

Connect:Direct[®] for UNIX

Getting Started Guide

Version 3.8

**Connect:Direct for UNIX Getting Started Guide
Version 3.8**

First Edition

(c) Copyright 1999-2006 Sterling Commerce, Inc. All rights reserved. Additional copyright information is located at the end of this guide.

STERLING COMMERCE SOFTWARE

*****TRADE SECRET NOTICE*****

THE CONNECT:DIRECT SOFTWARE ("STERLING COMMERCE SOFTWARE") IS THE CONFIDENTIAL AND TRADE SECRET PROPERTY OF STERLING COMMERCE, INC., ITS AFFILIATED COMPANIES OR ITS OR THEIR LICENSORS, AND IS PROVIDED UNDER THE TERMS OF A LICENSE AGREEMENT. NO DUPLICATION OR DISCLOSURE WITHOUT PRIOR WRITTEN PERMISSION. RESTRICTED RIGHTS.

This documentation, the Sterling Commerce Software it describes, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of Sterling Commerce, Inc., its affiliated companies or its or their licensors, and may not be used for any unauthorized purpose, or disclosed to others without the prior written permission of the applicable Sterling Commerce entity. This documentation and the Sterling Commerce Software that it describes have been provided pursuant to a license agreement that contains prohibitions against and/or restrictions on their copying, modification and use. Duplication, in whole or in part, if and when permitted, shall bear this notice and the Sterling Commerce, Inc. copyright notice. As and when provided to any governmental entity, government contractor or subcontractor subject to the FARs, this documentation is provided with RESTRICTED RIGHTS under Title 48 52.227-19. Further, as and when provided to any governmental entity, government contractor or subcontractor subject to DFARs, this documentation and the Sterling Commerce Software it describes are provided pursuant to the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation.

These terms of use shall be governed by the laws of the State of Ohio, USA, without regard to its conflict of laws provisions. If you are accessing the Sterling Commerce Software under an executed agreement, then nothing in these terms and conditions supersedes or modifies the executed agreement.

Where any of the Sterling Commerce Software or Third Party Software is used, duplicated or disclosed by or to the United States government or a government contractor or subcontractor, it is provided with RESTRICTED RIGHTS as defined in Title 48 CFR 52.227-19 and is subject to the following: Title 48 CFR 2.101, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14, and FAR 52.227-19(c)(1-2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation including DFAR 252.227-7013, DFAR 252,227-7014, DFAR 252.227-7015 and DFAR 252.227-7018, all as applicable.

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as described in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Sterling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

Connect:Direct is a registered trademark of Sterling Commerce. Connect:Enterprise is a registered trademark of Sterling Commerce, U.S. Patent Number 5,734,820. All Third Party Software names are trademarks or registered trademarks of their respective companies. All other brand or product names are trademarks or registered trademarks of their respective companies.

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Chapter 1 About Connect:Direct for UNIX 7

Server Components	7
Process Manager	7
Command Manager	8
Session Manager	8
File Agent	8
Connect:Direct Secure+ Option for UNIX	9
User Interfaces	9
Applications Programming Interface	9
Command Line Interface	9
Sterling Control Center	10
Connect:Direct Browser User Interface	11
Connect:Direct Concepts	12
Local and Remote Nodes	12
Processes	12
Transmission Control Queue	13
Commands	14
Network Map	14
User Authorization	15
Process Restart	16
Archive Statistics Files	17
Sample Processes, Shell Scripts, and API Processes	17
Connect:Direct for UNIX Files	18
Connect:Direct for UNIX Configuration Files	18
Connect:Direct for UNIX Directory Structure	19
Connect:Direct for UNIX Documentation	21
About This Guide	21
Task Overview	22

Chapter 2 Installing Connect:Direct for UNIX 23

Before You Begin	23
Configuration Types	23
Preparing to Install Connect:Direct for UNIX in a Cluster Environment	23
High-Availability Cluster Environments	24
Load-Balancing Cluster Environments	24
Preparing to Install Connect:Direct for UNIX on the Linux for S/390 Operating System	26

Installing Connect:Direct for UNIX	27
Customizing Connect:Direct for UNIX	30
Setting Up the Connect:Direct for UNIX Server.	32
Defining the Connect:Direct Node Name	32
Defining the Initialization Parameters File	32
Defining the Network Map File	33
Customizing the User Authorization Information File	34
Connect:Direct Creates an Authentication Key File	36
Setting Up the Connect:Direct for UNIX Client	36
Customizing the Client Configuration File	36
Customizing the Client Authentication Key File	37
Creating a Strong Access Control List File	37
Changing File Ownership and Permissions.	38
Installing File Agent	41
Installing Secure+ Option	42
Configuring SNA Support for Connect:Direct for UNIX	46
Defining High-Availability Settings in the Configuration Files	46
Additional Configuration Requirements in a SunCluster 3.0 Environment	47
Additional Configuration Requirements in a SunCluster 2.2 Environment	47
Additional Configuration Requirements for IBM HACMP	48
Additional Configuration Requirements for Hewlett-Packard MC/ServiceGuard	48
Verifying the Installation	49

Chapter 3 Managing Files with Connect:Direct File Agent 51

Connect:Direct File Agent	51
Running File Agent	52
File Agent Logging Capabilities.	53
File Agent Configuration Interface and Help	53
Planning the File Agent Configuration	53
Connect:Direct File Agent Configuration Examples.	57
Detecting a File Added to a Watched Directory on an OS/390 or z/OS System	57
Detecting a File by File Size on a Windows System	57
Detecting a System Event by Title on a Windows System	59
Passing the UNIX Pathname for a Detected File to a Process.	60

Appendix A Installation Worksheets 61

Installation Worksheet	62
Customization Worksheet	62
User Authorization Information File Worksheet	63
Remote User Information Record	63
Local User Information Record	64
CLI/API Configuration File Worksheet	68
Network Map Remote Node Information File Worksheet (TCP/IP Only)	69
Server Authentication Key File Worksheet	70
Client Authentication Key File Worksheet	70

Appendix B SNA LU6.2 Connectivity **71**

About SNA LU6.2 Connections	71
Supported Interfaces	71
Session Support	71
APPC Requirements	72
Configuration Requirements	72
SNA Considerations	72
Installing and Configuring the AIX SNA Server	73
Manually Configuring the AIX SNA Server	73
About the Configuration Script	74
Running the Configuration Script	75
HP SNAplus2 Configuration Requirements	77
SNAP-IX SNA Gateway Support Configuration Requirements	77
Brixton 4.1 SNA for Sun Solaris Requirements	81
Configuring BrxGMAN Software	81
Configuring BrxGMI Software	83
Configuring BrxPU21 Software	84
Starting BrxGMAN	85
Sample Brixton BrxPU2.1 Configuration	86
SunLink SNA 9.1 for Sun Solaris Configuration Requirements	88
Sample MVS Definitions for an LU6.2 Connection	92
Token Ring 3174-R Gateway Controller Configuration	93
Token Ring 3745 Token Ring Interface Coupler (TIC) Configuration	95
VTAM Application Definition	96
VTAM Logmode Table Entries	96
NTRI Switched Major Node Definition	97
ILU CDRSC Definitions	97
Connect:Direct Remote Node Entry	98
Special Considerations	98
Required Changes to the File Specified with the comm.info Parameter	98
Obtaining Traces for the Brixton LU6.2 API and SunLink P2P	99
Stopping Connect:Direct on SNA Systems	99
Connectivity Between RS/6000 and AS/400 Systems	99
AIX SNA Error Messages	99

Appendix C Connect:Direct for UNIX Manual Pages **101**

Setting Up Connect:Direct for UNIX Manual Pages	101
Combining Manual Pages	101
Displaying Connect:Direct Manual Pages	102
Accessing Connect:Direct Manual Pages	102
Using MANPATH in the Bourne Shell	102
Using MANPATH in the C Shell	102
Accessing Manual Pages on an IBM RISC System/6000 or Sun SPARC Platform Using BSDI	103

Glossary **105**

Index **111**

About Connect:Direct for UNIX

Connect:Direct links technologies and moves all types of information between networked systems and computers. It manages high-performance transfers by providing such features as automation, reliability, efficient use of resources, application integration, and ease of use. Connect:Direct offers choices in communications protocols, hardware platforms, and operating systems. It provides the flexibility to move information among mainframe systems, midrange systems, desktop systems, and LAN-based workstations.

Connect:Direct is based on client-server architecture. The Connect:Direct server components interact with the user interfaces (API, CLI, Connect:Direct Browser User Interface, and Sterling Control Center) to enable you to submit, execute, and monitor Connect:Direct statements and commands.

Server Components

Connect:Direct has the following server components:

Process Manager

The Process Manager (PMGR) is the daemon that initializes the Connect:Direct server environment. The PMGR provides the following functions:

- ◆ Initializes Connect:Direct
- ◆ Accepts connection requests from Connect:Direct client APIs and remote nodes
- ◆ Creates Command Manager and Session Manager child Processes to communicate with APIs and remote nodes
- ◆ Accepts requests from Command Managers and Session Managers when centralized Connect:Direct functions are required
- ◆ Stops Connect:Direct

Note: Any application, including End User Applications (EUA), can run on any computer as long as it can connect to the PMGR.

Command Manager

A Command Manager (CMGR) is created for every API connection that is successfully established. The number of Command Managers that a PMGR can create is system-dependent and limited by the number of file descriptors available for each UNIX Process. The number of file descriptors set up by the UNIX operating system may affect Connect:Direct operation. You must define enough file descriptors to handle the number of concurrent Connect:Direct sessions allowed, which can be as many as 999.

The CMGR provides the following functions:

- ◆ Executes commands sent by the API and sends the results back to the API
- ◆ Carries out the Connect:Direct authentication procedure, in conjunction with the API, to determine access to Connect:Direct
- ◆ Interacts with the PMGR when executing commands

Session Manager

The Session Manager (SMGR) is created and invoked by the PMGR when resources are available and either a Process is ready to run or a remote node requests a connection with a local node. The SMGR provides the following functions:

- ◆ Performs the necessary Connect:Direct work
- ◆ Acts as a primary node (PNODE) and initiates Process execution
- ◆ Acts as a secondary node (SNODE) to participate in a Process initiated by the PNODE

When an SMGR is created to execute a Process submitted to a node, it creates the connection to the remote node. If the SMGR is started by the PMGR to execute local Processes, the SMGR runs each Process on this session until all Processes are completed.

If an SMGR is created because a remote node initiated a connection, the SMGR completes the connection. If the SMGR is started by the PMGR to execute remote Processes, the SMGR executes remote Process steps supplied by the remote SMGR until the remote SMGR completes all of its Processes.

The SMGR depends on the PMGR for Transmission Control Queue (TCQ) services and other centralized services. Refer to the *Transmission Control Queue* on page 1 for an overview of the TCQ.

File Agent

Connect:Direct File Agent is a feature of Connect:Direct, which provides unattended file management. File Agent monitors *watched* directories to detect new files. When File Agent detects a new file, it either submits a default Process or evaluates the file using rules to override the default Process and to determine which Process to submit. You create rules to submit different Processes based on the following properties:

- ◆ Specific or partial file names
- ◆ File size
- ◆ System events

You create the Processes used by File Agent on Connect:Direct; you cannot create them using File Agent.

To achieve optimum performance, configure File Agent to communicate with the Connect:Direct node where it is installed. File Agent can be installed on UNIX, Windows, and z/OS operating systems. For information to help you plan how to implement File Agent, see the *Managing Files with Connect:Direct File Agent* chapter in your Connect:Direct administration guide or getting started guide. The Connect:Direct File Agent Help contains instructions for configuring File Agent.

Connect:Direct Secure+ Option for UNIX

The Connect:Direct Secure+ Option application provides enhanced security for Connect:Direct and is available as a separate component. It uses cryptography to secure data during transmission. You select the security protocol to use with Secure+ Option.

To use Connect:Direct Secure+ Option for communications with remote nodes, you must have node records in the Secure+ Option parameters file that duplicate the adjacent node records in the Connect:Direct network map. You can populate the Secure+ Option parameters file from entries defined in an existing network map. For more information about creating the Connect:Direct Secure+ Option parameters file and configuring nodes for Secure+ Option, refer to the *Connect:Direct Secure+ Option for UNIX Implementation Guide*.

User Interfaces

Connect:Direct has the following user interfaces, which enable you to create, submit, and monitor Processes.

Applications Programming Interface

The UNIX Applications Programming Interface (API) enables you to write programs that work with Connect:Direct. Four API functions are provided to allow an End User Application (EUA) to perform the following tasks:

- ◆ Establish an API connection to the Connect:Direct server
- ◆ Terminate an API connection to the Connect:Direct server
- ◆ Send a command to Connect:Direct
- ◆ Receive responses from commands

Command Line Interface

The Command Line Interface (CLI) enables you to perform the following tasks:

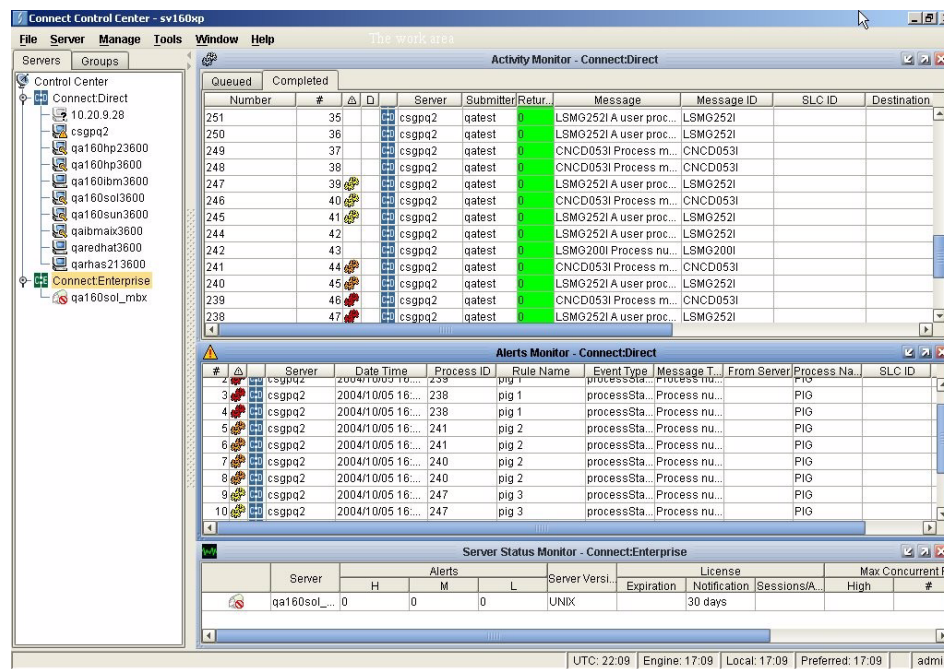
- ◆ Issue Connect:Direct commands
- ◆ Monitor Processes

The default CLI command prompt is **Direct >**. Refer to Chapter 2, *Controlling and Monitoring Processes* in the *Connect:Direct for UNIX User's Guide* for additional information about the CLI.

Sterling Control Center

Sterling Control Center is a centralized management system that provides operations personnel with continuous enterprise-wide business activity monitoring capabilities for Connect:Direct for z/OS, Connect:Direct for UNIX, Connect:Direct for Windows, Connect:Direct for HP NonStop, Connect:Direct Select, and Connect:Direct OS/400 (iSeries) servers, and Connect:Enterprise for UNIX and Connect:Enterprise for z/OS servers. Sterling Control Center enables you to:

- ◆ Manage multiple servers
 - ◆ Group individual servers into server groups for a single view of system-wide activity
 - ◆ View status and statistics on active or completed processing
 - ◆ Suspend, release, stop, and delete Connect:Direct Processes on z/OS, UNIX, Windows, Select, and HP NonStop platforms
 - ◆ Stop Connect:Direct servers on z/OS, Windows, HP NonStop, and UNIX platforms.
- ◆ Monitor service levels
 - ◆ View processing across Connect:Direct for z/OS, UNIX, Select, Windows, HP NonStop, and OS/400 (iSeries) servers, and Connect:Enterprise for UNIX and Connect:Enterprise for z/OS servers within your network and retrieve information about active and completed processing



- ◆ Receive notification of data delivery events that occur or do not occur as scheduled
- ◆ Define rules that, based on processing criteria, can generate an alert, send an e-mail notification, generate a Simple Network Management Protocol (SNMP) trap to an Enterprise Management System (EMS), run a system command, or issue a server command
- ◆ Monitor for alerts, such as a server failure or a Process not starting on time

- ◆ Create service level criteria (SLCs) that define processing schedules, monitor Processes, files within Processes, and file transfers for compliance with these schedules, and generate alerts when the schedules are not met
- ◆ Analyze key operational metrics
- ◆ Create customized reports to document and analyze processing activity based on criteria you define
- ◆ Validate the authenticity of a user logging on to Sterling Control Center, using one or more of four authentication methods including password validation, host name identification, Windows domain, and TCP/IP address
- ◆ Identify additional servers that may need to be monitored based on communications with a currently monitored server using the Guided Node Discovery feature

Sterling Control Center enhances operational productivity and improves the quality of service by:

- ◆ Ensuring that critical processing windows are met
- ◆ Reducing impact on downstream processing by verifying that expected processing occurs
- ◆ Providing proactive notification for at-risk business processes
- ◆ Consolidating information for throughput analysis, capacity planning, post-processing operational or security audits, and workload analysis
- ◆ Reducing the risk of errors associated with manual system administration, including eliminating individual server logon to view activity, and the need to separately configure each server for error and exception notifications

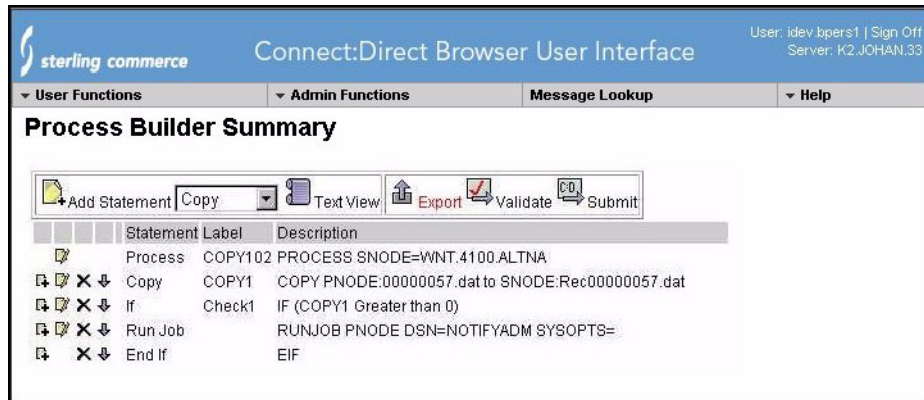
Sterling Control Center is available for purchase as a separate product. Contact your Sterling Commerce representative to learn more about Sterling Control Center.

