



September 2008

COMredirect HP-UX v11 User Guide

Version 6.2

5500206-13

CUSTOMER Order **toll-free** in the U.S 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
SUPPORT FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
INFORMATION Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** * E-mail **info@blackbox.com**

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá de lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - a. El cable de poder o el contacto ha sido dañado; u
 - b. Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - c. El aparato ha sido expuesto a la lluvia; o
 - d. El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - e. El aparato ha sido tirado o su cubierta ha sido dañada.

FCC Requirements for Telephone-Line Equipment

1. The Federal Communications Commission (FCC) has established rules which permit this device to be directly connected to the telephone network with standardized jacks. This equipment should not be used on party lines or coin lines.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until the repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. If you have problems with your telephone equipment after installing this device, disconnect this device from the line to see if it is causing the problem. If it is, contact your supplier or an authorized agent.
4. The telephone company may make changes in its technical operations and procedures. If any such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes.
5. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number that this unit is connected to.
 - b. The ringer equivalence number.
 - c. The USOC jack required: RJ-11C.
 - d. The FCC registration number.

Items (B) and (D) can be found on the unit's FCC label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five. If too many devices are attached, they may not ring properly.

6. In the event of an equipment malfunction, all repairs should be performed by your supplier or an authorized agent. It is the responsibility of users requiring service to report the need for service to the supplier or to an authorized agent.

Certification Notice for Equipment Used in Canada

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications-network protective, operation, and safety requirements. Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility—in this case, Black Box. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The LOAD NUMBER (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices, subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le Industrie Canada.

Table of Contents

What is COMredirect?	7
COMredirect Full Mode vs Lite Mode	7
Full Mode.....	7
Lite Mode.....	7
Uninstalling COMredirect.....	8
Installing COMredirect.....	8
Configuring COMredirect on a Terminal Server	9
Server-Initiated Mode	9
Client-Initiated Mode	9
Configuring Ports on the COMredirect Host	10
COMredirect Device Names.....	10
Configuration Methods	10
COMredirect addports Script Options	11
Examples.....	13
Adding Server-Initiated Mode Ports	13
Adding Client-Initiated Ports.....	13
COMredirect Administration Tool (crdadm) Commands	14
Syntax.....	14
Examples.....	17
Adding a Port	17
Deleting a Port	17
Displaying Port Entries.....	17
Starting the COMredirect Daemon.....	17
config.crd File Syntax.....	18

Managing Ports on the COMredirect Host	20
Starting COMredirect.....	20
As a Transparent Printer	20
In Full Mode.....	20
In Lite Mode.....	21
Deleting a Single Port.....	21
Deleting All Ports	21
Managing Logins	22
crdlogin.....	22
Syntax.....	22
Examples.....	23
addlogins	23
Syntax.....	23
Examples.....	23
rmlogins.....	24
Syntax.....	24
Examples.....	24
Configuring Packet Forwarding	25
Configuration Script	25
pktfwdcfg.crd File Format	27
Configuring SSL/TLS	28
SSL/TLS Configuration Information.....	28
SSL/TLS Support Files	29
COMredirect Port Configured as SSL/TLS Server	29
COMredirect Port Configured as SSL/TLS Client.....	29
Pseudo Random Number Generator.....	30
sslcfg.crd File Format.....	30
SSL/TLS Trouble Shooting	31

What is COMredirect?

You use COMredirect when you want to connect extra terminals to a server using a Terminal Server rather than a multi-port serial card; it is a tty device redirector. COMredirect is especially useful when you want to improve data security, as you can create an SSL/TLS connection between the COMredirect host port and the Terminal Server, which will encrypt the data between the two points.

COMredirect Full Mode vs Lite Mode

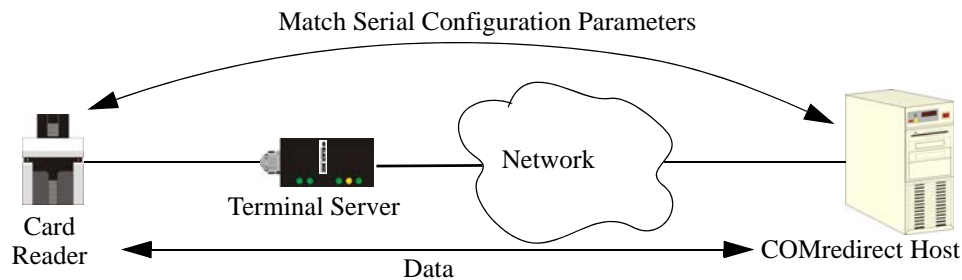
You can configure COMredirect on HP-UX version 11 in either Full Mode or Lite Mode. When you start COMredirect in Full Mode, the serial configuration parameters are set on the COMredirect host. When you start COMredirect in Lite Mode, the serial configuration parameters are set on the terminal server. On HP-UX, serial configuration parameters consist of bits per second (baud rate speed), data bits, parity, stop bits, flow control, and any other standard stty I/O parameters. In either mode, the data is passed in raw format, although you can enable the SSL/TLS connection option to encrypt the data going through a port.

Full Mode

This mode allows complete device control and operates exactly like a directly connected serial port. It provides a complete tty device interface between the attached serial device and the network, providing hardware and software flow control.

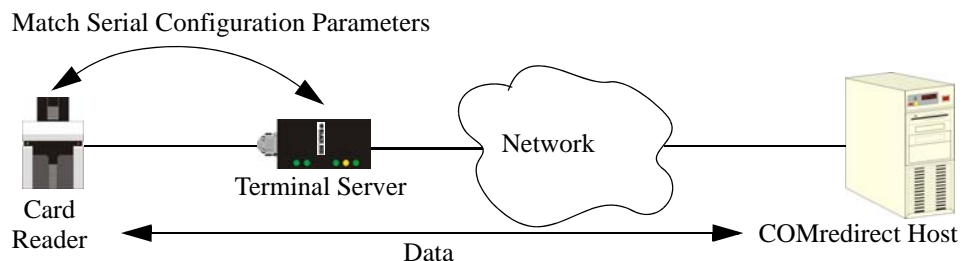
COMredirect 6.1 and Terminal Server firmware 3.4 and lower in Full Mode use the TCP protocol on the configured port and the UDP protocol on port 668 (some firewalls block UDP packets by default and might need to be reconfigured to support Full Mode communication). COMredirect 6.2 and higher and Terminal Server firmware 3.5 and higher do not use the UDP protocol.

