desired LAT service.

After you issue this command, expect the following to occur:

- The server product down-line loads several initial fonts for the DECwindows login display.

- The terminal displays the DIGITAL logo and DECwindows login box.

Log on to the system. Upon completion of login, more fonts are loaded, and the remote session begins.

Note Due to heavy font usage, DECwindows applications can take longer than expected to start when using XRemote. Once the application starts, performance and access times should be as expected.

Example

The following example begins connection with a LAT service named "WHIRL":

```
cs> xremote lat WHIRL
```

Manual XRemote Session Startup

If you do not use a host computer that supports XDMCP or LAT, you must use manual session startup. Manual session startup involves several steps:

1 Enable XRemote manually on the server product port.

2 Connect to the host computer.

3 Set the location of the X display.

4 Start up client applications.

5 Return to the EXEC prompt.

6 Enable XRemote manually again on the server product port.

The following sections describe these tasks.

Enable XRemote Manually

To prepare the server product for manual startup, enter the **xremote** EXEC command at the system prompt.

xremote

This command begins the instructions that prompt you through the connection.

Example

The following example illustrates how a successful manual XRemote session begins:

```
dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

The system replies with a message informing you of your X display location. You will use this information to tell the host the location of your X display server product.

If no clients are found, you see the following message:

```
No X clients waiting - check that your display is darkstar:2006
```

Check your hosts to determine whether an error has occurred when the session started. The most likely cause is that there is an improperly specified display location or the host computer did not recognize the name of your server product.

Connect to the Host Computer

You can connect to a host using one of the following connection commands, and log on as usual:

telnet
lat
rlogin

Set the Location of the X Display

At this point, you are logged in to the remote host.

Note If you are using a version of Telnet on the remote host that supports the "X Display Location" option (RFC 1096), skip this step and go on to the "Start Up Client Applications" section.

Inform the host computer of your X display location, which the server product provided when you enabled XRemote manually.

For most versions of the UNIX operating system, the X display location is set by using the **setenv** command to set the DISPLAY environment variable . Refer to your UNIX system's online **X(1)** manual page for more information.

On VAX/VMS systems, use the **SET DISPLAY** command to set the X display location. For more information, refer to the *VMS DCL Dictionary.*

Note You must install either the TCP/IP transport from Digital or a third-party TCP/IP transport. Contact your VAX/VMS system administrator for the appropriate TCP/IP transport name.

Start Up Client Applications

Now you start your client applications for your host operating system.

The server product accepts the X connection attempt from the client application and places the client in a dormant state.

Return to the EXEC Prompt

If it is possible to log off the host computer and keep your X clients running in the background, you can do so now. This conserves resources on both the host and the server product that would otherwise be inaccessible until you exited from XRemote state.

If you cannot log off the host computer and keep your clients running, escape back to the server product prompt using the escape sequence (Ctrl-^ X by default).

Reenable XRemote Manually

Begin a manual remote session again (refer to the "Enable XRemote Manually" section earlier in this chapter). If the X clients connected successfully, the session is put into XRemote mode, and the clients complete their startup.

If no clients are found, you see the following message:

```
No X clients waiting - check that your display is darkstar:2018
```

Check your hosts to determine whether an error has occurred when the session started. The most likely cause is an improperly specified display location. Or the host computer did not recognize the name of your server product.

What to Do if a Session Terminates

In manual operation, the server product and X terminal remain in XRemote mode until all clients disconnect or a reset request is received from the X terminal.

A session might terminate during startup because you invoked transient X clients that set some parameters and then disconnected (such as **xset** or **xmodmap**). There must always be one session open or the connection will be reset.

Establish XRemote Sessions between Servers

A user on an X display server product that does not support XRemote can run the XRemote protocols. An X display server product (such as a PCX, MacX or UNIX workstation) connected to an Ethernet network can dial out through a server product on a conventional modem to access an X client program on a host residing on another network. The server product provides the server-side helper process.

To run XRemote, connect to one of the XRemote ports.

Note The NCD helper process does not support X display devices that use a maximum request and response size larger than 64 kilobytes.

Find out from your administrator whether the connection from your X display terminal is configured as an individual line or a rotary connection.

- To connect to an individual line, use Telnet to connect from the X display terminal to port 9000 plus the decimal value of the line number.

- To make a rotary connection, use Telnet to connect from the X display server product to port 10000 plus the decimal value of the line number.

For information about how to configure individual lines and rotary connections, refer to the publications *Access and Communication Servers Configuration Guide* and the *Access and Communication Servers Command Reference*.

Figure 4-2 illustrates a configuration in which a display server product is not running XRemote. In this configuration, the server-side XRemote helper is running on Communication Server 1, and the client-side XRemote helper is running on Communication Server 2.

Figure 4-2 **XRemote Session between Communication Servers**
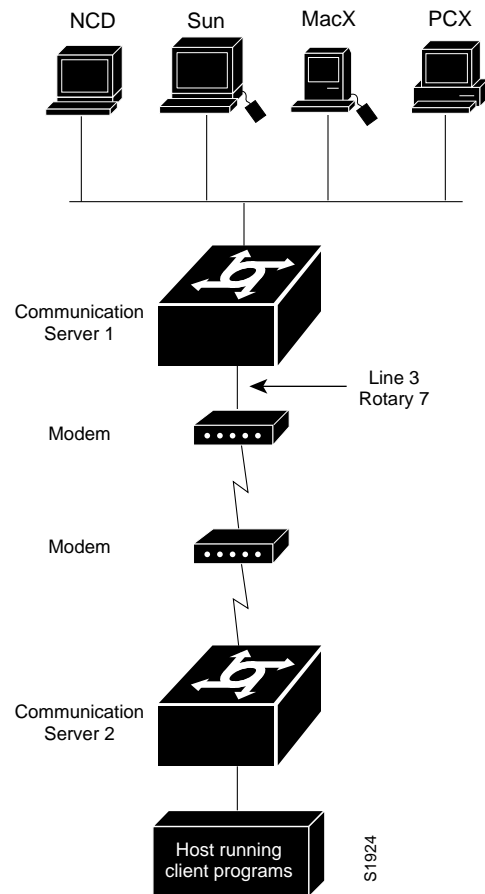
Exit XRemote Sessions

You can issue any of the following commands to terminate a terminal session:

exit
quit
logout

XRemote Examples

Use the examples in this section to understand how to make XRemote connections.

Connecting an X Display Terminal

The following example shows a connection from an X display terminal through a server product to a host running client programs.

1 Enter the **xremote** command at the EXEC prompt:

```
dialup> xremote
```

2 Read and follow the instruction from the host:

```
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

3 Connect to the client:

```
dialup> telnet eureka
Trying EUREKA.NOWHERE.COM (252.122.1.55)... Open

SunOS UNIX (eureka)
```

4 Log on at the prompt:

```
login: deal
Password:

Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994
```

5 At the client prompt, enter the display name from step 2 and the **xterm** command:

```
eureka% setenv DISPLAY dialup:2006
eureka% xterm &
[1] 15439
```

6 Disconnect from the client:

```
eureka% logout

[Connection to EUREKA closed by foreign host]
```

7 Begin the XRemote session:

```
dialup> xremote
Entering XRemote
```

The server product and X terminal stay in XRemote mode until either the display manager terminates the session or a reset request is received from the X terminal:

```
Connection closed by foreign host.
eureka%
```

Making XRemote Connections between Servers

This section provides two examples of XRemote connections between server products.

The following steps show how an XRemote connection is established for a configuration like the one shown in Figure 4-2. These steps assume that the administrator has set the user's display environment variable to identify the user's X display terminal.

1 From the PCX, MacX, or UNIX machine in Figure 4-2, the user connects to port 9003 on communication server 1. If your administrator has configured a rotary number 7, the user connects to port 10007. For more information about rotary groups, refer to the *Access and Communication Servers Configuration Guide* and the *Access and Communication Servers Command Reference* publication.

2 Communication server 1 connects the user to a modem.

3 The modem calls communication server 2.

4 The user enters **xremote** at the communication server 2 prompt.

5 The user connects to the remote host from communication server 2 using the **telnet** command.

6 The user starts the X client program that will run on the remote host and display on the X display server product (PCX, MacX, or UNIX host).

7 The user escapes from the remote host back to the communication server 2, or logs out if clients were run in the background, and enters **xremote** again at the communication server 2 prompt.

The following example shows the steps to make an XRemote connection between server products. The number 9016 in the first line of the display indicates a connection to individual line 16. If the administrator had configured a rotary connection, the user would enter 10000 plus the number of the rotary instead of 9016.

1 Enter the **telnet** command to make the connection:

```
space% telnet golden-road 9016
Trying 192.31.7.84 ...
Connected to golden-road.cisco.com.
Escape character is '^]'.
```

2 Supply the password for TACACS verification:

```
User Access Verification

Password:
Password OK

 --- Outbound XRemote service ---
Enter X server name or IP address: innerspace
Enter display number [0]:

 Connecting to tty16... please start up XRemote on the remote system
```

3 Dial in to the remote system using the modem, and then log on:

```
atdt 13125554141
DIALING
RING
CONNECT 14400

User Access Verification
Username: deal
Password:
  Welcome to the cisco dial-up remote access server.
```

4 Enter the **xremote** command at the EXEC prompt, then follow the instructions from the host:

```
dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

5 Connect to the client:

```
dialup> telnet sparks
Trying SPARKS.NOWHERE.COM (252.122.1.55)... Open

SunOS UNIX (sparks)

login: deal
Password:
Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994
```

6 At the client prompt, enter the display name from step 4 and the **xterm** command:

```
sparks% setenv DISPLAY dialup:2006
sparks% xterm &
[1] 15439
```

7 Disconnect from the client:

```
sparks% logout

[Connection to SPARKS closed by foreign host]
```

8 Begin the XRemote session:

```
dialup> xremote
Entering XRemote
```

Once the connection is closed by the foreign host, the Xterm window appears on the local workstation screen:

```
Connection closed by foreign host.
sparks%
```