Connect:Direct Browser User Interface

Connect:Direct Browser User Interface allows you to build, submit, and monitor Connect:Direct Processes from an Internet browser, such as Microsoft Internet Explorer.

You can also perform Connect:Direct system administration tasks, such as viewing and changing the network map or initialization parameters, from Connect:Direct Browser. The specific administration tasks that you can perform depend on the Connect:Direct platform that your browser is signed on to and your security level.

Connect:Direct Browser is distributed on CD-ROM with Connect:Direct for z/OS, Connect:Direct for Windows, Connect:Direct for UNIX, and Connect:Direct for HP NonStop. It can also be downloaded from the Sterling Commerce Web site. Connect:Direct Browser is installed on a Web server and can be accessed by administrators and users through a URL. The following example shows the page used to graphically build a Process:



To learn more about Connect:Direct Browser, see the documentation on the Connect:Direct Browser CD-ROM or available online from the Sterling Commerce Documentation Library.

Connect:Direct Concepts

This section introduces concepts and definitions to help you understand system operations.

Local and Remote Nodes

Each data transfer involves a local and a remote node. The Connect:Direct server is the local node and the partner node is the remote node. The two servers (local and remote) function together to perform the work. Either Connect:Direct node can initiate the work.

Local and remote node connections are set up in the network map file. Refer to Chapter 5, *Maintaining the Network Map File*, in the *Connect:Direct for UNIX Administration Guide* for a description of the network map file.

Connect:Direct must be installed on each node. When Connect:Direct establishes a session between the local node and remote node, the node that initiates the session has primary control (PNODE). The other serves as the partner and has a secondary function (SNODE). The node that initiates the session has primary control, regardless of the direction of information flow. The Process can specify work destined for either the local or remote node. When Connect:Direct establishes a session, the two nodes work together to transfer the information.

Processes

The Connect:Direct Process language provides instructions for transferring files, running programs, submitting jobs on the adjacent node, and altering the sequence of Process step execution. You can include one or more steps in a Process. A Process consists of a Process definition statement (**process** statement) and one or more additional statements. Parameters further qualify Process instructions.

The following table lists Process statements and their functions:

Process Statement	Function
copy	Copies files from one node to another.
conditionals	Alters the sequence of Process execution based on the completion code of previous steps with the if , then , else , endif (end if), goto , and exit statements.
process	Defines general Process characteristics.
run job	Enables you to specify UNIX commands in a Process. The Process does not wait until the job has finished running before executing the next step in the Process.
run task	Enables you to specify UNIX commands in a Process. The Process waits until the job has finished running before executing the next step in the Process.
submit	Starts another Process to either the local or remote node during execution of a Process.
pend	Marks the end of a Connect:Direct for UNIX Process.

Following is a sample Process:

```

ckpt01 process snode=unix.node
step01 copy from (
    file=file1
    snode
)
    ckpt=1M
    to (
        file=file2
        disp=new
        pnode
    )
pend;

```

Refer to the Connect:Direct Processes Web site at <http://www.sterlingcommerce.com/documentation/processes/processhome.html> for instructions on building a Process.

Transmission Control Queue

The Transmission Control Queue (TCQ) controls when Processes run. Connect:Direct stores submitted Processes in the TCQ. The TCQ is divided into four logical queues: Execution, Wait, Timer, and Hold. Processes are run from the Execution queue.

Connect:Direct places a Process in the appropriate queue based on Process statement parameters, such as the **hold**, **retain**, and **startt** parameters.

Connect:Direct runs Processes based on their priority and when the Process is placed in the Execution queue. Higher priority Processes are selected for execution ahead of Processes with a lower priority. You can access the queues and manage the Processes through Connect:Direct commands.

Refer to the *Connect:Direct for UNIX User's Guide* for more information on scheduling Processes in the TCQ.

Commands

You use commands to submit Processes to the TCQ. You can also use commands to perform the following tasks:

- ◆ Manage Processes in the queue
- ◆ Monitor and trace Process execution
- ◆ Produce reports on Process activities
- ◆ Stop Connect:Direct operation

The following table lists the commands and their functions:

Command	Function
change process	Changes the status and modifies specific characteristics of a nonexecuting Process in the TCQ.
delete process	Removes a nonexecuting Process from the TCQ.
flush process	Removes an executing Process from the TCQ.
trace	Runs Connect:Direct traces.
select process	Displays or prints information about a Process in the TCQ.
select statistics	Displays or prints statistics in the statistics log.
stop	Stops Connect:Direct operation.
submit	Submits a Process for execution.

For example, the following command submits the Process called **onestep** to the TCQ with a hold status of yes:

```
Direct> submit file=onestep hold=yes;
```

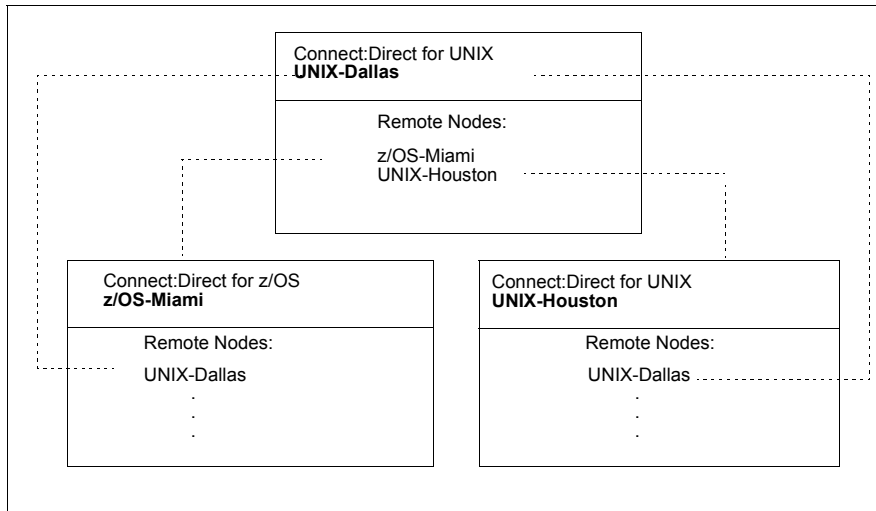
Network Map

During the transfer of data, the Connect:Direct server where the Process is submitted is the primary node and the secondary node is the partner node. Connect:Direct identifies the remote nodes that

the local node is able to communicate with through the use Connect:Direct network map (or netmap).

The network map includes the names of all the remote nodes that the Connect:Direct local node can communicate with, the paths to contact those remote nodes, and characteristics of the sessions for communication.

The remote Connect:Direct nodes also have network maps for their remote nodes. The following sample displays the corresponding network map entries of UNIX-Dallas, z/OS-Miami, and UNIX-Houston:



User Authorization

Connect:Direct can authorize local and remote users to perform certain Connect:Direct tasks. In order to use Connect:Direct, each user must have a record defined in the user authorization file, called `userfile.cfg`. Each local user must have a record in the user authorization file, and each remote user must be mapped to a local user ID in a proxy relationship.

To provide a method of preventing an ordinary user from gaining root access through Connect:Direct for UNIX, a second access file called the Strong Access Control file (SACL) is created when you install Connect:Direct for UNIX and is named `sysacl.cfg`. Creating an SACL file improves the security of Connect:Direct for UNIX and prevents a user from obtaining root access control. At installation, the default value for the `root:deny.access` parameter is `y` (yes). If you want to allow root access, you must access the `sysacl.cfg` and specify `root:deny.access=n`. If the file is deleted or corrupted, access to Connect:Direct is denied to all users.

The Connect:Direct administrator maintains these authorizations. Refer to Chapter 6, *Maintaining Access Information Files* in the *Connect:Direct for UNIX Administration Guide* for more information about authorizations.

Process Restart

Several facilities are provided for Process recovery after a system malfunction. The purpose of Process recovery is to resume execution as quickly as possible and to minimize redundant data transmission after a system failure. The following Connect:Direct facilities are available to enable Process recovery:

- ◆ **Process step restart**—As a Process runs, the steps are recorded in the TCQ. If a Process is interrupted for any reason, the Process is held in the TCQ. When you release the Process to continue running, the Process automatically begins at the step where it halted.
- ◆ **Automatic session retry**—Two sets of connection retry parameters are defined in the remote node information record of the network map file: short-term and long-term. If you do not specify a value for these parameters in the remote node information record, default values are used from the local.node entry of the network map file. The short-term parameters allow immediate retry attempts. Long-term parameters are used after all short-term retries are attempted. Long-term attempts assume that the connection problem cannot be fixed quickly and retry attempts occur after a longer time period, thus saving the overhead of connection retry attempts.
- ◆ **Checkpoint restart**—This feature is available with the **copy** statement. Checkpoint restart can be explicitly configured within a **copy** step through the **ckpt** parameter. (Refer to the Connect:Direct Processes Web site at <http://www.sterlingcommerce.com/documentation/processes/processhome.html>) If it is not configured in the **copy** step, it can be configured in the Initparms through the **ckpt.interval** parameter. (See the *Connect:Direct for UNIX Administration Guide* for more information on this parameter.)
- ◆ **Run Task restart**—This feature is used if the PNODE and SNODE cannot resynchronize during a restart after a run task interruption. If a Process is interrupted when a run task on an SNODE step is executing, Connect:Direct attempts to synchronize the previous run task step on the SNODE with the current run task step. Synchronization occurs in one of the following ways:
 - ◆ If the SNODE is executing the task when the Process is restarted, it waits for the task to complete, and then responds to the PNODE with the task completion status. Processing continues.
 - ◆ If the SNODE task completes before the Process is restarted, it saves the task results. When the Process is restarted, the SNODE reports the results, and processing continues.

If synchronization fails, Connect:Direct reads the **restart** parameter in the **run task** step or the initialization parameters file to determine whether to perform the **run task step** again. The **restart** parameter on the **run task** step overrides the setting in the initialization parameter.

For example, if the SNODE loses the run task step results due to a Connect:Direct cold restart, Connect:Direct checks the value defined in the **restart** parameter to determine whether to perform the **run task** again.

Note: Run task restart works differently when Connect:Direct for UNIX runs behind a connection load balancer. For more information on the considerations you need to know when running Connect:Direct for UNIX in a load balancing environment, see the *Connect:Direct for UNIX Release Notes* and the *Connect:Direct for UNIX Administration Guide*.

- ◆ Interruption of Process activity when the SNODE is a Connect:Direct for UNIX node—When the SNODE is a Connect:Direct for UNIX node and the PNODE interrupts Process activity by issuing a command to suspend Process activity, deleting an executing Process, or when a link fails or an I/O error occurs during a transfer, the Process is placed in the Wait queue in WS status.

If Process activity does not continue, you must manually delete the Process from the TCQ. Refer to the *Connect:Direct for UNIX User's Guide* for command syntax and parameter descriptions for the **delete process** command.

Note: You cannot issue a **change process** command from the SNODE to continue Process activity; the Process can only be restarted by the PNODE, which is always in control of the session.

Archive Statistics Files

Connect:Direct for UNIX provides a utility to archive and purge statistics files. When you configure Connect:Direct for UNIX, you identify when to archive a statistics file by setting the parameter, **max.age**, in the stats record of the initialization parameters file. The **max.age** parameter defines how old a statistics file must be before you want to archive the file.

Once a day, the script called `statarch.sh` is started. This script identifies the statistics files that are equal to the **max.age**. It then runs the `tar` command and the `compress` command to create a compressed archived file of all the statistics records that match the **max.age** parameter. Once the statistics files are archived, these files are purged. For files archived on a Linux computer, the archived statistics files have the `.gz` suffix since these files are compressed with the `gzip` format. Archived files on all other UNIX platforms have the `.Z` suffix to indicate they are compressed using the `compress` format.

The archived files are stored in the directory where the statistics files and TCQ are stored. The shell script, `statarch.sh`, is located in the `ndm/bin` directory. If necessary, modify the script to customize it for your environment.

If you want to restore statistics files that have been archived, run the **statrestore.sh** script. It uses the **uncompress** and **tar** commands to restore all the statistics files in the archive. You supply two arguments to the **statrestore** command. The first argument is the directory path where the statistics files are located and the second argument identifies the archived file name followed by as many archived file names as you want to restore. Below is a sample **statrestore** command:

```
qa160sol: ./statrestore.sh /export/home/users/cd3800/ndm/bin archive1
```

After files are restored, the statistics records can be viewed using the `select statistics` command.

Sample Processes, Shell Scripts, and API Processes

Connect:Direct provides sample Processes and shell scripts in `d_dir/ndm/src`, where `d_dir` indicates the destination directory of the Connect:Direct software. You can create similar files with a text editor. In addition, instructions for creating shell scripts are in the `README` file in the same directory.

The following table displays the file names of sample Processes. Modify the Processes as required.

File Name	Type of Process
cpunx.cd	copy
rtunx.cd	run task
rjunx.cd	run job
sbunx.cd	submit

The following table displays the file names of sample shell scripts. Modify the shell scripts as required.

File Name	Type of Shell Script
selstat.sh	select statistics
send.sh	send
recv.sh	receive
wildcard	send multiple files to an OS/390 PDS
statarch.sh	archive statistics files
statrestore.sh	restore statistics files that have been archived
lcu.sh	launch the Local Connection Utility tool
spadmin.sh	launch the Secure+ Option Admin Tool
spcli.sh	launch the Secure+ Option CLI (SPCLI)
spcust_sample1.sh	configure Secure+ Option for the STS protocol
spcust_sample2.sh	configure Secure+ Option for the STS protocol
spcust_sample3.sh	configure Secure+ Option to use the SSL or TLS protocol

Connect:Direct for UNIX Files

This section describes the configuration files, illustrates the directory structure of Connect:Direct for UNIX, and lists the individual files that are installed.