The port serial configuration parameters set on the COMredirect host must match the serial configuration parameters set on the device (in this example, to the Card Reader), as shown below:



Lite Mode

This mode provides a simple raw data interface between the device and the network. Although the port will still operate as a tty device, control signals are ignored. Lite Mode uses the TCP protocol on the configured port. In this mode, the serial communications parameters are configured on the terminal server and must match those configured on the device (in this example, a Card Reader), as shown below:



Uninstalling COMredirect

Before you install a new version of COMredirect, you should uninstall the current version of COMredirect. To uninstall COMredirect, do the following:

1. Login as a root user.
2. Type the following:

```
# swremove
```
3. Select COMredirect from the list of applications.
4. Select **Actions, Remove** and click **OK** and **Yes** to start the uninstall process.
5. When the uninstall process is complete, click **Done**. The system may need to be rebooted to rebuild the kernel.

Installing COMredirect

Installation uses the swinstall utility. The installable package is contained in the file **crdhpux11-<n.n.n>.depot.Z** where **<n.n.n>** is the version number of the release. This is a compressed software depot. To install the software, do the following:

1. Login as a root user and copy the installation package to **/tmp**.
2. Decompress the depot.

```
# uncompress crdhpux11-<n.n.n>.depot.Z
```
3. Run swinstall to install the product with the following command:

```
swinstall -s <absolute path to depot file>
```

For Example:

```
# swinstall -s /tmp/crdhpux11-<n.n.n>.depot
```

4. When the **SD Install - Software Selection** window appears, select **COMredirect** and then select **Actions, Mark for Install**.

Note: When selecting the COMredirect bundle for installation, the “marked” status will always be “partial”. This is due to both PA-RISC and Itanium components being supplied in the product and is considered normal.

5. Next select **Actions, Install**.
6. Follow the instructions on the screen, you can view the product description and README after the files have been installed on the computer.
7. When the installation is complete you will be prompted to click **Done** and the system may be rebooted. You can check that the software has been correctly installed with the **lsdev** command. In the list of installed devices, **tpm** and **tps** should be listed. Once software installation is complete, you are required to configure your terminal servers to use the COMredirect service and to enable ports on your server computer.

Configuring COMredirect on a Terminal Server

When you add a port, you need to configure the port(s) on the host running COMredirect and you also need to configure the port(s) on the terminal server.

Server-Initiated Mode

When you configure COMredirect for Server-Initiated mode, the terminal server will initiate communication to the COMredirect host.

To configure a terminal server for Server-Initiated mode (which is the default mode), you need to set the **Line Service** to **COMredirect** (firmware version 3.3 or higher) or **Silent Raw** and assign the port number to be the same port number configured on the COMredirect host (by default, this number starts at 10000).

The following instructions provide an example of how to set up four ports on the Terminal Server for COMredirect. On a 1-port model you won't specify a line number.

1. Connect to the Terminal Server (for example, via Telnet).
2. Log in to the Terminal Server as the **admin** user.
3. Add the host running COMredirect to the host table using the add host command as shown in the following example:

```
add host hpux50 192.152.247.61
```

You are now ready to configure the ports that will connect to the COMredirect host.

4. To configure the ports, enter each of the following commands:

```
set line 1 service comredirect hpux50 10000
set line 2 service comredirect hpux50 10001
set line 3 service comredirect hpux50 10002
set line 4 service comredirect hpux50 10003
kill line 1-4
```

5. At the command prompt, type **save** and press **Enter**.
6. At the command prompt, type **logout** and press **Enter**.

The configuration of terminal server ports is now complete.

Client-Initiated Mode

Note: Client-Initiated mode is available on Terminal Server, Device Server, and Console Server models with firmware 3.3 or higher.

When you configure COMredirect for Client-Initiated mode, the COMredirect host will initiate communication with the Terminal Server.

To configure a Terminal Server for Client-Initiated mode, you need to set the **Line Service** to **COMredirect**, enable the **Client Initiated** option, and assign the port number to be the same port number configured on the client-initiated configured COMredirect host (by default, this number starts at 10001).

The following instructions provide an example of how to set up 4 ports on a Terminal Server for COMredirect Client-Initiated mode.

1. Connect to the Terminal Server (for example, via Telnet).
2. Log in to the Terminal Server as the **admin** user.

3. To configure the ports, enter each of the following commands:

```
set line 1 service comredirect client-initiated on 10001
set line 2 service comredirect client-initiated on 10002
set line 3 service comredirect client-initiated on 10003
set line 4 service comredirect client-initiated on 10004
kill line 1-4
```
 4. At the command prompt, type **save** and press **Enter**.
 5. At the command prompt, type **logout** and press **Enter**.
- The configuration of the Terminal Server is now complete.

Configuring Ports on the COMredirect Host

After you have configured the ports on the terminal server, you need to configure corresponding ports on the COMredirect host. COMredirect administrative files and utilities are installed in the `/etc/COMredirect` directory.

To enable a range of ports, we have provided a script `/etc/COMredirect/addports` that starts the COMredirect service. The `addports` command creates the device nodes, edits the COMredirect configuration files, and starts the required daemons and drivers. See [COMredirect addports Script Options on page 11](#) for more information.

COMredirect Device Names

COMredirect for HP-UX supports up to 4000 COMredirect serial device nodes; however, you must enable these ports before they can be used. Each installed TTY is assigned a name by the operating system that will be in the range 0-3999.

The HP-UX COMredirect serial device naming convention are as follows:

- Client-Initiated and Full mode devices:

```
/dev/ttys0 through /dev/ttys3999 for the non-modem open devices
/dev/ttyS0 through /dev/ttyS3999 for the modem open devices
/dev/ttyt0 through /dev/ttyt3999 for the pseudo modem open
```
- Server-Initiated Lite mode devices:

```
/dev/ttyX0 through /dev/ttyX3999
```
- Auxiliary Printers

```
/dev/ttyX0p through /dev/ttyX3999p
```

Configuration Methods

After you have configured the ports on the terminal server, you have to configure the same port numbers on the COMredirect host. The COMredirect Host can be configured in the following ways:

1. Use the `addports` script, which will automatically enable and start each port as it is configured. See [COMredirect addports Script Options on page 11](#) for more information.
2. Use the `addports` script to create the total range of TTY ports you require and then use the `crdadm` administration tool. See [COMredirect Administration Tool \(crdadm\) Commands on page 14](#) to remove/configure ports in the `config.crd` file using `crdadm`.
3. Use the `addports` script to create the total range of TTY ports and then edit the `/etc/COMredirect/config.crd` file (see [config.crd File Syntax on page 18](#)), the `/etc/COMredirect/sslcfg.crd` file (see [sslcfg.crd File Format on page 30](#)), and the `/etc/COMredirect/pktfwdcfg.crd` file (see [pktfwdcfg.crd File Format on page 27](#)).

COMredirect addports Script Options

The **addports** script allows you to add a range of ports to the **config.crd** file and automatically start them, without having to use the **crdadm** utility. You can run **addports** after the COMredirect host software is installed. The addports options are as follows:

For Server-Initiated Mode:

```
addports [-l] [-hup] [-ssl] [-k <seconds>] [-ap]
[-opmode optimize_lan|low_latency|packet_idle_timeout|custom]
[-pktidletime <timeout>] [-pf] [-server <host>] [-openwaittime <seconds>]
[-trace <level>] <firstport> <lastport>
```

For Client-Initiated Mode:

```
addports [-l] [-hup] [-ssl] [-k <seconds>] [-ap]
[-opmode optimize_lan|low_latency|packet_idle_timeout|custom]
[-pktidletime <timeout>] [-pf] -client <host>[:<TCP-port>] [-nodisc]
[-retrytime <time>] [-retrynum <number>] [-initconnect]
[-openwaittime <seconds>] [-closedelaytime <seconds>] [-norestorenet]
[-trace <level>] <firstport> <lastport>
```

Parameter	Description
-l	(lower case L) Specifies that the COMredirect port will be started in Lite mode. addports will configure COMredirect for Full mode by default.
-hup	Causes the tty device to automatically close or hang-up when the TCP connection is closed.
-ssl	Enables SSL/TLS on the port. You will automatically be prompted by the SSL/TLS configuration script. For more information see Configuring SSL/TLS on page 28 .
-k <seconds>	The time, in seconds, to wait on an idle connection before sending a keep-alive message.
-ap	Allows the COMredirect daemon to autopush the ptem and ldterm modules on to a Server-Initiated Lite Mode device node. This is required for the getty to properly display the login prompt.
-opmode optimize_lan low_latency packet_idle_timeout custom	Specify one of the following optimization modes: <ul style="list-style-type: none"> • optimize_lan—This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN. • low_latency—This option ensures that all application data is immediately forwarded to the serial device. Select this option for timing-sensitive applications. • packet_idle_timeout—This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages. • custom—This option allows you to define the packet forwarding rules based on the packet definition or the frame definition. This is the same as the -pf option and will launch the Packet Forwarding configuration script (see Configuring Packet Forwarding on page 25). Specify either -pf or -opmode <mode> , as these options are mutually exclusive.

Parameter	Description
-packetidletime <timeout>	The minimum time, in milliseconds, between messages that must pass before the data is forwarded to the Terminal Server. The range is 0-65535. The default is 10 ms.
-pf	Enables packet forwarding on the port. You will automatically be prompted by the packet forwarding configuration script. For more information see Configuring Packet Forwarding on page 25 . Specify either -pf or -opmode <i><mode></i> , as these options are mutually exclusive.
-server <i><host></i>	You can optionally supply the remote host name or IP address that a connection request will be accepted from. The default is to accept connections from any host. The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].
-client <host>[:<TCP-port>]	Specifies a client-initiated connection (meaning that the COMredirect host will initiate the connection). You can optionally supply the starting destination TCP port for the connection (the default is 10001, see <i><firstport></i> option below). The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].
-nodisc	Does not drop the TCP connection for a client-initiated connection when the application closes the slave TTY port.
-retrytime <i><time></i>	Specifies the number of seconds between TCP connection retries after a client-initiated connection failure. Valid values are 1-255. The default is 30 seconds.
-retrynum <i><number></i>	Specifies the number of additional retry attempts for a client-initiated connection, beyond the first attempt. Valid values are -1 to 255. If this option is -1, COMredirect will attempt to reconnect forever. If this option is set to 0 (zero) and -norestorenet is not specified, COMredirect will try to recover a TCP connection once. The default is -1, retry forever.
-initconnect	Specifies that the COMredirect host will try to connect to the Terminal Server when the COMredirect daemon starts, as opposed to waiting for the application to open the serial port before initiating the connection to the Terminal Server.

Parameter	Description
-openwaittime <seconds>	<p>Specifies the maximum amount of time to wait, in seconds, for a COMredirect connection to be established before returning to an application opening the serial port (not supported in Server-Initiated Lite Mode). You can specify the following values:</p> <ul style="list-style-type: none"> • -1, open the serial port without waiting, even if there is no network connection, and don't give an error. Any written data is discarded if the COMredirect connection is not up. • 0, open the serial port without waiting, and return an error (EIO) if the COMredirect connection is not up. If a network connection exists, then no error is returned. • 1-30, wait up to the specified seconds for a COMredirect connection to be fully established. If a timeout occurs before a network connection is established, an error is returned (EIO). <p>The COMredirect connection is fully established when:</p> <ul style="list-style-type: none"> • The TCP connection between the Terminal Server and the COMredirect host is up. • The SSL/TLS negotiation succeeds (if used). • The COMredirect Full mode protocol negotiation succeeds (if used). <p>The range is -1 to 30. The default is 30 seconds.</p>
-closedelaytime <seconds>	<p>Specifies the amount of time, in seconds, to wait after an application closes the serial port, before the TCP connection is closed to avoid bringing the TCP connection down and up if the application is closing and opening the COM port often. The range is 0-65535. The default is 3 seconds.</p>
-norestorenet	<p>By default, when the network connection fails for client-initiated mode, COMredirect will attempt to restore it. If this option is specified, and the network connection fails, there is no attempt to restore it.</p>
-trace <level>	<p>The trace level for debugging purposes. The default is 1. The trace file for each port can be found under <code>/etc/COMredirect/trace.<tty-name></code>, where <code><tty-name></code> is either <code>tpmn</code> or <code>ttyXn</code>, where <code>n</code> is the TTY port number.</p>
<firstport>	<p>The first TTY to add starting at 0 (added as port 10001 for a client-initiated (COMredirect) connection or port 10000 for a server (terminal server) initiated connection).</p>
<lastport>	<p>The last TTY to add.</p>

Examples

Adding Server-Initiated Mode Ports

The following **addports** command will create 4 ports configured for Server-Initiated mode which will listen for connections from host **myhost** on TCP ports 10000 to 10003, while running in COMredirect Full mode.

```
addports -server myhost 0 3
```

Adding Client-Initiated Ports

The following **addports** command will create 4 ports configured for Client-Initiated mode which will connect to host **myhost4** on TCP ports 10001 to 10004, while running in COMredirect Lite mode.

```
addports -l -client myhost4 0 3
```

COMredirect Administration Tool (crdadm) Commands

This section describes the commands and syntax for the COMredirect Administration tool. You must use the **addports** script to enable the device nodes you can create using the **crdadm** utility; see [COMredirect addports Script Options on page 11](#) for more information about the **addports** script.

Syntax

Description You can use the **crdadm** utility to list, start, and delete ports (use the **addports** script to create and enable the device nodes).