Connect:Direct for UNIX Configuration Files

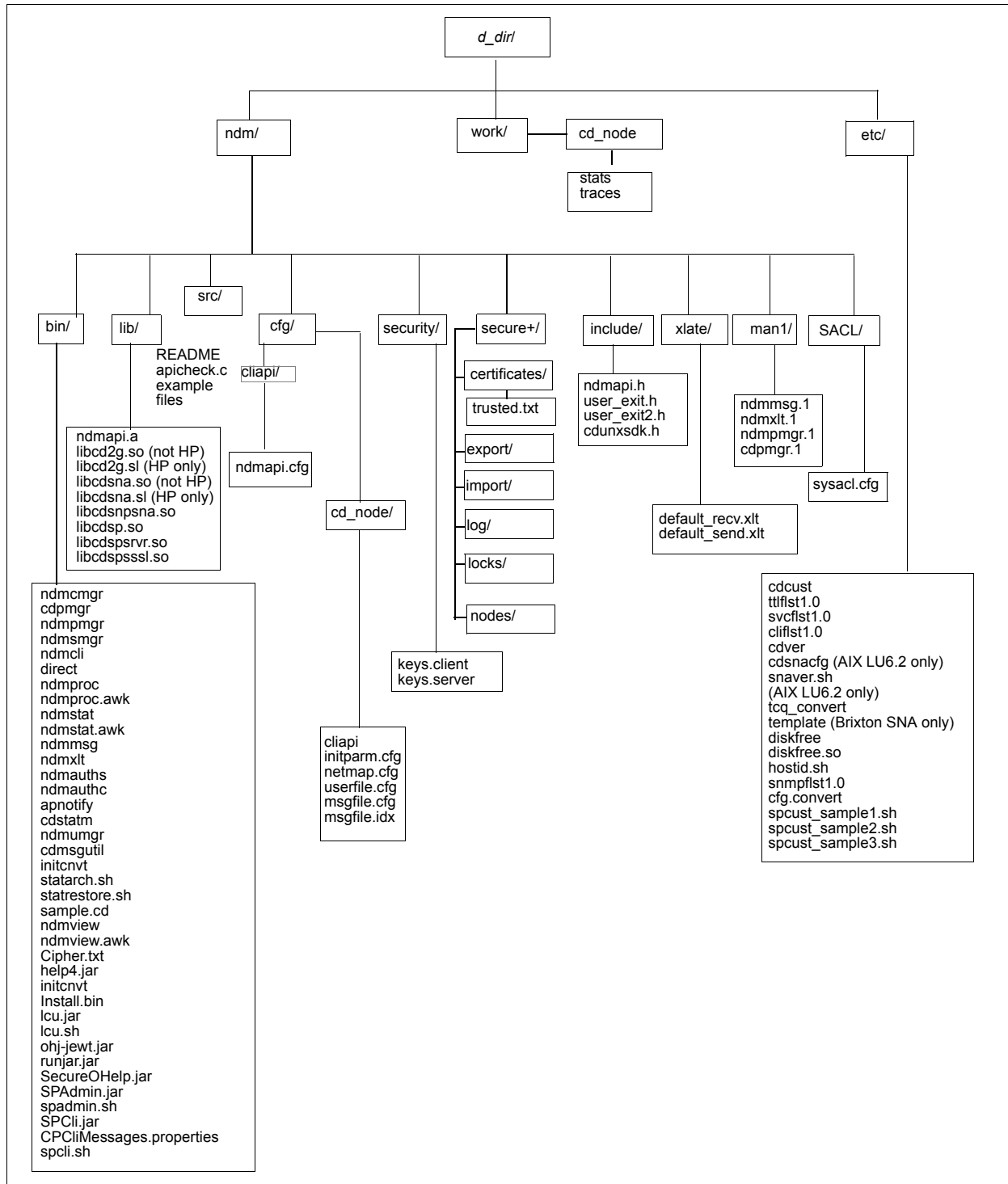
Connect:Direct for UNIX creates the following configuration files during installation and customization. These files are required for the Connect:Direct server to operate correctly.

Configuration File	Description
Initialization parameters file	Provides information to the server to use at start up. During the installation, you identify the settings necessary for the initialization parameters file.
User authorization information file	Contains the local user information and remote user information record types. You customize this file during installation to map remote user IDs to local user IDs and create remote user information records in the user authorization information file.
Strong access control file	Improves the security of Connect:Direct for UNIX and prevents a user from obtaining root access control. Initially, the file is empty and contains no restrictions. However, if you want to prevent the root user or any user with root permissions from gaining access to Connect:Direct for UNIX, you define a restriction parameter in this file. If the file is deleted or corrupted, access to Connect:Direct is denied to all users.
Network map file	Describes the local node and other Connect:Direct nodes in the network. You can define a remote node record for each node that Connect:Direct for UNIX communicates with.
Server authentication key file	Verifies client API connection requests. Only clients are granted a connection.
Client configuration file	Identifies the port and host name used by a client to connect to Connect:Direct.
Client authentication key file	Identifies Connect:Direct servers that a Connect:Direct node connects to. You can have multiple entries for multiple servers.

Connect:Direct for UNIX Directory Structure

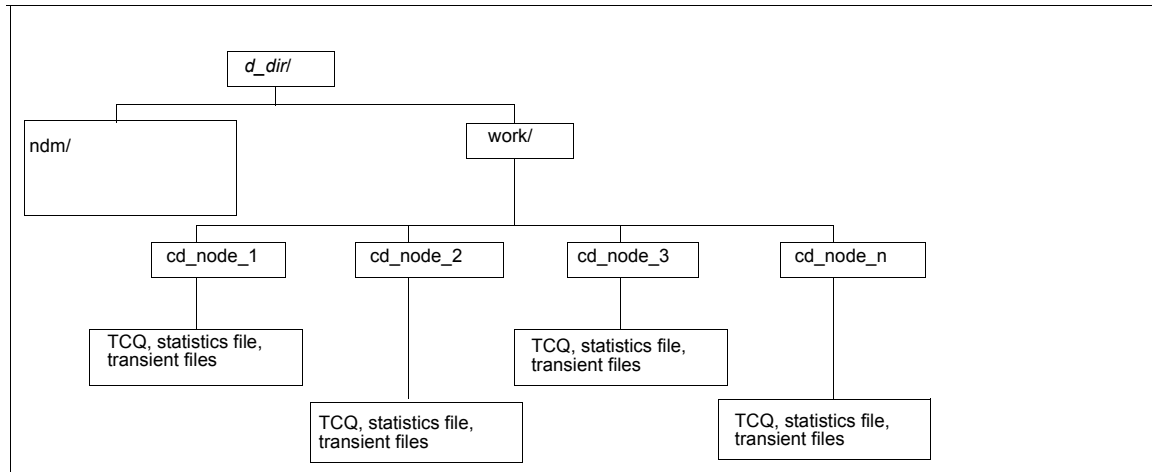
The following figure illustrates the Connect:Direct for UNIX directory structure. The directory tree starts at *d_dir/*, the destination directory where the software is installed. This directory structure provides for multiple nodes on the same network and possibly on the same computer. The directory structure organization enables you to share Connect:Direct programs, such as *cdpmgr* and *dmcmgr*. If multiple nodes exist, each node must have its own *d_dir/ndm/cfg/cd_node/* directory structure for configuration files, where *cd_node* is the Connect:Direct node name.

Note: The secure+ directory is available only when Secure+ Option is purchased.



Note: See the following figure to view the work directory for a node.

A `d_dir/work/cd_node` directory is created for each node. The following figure displays the work directory for multiple nodes and illustrates the working files created for each node, such as TCQ files:



Note: See the previous figure for details on the ndm directory structure.

Connect:Direct for UNIX Documentation

See *Connect:Direct for UNIX Release Notes* for a complete list of the product documentation.

About This Guide

The *Connect:Direct for UNIX Getting Started Guide* is for programmers and network operations staff who install Connect:Direct for UNIX. By reading this document, you gain the knowledge required to install Connect:Direct.

This guide assumes knowledge of the UNIX operating system, including its applications, network, and environment. For LU6.2 connectivity, a proficiency in configuring the SNA package to support independent LU6.2 connections is required.

Task Overview

The following table guides you to the information required to perform *Connect:Direct for UNIX* installation tasks:

Task	Reference
Understanding Connect:Direct for UNIX	Chapter 1, <i>About Connect:Direct for UNIX</i>
Installing Connect:Direct for UNIX	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Customizing Connect:Direct for UNIX	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Setting up the Connect:Direct for UNIX server	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Setting up the Connect:Direct for UNIX client	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Creating the Strong Access Control file	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Changing file permissions on session manager, process manager, command manager, and user manager programs	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Installing File Agent	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Installing Secure+ Option	Chapter 2, <i>Installing Connect:Direct for UNIX</i>
Managing files with File Agent	Chapter 3, <i>Managing Files with Connect:Direct File Agent</i>
Recording the information necessary to install and customize Connect:Direct	Appendix A, <i>Installation Worksheets</i>
Configuring an LU6.2 connection	Appendix B, <i>SNA LU6.2 Connectivity</i>
Accessing and displaying manual pages	Appendix C, <i>Connect:Direct for UNIX Manual Pages</i>

Installing Connect:Direct for UNIX

This section describes the tasks necessary to install and customize Connect:Direct for UNIX. It also describes preparations for installing Connect:Direct for UNIX in a cluster environment and on the Linux for S/390 operating system.

Before You Begin

Before you install Connect:Direct for UNIX, complete the following tasks:

- ◆ Read the *Connect:Direct for UNIX Release Notes* for any additional system requirements and upgrade considerations.
- ◆ Complete the worksheets in Appendix A, *Installation Worksheets*, to identify all information required to perform the installation.

Configuration Types

Connect:Direct for UNIX requires that you install a server and at least one client location. You can install Connect:Direct for UNIX in two different configurations:

- ◆ Install the server on a local system and the clients on remote systems
- ◆ Install the server and at least one client on a local system and the remaining clients on remote systems

Caution: Install Connect:Direct for UNIX on a local drive. Do *not* install Connect:Direct for UNIX on a Network File System (NFS) resource.

Preparing to Install Connect:Direct for UNIX in a Cluster Environment

Connect:Direct for UNIX supports clustering software to allow two or more computers to appear to other systems as a single system. All computers in the cluster are accessible through a single IP address. Connect:Direct for UNIX can be installed in two types of clustering environments: high availability and load balancing clustering environments.

High-Availability Cluster Environments

Consider the following information when planning to use Connect:Direct for UNIX in a high-availability cluster environment.

Supported High-Availability Cluster Environments

Connect:Direct for UNIX is certified to operate in the following high-availability cluster environments:

- ◆ IBM high-availability cluster multiprocessing (HACMP) environment
- ◆ Hewlett-Packard MC/Service Guard
- ◆ SunCluster versions 2.2 and 3.0

If you plan to install Connect:Direct for UNIX in a high-availability cluster environment, complete the following tasks:

- ◆ Install the clustering software on each computer in the cluster, including setting up a logical host or application package.
- ◆ Create a user with the same name and user ID on each cluster node.
- ◆ Create a Secure+ Option subdirectory on a shared file system on a shared volume group.
- ◆ Ensure that the shared file system is owned by the Connect:Direct user.
- ◆ Install Connect:Direct for UNIX on the shared file system.
- ◆ Perform the procedures necessary to define the high-availability settings and configure the cluster environment.

Limitations of High-Availability Clusters

When running Connect:Direct for UNIX in a high-availability cluster environment, be aware of the following limitations:

- ◆ If a failure occurs, all Processes being held will be restarted when Connect:Direct is restarted. This includes Processes that are held by the operator as well as Processes held in error. This could cause a security risk.
- ◆ When a Connect:Direct ndmsmgr process associated with a Connect:Direct Process is killed, the Process is not automatically restarted and is put in the Held in Error state. It must be manually restarted; otherwise, the Connect:Direct Process is restarted when the cluster restart occurs.
- ◆ On the Hewlett-Packard MC/Service Guard High Availability software, the SNMP daemon cannot be used.

Load-Balancing Cluster Environments

In a load-balancing cluster environment, an incoming session is distributed to one of the Connect:Direct for UNIX instances based on criteria defined in the load balancer. Generally, from the point of view of the nodes behind the load balancer, only incoming or SNODE sessions are affected by the load balancer. PNODE, or outgoing sessions, operate the same way as non-cluster Connect:Direct for UNIX PNODE sessions.

SNODE Server Considerations for Load-Balancing Clusters

Consider the following when planning and setting up the Connect:Direct for UNIX SNODE servers in a load balancing cluster:

- ◆ The servers used for the Connect:Direct for UNIX instances behind the load balancer must all have access to common shared disk storage because of the following:
 - ◆ Any **copy** statement source and destination files for SNODE processes must reside in directories accessible to all servers.
 - ◆ All nodes must have access to a common SNODE work area and that area must be on a cluster file system and not a Network File System (NFS) resource.
 - ◆ All servers must be of the same platform type (for example, all Solaris SPARC or all Linux Intel) and the same Connect:Direct for UNIX version and maintenance level.
- ◆ The system clocks on all servers must be synchronized in order for **copy** checkpoint/restart and **run task** synchronization to work.
- ◆ The administrator user ID used to install Connect:Direct for UNIX must be defined on each server and must be the same user and group number on each server.

Connect:Direct for UNIX SNODE Setup for Load-Balancing Clusters

Consider the following when planning and setting up the Connect:Direct for UNIX SNODEs in a load-balancing cluster:

- ◆ One Connect:Direct for UNIX node should be installed on each server behind the load balancer.
- ◆ Each node should be installed by the same user ID.
- ◆ Each node should have the same Connect:Direct for UNIX node name.
- ◆ Each node should have the same node-to-node connection listening port.
- ◆ A directory should be established for the shared SNODE work area used by the Connect:Direct for UNIX nodes behind the load balancer. This directory should be owned by the Connect:Direct for UNIX administrator ID and must be accessible to all of the servers behind the load balancer.
- ◆ Each node should specify the same path to the directory used for the shared SNODE work area. Specify this path in the **snode.work.path** parameter of the ndm.path record in the initialization parameter file.

For more information on the initialization parameters file and the **snode.work.path** parameter, see the *Connect:Direct for UNIX Administration Guide*.

Limitations of Load Balancing Clusters

When running Connect:Direct for UNIX in a cluster environment, be aware of the following limitations:

- ◆ If an incoming session fails and is restarted by the PNODE, then the restarted session may be assigned to any of the instances behind the load balancer and will not necessarily be established with the original SNODE instance.
- ◆ When shared SNODE work areas are configured and the **run task** is on the SNODE, then at restart time, Connect:Direct for UNIX cannot determine whether the original task is still active

or not because the restart session may be with a different server. If you set the global run task restart parameters to yes in the initialization parameters file, a task could be restarted even though it may be active on another machine. Therefore, exercise caution when specifying `restart=y`.

- ◆ Each SNODE instance that receives a session for a given Process creates a TCQ entry for the Process. Each SNODE instance has its own TCQ file, and these files are not shared among SNODE instances. Only the work files created in the shared work area are shared among SNODE instances.
- ◆ When a Process is interrupted and restarted to a different SNODE instance, the statistics records for that Process is distributed between the two SNODE instances involved. As a result, you cannot select all the statistics records for a Process.

Preparing to Install Connect:Direct for UNIX on the Linux for S/390 Operating System

Connect:Direct for UNIX is distributed on a CD-ROM. Because the Linux for S/390 operating system does not support the CD-ROM drive installation, you must use ftp to transfer installation files from a UNIX or Windows operating system. To transfer the files from a Windows or UNIX platform to the Linux for S/390 operating system, use the following procedure:

1. Create a temporary directory on the computer running Linux for S/390.
2. Insert the CD-ROM into the appropriate drive on the computer running Windows or UNIX and perform one of the following actions:
 - ◆ From Windows, select **Start > Programs > Accessories>Command Prompt**.
 - ◆ From UNIX, use the mount command to locate the CD-ROM drive.
3. Type the following command, where *ip address* is the IP address of the computer running Linux for S/390:

```
ftp ip address
```

4. At the prompt, type the user name and password for a user on the computer running Linux for S/390.
5. At the ftp prompt, set the transfer mode to binary by typing the following command:

```
binary
```

6. Change to the temporary directory you created on the computer running Linux for S/390 by typing the following command, where *temp_dir* is the directory you created in step 1:

```
cd temp_dir
```

7. To copy the installation script from the CD-ROM to the computer running Linux for S/390, perform one of the following actions:
 - ◆ From Windows, type the following command, where *x* is the location of the CD-ROM drive:

```
put x:\IBMS390_linux\cdinstall cdinstall
```

- ◆ From UNIX, type the following command:

```
put /cdrom/IBMS390_linux/cdinstall cdinstall
```

- To copy the Connect:Direct cpio file from the CD-ROM to the computer running Linux for S/390, perform one of the following actions:

- ◆ From Windows, type the following command, where *x* is the location of the CD-ROM drive:

```
put x:\IBMS390_linux\cdunix cdunix
```

- ◆ From UNIX, type the following command:

```
put /cdrom/IBMS390_linux/cdunix cdunix
```

- To exit the ftp application, type **quit**.

Installing Connect:Direct for UNIX

Observe the following conventions when you install Connect:Direct for UNIX:

- ◆ If a file name contains a semicolon, precede the semicolon with a backslash (\) character; otherwise, the shell interprets the semicolon as the start of a new command. For example, specify the file name SNA;1 as SNA\;1.
- ◆ Acceptable responses to prompts are listed in brackets, where **y** specifies yes, **n** specifies no, and **a** specifies all.
- ◆ The default response is capitalized. Press **Enter** to accept the default value.
- ◆ Do not use colons (:) for values in the installation and customization scripts.
- ◆ Do not use keywords for values.
- ◆ Press **Enter** after each entry to continue.
- ◆ Terminate any procedure by pressing **Control-C**.

To install Connect:Direct for UNIX:

- Log on to the UNIX system with the privileges required to install software. You can create an account specifically for this purpose.

Caution: Do not install as root.

2. You are prompted for the path and filename of the installation files. Depending upon how you obtained the product, take one of the following actions:
 - ◆ If you have the product distribution media, select the CD for your platform. Type the following command and press **Enter** to change to the CD-ROM drive and the directory that correspond to the UNIX platform:

```
cd /cdrom/<platform directory>
```

Refer to the following table for the name of the platform directory for each platform.