Syntax

```
crdadm -a <new_portnumber> [-m|-n]
[--opmode optimize_lan|low_latency|packet_idle_timeout|custom]
[--pktidletime <milliseconds>] [--openwaittime <seconds>]
[-e|-F|-e -F [-c [<existing_host>:]<existing_portnumber>]] [-h]
[-C <host> [-q <seconds>] [-R <retries>] [-o] [--ap]
[--initconnect] [--closedelaytime <seconds>] [--noestorenet]]
[-S <host>] [-T <level>] -p <tty_letter>[<port#>]
[-k <seconds>] [-t <termtype>] [-i <start_port>] [-r <range>]
```

```
crdadm -l <portnumber>|<host>:|<host>:<TCP_number>|ALL
```

```
crdadm -s <portnumber> [-r <range>]|
<host>: [-r <range>]|<host>:<TCP_number> [-r <range>]|ALL
```

```
crdadm -d <portnumber>|<host>:|<host>:<TCP_number>
```

Options **-a** <new_portnumber>

The TCP/IP port number configured for the port on the remote terminal server. We recommend that you use the range 10000+.

-m

Adds a terminal in COMredirect Full Mode (not Lite Mode) for full device control. This is the default.

-n

Adds a terminal in COMredirect Lite Mode (not Full Mode) for terminal server device control.

-e

Enables SSL/TLS for the port. You will automatically be prompted for the SSL/TLS configuration information when you use this command line option. See [Configuring SSL/TLS on page 28](#) for more information.

-F

Enables packet forwarding for this port. You will automatically be prompted for the Packet Forwarding configuration information when you use this command line option. See [Configuring Packet Forwarding on page 25](#) for more information.

Specify either **-F** or **--opmode <mode>**, as these options are mutually exclusive.

-c [<existing_host>:]<existing_portnumber>

Copies the specified SSL/TLS and/or packet forwarding configuration data from the specified entry to the new port entry being created.

-C <host>

Enables a client-initiated connection (by the COMredirect host) for this session and will connect to the specified host and port number. The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].

-q <seconds>

Specifies the number of seconds between TCP connection retries after a client-initiated connection failure. Valid values are 1-255. The default is 30 seconds.

-R <retries>

Specifies the number of additional retry attempts for a client-initiated connection, beyond the first attempt. Valid values are -1 to 255. If this option is -1, COMredirect will attempt to reconnect forever. If this option is set to 0 (zero) and **-noresetnet** is not specified, COMredirect will try to recover a TCP connection once. The default is -1, retry forever.

-o

Keeps the client-initiated TCP connection open even when the application closes the slave TTY port.

-S <host>

Specifies the remote host name or IP address that a connection request will be accepted from in Server mode. The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].

-T <level>

Sets the trace level for debugging. The default is 1.

-h

Causes the tty device to automatically be closed when the TCP connection is closed.

-p <tty_letter>[<port#>]

<tty_letter> is the TTY name suffix for the port and should be used when adding a range of ports. Use X for Server-Initiated Lite Mode ports and use m for Client-Initiated or Full Mode ports.

<port#> is the port number and should be used when adding a single port and not a range.

-k <seconds>

The time, in seconds, to wait on an idle connection before sending a keep-alive message.

--ap

Allows the COMredirect daemon to autopush the **ptem** and **ldterm** modules on to a Server-Initiated Lite Mode device node. This is required for the getty to properly display the login prompt.

-t <termtype>

A terminal type listed in the file **printcap.crd**. This option turns on auxiliary printing; you must specify the type of terminal that is connected to the printer.

-i <start_port>

Starting port number for use in the TTY device node names (range is from 0 to 3999).

-r <range>

Number of ports/device nodes to configure or start (range is from 0 to 3999).

-l <portnumber>|<host>:|<host>:<TCP_number>|**ALL**

Displays specific or all port entries in the **config.crd** file.

-d <portnumber>|<host>:|<host>:<TCP_number>

Deletes the specified port entry from the **config.crd** file. The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].

-s <portnumber>|<host>:<host>:<TCP_number>|ALL

Starts a specific COMredirect port or all the COMredirect ports. The host can be an IPv4 or IPv6 address or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].

--opmode optimize_lan|low_latency|packet_idle_timeout|custom

Specify one of the following optimization modes:

- **optimize_lan**—This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN.
- **low_latency**—This option ensures that all application data is immediately forwarded to the serial device. Select this option for timing-sensitive applications.
- **packet_idle_timeout**—This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages.
- **custom**—This option allows you to define the packet forwarding rules based on the packet definition or the frame definition. This is the same as the -F option and will launch the Packet Forwarding configuration script (see [Configuring Packet Forwarding on page 25](#)).

Specify either **-F** or **--opmode <mode>**, as these options are mutually exclusive.

--pktidletime <milliseconds>

The minimum time, in milliseconds, between messages that must pass before the data is forwarded to the Terminal Server. The range is 0-65535. The default is 10 ms.

--openwaittime <seconds>

Specifies the maximum amount of time to wait, in seconds, for a COMredirect connection to be established before returning to an application opening the serial port (not supported in Server-Initiated Lite Mode). You can specify the following values:

- **-1**, open the serial port without waiting, even if there is no network connection, and don't give an error. Any written data is discarded if the COMredirect connection is not up.
- **0**, open the serial port without waiting, and return an error (EIO) if the COMredirect connection is not up. If a network connection exists, then no error is returned.
- **1-30**, wait up to the specified seconds for a COMredirect connection to be fully established. If a timeout occurs before a network connection is established, an error is returned (EIO).

The COMredirect connection is fully established when:

- The TCP connection between the Terminal Server and the COMredirect host is up.
- The SSL/TLS negotiation succeeds (if used).
- The COMredirect Full mode protocol negotiation succeeds (if used).

The range is -1 to 30. The default is 30 seconds.

--initconnect

Specifies that the COMredirect host will try to connect to the Terminal Server when the COMredirect daemon starts, as opposed to waiting for the application to open the serial port before initiating the connection to the Terminal Server.

--closedelaytime <seconds>

Specifies the amount of time, in seconds, to wait after an application closes the serial port, before the TCP connection is closed to avoid bringing the TCP connection down and up if the application is closing and opening the COM port often. The range is 0-65535. The default is 3 seconds.

--norestorenet

By default, when the network connection fails for client-initiated mode, COMredirect will attempt to restore it. If this option is specified, and the network connection fails, there is no attempt to restore it.

Examples

Adding a Port

To add a Server-Initiate port in Lite Mode with SSL/TLS enabled, use the following command:

```
crdadm -a 10000 -n -e -p X0
```

To add a client-initiated port to connect to host **myhost4** on remote port 10001 with packet forwarding enabled, use the following command:

```
crdadm -a 10001 -F -p m2 -C myhost4
```

Deleting a Port

To delete port 10000, use the following command:

```
crdadm -d 10000
```

To delete port 10001 on host **myhost** use the following command:

```
crdadm -d myhost:10000
```

Note: The `<host>:<port>` combination you use must exist in the **config.crd** configuration file. When you remove a terminal using this command, it does not stop the software running, it just deletes the entry for this terminal in the **config.crd** configuration file. You must then kill the COMredirect daemon process.

Displaying Port Entries

To displays the ports configured in the config.crd file, use the following command:

```
crdadm -l all
```

To display all the ports for a specific host in the config.crd file, use the following command:

```
crdadm -l myhost:
```

To display a specific port for a specific host in the configuration file, use the following command:

```
crdadm -l myhost:10002
```

Starting the COMredirect Daemon

To start port number 10000, use the following command:

```
crdadm -s 10000
```

To start all configured ports, use the following command:

```
crdadm -s ALL
```

To start port number 10001 on host 172.16.45.8, use the following command:

```
crdadm -s 172.16.45.8:10001
```

To start all configured ports on host **myhost**, use the following command:

```
crdadm -s myhost:
```

config.crd File Syntax

Note: If you use **addports** to enable COMredirect you do not need to use the **crdadm** utility.

An entry in the **config.crd** configuration file used to control a terminal in server Full Mode via Server-Initiated mode with some of the options enabled looks like this:

```
crdd -full -ssl -pf -hup -tty /dev/tpm0 -port 10000 -server myhost
    -ka 30 -trace 4 -aux /dev/ttyX0p -term vt100
```

An entry in the **config.crd** configuration file used to control a Terminal Server in Full Mode via Client-Initiated mode with some of the options enabled looks like this:

```
crdd -full -ssl -pf -hup -tty /dev/tpm0 -port 10001 -client myhost4
    -ka 30 -trace 4 -aux /dev/ttyX0p -term wy60
```

The **config.crd** port parameter options are:

-full	Enables COMredirect Full Mode (not COMredirect Lite) for full device control.
-ssl	Enables SSL/TLS on the port.
-hup	Causes the tty device to automatically close or hang up when the TCP connection is closed. This option is not supported in Server-Initiated Lite Mode.
-tty <ttyname>	<ttyname> is the tty name for the port. This must be the complete path name. Use /dev/ttyXn for Server-Initiated Lite Mode ports or use /dev/tpmn for Client-Initiated or Full Mode ports, where n is the port number.
-port <port_number>	For a server-initiated connection (terminal server), the TCP port number the COMredirect daemon will listen on for connection requests. For a client-initiated connection (COMredirect host), the Terminal Server TCP port number (DS Port) the COMredirect daemon will attempt to connect to. We recommend that you use the range 10000+.
-ap	This option allows the COMredirect daemon to autopush the ptem and ldterm modules on to a Lite Mode device node. This is required for the getty to properly display the login prompt.
-ka <seconds>	<seconds> is the number of seconds to wait on an idle connection before sending a keep-alive message.
-trace <1-4>	<1-4> is the trace level for debugging purposes, the default is 1.
-aux <auxdevname>	Sets the auxiliary printer device name.
-term <type>	Sets the terminal type of terminal that the auxiliary printer is attached to.
-client <host>	Indicates a client-initiated connection. The <host> can be IPv4, IPv6, or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].
-retrytime <seconds>	Specifies the number of seconds between TCP connection retries after a client-initiated connection failure. Valid values are 1-255. The default is 30 seconds.
-retrynum <number>	Specifies the number of additional retry attempts for a client-initiated connection, beyond the first attempt. Valid values are -1 to 255. If this option is -1, COMredirect will attempt to reconnect forever. If this option is set to 0 (zero) and -norestornet is not specified, COMredirect will try to recover a TCP connection once. The default is -1, retry forever.
-nodisc	For client-initiated connections, does not close the TCP connection when the application closes the slave TTY port.

-pf	<p>Enables packet forwarding on the port, reading the packet forwarding configuration from the <code>pktfwdfg.crd</code> file. For more information see Configuring Packet Forwarding on page 25.</p> <p>Specify either -pf or -opmode <mode>, as these options are mutually exclusive.</p>
-server <host>	<p>Specifies the remote host name or IP address that a connection request will be accepted from in Server mode. The default is to accept connections from any host. The <i><host></i> can be IPv4, IPv6, or a resolvable host name. If specifying an IPv6 address, the address must be enclosed in square brackets ([]), for example [2001:0db8:85a3:08d3:1319:8a2e:0370:7348].</p>
-nagleoff	<p>For client-initiated connections, turn off the TCP Nagle Algorithm, which inserts a short delay so that each character is not sent individually, but sent in small packets instead. The default is On.</p>
-initconnect	<p>Specifies that the COMredirect host will try to connect to the Terminal Server when the COMredirect daemon starts, as opposed to waiting for the application to open the serial port before initiating the connection to the Terminal Server.</p>
-openwaittime <seconds>	<p>Specifies the maximum amount of time to wait, in seconds, for a COMredirect connection to be established before returning to an application opening the serial port (not supported in Server-Initiated Lite Mode). You can specify the following values:</p> <ul style="list-style-type: none"> • -1, open the serial port without waiting, even if there is no network connection, and don't give an error. Any written data is discarded if the COMredirect connection is not up. • 0, open the serial port without waiting, and return an error (EIO) if the COMredirect connection is not up. If a network connection exists, then no error is returned. • 1-30, wait up to the specified seconds for a COMredirect connection to be fully established. If a timeout occurs before a network connection is established, an error is returned (EIO). <p>The COMredirect connection is fully established when:</p> <ul style="list-style-type: none"> • The TCP connection between the Terminal Server and the COMredirect host is up. • The SSL/TLS negotiation succeeds (if used). • The COMredirect Full mode protocol negotiation succeeds (if used). <p>The range is -1 to 30. The default is 30 seconds.</p>
-closedelaytime <seconds>	<p>Specifies the amount of time, in seconds, to wait after an application closes the serial port, before the TCP connection is closed to avoid bringing the TCP connection down and up if the application is closing and opening the COM port often. The range is 0-65535. The default is 3 seconds.</p>
-norestorenet	<p>By default, when the network connection fails for client-initiated mode, COMredirect will attempt to restore it. If this option is specified, and the network connection fails, there is no attempt to restore it.</p>