UNIX Platform	Platform Directory Path
HP 9000 series	HP_PA-RISC
HP UX Itanium	HP_Itanium
IBM System p5	IBM
Sun SPARC systems	Sun_Solaris
Red Hat	RedHat_linux
SuSE	SuSE_linux
HP/Alpha Tru64 UNIX	HP_Tr64
Linux zSeries	IBMS390_linux
Solaris/x86	Solaris_x86

- ◆ If you downloaded the product from the ESD Portal, type the following command and press **Enter** to change to the location of the product download:

```
cd /<location of product download>
```

3. Type the following command to invoke the installation script and press **Enter**:

```
cdinstall
```

The following screen is displayed:

```

=====
Sterling Commerce, Inc., (TM) Connect:Direct(TM) for UNIX(TM)
Installation Procedure

You are beginning the Connect:Direct for UNIX Installation
Procedure.  You will be asked to specify a directory (called
the destination directory) where the Connect:Direct for UNIX
files will be stored.

Please follow the Getting Started Guide and/or Release Notes for the
proper Media Name.

Sterling Commerce, Inc. (TM) and Connect:Direct(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

UNIX is a registered trademark of The Open Group
=====

Press ENTER when ready.

```

4. Read the information and press **Enter**. The following screen is displayed:

```

Enter the FULL path of the directory where
Connect:Direct for UNIX 3.8.00 will be installed.
You can use $HOME to shorten the name:[$HOME/cdunix]

```

5. Type the path name of the directory where Connect:Direct for UNIX will be installed and press **Enter**.
6. When you are prompted to confirm the installation location, press **Enter**. The following screen is displayed:

Note: The option for installing Connect:Direct for UNIX SNMP Agent will not display for platforms where this option is not supported.

```

Please select one of the following installation options:

(1) Connect:Direct for UNIX server and client (CLI/API)
(2) Connect:Direct for UNIX server
(3) Connect:Direct for UNIX client (CLI/API)
(4) Connect:Direct for UNIX File Agent
(5) Connect:Direct Secure+ Option for UNIX
(6) Connect:Direct for UNIX SNMP Agent
(7) EXIT

Enter your choice:[1]

```

7. Do one of the following:
 - ◆ Type **1** to install the server and client on the same computer and press **Enter**.
 - ◆ Type **2** to install the server only and press **Enter**.
 - ◆ Type **3** to install the client only and press **Enter**.

The following screen is displayed:

```
Enter the path "AND filename" where the installation file is mounted or
where the ESD portal download is extracted (e.g. /cdrom/HP_PA-RISC/cdunix):
```

8. Type the location of the installation file and press **Enter**.

If you select **1** in step 7 to install the server and client, the following screen is displayed. If you select option **2** or **3**, the screen displays the software that will be installed.

```
Both Connect:Direct for UNIX Server and client (CLI/API) Version 3800
will be installed in your system. Do you want to continue?:[Y/n]
```

9. Press **Enter** to continue.

If the destination directory does not have enough free disk space, the script suggests you delete enough files to provide the necessary disk space and then exits.

If sufficient disk space is available, the installation script copies files from the distribution media to the destination directory and verifies that the correct number of files and blocks are copied.

The customization script starts automatically when the installation is complete.

Customizing Connect:Direct for UNIX

The customization script starts automatically after the installation is complete. It sets up the Connect:Direct for UNIX operating environment. It is located in *d_dir/etc/cdcust*, where *d_dir* is the Connect:Direct installation directory, and may be run by itself if needed for future configuration changes. The option you select determines what Connect:Direct for UNIX operating environment is configured: the Connect:Direct for UNIX server only, the Connect:Direct for UNIX client only, or the Connect:Direct for UNIX server and client.

After you customize the environment, you will be returned to the customization option selection screen. You will need to exit the customization script before you perform the following customization procedures:

- ◆ Create the SACL (Strong Access Control List).
- ◆ Set owner and permissions of Connect:Direct executables.

After you exit the customization script, launch *cdcust* using *sudo* to become root before creating the SACL and setting the owner and permissions of the Connect:Direct for UNIX executables.

Note: You must create the SACL file and set the owner and permissions to run Connect:Direct for UNIX.

The customization script displays the following message and prompts you to continue the customization procedure. Complete the following steps to customize Connect:Direct for UNIX:

```

=====
Sterling Commerce Connect:Direct for UNIX Customization

The customization procedure sets up the Connect:Direct for UNIX
operating environment. In the following, please answer questions
when prompted and when in doubt, enter (?) followed by the ENTER
key for help. To abort the process, enter Control-C.

As a short hand, entering ENTER at the prompt means "yes", or
the default value, if any, will be taken.
=====

Press ENTER when ready.

```

1. Read the information and press **Enter**. Complete the following steps to customize Connect:Direct for UNIX:

```

The customization procedure allows you to create configuration
files for:

(1) Configure the Connect:Direct for UNIX server.
(2) Configure the Connect:Direct for UNIX client.
(3) Configure the Connect:Direct for UNIX server and client.
(4) Create the SACL (Strong Access Control List).
(5) Set owner and permissions of Connect:Direct executables.
(6) EXIT.

Enter your choice:[3]

```

2. Do one of the following:

Note: Be sure to select the same configuration you selected during the installation in step 7 on page 30.

- ◆ Type **3** to customize the server and client on the same computer and press **Enter**.
If you are installing the Connect:Direct for UNIX server only, complete the procedures in the next section, *Setting Up the Connect:Direct for UNIX Server* on page 32.
- ◆ Type **2** to customize the client only and press **Enter**.
If you are installing the client only, complete the procedure *Setting Up the Connect:Direct for UNIX Client* on page 36.
- ◆ Type **1** to customize the server only and press **Enter**.
If you are installing both the client and the server, complete all of the procedures in *Setting Up the Connect:Direct for UNIX Server* on page 32 and *Setting Up the Connect:Direct for UNIX Client* on page 36.

Setting Up the Connect:Direct for UNIX Server

After you install and customize Connect:Direct for UNIX, you need to define the parameters needed by the server for start up. If you installed the server software, the process to set up the server starts automatically.

To set up the server, perform the following tasks:

- ◆ Define your node name.
- ◆ Define SNA settings, if applicable.
- ◆ Define the initialization parameters file.
- ◆ Define the network map file.
- ◆ Define the user authorization information file.

Defining the Connect:Direct Node Name

If you selected option 1 or 3 in step 2 of *Customizing Connect:Direct for UNIX* on page 30, the following screen is displayed:

```
Please enter name of Connect:Direct node you want to customize: hpnode
Index file has been created for: [/sci/users/qatest/cd3800/ndm/cfg/msgfile.cfg]
```

Type the name of the node, up to 16 characters, that you want to customize and press **Enter**. The following screen is displayed:

Defining the Initialization Parameters File

Connect:Direct processes initialization parameters during startup. Some parameters identify files that provide information to the server. If you selected option 1 to install only the server or option 3 to install the both the server and client, the following screen is displayed:

```
If you purchased SNA support for Connect:Direct and SNA is properly installed
on your system, do you want to add the appropriate SNA entry
to your initparm file?:[Y/n]
```

1. If you purchased SNA support and have SNA configured on your system, press **Enter** to configure SNA in the Connect:Direct initialization parameters file. If you do not use SNA, type **n** and press **Enter** to continue customizing Connect:Direct for UNIX.

The following screen is displayed:

```
Enter TCP/IP port to listen for a remote connection request:[1364]
```

2. Type the TCP/IP port number that Connect:Direct monitors for requests from remote nodes. If available, use the default port, 1364. If the default port number is being used by another service, use any other available port.

This value is entered into the initialization parameters file as the **comm.info** parameter.

The following screen is displayed:

```
Enter TCP/IP port to listen for a client connection request:[1363]
```

3. Type the TCP/IP port number that Connect:Direct monitors for requests from clients. If available, use the default value of **1363**. If the default port number is being used by another service, use any other available port.

This value is entered into the network map file as the **tcp.api** parameter. Connect:Direct creates the network map file and displays the directory path and file name.

Defining the Network Map File

After you define the initialization parameters file, the customization script creates the network map file and displays the directory path and file name. Connect:Direct adds a remote node record to the network map file. The remote node record is assigned the name of the local node you specified in *Defining the Connect:Direct Node Name* on page 32.

Note: For information on adding remote node records for other nodes, refer to Chapter 2, *Maintaining Configuration Files*, in the *Connect:Direct for UNIX Administration Guide*.

The initialization parameters file and the network map file are created and the path and file name for each file is displayed:

```
=====
A initparm file has been created. This initparm file consists of
initialization parameter records used by Connect:Direct during
startup. To modify the initparm file, please refer to the
"Maintaining the Initialization Parameter File" chapter
in the Administration Guide for details.

Initparm file is located at
/sci/users/servername/cdunix/ndm/cfg/hpnode/initparm.cfg
=====

=====
A netmap file has been created. This netmap file contains a
network definition for the installed Connect:Direct node. To
add network definitions for other nodes, please refer to the
"Maintaining the Network Map File" chapter in the Administration
Guide for details.

Netmap file is located at
/sci/users/servername/cdunix/ndm/cfg/hpnode/netmap.cfg.
=====
Press Enter when ready.
```

Press **Enter** to continue. The user authorization information file is automatically created.

Customizing the User Authorization Information File

After the user authorization information file is created, you are ready to customize the file. Use this procedure to map remote user IDs to local user IDs and create remote user information records in the user authorization information file.

After the user authorization information file is created, the following screen is displayed:

```

=====
User Authorization file has two types of records: local user
record and remote user record. Refer to the
"Maintaining the User Authorization Information File" chapter in the Administration
Guide for details.

User Authorization file is located at
/sci/users/servername/cdunix/ndm/cfg/hpnode/userfile.cfg
=====

```

The following screen is displayed to prompt you to create an authorization information record for a remote user:

```

Insert remote user record? [Y/n]

```

1. Press **Enter** to add a remote user record. The following screen is displayed:

```

Enter remote userid:

```

2. Type the login name or ID of the remote user and press **Enter**. The following screen is displayed:

```

Enter remote Connect:Direct node name:

```

3. Type the name of the remote node and press **Enter**. The submitter ID and remote node name become the record name for the remote user information record. The following screen is displayed:

```

Enter local userid:

```

4. Type the local user ID to which the remote user ID will be mapped and press **Enter**. The local user ID is the UNIX account name. This value is associated with **local.id** in the remote user information record and defines the local user ID used to check security for the remote user. The following screen is displayed:

```

Insert another remote user record?:[Y/n]

```

5. Do one of the following:
 - ◆ To create another remote user record, press **Enter** and repeat steps 2-4.
 - ◆ Type **n** and press **Enter** if you do not want to create another remote user record.

The following screen is displayed:

```
Insert local user record?: [Y/n]
```

6. Do one of the following:
 - ◆ If you do not want to create a local user record, type **n** and press **Enter**. Go to *Connect:Direct Creates an Authentication Key File* on page 36 to continue configuring Connect:Direct for UNIX.
 - ◆ To create a local user record, press **Enter**.

The following screen is displayed:

```
Enter userid:
```

7. Type the user ID for the local user and press **Enter**. This value is associated with **userid** in the user authorization information file. The following screen is displayed:

```
Grant administrative authority:[Y/n]
```

8. Press **Enter** to grant administrative authority to the local user ID. All Connect:Direct capabilities that you specify in the local user information record are assigned to the user. This value is assigned to **admin.auth** in the local user information record.

The following screen is displayed:

```
Insert another local user record? [Y/n]
```

9. Do one of the following:
 - ◆ Press **Enter** and repeat this procedure to create another local user record.
 - ◆ Type **n** and press **Enter** to continue to the next task.

Connect:Direct Creates an Authentication Key File

A server authentication key file verifies connection requests. Only authorized clients are granted a connection. Connect:Direct generates the server authentication key file automatically. After the file is generated, Connect:Direct displays the following message:

```
A server authentication key file has been created. The default
key is CD4UNIX. Please refer to the "Maintaining Client
and Server Authentication" chapter in the Administration Guide
for details.
=====
Press Enter when ready.
```

Press **Enter** to continue.

Setting Up the Connect:Direct for UNIX Client

After you install and customize Connect:Direct for UNIX, you need to define the parameters needed by the client for startup. To set up the client, perform the following tasks:

- ◆ Customize the client configuration file
- ◆ Customize the client authentication key file

Customizing the Client Configuration File

The client configuration file is automatically created during the customization process. Use the following procedure to customize the client configuration file. After the client configuration file is created, the following screen is displayed:

```
=====

          Configuring Connect:Direct for UNIX client

=====

The client configuration file defines connection information
to the Connect:Direct server. A network-wide configuration file
with records defining connection information for different
servers can be set up. Please refer to the "Modifying
the Client Configuration File" chapter in the Administration
Guide for details.

The client configuration is located at
/sci/users/servername/cdunix/ndm/cfg/cliapi/ndmapi.cfg.
=====

Enter port of the Connect:Direct server this client will connect to:[1363]
```

1. Type the port number of the server that the client connects to and press **Enter** when ready.

This value is associated with **tcp.port** in the client configuration file. The following screen is displayed:

2. Press **Enter** to accept the port number entered.

```
Enter hostname of the Connect:Direct server this client will connect to:[hpnode]
```

3. Press **Enter** to accept the host name.

This value is displayed in the **tcp.hostname** parameter in the client configuration file.

Customizing the Client Authentication Key File

The client authentication key file identifies all Connect:Direct servers that this Connect:Direct node connects to. This file is automatically generated during customization. After the file is generated, the following message is displayed:

```
A client authentication key file has been created. The default
key is CD4UNIX. Please refer to the "Maintaining Client
and Server Authentication" chapter in the Administration Guide
for details.
```

Press **Enter** to continue.

Creating a Strong Access Control List File

Creating a SACL file improves the security of Connect:Direct for UNIX and prevents a user from obtaining root access control.

After you customize the environment, you will be returned to the customization option selection screen. You will need to exit the customization script before create the SACL (Strong Access Control List).

After you exit the customization script, launch cdcust (located in `<product install directory>/etc/cdcust`) using sudo to become root before creating the SACL.

Note: You must create the SACL file to run Connect:Direct for UNIX.

Use the following procedure to customize the SACL file. After the SACL file is created, the following screen is displayed.

```
The customization procedure allows you to create configuration
files for:

(1) Configure the Connect:Direct UNIX server.
(2) Configure the Connect:Direct UNIX client.
(3) Configure the Connect:Direct UNIX server and client.
(4) Create the SACL (Strong Access Control List).
(5) Set owner and permissions of Connect:Direct executables.
(6) EXIT.

Enter your choice:[3]
```

1. Type **4** and press **Enter**.
2. To create a new SACL file, type **Y** and press **Enter**. The following message is displayed:

```
=====
                Configuring Connect:Direct for UNIX SACL
=====

WARNING: Connect:Direct for UNIX, by default, will deny proxy to root

This option requires root password. Continue?:[Y/n]

Please enter the root password at the following prompt.
Password:
```

3. Type your password and press **Enter**.
If you type the root password incorrectly, a message informs you that the SACL file was not properly configured. Otherwise, a SACL file is created and you are returned to the Customization menu.

Note: You must successfully create a SACL file to operate Connect:Direct for UNIX.

4. Press **Enter** to continue.

Changing File Ownership and Permissions

After you customize the environment, you will be returned to the customization option selection screen. You will need to exit the customization script before you set owner and permissions of Connect:Direct executables.

After you exit the customization script, launch cdcust (located in /<product install directory>/etc/cdcust) using sudo to become root before setting the owner and permissions of the Connect:Direct for UNIX executables.

Note: You must set the owner and permissions to run Connect:Direct for UNIX.

You must change the file attributes of the Session Manager (`d_dir/ndm/bin/ndmsmgr`), Process Manager (`d_dir/ndm/bin/cdpmgr`), Command Manager (`d_dir/ndm/bin/ndmcmgr`) User Manager (`d_dir/ndm/bin/ndmumgr`), Statistics Manager (`d_dir/ndm/bin/cdstatm`), Client Authenticator (`d_dir/ndm/bin/ndmauthc`), Server Authenticator (`d_dir/ndm/bin/ndmauths`), and `hostid.sh` utility program on Linux Intel (`d_dir/ndm/bin/cd_hostid`).

The file attributes are automatically changed during the customization process. Use the following procedure to change file ownership. The following dialog box is displayed:

```
The customization procedure allows you to create configuration
files for:

(1) Configure the Connect:Direct UNIX server.
(2) Configure the Connect:Direct UNIX client.
(3) Configure the Connect:Direct UNIX server and client.
(4) Create the SACL (Strong Access Control List).
(5) Set owner and permissions of Connect:Direct executables.
(6) EXIT.

Enter your choice:[3]
```

1. Type **5** and press **Enter**. The following message is displayed:

```
This option requires root password. Continue? [Y/n]
```

2. Press **Enter** to continue.
3. Type the root password and press **Enter**.

If you type the root password incorrectly, a message informs you that the permissions of the files were not properly configured. Otherwise, the permissions on the files have been changed.

Note: You must successfully change the permissions of Session Manager, Process Manager, Command Manager, User Manager, and Statistics Manager to operate Connect:Direct for UNIX.