-opmode optimize_lan low_latency packet_idle_timeout custom	<p>Specify one of the following optimization modes:</p> <ul style="list-style-type: none"> • optimize_lan—This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN. • low_latency—This option ensures that all application data is immediately forwarded to the serial device. Select this option for timing-sensitive applications. • packet_idle_timeout—This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages. • custom—Enables packet forwarding on the port, reading the packet forwarding configuration from the <code>pktfwdcfg.crd</code> file. For more information see Configuring Packet Forwarding on page 25. <p>Specify either -pf or -opmode <mode>, as these options are mutually exclusive.</p>
-pktidletime	<p>The minimum time, in milliseconds, between messages that must pass before the data is forwarded to the Terminal Server. The range is 0-65535. The default is 10 ms.</p>

Managing Ports on the COMredirect Host

Starting COMredirect

A COMredirect daemon needs to be run for each port configured. There are three ways to start COMredirect daemons:

- Use the **addports** script, which will automatically start each port as it is configured.
- When the COMredirect host reboots, a COMredirect daemon for each port configured in the `config.crd` file will automatically be started by the **COMredirect** script, which can be found in the `/etc/init.d/COMredirect` script. The **COMredirect** script is enabled when the COMredirect software is installed.
- Enter the **crdadm -s** command to start specific individual ports or all the ports at one time; see [COMredirect Administration Tool \(crdadm\) Commands on page 14](#) for the command syntax.

As a Transparent Printer

The **addports** script does not support adding a transparent print port so, so you must manually edit the `config.crd` file.

In Full Mode

1. An example of a Server-Initiated Full Mode port entry is:

```
crdd -full -tty /dev/tpm0 -port 10000 -ka 30
```
2. To configure that entry as a transparent print port (aux port), you need to add:

```
crdd -full -tty /dev/tpm0 -port 10000 -ka 30 -aux /dev/ttyX0p  
-term vt100
```

where the transparent printer port is called `/dev/ttyX0p` and the term type is **vt100** (this is required).

In Lite Mode

1. An example of a Server-Initiated Lite Mode port entry is:

```
crdd -tty /dev/ttyX0 -port 10000 -ka 30
```
2. To configure that entry as a transparent print port (aux port), you need to add:

```
crdd -tty /dev/ttyX0 -port 10000 -ka 30 -aux /dev/ttyX0p -term vt100
```

where the transparent printer port is called `/dev/ttyX0p` and the term type is `vt100` (this is required).

Deleting a Single Port

To delete serial ports, do the following:

1. In the `/etc/COMredirect` directory, use an editor to delete the port entry in the `config.crd` file or type the following command:

```
crdadm -d <portnumber>|<host>|<host>:<portnumber>
```
2. You must then kill the COMredirect daemon process.
3. If you had configured a login for this port, you should remove it using the `crdlogin -r` command (see [crdlogin on page 22](#) for more information).

Deleting All Ports

There is a script you can run called `cleanports` that will kill all the COMredirect daemon processes and delete all entries in the `config.crd`, `sslcfg.crd`, and `pktfwdcfg.crd` files, with the exception of any lines that have been commented out.

If you configured any logins, you should remove them by using the `rmlogins` command (see [rmlogins on page 24](#) for more information).

Managing Logins

Several configuration scripts are included in your COMredirect installation, which can be used to manage logins for the configured COMredirect devices.

crdlogin

The **crdlogin** script adds, enables, disables, removes, or lists configured logins for a COMredirect device.

Note: To add or remove logins for more than one port, you may wish to use the **addlogins** and **rmlogins** scripts.

Syntax

Description Uses the system's **/etc/getty** to add, enable, disable, remove, or lists configured logins for a COMredirect device.

Syntax **crdlogin -a <port_name> [<getty_label>]**

crdlogin -e <port_name>

crdlogin -d <port_name>

crdlogin -r <port_name>

crdlogin -l

Options

-a

Adds the port.

-e

Enables a port.

-d

Disables a port.

-r

Removes a port.

-l

Lists the login entries.

<port_name>

Adds a getty entry in the **/etc/inittab** file for the device, valid values are:

- **Xn**—for **/dev/ttyXn** lite mode (server-initiated) devices
- **Sn**—for **/dev/ttySn** modem devices
- **sn**—for **/dev/ttySn** direct terminal devices
- **tn**—for **/dev/ttytn** pseudo modem devices

where **n** is port number.

<getty_label>

The label in the **/etc/gettydefs** file (to set speed, parity, etc.). The default is **H**.

Examples

crdlogin -a s10 19200

This example adds a login for device `/dev/ttys10` at 19200 baud with 7 data bits and even parity.

crdlogin -a X21

This example adds a login for device `/dev/ttyX21` (a Lite mode port). The default `gettydefs` label `m` will be used.

crdlogin -r s10

This example removes the login for `/dev/ttys10` created in the first example.

crdlogin -d X21

This example disables the login for `/dev/ttyX21`, but does not remove it.

addlogins

The **addlogins** script adds logins for a range of ports, using the **crdlogin** script.

Syntax

Description Adds logins for a range of ports by calling the **crdlogin** script.

Syntax **addlogins** [-l <tty_letter>] [-t <getty_label>] <first> <last>

Options -l <tty_letter>

Indicates the mode, where <tty_letter> is:

- **X**—for Lite mode devices
- **s**—for Direct Terminal devices (default)
- **S**—for Modem devices
- **t**—for pseudo Modem devices

-t <getty_label>

Indicates that the following parameter is the `ttydefs` label to use. If not given, the **crdlogin** script's default will be used (**H**).

<first>

The number that specifies the start of the range of ports to add logins for. A login for a single port can be added by setting both *first* and *last* to that port's number.

<last>

The number that specifies the end of the range of ports to add logins for. A login for a single port can be added by setting both *first* and *last* to that port's number.

Examples

addlogins -l s -t 4800 0 95

This example adds logins for devices `/dev/ttys0` to `/dev/ttys95`. The ports will be set to 4800 baud with 7 data bits and even parity.

addlogins -l X 5 12

This example adds logins for Lite mode devices `/dev/ttyX5` to `/dev/ttyX12`.

rmlogins

The **rmlogins** removes logins for a range of ports, using the **crdlogin** script. Its usage is similar to the **addlogins** script used to create logins.

Syntax

Description Removes logins for a range of ports by calling the **crdlogin** script.

Syntax **rmlogins** [-l <tty_letter>] <first> <last>

Options -l <tty_letter>

Indicates the mode, where <tty_letter> is:

- **X**—for Lite mode devices
- **s**—for Direct Terminal devices (default)
- **S**—for Modem devices
- **t**—for pseudo Modem devices

<first>

The number that specifies the start of the range of ports to remove logins for. A login for a single port can be removed by setting both *first* and *last* to that port's number.

<last>

The number that specifies the end of the range of ports to remove logins for. A login for a single port can be removed by setting both *first* and *last* to that port's number.

Examples

rmlogins 0 95

Removes logins for devices `/dev/ttys0` to `/dev/ttys95`.

rmlogins -l X 5 12

Removes logins for Server-Initiated Lite mode devices `/dev/ttyX5` to `/dev/ttyX12`.

Configuring Packet Forwarding

The Packet Forwarding feature allows you to control how the data written by a HP-UX application to the slave TTY port is packetized before forwarding the packet onto the LAN network.

Configuration Script

When you specify the packet forwarding option, a configuration script is automatically launched as follows:

```
Enable Packet Definition (y/n): y
Packet Size [0] ( 1 - 1024):
Idle Time ([0] - 65535):
Force Transmit Time ([0] - 65535):
Enable End Trigger1 (y/n): y
End Trigger1 Character ([0] - ff):
Enable End Trigger2 (y/n):
End Trigger2 Character ([0] - ff):
Enter the Forwarding Rule ([trigger], trigger+1, trigger+2, strip-trigger):
```

```
Enable Packet Definition (y/n): n
Enable Frame Definition (y/n): y
SOF1 Character ([0] - ff):
Enable SOF2 (y/n):
SOF2 Character ([0] - ff):
Transmit SOF Character(s) ([on]/off):
EOF1 Character ([0] - ff):
Enable EOF2 (y/n):
EOF2 Character ([0] - ff):
Enter the Forwarding Rule ([trigger], trigger+1, trigger+2, strip-trigger):
```

The following table describes the options:

Packet Definition	This section allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, if you set a Force Transmit Timer of 1000 ms and a Packet Size of 100 bytes, whichever criteria is met first is what will cause the packet to be transmitted.
Packet Size	The number of bytes that must be written by the application before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-1024 bytes. The default is 0.
Idle Time	The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.
Force Transmit Timer	When the specified amount of time, in milliseconds, elapses after the first character is written by the application, the packet is transmitted. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.
End Trigger1 Character	When enabled, specifies the character that when written by the application will define when the packet is ready for transmission. The content of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

End Trigger2 Character	When enabled, creates a sequence of characters that must be written by the application to specify when the packet is ready for transmission (if the End Trigger1 character is not immediately followed by the End Trigger2 character, COMredirect waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The content of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.
Frame Definition	This section allows you to control the frame that is transmitted by defining the start and end of frame character(s). If the internal buffer (1024 bytes) is full before the EOF character(s) are received, the packet will be transmitted and the EOF character(s) search will continue. The default frame definition is SOF=00 and EOF=00.
SOF1 Character	When enabled, the Start of Frame character defines the first character of the frame, any character(s) received before the Start of Frame character is ignored. Valid values are in hex 0-FF. The default is 0.
SOF2 Character	When enabled, creates a sequence of characters that must be received to create the start of the frame (if the SOF1 character is not immediately followed by the SOF2 character, COMredirect waits for another SOF1 character to start the SOF1/SOF2 character sequence). Valid values are in hex 0-FF. The default is 0.
Transmit SOF Character(s)	When enabled, the SOF1 or SOF1/SOF2 characters will be transmitted with the frame. If not enabled, the SOF1 or SOF1/SOF2 characters will be stripped from the transmission.
EOF1 Character	Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The content of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.
EOF2 Character	When enabled, creates a sequence of characters that must be received to define the end of the frame (if the EOF1 character is not immediately followed by the EOF2 character, COMredirect waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The content of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.
Trigger Forwarding Rule	<p>Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options:</p> <ul style="list-style-type: none">● Strip-Trigger—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.● Trigger—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.● Trigger+1—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger.● Trigger+2—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger.

pktfwdcfg.crd File Format

The packet forwarding configuration file is called **pktfwdcfg.crd** and is broken up into ports and their defined values as shown in the example below:

```
[10001]
packet_size = 1
idle_time = 2
force_transmit_time = 3
[mysds:10002]
SOF1_char = aa
SOF2_char = bb
transmit_SOF_chars = off
EOF1_char = cc
EOF2_char = dd
trigger_forwarding_rule = trigger
[yoursds:10003]
packet_size = 1000
idle_time = 99
force_transmit_time = 10000
end_trigger1_char = aa
end_trigger2_char = bb
trigger_forwarding_rule = trigger
[172.16.44.21:10004]
packet_size = 1000
idle_time = 99
force_transmit_time = 10000
end_trigger1_char = aa
end_trigger2_char = bb
trigger_forwarding_rule = trigger
```

Configuring SSL/TLS

The SSL/TLS feature is designed to work with the Secure Terminal Server, Secure Device Server, and Secure Console Server models. When COMredirect is used with the Terminal Server, the cipher specified by the Terminal Server will be used for the COMredirect connection. Also, if the Terminal Server is set for **SSL/TLS Type Server**, then you need to set the **COMredirect SSL type** to **client**, and vice versa.

SSL/TLS Configuration Information

SSL/TLS is configured using the **addports** or **crdadm** utilities. If SSL/TLS is enabled, the following prompts will ask for the SSL/TLS configuration information:

```
Certificate file name (full path and file name): /etc/COMredirect/sslcert.pem
SSL type (client or server): client
SSL/TLS version (any, TLSv1, or SSLv3): any
Perform peer verification (y/n): y
```

The next section is asked only if peer verification is performed. If you press **Enter** instead of entering a value, the parameter will not appear in the **sslcfg.crd** file for peer validation.

Note: The values that you enter here are case sensitive, so the peer certificate must match exactly or the connection will fail.

```
CA file name (full path and file name): /etc/COMredirect/ca.pem
Country (2 letter code): CA
State or Province: Ontario
Locality (e.g., city): Markham
Organisation (e.g., company): Acme Software
Organisation Unit (e.g., section): Engineering
Common Name (e.g., your name or your server's hostname): hpux50
Email Address: engineering@acme.com
```

The following section provides more information about the SSL/TLS configuration parameters:

Certificate file name The full path and file name of the certificate file. If you press **Enter**, the default path, **/etc/COMredirect/sslcert.pem**, will be used.

SSL type Specify whether the COMredirect daemon will act as an SSL/TLS client or server.

SSL/TLS version Specify whether you want to use:

- **Any**—The COMredirect daemon will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try an SSLv2 connection.
- **TLSv1**—The connection will use only TLSv1.
- **SSLv3**—The connection will use only SSLv3.

Perform peer validation The certificate received from the peer will be verified against the CA list, along with any values entered in the validation criteria, for an SSL connection; any fields left blank will not be validated against the peer certificate.

CA file name The full path and file name of the CA (certificate authority) file. If you press **Enter**, the default path, **/etc/COMredirect/ca.pem**, will be used.