4. Press **Enter** to continue.
5. Type **6** to exit the Connect:Direct for UNIX customization script. Connect:Direct generates the `sample.cd` file for the purpose of testing the installation. After this file is generated, the following message is displayed:

```

=====
A sample pnode equal to snode process has been created
to test the Connect:Direct for UNIX installation. It is
located at /data/cdtest/ndm/bin/sample.cd.
More example processes can be found in sub-directory
/data/cdtest/ndm/src.
=====
Connect:Direct for UNIX configuration completed.
Before starting Connect:Direct for UNIX, please
set the environment variable NDMAPICFG to point to the
client configuration file. Please refer to the "Installing
Connect:Direct for UNIX" chapter in the Getting Started Guide
for details.
Thank you for using Connect:Direct for UNIX.
=====
Would you like to return to the installation menu?:[Y/n]

```

6. Do one of the following:

- ◆ If you want to install File Agent, press **Enter**. Continue with *Installing File Agent* on page 41.
- ◆ To exit the customization without installing File Agent, type **n** and press **Enter**.

The following parameters were modified during the customization:

Parameter	Value	File
SNAFILE=/ndm/lib/libcdsna.s	Defines SunLink as the SNA software	Initialization parameters file
BRXSNAFILE=/ndm/lib/libcdbrxsna.s	Defines Brixton as the SNA software	Initialization parameters file
SNPSNAFILE=/ndm/lib/libcdsnpsna.so	Defines SNAP-IX as the SNA software	Initialization parameters file
comm.info=1364	Identifies the TCP/IP port number that Connect:Direct monitors for requests from remote nodes	Initialization parameters file
tcp.api	Identifies the port monitored by Connect:Direct for requests from clients	Initialization parameters file
rnode.listen	Identifies the host used to monitor for connections when using LU6.2	Initialization parameters file
admin.auth	Determines if user ID user has administrative authority	User authorization information file
tcp.port	Specifies port number of the server that the client connects to	Client configuration file
tcp.hostname	Specifies host name of the server that the client connects to	Client configuration file

Installing File Agent

You may continue with the File Agent installation after completing the Connect:Direct for UNIX installation or you can complete this installation at any time. Complete the following steps to install File Agent.

Note: If you are installing File Agent on the HP Integrity system with Itanium processor, Compaq Tru64, or Linux zSeries, you must download the Java 1.4 software from the manufacturer's Web site before continuing the installation.

1. Do one of the following:

- ◆ If this is a stand-alone installation, type `cdinstall`.
- ◆ If you are installing File Agent after the Connect:Direct for UNIX installation, select `y` to return to the installation menu.

The following installation options menu is displayed:

```

Please select one of the following installation options:

(1) Connect:Direct for UNIX server and client (CLI/API)
(2) Connect:Direct for UNIX server
(3) Connect:Direct for UNIX client (CLI/API)
(4) Connect:Direct for UNIX File Agent
(5) Connect:Direct Secure+ Option for UNIX
(6) Connect:Direct for UNIX SNMP Agent
(7) EXIT

Enter your choice:[1]

```

2. Select **4** and press **Enter**. The following message is displayed:

```

Connect:Direct UNIX File Agent will be installed in your system. Do you want to
continue?:[Y/n] y

```

3. Press **Enter** to continue.

4. If you are installing File Agent as a stand-alone installation, perform the following actions:

- a. Type the path name of the destination directory where you want to install Connect:Direct File Agent or press **Enter** to use the suggested directory. The following screen is displayed:

```

You have chosen /sci/users/servername/file_agent
as destination directory. Please confirm it:[Y/n]

```

- b. Press **Enter** if the destination directory is correct.

After the File Agent files are extracted, the following message is displayed.

```
Would you like to return to the installation menu?:[Y/n] n
```

5. Type **n** and press **Enter** to exit the installation.

Installing Secure+ Option

You can continue with the Secure+ Option installation after completing the Connect:Direct for UNIX installation or you can complete this installation at any time after installing the Connect:Direct for UNIX.

Note: If you already have Secure+ Option installed, when you are prompted to upgrade your installation, type **y**.

Complete the following steps to install the Secure+ Option:

Note: If you have completed the server installation and are still in the installation program, return to the main installation menu and begin with step 8.

1. Log on to the UNIX system with the privileges required to install software. You can create an account specifically for this purpose.

Caution: Do not install as root.

2. You are prompted for the path to the installation files. Depending upon how you obtained the product, take one of the following actions:
 - ◆ If you have the distribution media, select the CD for your platform. Type the following command and press **Enter** to change to the CD-ROM drive and the directory that correspond to the UNIX platform:

```
cd /cdrom/<platform directory>/cdunix
```

Refer to the following table for the name of the platform directory for each platform.

UNIX Platform	Platform Directory Path
HP 9000 series	HP_PA-RISC

UNIX Platform	Platform Directory Path
HP UX Itanium	HP_Itanium
IBM System p5	IBM
Sun SPARC systems	Sun_Solaris
Red Hat	RedHat_linux
SuSE	SuSE_linux
HP/Alpha Tru64 UNIX	HP_Tru64
Linux zSeries	IBMS390_linux
Solaris/x86	Solaris_x86

- ◆ If you downloaded the product from the ESD Portal, type the following command and press **Enter** to change to the location of the product download:

```
cd /<location of product download>/cdunix
```

3. Type the following command to invoke the installation script and press **Enter**:

```
cdinstall
```

The following screen is displayed:

```

Sterling Commerce, Inc., (TM) Connect:Direct(TM) for UNIX(TM)
Installation Procedure

You are beginning the Connect:Direct for UNIX Installation
Procedure. You will be asked to specify a directory (called
the destination directory) where the Connect:Direct for UNIX
files will be stored.

Please follow the Getting Started Guide and/or Release Notes for the
proper Media Name.

Sterling Commerce, Inc.(TM) and Connect:Direct(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

UNIX is a registered trademark of The Open Group
=====

Press ENTER when ready.
```

4. Read the information and press **Enter**. The following screen is displayed:

```

Enter the FULL path of the directory where
Connect:Direct for UNIX 3.8.00 will be installed.
You can use $HOME to shorten the name:[$HOME/cdunix]
```

5. Type the path and press **Enter**.

```
WARNING: "<directory path>" : Directory exists
Files in <directory path> could be overwritten by the
installation. Do you want to continue: [Y/n]
```

6. Press **Enter** to continue. The following screen is displayed:

```
Installed components detected in this directory.

A previous version of C:D for UNIX was detected.

Would you like this procedure to detect and upgrade your currently installed
options with minimal interaction?
If yes, the configuration files will be left in place and reused.
If not, the full installation procedure will prompt to either reuse, or purge
and rebuild, each configuration file.

Caution: If you are upgrading from C:D for UNIX versions 3.4 or 3.5 that are on a
maintenance level prior to December 2004, then any existing Processes
in the TCQ will need to be deleted and resubmitted.

Type y or press Enter to continue with the upgrade procedure, or
type n to run the full installation procedure:[Y/n]
```

7. Type **n** and press **Enter** to run the full installation procedure. The following screen is displayed:

```
Connect:Direct for UNIX installation directory specified:
[directory path]

Please select one of the following installation options:

(1) Connect:Direct for UNIX server and client(CLI/API)
(2) Connect:Direct for UNIX server
(3) Connect:Direct for UNIX client(CLI/API)
(4) Connect:Direct for UNIX File Agent
(5) Connect:Direct Secure+ Option for UNIX
(6) Connect:Direct for UNIX SNMP Agent
(7) EXIT

Enter your choice:[1]
```

8. Type **5** and press **Enter**. The following screen is displayed:

```
Enter the path "AND filename" where the installation file is mounted or
where the ESD portal download is extracted (e.g. /cdrom/IBM/cdunix):
```

9. Type the full Connect:Direct UNIX installation path and filename and press **Enter**. You are prompted to confirm the installation path.

```
Connect:Direct Secure+ Option for UNIX 3.8.00 will be
installed on your system. Do you want to continue?:[Y/n]
```

10. Press **Enter** to continue. The program determines if enough free space exists to complete the operation.
- ◆ If sufficient space is available, the Secure+ installation script and cpio files are extracted.
 - ◆ If the space is insufficient, the program suggests that you delete enough files to provide the necessary disk space and then exits. After you have cleared enough space, restart the installation procedure.

After the files are extracted, the following screen is displayed:

```

Sterling Commerce, Inc., (TM) Connect:Direct(TM) Secure+ Option
for UNIX(TM) Installation Procedure

You are beginning the Connect:Direct Secure+ Option for UNIX Installation
Procedure. You will be asked to specify a directory (called
the destination directory) where the Connect:Direct for UNIX
files are stored. The Secure+ Module will be installed in this
same directory where Connect:Direct is installed.

Sterling Commerce, Inc.(TM) and Connect:Direct(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

UNIX is a registered trademark of The Open Group

Press ENTER when ready.

```

11. Read the screen and press **Enter**. The following screen is displayed:

```

You have selected <installation directory> for installation. Do you want to
continue?:[Y/n]

```

12. Press **Enter** to continue. A message is displayed regarding the amount of disk space required to install Secure+ Option for your platform, and then the installation program determines if sufficient space exists:
- ◆ If sufficient space is available, you are prompted to continue the installation, press Enter to continue.
 - ◆ If the space is insufficient, the script suggests that you delete enough files to provide the necessary disk space and then exits. After you have cleared enough space, restart the installation procedure.
13. A screen is displayed as the files are extracted from the media and the JRE is configured. When the installation is complete, the following screen is displayed:

```

Would you like to return to the installation menu?:[Y/n]

```

Configuring SNA Support for Connect:Direct for UNIX

For LU6.2 connectivity, you must configure SNA support. Refer to Appendix B, *SNA LU6.2 Connectivity* for instructions on modifying both the initialization parameters and network map files.

Defining High-Availability Settings in the Configuration Files

After you install Connect:Direct for UNIX on a shared file system, you must modify some of the Connect:Direct for UNIX parameters to support a clustering environment. Complete the following procedure to modify the configuration files for a cluster environment:

Note: You must install Connect:Direct for UNIX on a shared cluster file system to use it in a cluster environment.

1. Modify the following parameters:
 - ◆ In the initialization parameters file (`initparm.cfg`), set `:comm.info=0.0.0.0;nnnn:\` where `nnnn` is the number of the listening port you defined during installation.
 - ◆ In the `api.parms` record of the NDMAPI configuration file (`ndmapi.cfg`), set `:tcp.hostname=logical_host_ip_name:\`
 - ◆ In the network map file (`netmap.cfg`), set `:tcp.api=logical_host_ip_name;nnnn:\` where `nnnn` is the API port you defined during installation.
2. In the network map file (`netmap.cfg`), set the outgoing address parameter in the `local.node` record to specify the local host IP name or address of the floating address to the following value. The remote node will also use this value for network map checking.

```
:outgoing.address=(host name |nnnnnn.nnn):\
```

3. Modify the following records in the network map file:
 - ◆ Set `:comm.info=logical_host_ip_name;1364:\` to configure the loopback remote node record.
 - ◆ Set `tcp.max.time.to.wait` to a value other than zero and less than the value set in the resource group manager of the cluster software to allow for clean shutdowns.
4. Acquire an asset protection key that includes the CPUs of all computers in the cluster.
5. In the same volume group as the installation file system, create a user data file system that is shared by all cluster nodes.

Additional Configuration Requirements in a SunCluster 3.0 Environment

In addition to modifying the configuration files, complete the following procedure to set up a SunCluster 3.0 cluster:

1. Type the following command to create the cluster resource:

```
scdscreate -V SCI -T cd
```

Use the *V* parameter to define the vendor ID and *T* parameter to define the resource ID.

2. Type the following command to configure the custom resource scripts:

```
scdsconfig
```

3. Edit the SCI.cd resource file and change the value of RT_BASEDIR as follows:

```
RT_BASEDIR=/opt/SCIcd/bin;
RT_BASEDIR=/global/vol1/sci/cduserk1/3.5.00/suncluster+scripts/SCIcd/bin;
```

Additional Configuration Requirements in a SunCluster 2.2 Environment

In addition to modifying the configuration files, complete the following steps to complete the SunCluster 2.2 setup:

1. Place the following sample scripts and configuration files in a directory that is available to SunCluster 2.2 software:
 - ◆ cd_start.sh
 - ◆ cd_stop.sh
2. Update the scripts as required for your environment.
3. Copy the sample scripts to all nodes in the cluster.
4. Issue the **hareg** command to register the Connect:Direct data service. Refer to the SunCluster documentation for more information. Following is a sample command:

```
hareg -r cd \
  -b /control/scripts/directory \
  -m START_NET=cd_start_net.sh \
  -m STOP_NET=cd_stop_net.sh \
  -m ABORT_NET=cd_abort_net.sh \
  -m START=cd_start.sh \
  -m STOP=cd_stop.sh \
  -m ABORT=cd_abort.sh \
  -t START_NET=60 \
  -t STOP_NET=60 \
  -t START=30 \
  -t STOP=30 \
  -h logicalhost \
  -v 3.3.02
```

5. Complete the following steps if the Connect:Direct for UNIX SNMP Agent is installed on your system:
 - a. Copy `/etc/srconf/agt` to `d_dir/srconf/agt`.
 - b. Copy `/etc/srconf/mgr` to `d_dir/srconf/mgr`.
 - c. Ensure that the following environment variables are defined in the user's profile:
 - `SR_AGT_CONF_DIR=d_dir/srconf/agt`
 - `SR_MGR_CONF_DIR=d_dir/srconf/mgr`
 - d. If the SUN master SNMP agent is activated and in use by another application and is using the default ports of 1361 and 1362, add the following environment variables to the user's profile:
 - `SR_SNMP_TEST_PORT=1361` (or other available port)
 - `SR_TRAP_TEST_PORT=1362` (or other available port)

Additional Configuration Requirements for IBM HACMP

In addition to modifying the configuration files, complete the following steps to complete the IBM high-availability cluster multiprocessing (HACMP) setup:

1. Place the following sample scripts and configuration files in a directory that is available to the IBM HACMP software:
 - ◆ `cd_start_net.sh`
 - ◆ `cd_stop_net.sh`
2. Update the scripts as required for your environment.
3. Copy the sample scripts to all nodes in the cluster.
4. Complete the following steps if the Connect:Direct for UNIX SNMP Agent is installed on your system:
 - a. Copy `/etc/srconf/agt` to `d_dir/srconf/agt`.
 - b. Copy `/etc/srconf/mgr` to `d_dir/srconf/mgr`.
 - c. Ensure that the following environment variables are defined in the user's profile:
 - `SR_AGT_CONF_DIR=d_dir/srconf/agt`
 - `SR_MGR_CONF_DIR=d_dir/srconf/mgr`
 - d. Configure the SNMP agent to use ports other than the default ports of 1361 and 1362.
 - e. Add the following environment variables to the user's profile:
 - `SR_SNMP_TEST_PORT=1361` (or other available port)
 - `SR_TRAP_TEST_PORT=1362` (or other available port)

Additional Configuration Requirements for Hewlett-Packard MC/ServiceGuard

The HP Solutions Competency Center (SCC) has successfully integrated Connect:Direct for UNIX with MC/Service Guard. The implementation and certification of Connect:Direct for UNIX followed the SCC's high availability Implementation and Certification Process. Refer to the *Implementation and Certification With Hewlett-Packard's MC/ServiceGuard High Availability Software* document located under downloads on the Support on Demand Web site.

Verifying the Installation

After you complete the installation, perform the following steps to verify the installation:

1. Type the following command to identify the release and platform operating system release for Connect:Direct, where *d_dir* is the destination directory and *binaryx* is a file in the bin/ directory (for example, **cdpmgr**):

```
% d_dir/etc/cdver d_dir/ndm/bin/[binary1 binary2 ...]
```

2. Log in with the user account under which Connect:Direct was installed.
3. Type the following command, where *d_dir* is the destination directory and *cd_node* is the Connect:Direct node name.

```
$ d_dir/ndm/bin/cdpmgr -i d_dir/ndm/cfg/cd_node/initparm.cfg
```

4. Do the following to set the environment variable NDMAPICFG to point to the client configuration file:
 - ◆ If you are using the Bourne or Korn shell, type the following command:

```
$ NDMAPICFG=d_dir/ndm/cfg/cliapi/ndmapi.cfg  
$ export NDMAPICFG
```

- ◆ If you are using the C shell, type the following command:

```
% setenv NDMAPICFG d_dir/ndm/cfg/cliapi/ndmapi.cfg
```

5. Type the following command to invoke the Connect:Direct client:

```
$ d_dir/ndm/bin/direct
```

6. Type the following command:

```
Direct> select statistics;
```

Read the statistics information and ensure that the initialization started with no errors. If any errors are displayed, resolve the errors before continuing.

7. Type the following command to submit a sample Process:

```
Direct> submit file=d_dir/ndm/bin/sample.cd;
```

This sample Process copies a binary file named msgfile.cfg to the file cddelete.me in your HOME directory (your node is both the PNODE and the SNODE). The checkpointing interval is set to 2M and extended compression is used.

8. Type the following **select process** command to monitor data transmission activity:

```
Direct> select process pnumber=1;
```

Connect:Direct generates a report with the Process name and number, user, submitter node, queue, and status.