Country	A two character country code; for example, US.
State or Province	Up to a 128 character entry for the state/province; for example, IL.
Locality	Up to a 128 character entry for the location; for example, a city.
Organisation	Up to a 64 character entry for the organization; for example, Acme Software.
Organisation Unit	Up to a 64 character entry for the unit in the organization; for example, Payroll.
Common Name	Up to a 64 character entry for common name; for example, the host name or fully qualified domain name.
Email Address	Up to a 64 character entry for an email address; for example, acct@anycompany.com.

SSL/TLS Support Files

When you enable the SSL/TLS option for a port, you need to make sure the COMredirect host and Terminal Server have the appropriate support files: certificates/private keys and/or the CA list file. The Installation CD-ROM contains a self-signed RSA certificate named **samplecert.pem**. The **samplecert.pem** file can be used for both the certificate file on the SSL/TLS server and the CA list file on the SSL/TLS client.

COMredirect Port Configured as SSL/TLS Server

When the COMredirect port is configured as an SSL/TLS server, the SSL/TLS private key and certificate is required for all key exchange methods except ADH (Anonymous Diffie-Hellman). The private key cannot be encrypted since COMredirect on HP-UX does not support the configuration of an SSL/TLS passphrase. The private key needs to be appended to the certificate file, to create one certificate/private key file. This can be done using the HP-UX command **cat myprivatekey.pem >> mycert.pem**. This certificate/private key file then becomes the COMredirect certificate. Copy the COMredirect certificate file to the directory you specified in the SSL/TLS configuration.

If the COMredirect SSL/TLS server is configured to verify an SSL client, a CA list file is also required. The CA list file is a certificate, or list of certificates, of the Certificate Authorities (CA) who created and signed the peer certificates (the peer certificate(s) must be downloaded to the Terminal Server).

COMredirect Port Configured as SSL/TLS Client

When the COMredirect port is configured as an SSL/TLS client and peer verification is configured, a CA list file is required. The CA list file is a certificate, or list of certificates, of the Certificate Authorities (CA) who created and signed the peer certificates (the peer certificate(s) must be downloaded to the Terminal Server). This CA list file should be copied to the COMredirect host directory specified in the SSL/TLS configuration.

Pseudo Random Number Generator

If you want to use the SSL/TLS encryption on a COMredirect connection an external Random Number Generator is required on the host system. This is available for each of the following HP-UX versions:

- HP-UX 11iv2 and HP-UX 11iv3 have SRNG (Strong Random Number Generator) already built in.
- HP-UX 11i requires SRNG (Strong Random Number Generator) and can be downloaded from the HP website, [HP-UX Strong Random Number Generator](#).
- HP-UX 11.0 PRNG can be downloaded from: <http://freshmeat.net/projects/hpux11-random/>

sslcfg.crd File Format

The **sslcfg.crd** file is created in the following format:

```
[10001]
certificate-file = /etc/COMredirect/sslcert.pem
ssl-type = server
ssl-version = any
verify-peer = yes
CA-file = /etc/COMredirect/ca.pem
country = CA
state-province = Ontario
locality = Markham
organisation = Acme Software
organisation-unit = Engineering
common-name = hpux50
email = engineering@acme.com
[yoursds:10002]
certificate-file = /etc/COMredirect/sslcert.pem
ssl-type = client
ssl-version = TLSv1
verify-peer = yes
CA-file = /etc/COMredirect/ca.pem
country = UK
locality = London
common-name = hpuxuk
```

The [10001] specifies the port for which the SSL/TLS configuration parameters are configured.

SSL/TLS Trouble Shooting

If you are experiencing problems obtaining a successful SSL/TLS connection, you can add the **-trace 4** option at the end of the appropriate port entry in the **config.crd** file. After editing the **config.crd** file, you will have to kill the COMredirect daemon process for the port and restart it again. Adding the **-trace** option will create a trace file called **/etc/COMredirect/trace.xxxxx**, where **xxxxx** is the controlling TTY name; for example, **/etc/COMredirect/trace.crdm0**.

Could not obtain peer's certificate

Reason 1	User has selected a cipher key exchange of ADH (anonymous Diffie-Hellman) and enabled Peer verification. ADH does not use certificates so they will not be sent in an SSL/TLS handshake.
Solution 1	Disable Peer Verification or change to a cipher suite that uses certificates.
Reason 2	User has selected Peer Verification on the configured SSL/TLS server and has not configured a certificate for the client.
Solution 2	Either disable peer verification on the SSL/TLS server or configure a certificate for the SSL/TLS client.

SSL_accept failed on the SSL/TLS server device.

Reason	The device has failed to accept an SSL/TLS connection on top of a TCP connection that has just been established. This could indicate that the peer from which COMredirect is trying to accept a connection from is not configured for SSL/TLS.
Solution	Verify that the peer has been configured for an SSL/TLS client connection.

Certificate did not match configuration

Reason	The message is displayed when Verify Peer Certificate has been enabled, but the configured Validation Criteria does not match the corresponding data in the certificate received from the peer.
Solution	The data configured must match exactly to the data in the certificate. The data is also case sensitive.

Encrypted private keys are not supported in COMredirect

Reason	This message is displayed by the COMredirect daemon when the user has created a certificate with an encrypted private key for COMredirect. This applies to either Client-Initiated mode or Server-Initiated mode with configured peer validation criteria.
Solution	Create a certificate with a private key that is not encrypted.

unknown protocol message when trying to make an SSL/TLS connection

Reason 1	This will be displayed when both sides of the TCP connection are configured as SSL/TLS clients.
Solution 1	Change one of the end points to act as an SSL/TLS server.
Reason 2	One of the endpoints is not configured for SSL/TLS.
Solution 2	Make sure both endpoints are configured for SSL/TLS, verify that one is a client and the other is a server.

tlsv1 alert handshake failure or sslv3 alert handshake failure

Reason	The remote site has an SSL/TLS error and is sending this message with an alert message.
---------------	---

Solution	Look at the error messages on the remote end and fix the problem indicated.
-----------------	---

Certificate verify failed.

Reason 1	COMredirect has been configured to verify the peer certificate and there is a mismatch between the peer's certificate and the COMredirect CA list.
-----------------	--

Solution 1	Make sure the CA lists contains the certificate of the CA which signed the peer's certificate.
-------------------	--

Reason 2	The peer's certificate or the CA certificate might have expired. Each certificate is created with a valid date interval.
-----------------	--

Solution 2	Make sure the certificate of the peer and CA are up to date. Also verify that the host has the correct date/time. If the date configured on the host is not correct, it can make it look like the certificate is invalid.
-------------------	---



© Copyright 2008. Black Box Corporation. All rights reserved.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746