9. After the Process is complete, type the following **select statistics** command to review the statistics log for the Process:

```
Direct> select statistics pnumber=1;
```

10. Do one of the following:

- ◆ Type the following command to manually shut down the Connect:Direct server:

```
Direct> stop;
```

- ◆ When running Connect:Direct for UNIX with the LU6.2 feature on HP SNA, NCR SNA, Brixton SNA, or SunLink SNA, type the following command to stop Connect:Direct:

```
Direct> stop force;
```

- ◆ Type the following command to quit the Connect:Direct client without shutting down the server:

```
Direct> quit;
```

The client terminates automatically when you stop the server.

Refer to the *Connect:Direct for UNIX User's Guide* for syntax and parameters.

Managing Files with Connect:Direct File Agent

Connect:Direct File Agent is a component of Connect:Direct that provides unattended file management. Before using Connect:Direct File Agent, you must plan how to configure it to automate file management for your site. After planning what you need to accomplish, configure File Agent to connect to a Connect:Direct server, watch the directories that files of interest will be added to, and submit a specified Connect:Direct Process to the server when a file is detected.

Connect:Direct File Agent

Connect:Direct File Agent provides monitoring and detection capabilities that enhance the automation you accomplish with Connect:Direct Processes. You cannot create Processes with File Agent; however, File Agent variables can be used to pass arguments to a Process. File Agent does not delete, copy, or move files directly, but it helps you accomplish such tasks by submitting the Process you specify in the configuration to the Connect:Direct server. Before you specify a Connect:Direct Process in the File Agent configuration, you must create and test the Processes to ensure that it performs tasks as expected when File Agent submits the Process.

Using the File Agent configuration interface and Help system, you define the *default configuration file* (Default_Config.ser). The default configuration file defines the Connect:Direct server that Connect:Direct File Agent communicates with; the directory, or directories, that File Agent monitors; and how a file added to a watched directory or a detected system event are processed.

You can configure Connect:Direct File Agent to operate in either of the following ways:

- ◆ Watch for any file to appear in one or more *watched* directories and submit the default Process after detecting the newly added file.
- ◆ Override the default Process specified and apply either *watched file event* rules (Submit Process rule) or *system event* rules that is enabled for the configuration. File Agent applies a *watched file event* rule to a detected file by checking file properties to determine whether criteria specified by the rule are met. A *system event* rule checks whether a system event meets criteria specified by the rule. When all criteria for a rule are met, File Agent submits the Connect:Direct Process associated with that rule.

You can create File Agent rules based on the following properties:

- ◆ Full or partial name of the file detected in a watched directory
- ◆ Size of the file detected in a watched directory
- ◆ System event title
- ◆ System event contents (as included in a stack trace)

You can specify more than one rule in a File Agent configuration; each rule can have File Agent submit a different Process.

Note: Although you can create multiple rules as part of a File Agent configuration, File Agent processing ends when all criteria for a rule are met. Therefore, you should specify rules so that those with more specific criteria (properties) are listed first in the configuration.

For optimum performance, you should configure Connect:Direct File Agent to communicate with the Connect:Direct node where it is installed. You can configure File Agent to use continuous signon and remain connected to the API port for the Connect:Direct server at all times, or configure it to connect to the port only when it needs to. File Agent can be installed on UNIX, Windows, and OS/390 (and z/OS) operating systems. When you use Connect:Direct with UNIX or Windows, the watched directory is a UNIX pathname or a Windows path to the directory. When you use Connect:Direct with OS/390 and z/OS, the watched directory can be the HFS pathname for a file or a directory, the full MVS data set name, or a partial MVS data set name.

File Agent can monitor multiple directories, including local and network directories. File Agent scans the watched directories you specify in the configuration for newly added files (unless you specify a rule to force other operation). By default, Connect:Direct File Agent scans a watched directory once per minute. For example, if you start File Agent at 1:00 p.m., a file added to that watched directory at 12:55 a.m. is not detected as newly added. If you start File Agent at 1:00 p.m., and a file is placed in the watched directory at 1:01 p.m., then File Agent detects this newly added file. File Agent detects a file only one time, unless the file is accessed and saved with a later timestamp.

Using Connect:Direct File Agent requires an understanding of Connect:Direct Processes, operating systems, and scripting (for regular expression operator use with File Agent rules).

Running File Agent

You can run File Agent from a UNIX or command line, configure it to start automatically as a Windows Service at system startup, or configure it to run from a Windows shortcut. Use the command line to verify that File Agent is working correctly or to specify an alternate configuration file. After you run File Agent from the command line to verify that File Agent is operating correctly, run it using the method that requires the least user intervention.

When File Agent runs as a Windows service, it is fully automated, requiring little user intervention. On UNIX, you can modify the initialization sequence of the computer to call the `cdfa.sh` script and run Connect:Direct File Agent whenever you restart the computer. On OS/390 or z/OS, you must run the appropriate job to start the File Agent configuration interface, or start or shutdown the File Agent.

Depending on your network and how you use Connect:Direct, there might be more than one File Agent running (on different hosts). The first File Agent that connects to a Connect:Direct server becomes the File Agent *gate keeper*. The gate keeper port is used to keep track of locations monitored in case multiple File Agents are configured to watch a single directory. The gate keeper ensures that only one File Agent detects a file that appears in a watched directory.

File Agent Logging Capabilities

File Agent logging capabilities vary by platform. Running File Agent from a command line using the verbose argument turns on File Agent logging when it is available. When you run File Agent as Windows service, no information is logged unless an error occurs.

Connect:Direct File Agent provides the following levels of status information when logging is available on a platform:

- ◆ System log—Shows all system activity. This log is created only when you specify verbose mode or if an error occurs. If you are running verbose mode from the command line, this log information is shown in the command line window. If you are not running in verbose mode, the system log appears in the snaps directory (located in the File Agent installation directory), which is created when the first event occurs.
- ◆ First Failing Status (FFS) log—One or more logs created when an error occurs. The snaps directory is created as needed and contains the FFS logs for any errors encountered by File Agent.

Using trace commands provided for your platform can also help capture details related to File Agent operation.

File Agent Configuration Interface and Help

Instructions for configuring File Agent are available in the online Help system that you access from the configuration interface. Field-level Help is displayed in the bottom pane of the configuration interface. Clicking **Help** displays the online configuration procedures.

Planning the File Agent Configuration

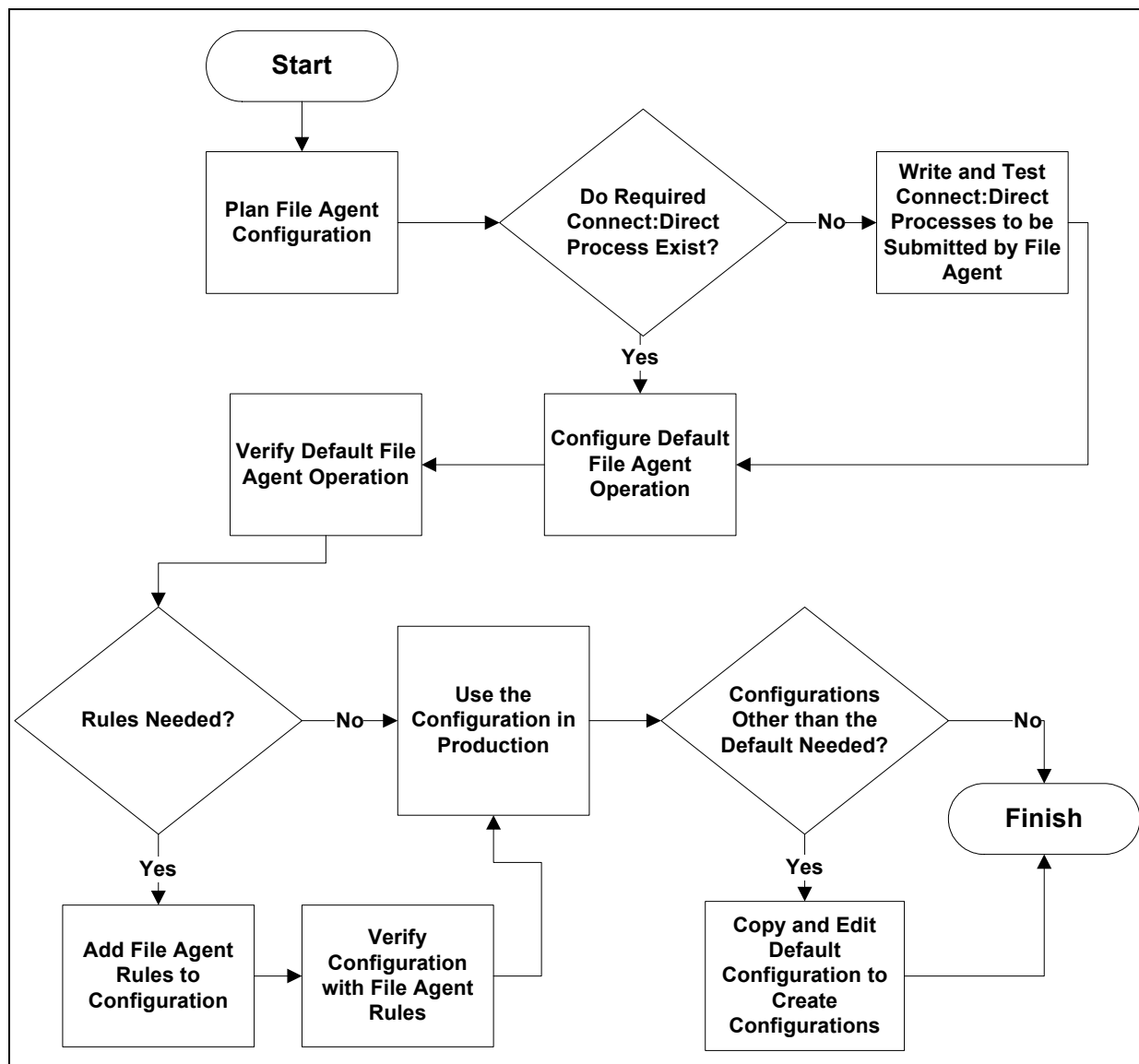
Before you begin configuring File Agent, you must use Connect:Direct to choose or create the Processes that perform the actions you want to automate. You will need to carefully configure File Agent to connect to the Connect:Direct server and to monitor and detect conditions (such as a file addition to a directory). At detection, Connect:Direct File Agent submits the Process for executing actions that need to be performed in response to those conditions.

Refer to *Connect:Direct File Agent Configuration Examples* on page 3-57 to review some configuration scenarios that can help you plan your File Agent configuration. When you configure File Agent, it is best to take an incremental approach; that is, first specify the server connection, a default Process, and the watched directories. Run a test from the command line to ensure that the default File Agent configuration is working correctly. After a successful test of the default configuration, you can run the File Agent Configuration Interface again to start building and testing

any File Agent rules that you want to apply, one by one. After you successfully create a default configuration, you can use the file as the basis for other configuration files.

Use the *File Agent Worksheet* on page 3-55 to gather the information you need to configure File Agent. Contact your system administrator for the site-specific information you will need to establish a connection to the Connect:Direct server. As you complete the worksheet, run the File Agent Configuration Interface and use the File Agent Help system to learn about entering parameters. The Help system and field-level help provide complete descriptions of parameters and arguments you can specify in the configuration file. Make copies of this worksheet if you have to configure File Agent on multiple Connect:Direct servers.

The following diagram illustrates the flow of steps for setting up File Agent for use in a production environment.



File Agent Worksheet

Connect:Direct Server Connection Information	
Userid for API (for connecting to the Connect:Direct server) Required Must match the user ID used to submit the default Process.	<input style="width: 95%; height: 20px;" type="text"/>
Password for API (for connecting to the Connect:Direct server) Required Must match the password used to submit the default Process.	<input style="width: 95%; height: 20px;" type="text"/>
API host DSN name (name of the host on which the Connect:Direct server is located) Required	<input style="width: 95%; height: 20px;" type="text"/>
API port (default =1363) 1–5 digit port number that Connect:Direct File Agent uses to connect to the Connect:Direct server API. Required	<input style="width: 95%; height: 20px;" type="text"/>
Gatekeeper port (default=65530) Port used to track directory monitoring and ensure that multiple File Agents do not monitor a single directory. Required	<input style="width: 95%; height: 20px;" type="text"/>
Gate keeper DNS name (optional) (default=127.0.0.1)	<input style="width: 95%; height: 20px;" type="text"/>
Default Process and Watched Directory Information	
Watched directories: For Windows and UNIX, one or more valid specifications of paths (Windows) or pathnames (UNIX). For OS/390 and z/OS, one or more fully specified HFS pathnames of a file or directory, or a full or partial MVS data set name. Required List one valid entry per line.	<input style="width: 95%; height: 100px;" type="text"/>
<input style="width: 95%; height: 20px;" type="text"/>	
<input style="width: 95%; height: 20px;" type="text"/>	
<input style="width: 95%; height: 20px;" type="text"/>	
<input style="width: 95%; height: 20px;" type="text"/>	
<input style="width: 95%; height: 20px;" type="text"/>	
Default Process and Watched Directory Information	

<p>Default Process: Windows and UNIX: Valid path and name of the file that contains the default Process on the Connect:Direct server. OS/390 and z/OS: Member Name in DMPUBLIB Note: If you do not specify a default Process or create a rule, no processing is performed when a file or event is detected.</p>	<hr/> <hr/>
<p>Default arguments (See Help for complete list.) Argument string to pass to the default Process in the following format: &FA_XXXX_XXX. Note: The percent sign (&) and period (.) are required.</p>	<hr/> <hr/>
<p>Error Process:</p>	<hr/> <hr/>
<p>Error arguments</p>	<hr/> <hr/>
<p>Process class (default=1) Required</p>	<hr/> <hr/>
<p>Process priority (default=1)</p>	<hr/> <hr/>
<p>Watched file interval (default=1 minute)</p>	<hr/> <hr/>
<p>File completion delay (default=1 minute)</p>	<hr/> <hr/>

Note: If you are using X Windows, the X11 display variable is used to connect to the GUI server for terminal emulation. The File Agent Configuration Interface will display on the monitor specified for the X11 display variable. If you want to display the File Agent Configuration Interface on a Windows computer, you must specify the network ID of the terminal you want to use for displaying the File Agent Configuration Interface.

Connect:Direct File Agent Configuration Examples

The following examples illustrate three typical scenarios for using Connect:Direct File Agent. Fields that are not required to be set for the operation demonstrated in the example are not included in the tables of configuration parameters. Required fields are indicated by an asterisk(*) in the File Agent Configuration Interface, and all fields are described in field-level Help. You can use the sample scenarios to become familiar with settings for parameters you must set using the configuration interface in order to accomplish watched directory monitoring and file detection needs.

See the *File Agent Worksheet* on page 55 for a description of the parameters required to establish the connection. The tables of sample data for these scenarios assume that you have already configured the site-specific parameters required to establish a connection to the Connect:Direct server where File Agent is installed. The sample scenarios also assume that the Connect:Direct Processes that will perform tasks associated with Connect:Direct File Agent file detection activities have been created.

Detecting a File Added to a Watched Directory on an OS/390 or z/OS System

Some users need to access a report file that is expected to be transferred to a location that only administrators can access. File Agent can be configured to perform the processing on an OS/390 or z/OS system:

- ◆ Monitor the watched data set called EASTERN.Q1.REPTS.
- ◆ Submit a default Process called DEFPROC. The default Process has been created to copy a file detected in the watched data set to a specified location for access by users.

Tab	Field	Sample or Description
File agent	Watched directories	Type EASTERN.Q1.REPTS to specify the fully qualified MVS data set name to watch.
	Default Process	Type DEFPROC, the member name for the Process in DMPUBLIB. Note: If no default Process is specified and the file does not match a rule, then no processing occurs.

Detecting a File by File Size on a Windows System

Customer transaction files are regularly transferred into the Windows directory c:\monthend\datafile. Files larger than 1 MB require special processing that will automatically be performed on files in a certain directory.

The sample values in the following table accomplish the following processing:

- ◆ Monitor the watched directory c:\monthend\datafile
- ◆ Apply the rule titled Find big file to detect files larger than 1 MB.

- ◆ Override the default Process and submit a Process that is associated with the Check file size rule. This fixbigfile.cdp Process will copy a file larger than 1 MB from the c:\monthend\datafile directory to the c:\reprocess directory.
- ◆ Pass the path and file name of the file that meets the criteria for the find big file rule to the Process fixbigfile.cdp.

Tab	Field or Dialog Box	Actions and Sample Entry
File agent	Watched directories field	Specify the directory to watch. Type the directory path for the directory that File Agent will watch: c:\monthend\datafiles
Rules	Create rule dialog box	Click New and type the name you want to give the rule in the field: find big file Click find big file in the list of rules and click Edit .
	Match criteria list for rule “find big file”	Specify the criterion to check for a detected file. Select the default criterion name, Not enabled: system event title matches “ ” and click Edit match .
	Edit match criterion for rule “find big file” dialog box	<ul style="list-style-type: none"> ◆ Click Enabled to enable the criteria you are about to specify. ◆ Click Size of the newly arrived file ◆ Click Matches to display the options for the comparison. Click Greater than to define the how the file size should compare. ◆ Type 1024 in the Compare size field and click OK.
	Process name field	Scroll down to view the Submit Process information for watched file event rule “find big file” . Type the directory path and filename for the Process that File Agent is to submit when the rule Find big file results in a match: c:\processes\fixbigfile.cdp Click Done and then click Save .

Detecting a System Event by Title on a Windows System

`IndexOutOfBoundsException` is the title of an event that indicates a number is outside of an expected range. In the following example, File Agent is used to detect an event with `IndexOutOfBoundsException` in the title, pass a string (the event title) to a `Connect:Direct Process`, and then submit a `Process` to the `Connect:Direct` server that will perform actions the environment requires for this type of event. In this scenario, the event `IndexOutOfBoundsException` could indicate activity that a network administrator should investigate. Because the site uses a `Connect:Direct` mailbox system, the configuration will include the administrator's account to be notified when `Connect:Direct File Agent` submits a `Process` for the `IndexOutOfBounds` rule.

The sample values in the following table accomplish the following processing:

- ◆ Override the default `Process` and submit `\processfolder\oo_boundserproc.cdp`
- ◆ Send a message to the administrator's mailbox system account after submitting the `oo_boundserproc.cdp` `Process` for the rule.

Tab	Dialog Box, Window, or Field	Description/Example
Rules	Create rule dialog box	Type index out of bounds as the name of the rule you are creating.
	Match criteria list for rule "index out of bounds" window	Select the default criteria Not enabled: System event title matches " " and click Edit match .
	Edit match criterion for rule "index out of bounds" dialog box	<ul style="list-style-type: none"> ◆ Click Enabled to enable the criteria you are about to specify. ◆ Click System event title as the criterion to match for the rule. ◆ Click Matches on the drop-down field to see the options for comparison to a string. ◆ Click Contains to specify how the compare string should relate to a system event title that File Agent detects. ◆ Type IndexOutoffBounds as the Compare String to indicate that the system event title should include this string. ◆ Click OK.
	Submit Process information for system event rule "index out of bounds" window	Type information into the fields that will define the <code>Process</code> to submit and the mailbox user to notify after the <code>Process</code> is submitted.
	Process name field	Type <code>c:\processfolder\errproc.cdp</code> to specify the path and file name for the <code>Process</code> File Agent submits when a file meets the rule criteria.
	Notification userid field	Type <code>adminjim@company.com</code> to specify the user to notify when File Agent submits the <code>Process</code> .

Passing the UNIX Pathname for a Detected File to a Process

Because Connect:Direct File Agent can watch multiple directories for the appearance of a new file, the Connect:Direct Process that File Agent is to submit to the server at the appearance of a new file might need to reference the Windows Path or UNIX pathname for the detected file as part of commands and statements in the Process.

In the following example, a UNIX pathname is passed to the default Process, copynewfile.cdp.

Tab	Dialog box, Window, or Field	Sample Entry
File agent	Watched directories	Type one UNIX pathname per line for each location File Agent is to watch for the appearance of files: user/bin/monthend/ quartend/easterndiv/errorfiles managers/special/reports File Agent checks these pathnames for new files.
	Default process	Type the UNIX pathname and filename for the Connect:Direct Process that File Agent is to run when a file appears in any watched directory specified: user/bin/admin/copynewfile.cdp The pathname where File Agent detected a new file is passed to this Process.
	Default arguments	Type the File Agent variable for passing a UNIX pathname or Windows path, including the leading percent sign (%) and the ending period (.): &FAP=%FA_PATH_FOUND. In this example, &FAP is the variable to which File Agent will pass the UNIX pathname where the file was detected. %FA_PATH_FOUND. is the File Agent variable used to indicate the information to pass to the Connect:Direct Process.

Installation Worksheets

Before you begin installing Connect:Direct for UNIX, complete the worksheets in this appendix to help you gather the information you need to complete the installation procedure.

Complete the following worksheets before beginning the installation procedure:

- ◆ *Installation Worksheet* on page 62
- ◆ *Customization Worksheet* on page 62
- ◆ *User Authorization Information File Worksheet* on page 63
- ◆ *CLI/API Configuration File Worksheet* on page 68

Connect:Direct automatically generates the network map and server and client authentication key files. However, you may want to further customize these files. The following worksheets are provided for your convenience:

- ◆ *Network Map Remote Node Information File Worksheet (TCP/IP Only)* on page 69
- ◆ *Server Authentication Key File Worksheet* on page 70
- ◆ *Client Authentication Key File Worksheet* on page 70

In the following worksheets, host name refers to the TCP/IP computer name, and node name refers to the Connect:Direct node name.

Installation Worksheet

Complete this worksheet to assist you during the installation procedure.

Parameter	Value
TCP/IP host name of the computer where the Connect:Direct server is installed	
Directory or path on which the distribution media will be mounted	
Destination directory where Connect:Direct will be installed, including the full path name	

Customization Worksheet

Use this worksheet during customization. Refer to the *Customizing Connect:Direct for UNIX* on page 30.

Parameter	Default Value	Value to Use
Connect:Direct node name you are customizing, up to 16 characters long.		
Initialization Parameters File Information		
TCP/IP port number that the server monitors or an API connection request.	1363	
TCP/IP port number that the server monitors for a remote Connect:Direct connection request:	1364	
Note: Use the default port number, if available. If the default port number is being used by another service, use any other available port. Check the <code>/etc/services</code> file for a list of ports.		

User Authorization Information File Worksheet

Use this worksheet when you are defining the user authorization information file. The user authorization information file includes the remote user information records and local user information records.

All Connect:Direct users must have an entry in the user authorization information file.

Remote User Information Record

Connect:Direct uses the remote user information record to establish a proxy relationship between remote and local user IDs. Remote user IDs are translated to valid local user IDs on the system where you are installing Connect:Direct for UNIX. Connect:Direct also uses the remote and local user information records to determine the functionality of the user IDs that are translated and connected to it through a client using a Connect:Direct API.

Use the following table to create a list of remote user IDs and the local user IDs to which they will be mapped. If necessary, make copies of this page to record additional remote user IDs and local user IDs.

For more information on creating remote user information records and for information on using special generic characters to map remote user IDs, refer to the *Connect:Direct for UNIX Administration Guide*.

Remote User ID	at	Remote Node Name	mapped to	Local User ID
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	
	@		=	

Local User Information Record

Use the following table to record the local user ID records to create and the parameters to define. Define the additional parameters by editing the `userfile.cfg` file using any standard UNIX editor.

Default values are shown as capital letters in brackets. Before you begin defining local user information records, make copies of this worksheet for the number of users you plan to create.

Local User ID	Parameter	Description	Value to Assign
	<code>admin.auth</code>	Determines if the user has administrative authority. y —All the other command parameter capabilities in the local user information record are automatically assigned to this user. n —You must grant specific command parameters individually.	
	<code>cmd.chgproc</code>	Specifies whether the user can issue the change Process command. y —Allows the user to issue the command. n —Prevents the user from issuing the command. a —Allows all users to issue this command.	
	<code>cmd.delproc</code>	Specifies whether the user can issue the delete Process command. y —Allows the user to issue the command. n —Prevents the user from issuing the command. a —Allows all users to issue this command.	y or n or a y —Default a —For all users
	<code>cmd.flsproc</code>	Specifies whether the user can issue the flush Process command. y —Allows the user to issue the command. n —Prevents the user from issuing the command. a —Allows all users to issue this command.	y or n or a y —Default a —For all users

Local User ID	Parameter	Description	Value to Assign
	cmd.selproc	Specifies whether the user can issue the select Process command. y —Allows the user to issue the command. n —Prevents the user from issuing the command. a —Allows all users to issue this command.	
	cmd.selstats	Specifies whether the user can issue the select statistics command. y —Allows the user to issue the command. n —Prevents the user from issuing the command. a —Allows all users to issue this command.	
	cmd.stopndm	Specifies whether the user can issue the stop command. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	cmd.submit	Specifies whether the user can issue the submit Process command. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	cmd.trace	Specifies whether the user can issue the trace command. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	descrip	Permits the administrator to add descriptive notes to the record.	text string
	name	Specifies the name of the user.	user name _____
	phone	Specifies the telephone number of the user.	user phone _____

Local User ID	Parameter	Description	Value to Assign
	pstmt.copy	Specifies whether the user can issue the copy command. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	pstmt.copy.ulimit	Specifies the action to take when the limit on a user output file size is exceeded during a copy operation. The value for this parameter overrides the equivalent value for the ulimit parameter in the initialization parameters file. If a value is not defined in the initialization parameters file, the default is n . y or n or nnnnnnnK or nnnnM or nG where nnnnnnnK , nnnnM or nG establishes a default output file size limit for all copy operations. K —Thousands of bytes. M —Denotes millions of bytes. G —Denotes trillions of bytes. The maximum value you can specify is 1 terabyte.	
	pstmt.download	Specifies whether the user can download files. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	pstmt.download_dir	Specifies the directory to which the user can download files.	
	pstmt.runjob	Specifies whether the user can issue the run job statement. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	pstmt.runtask	Specifies whether the user can issue the run task statement. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	

Local User ID	Parameter	Description	Value to Assign
	pstmt.submit	Specifies whether the user can issue the submit statement. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	snode.ovrd	Specifies whether the user can code the snodeid parameter on the submit command and Process and submit statements. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	pstmt.upload	Specifies whether the user can upload files. y —Allows the user to issue the command. n —Prevents the user from issuing the command.	
	pstmt.upload_dir	Specifies the directory from which the user can upload files.	
	run_dir	Specifies the directory that contains the programs and scripts the user can execute.	
	submit_dir	Specifies the directory from which the user can submit Processes.	

CLI/API Configuration File Worksheet

Use this worksheet to define the parameters needed to create a client configuration file. Create a separate file for each client attached to the server. Refer to *Connect:Direct for UNIX Administration Guide* for details on modifying the file.

Parameter	Default Value	Value To Use
Port number of the Connect:Direct for UNIX server to which this client will connect.	1363	
Note: Use the default port number if available. If the default port number is being used by another service, use any other available port. Check the <code>/etc/services</code> file for a list of ports.		
Host name of the Connect:Direct for UNIX server to which this API will connect.		
You can also type the IP address of the server.		

Network Map Remote Node Information File Worksheet (TCP/IP Only)

Submit a Process to a remote node that does not have a record in the remote node information file by specifying an IP address or host name with the SNODE parameter. However, if you do not specify an IP address or host name, you must define a remote node information record for each remote node in the network with which this node will communicate through TCP/IP.

The initial network map file containing a local node definition is created for you during the installation procedure; however, you need to add a remote node record to the network map for each remote node you will communicate with.

Use the information on this worksheet when you modify the network map. Refer to the *Connect:Direct for UNIX Administration Guide* for details on modifying the file.

Make a copy of this worksheet for each remote node in the network.

Parameter	Default Value	Value To Use
Remote Connect:Direct node name		
Host name or IP address on which the remote Connect:Direct server will run.		
Note: Use the default port number, if available. If the default port number is being used by another service, use any other available port. Check the /etc/services file for a list of ports.		
Communication port number to call the remote Connect:Direct server:	1364	

Server Authentication Key File Worksheet

The initial server authentication key file is created during the installation procedure; however, you can update your key later. Use the information on this worksheet when you modify your key. Refer to the *Connect:Direct for UNIX Administration Guide*, when determining appropriate values.

Parameter	Default Value	Value To Use
The host name on which the API is executed.	*	
An asterisk (*) stands for any host.		

Connect:Direct security depends on a key (similar to a password) in a Connect:Direct server and an identical key in each API that communicates with that server. The keys are defined and coordinated by the system administrator of the specific node or nodes, and should be kept secure. Be sure the authentication keys are available during installation, but do not record them on this worksheet or where they can be lost.

Client Authentication Key File Worksheet

The initial client authentication key file is created automatically during the installation; however, you can update your key at a later date. Use the information on this worksheet when you modify the key. Refer to the *Connect:Direct for UNIX Administration Guide*, when determining appropriate values.

Parameter	Default Value	Value To Use
The host name on which a Connect:Direct is executed.	*	
An asterisk (*) stands for any host.		

Connect:Direct security depends on a key, similar to a password, in a Connect:Direct server and an identical key in each API that will communicate with that server. The keys are defined and coordinated by the system administrator of the specific node or nodes, and should be kept secure.

Have the authentication keys you will use available during installation, but do not record them on this worksheet or anywhere else that could compromise security.

SNA LU6.2 Connectivity

This appendix instructs you on installing Connect:Direct for UNIX on SNA systems. It assumes that you have already installed an SNA package and that you are familiar with configuring the SNA package to support independent LU6.2 connections.

About SNA LU6.2 Connections

The Connect:Direct for UNIX product supports SNA LU6.2 connections in addition to TCP/IP connections. SNA LU6.2 connectivity is a separately licensed Connect:Direct feature.

For a list of platforms that are supported for LU6.2 connectivity, refer to the *Connect:Direct for UNIX Release Notes*.

Supported Interfaces

Following is a list of supported interfaces:

- ◆ Token ring
- ◆ Ethernet
- ◆ SDLC
- ◆ X.25 (QLLC)

Session Support

Connect:Direct for UNIX supports both independent and dependent LU6.2 sessions. Configuring independent LU sessions simplifies the management of communication between nodes and ensures appropriate recovery in some situations. Dependent LU sessions must be managed manually for communications between Connect:Direct nodes and do not recover properly in some situations.

The maximum number of independent LU sessions you configure defines the maximum number of concurrent transfers between nodes. The total number of sessions determines the number of UNIX transfers that can run simultaneously. Type an even number for the maximum number of sessions so that you can divide equally between the number of contention winner and contention loser

sessions. The recommended number of maximum sessions is 8. The recommended number of contention winner sessions is 4. If supported, the recommended number of automatically established sessions is 4.

APPC Requirements

APPC requirements are described in the following list:

- ◆ Connect:Direct for UNIX uses a fixed transaction program (TP) name, NNV2DTF.
- ◆ Connect:Direct for UNIX uses basic conversations, sync level = confirm, no conversation level security, and no PIP (program initialization parameters).
- ◆ Do not specify the transaction program (TP) name in hexadecimal.

Configuration Requirements

Configuration requirements are described in the following list:

- ◆ The Connect:Direct for UNIX daemon must start the session manager, the LU6.2 communications component of Connect:Direct for UNIX. The Connect:Direct for UNIX daemon monitors for inbound ALLOCATEs and starts a session manager to handle the Process submitted by the remote node. The SNA communications package cannot start a session manager.
- ◆ Do not configure the TP as dynamically attachable or as an autostart program.
- ◆ Do not configure a path name to a Connect:Direct for UNIX program when you define the TP.
- ◆ For SNA packages that require that you provide a program name for a TP definition, you must type a program name that does not exist.

SNA Considerations

SNA considerations are listed in the following section:

- ◆ Connect:Direct for UNIX is tested with the following link LU6.2 types. Currently, not all link types are tested on all platforms.
 - ◆ Token ring
 - ◆ Ethernet
 - ◆ SDLC leased line
 - ◆ X.25 (QLLC)
- ◆ Connect:Direct for UNIX, as an LU6.2 conversation partner, supports any defined link type supported by the SNA package manufacturer. There are no special support or configuration requirements in Connect:Direct for UNIX when using different link types to communicate with the remote node.
- ◆ The RU size selected for use with Connect:Direct for UNIX can strongly affect the observed file transfer throughput. Connect:Direct for UNIX is tested with 1K, 2K, and 4K RU sizes, with inbound and outbound pacing set to 7. Use a 1K RU size to confirm basic functionality, and then use 2K and 4K RU sizes while monitoring network congestion. You can realize a significant gain in throughput by increasing RU sizes from 1K to 4K. Increasing the RU size

beyond 4K or increasing the pacing above 7 generally provides marginal improvement, but can severely degrade network performance.

Note: VTAM resource names must be typed in uppercase.

Installing and Configuring the AIX SNA Server

For AIX SNA support, you must install and configure either the AIX SNA Server/6000 or the eNetwork Communications Server. You can perform the configuration manually or use the Connect:Direct for UNIX configuration script. The script generates a set of communications profiles, which are used by Connect:Direct for UNIX. Review and modify the values in the profile entries to suit your environment.

The following sections provide the parameter definitions required by Connect:Direct for UNIX and a description of the script included with Connect:Direct.

Manually Configuring the AIX SNA Server

You can manually configure AIX SNA by modifying the values in the default profile entries, as appropriate for your environment; however, Connect:Direct requires that you add a TP profile name with specific parameters.

To add the TP profile name, log in as root and type one of the following commands:

- ◆ For AIX SNA Server/6000

```
mksnaobj -t'local_tp' -c 'basic' -w '/usr/lpp/sna' CDUTPPRO
```

- ◆ For eNetwork Communications Server

```
smitsnaadmin -x define_tp, tp_name='CDUTPPRO' conv_type='BASIC', \
security_rqd='NO', sync_level='CONFIRM_SYNC_LEVEL', pip_allowed='YES'
```

The following table lists the parameters required by Connect:Direct. You can assign default values to all other parameters.

Parameter	Definition
Profile name	CDUTPPRO
Conversion type	basic
Full path to TP executable	/usr/lpp/sna

Note: The path must be a valid directory that differs from the Connect:Direct for UNIX installation directory.

About the Configuration Script

If you want to use a script to generate the Connect:Direct for UNIX configuration for AIX SNA Server/6000 support, run the script located in **etc/cdsnacfg**. After running the script, use SMIT to review the configuration to ensure that the profile values are appropriate for your environment. Sample profiles are provided as a reference.

Using the script, you can configure your RS/6000 workstation for any of the following options:

- ◆ Token ring
- ◆ SDLC leased line

Note: Do not use the cdsnacfg script to configure more than one connection. The script archives and deletes the current profile entries before adding values required by Connect:Direct.

The script issues commands to perform the following tasks:

- ◆ Stop AIX SNA support.
- ◆ Back up the current configuration to **/snadirs/sna_XXXX.sav**, where **XXXX** is the current month and day.
- ◆ Delete the current AIX SNA profiles. You can restore or merge saved profiles with the **smit importsna** command.
- ◆ Regenerate base profiles.
- ◆ Configure AIX SNA support as required by Connect:Direct.
- ◆ Verify the AIX SNA configuration.
- ◆ Start AIX SNA support.
- ◆ Start the required SNA connections.

Running the Configuration Script

Complete the following steps to run the configuration script:

1. Log in as root.
2. From the `d_dir/etc` directory, type the following command:

```
# cdsnacfg
```

Note: The configuration script can run even if messages indicating irregular processing are returned. Read any messages as you proceed through the configuration. Refer to the AIX SNA documentation as required.

The following screen is displayed:

```
=====
                          Sample AIX SNA Configuration Script
                          COPYRIGHT (C) 1983, 1999 Sterling Commerce, Inc.
                          =====

Stopping SNA Support ... ..
0513-044 The stop of the sna Subsystem was completed successfully.

Backing up current SNA configuration ... ....
The backup file is /usr/lpp/sna/sna_1111.sav .

Deleting current profile entries ... ..

Regenerating base profiles ... ..

Stopping SNA Support again (overriding possible autostart) ...
0513-004 The Subsystem or Group, sna, is currently inoperative.

Build a sample SNA configuration to access an MVS
host with one of the following connections:

    (1). Token Ring
    (2). SDLC Leased Line

    (3). Exit.

Note 1: Host resource names must be entered in uppercase.

Note 2: When the script completes, use SMIT to verify that
        the selected SNA configuration options match your
        communications environment (e.g. NRZ vs. NRZI for
        SDLC, SAP address for Token Ring).

====> Enter your choice here [1]:
```

3. Do one of the following:
 - ◆ Type **1** to select Token Ring as the connection type and press **Enter**. The default is a token ring connection [1]. Go to step 5.
 - ◆ Type **2** to select SDLC Lease Line as the connection type and press **Enter**. Go to the next step.
4. Type the appropriate value for the following prompts or press **Enter** to select the default as listed in the brackets. The token ring adapter name is an AIX SNA assigned name. All other default values are samples that you can modify. For a VTAM host, the Adjacent Control Point Name is the SSCPNAME. Type host resource names in uppercase letters.

```

Please enter Network Name ..... [CDUNET] :
Please enter Adjacent Control Point Name ..... [HOSTTCP] :
Please enter PU name ..... [RS6PU01] :
Please enter Remote Link Address..... [400076543210] :
Please enter XID node ID..... [07143210] :
Please enter local LU name ..... [RS6LU01] :
Please enter remote LU name (C:D MVS APPLID) .. [NDMAPP4] :
Please enter mode name ..... [NDM621K] :
Please enter Token Ring Adapter name ..... [tok0] :
Please enter Token Ring Adapter name ..... [0]

```

5. Type the appropriate value for an SDLC leased line connection or press **Enter** to select the default values in brackets. The Portmaster Adapter/A port name is an AIX SNA assigned name. All other default values are samples that you can modify. For a VTAM host, the Adjacent Control Point Name is the SSCPNAME. Type host resource names in uppercase letters.

```

Please enter Network Name ..... [CDUNET] :
Please enter Adjacent Control Point Name ..... [HOSTTCP] :
Please enter PU name ..... [RS6PU01] :
Please enter PU address (decimal)..... [02] :
Please enter local LU name ..... [RS6LU01] :
Please enter remote LU name (C:D MVS APPLID) .. [NDMAPP4] :
Please enter mode name ..... [NDM621K] :
Please enter Portmaster Adapter/A port name ... [mpq0] :

```

6. Review the messages as the configuration script completes its final steps. If you receive a message that Connect:Direct is unable to determine the installed version of AIX SNA support, then perform the following steps:
 - ◆ Verify your installation with SMIT.
 - ◆ Run etc/snaver.sh to test for the correct installation of AIX SNA Server/6000.
 - ◆ Rerun the cdsnacfg script.

For special considerations for connectivity between RS/6000 and AS/400 systems, refer to *Special Considerations* on page 98.

Refer to the AIX SNA Server/6000 documentation for further information about AIX SNA Server/6000.

HP SNAplus2 Configuration Requirements

For HP SNA support, you must install and configure HP SNAplus2API, SNAplus2-Common, and SNAplus2-Link software. Perform the following steps to configure your system:

1. Use a text editor or **xsnapadmin** to create a configuration file named **/etc/opt/sna/sna_node.cfg**.
2. Add the following entry to the **/etc/opt/sna/sna_tps** file:

```
[ "NNV2DTF" ]
TYPE=QUEUED-BROADCAST
USERID=XXXXX
```

3. To start the SNA 3.0 support, log in as root and type the following command:

```
snap start
```

4. To validate or modify your configuration, start the local node, log in as root, and type the following command:

```
snapadmin
```

For additional information about configuring for SNAplus2 10.10 connectivity, refer to the Hewlett-Packard documentation.

The following example displays the contents of a file that contains the required Connect:Direct AT&T Servers SNA 3.0 Invokable TP definition. This file, **sna_tps**, is provided in the directory **d_dir/etc**.

```
[ "NNV2DTF" ]
TYPE=QUEUED-BROADCAST
```

SNAP-IX SNA Gateway Support Configuration Requirements

For SNAP-IX support, you must install and configure the SNAP-IX SNA server software.

Documentation about SNAP_IX can be found at the following Web site:

<http://www.dataconnection.com/sna/docs.htm> or with the SNAP_IX product.

Perform the following steps to configure SNAP_IX.

1. Log on as root before executing any SNAP_IX commands.
2. Type the following command to start the SNAP_IX SNA Server application:

```
/opt/sna/bin/sna start
```

3. Create a configuration file that defines configuration statements for your system, including the communications protocol. Either use the command line program `/opt/sna/bin/snaadmin` to create or modify the `/etc/opt/sna/sna_node.cfg` configuration file or use the `/opt/sna/bin/X11/xsnaadmin` program to create or modify a configuration file. Refer to the `SNAP_IX` documentation for a description of the available parameters.
4. Type the following command to define the `NNV2DTF` transaction program:

```
/opt/sna/bin/snaadmin
define_tp,tp_name=NNV2DTF,conv_type=BASIC,sync_level=CONFIRM_SYNC_LEVEL,pip_alled=NO
```

Following are sample statements in the file `/etc/opt/sna/sna_tps`, where 'xxxxxx' is a valid user ID.

```
[NNV2DTF]
LUALIAS = ""
DESCRIPTION = ""
USERID = xxxxxx
TIMEOUT = -1
TYPE = QUEUED-BROADCAST
```

Following is a sample configuration statement that is defined in the `SNAP_IX` `sna_node.cfg` file and defines a `SNAP_IX` SNA Server for LU6.2 connectivity between an Ethernet attached SUN Solaris 8 system and an OS/390 mainframe. It defines a single independent LU and one `Connect:Direct`

node LU on the mainframe. The VTAM resource names correspond to the samples given in this appendix.

```
[define_node]
cp_alias = CDUPU01
description = Control Point Node
fqcp_name = CDUNET.CDUPU01
node_type = END_NODE
mode_to_cos_map_supp = YES
mds_supported = YES
node_id = <01702160>

[define_ethernet_dlc]
dlc_name = ETHER0
description = Ethernet dlc
neg_ls_supp = YES
initially_active = NO
adapter_number = 0
lan_type = 802_3_DIX

[define_ethernet_port]
port_name = ETSAP0
description = Ethernet Port 0
dlc_name = ETHER0
port_type = PORT_SATF
port_number = 0
max_rcv_btu_size = 1033
[define_ethernet_ls]
ls_name = ETHL0
description = Ethernet Link Station
port_name = ETSAP0
adj_cp_name = <00000000000000000000000000000000>
adj_cp_type = LEARN_NODE
mac_address = <10005ad172fc>
solicit_sscp_sessions = YES
pu_name = ETHL0

[define_partner_lu]
plu_alias = NDMAPP4
description = QC.OS390.V4300 C:D Node
fqplu_name = CDUNET .NDMAPP4
plu_un_name = <0000000000000000>
parallel_sess_supp = YES

[define_local_lu]
lu_alias = CDULU01
list_name = ""
description = Local LU
lu_name = CDULU01
lu_session_limit = 0
pu_name = <0000000000000000>

[define_mode]
mode_name = NDM621K
description = NDM621K
default_ru_size = NO
max_ru_size_upp = 1024
```

```
Sample configuration statement (continued)

[define_mode]
mode_name = NDM622K
description = NDM622K
default_ru_size = NO
max_ru_size_upp = 2048

[define_mode]
mode_name = NDM624K
description = NDM624K
default_ru_size = NO
max_ru_size_upp = 4096

[define_directory_entry]
resource_name = CDUNET .CSDSA01
resource_type = ENCP_RESOURCE
description = MVSA SSCP
parent_name = <0000000000000000000000000000000000000000>
parent_type = ENCP_RESOURCE

[define_directory_entry]
resource_name = CDUNET .CSDSA01
resource_type = LU_RESOURCE
description = (Auto defined - default LU)
parent_name = CDUNET .CSDSA01
parent_type = ENCP_RESOURCE

[define_directory_entry]
resource_name = CDUNET .NDMAPP4
resource_type = LU_RESOURCE
description = QC.OS390.V4300 C:D Node
parent_name = CDUNET .CSDSA01
parent_type = ENCP_RESOURCE

[define_tp]
tp_name = NNV2DTF
description = C:D-UNIX TP
list_name = ""
conv_type = BASIC
security_rqrd = NO
sync_level = NONE
enabled = YES
pip_allowed = NO
tp_instance_limit = 0
```

Brixton 4.1 SNA for Sun Solaris Requirements

For Brixton SNA support, use the procedures in this section to install and configure the Brixton BrxPU2.1 SNA Server.

- ◆ For Brixton SNA support, Connect:Direct for UNIX requires Brixton software packages BrxAPPC, BrxGMAN, BrxGMI, and BrxPU21

Product	Description
BrxGMAN	Brixton Gateway Manager
BRXGMI	Brixton Graphical Management Interface
BrxAPPC	Brixton LU6.2 and CPI-C APIs

- ◆ Connect:Direct for UNIX requires that you configure BrxGMAN, BrxGMI, and BrxPU2.1 packages.
- ◆ The BrxGMI (Graphical Management Interface) generates a working configuration that can be altered to match your needs.

Note: This is not an SNA configuration.

Configuring BrxGMAN Software

Perform the following steps to configure the BrxGMAN software:

1. Type the following commands to run the PU2.1 setup program:

```
# cd /opt/BrxPU21
```

```
# ./brxsetup
```

The following screen is displayed:

```

The installation procedure allows you to install:

(1) Configure BrxGMAN Software.
(2) Configure BrxGMI Software.
(3) Configure BrxPU21 Software.
(4) Configure BrxGMAN Software.
(5) Start BrxGMAN Software.
(6) Start BrxPU21 Software
(7) Stop BrxGMAN Software
(8) Stop BrxPU21 Software
(9) Show BrxGMAN Software
(10) Show BrxPU21 Software

(q) Exit

Enter selection [q] 1

```

2. To configure the BrxGMAN software, type **1** and press **Enter**.

The BrxGMAN configuration file directory root is currently set to `/etc/brixton`. The following screen is displayed:

```

The BrxGMAN configuration file directory root is currently set to /etc/brixton.
Do you want to change it (Yes/No) [N]?

```

3. Type **n** and press **Enter** to use the default directory.

The BrxGMAN is configured for a site that runs a main DNS Server. The setup script prompts you to change the setting.

```

The BrxGMAN is configured for a site that runs a main DNS server. In this mode, the
main DNS server is configured to handle all resource lookups initially and direct
those that are in the Brixton sub-domain to the BrxGMAN running on this or other
systems.

Do you want to change this setting (Yes/No) [N]?

```

4. Type **n** and press **Enter** to use the default DNS server configuration.

The following screen is displayed. The DNS domain name is currently set to `stercomm.com`.

```

The DNS domain name is currently set to stercomm.com.
Do you want to change it (Yes/No) [N]?

```

5. Type **n** and press **Enter** to use the default DNS domain name.

The following screen is displayed. The Brixton subdomain name is currently set to `csg`.

```

The Brixton subdomain name is currently set to csg.
Do you want to change it (Yes/No) [N]?

```

6. Type **n** and press **Enter** to use the default Brixton subdomain name.

The following screen is displayed. BrxGMAN product is set to startup automatically each time your system reboots. The setup script prints you to change this setting.

```
The BrxGMAN product is set to startup automatically each time your system reboots.
Do you want to change it (Yes/No) [N]?
```

7. Type **n** and press **Enter** to continue to automatically start the BrxGMAN product at startup. The following screen displays a prompt to verify the BrxGMAN configuration:

```
The BrxGMAN can be configured as follows:
  Installation directory           /opt/BrxGMAN
  Working directory               /var/brixton
  Configuration file directory root /etc/brixton
  Brixton DNS configuration       Operate with existing DNS server
  Full DNS domain name           csg.stercomm.com
  Run startup script at boot     YES

Is this configuration correct (Yes/No) [Y]?
```

8. Type **y** and press **Enter** to confirm the configuration.

Configuring BrxGMI Software

Perform the following steps to configure the BrxGMI software.

The following setup script prompts you to select a task:

```
The installation procedure allows you to install:

(1) Configure BrxGMAN Software.
(2) Configure BrxGMI Software.
(3) Configure BrxPU21 Software.
(4) Configure BrxGMAN Software.
(5) Start BrxGMAN Software.
(6) Start BrxPU21 Software
(7) Stop BrxGMAN Software
(8) Stop BrxPU21 Software
(9) Show BrxGMAN Software
(10) Show BrxPU21 Software

(q) Exit

Enter selection [q] 2
```

1. To configure the BrxGMI software, type **2** and press **Enter**.

The following screen prompts you to change the current Help browser.

```
The BrxGMI help browser is currently set to mosaic.
Do you want to change it (Yes/No) [N]?
```

2. Type **n** and press **Enter** to use the default browser.

The script prompts you to change the working directory.

```
The BrxGMI working directory is currently set to /var/brixton.
Do you want to change it (Yes/No) [N]?
```

3. Type **n** and press **Enter** to use the default BrxGMI working directory.

The script prompts you to verify the configuration.

```
The BrxGMI can be configured as follows:
  Installation directory      /opt/BrxGMI
  Working directory          /var/brixton
  Help browser type          mosaic
  Help browser pathname/image mosaic
  Xterm command path         /usr/bin/X11/xterm

Is this configuration correct (Yes/No) [Y]?
```

4. If the configuration is correct, type **y** and press **Enter**.

Configuring BrxPU21 Software

Perform the following steps to configure the BrxPU21 software.

The following screen prompts you to select a task:

```
The installation procedure allows you to install:

(1) Configure BrxGMAN Software.
(2) Configure BrxGMI Software.
(3) Configure BrxPU21 Software.
(4) Configure BrxGMAN Software.
(5) Start BrxGMAN Software.
(6) Start BrxPU21 Software
(7) Stop BrxGMAN Software
(8) Stop BrxPU21 Software
(9) Show BrxGMAN Software
(10) Show BrxPU21 Software

(q) Exit

Enter selection [q] 3
```

1. Type **3** to and press **Enter** configure BrxPU21. The setup script prompts you to change the working directory.

```
The BrxPU21 working directory is currently set to /var/brixton.
Do you want to change it (Yes/No) [N]?
```

2. Type **n** and press **Enter**. The setup script prompts you to change the root directory.

```
The BrxPU21 configuration file directory root is currently set to /etc/brixton.
Do you want to change it (Yes/No) [N]?
```

3. Type **n** and press **Enter**. The setup script prompts you to change the startup setting.

```
The BrxPU21 product is set to startup automatically each time
your system reboots.
Do you want to change it (Yes/No) [N]?
```

4. Type **n** and press **Enter**. The setup script prompts you to verify the configuration.

```
The BrxPU21 can be configured as follows:
  Installation directory           /opt/BrxPU21
  Working directory                /var/brixton
  Configuration file directory root /etc/brixton
  Run startup script at boot       YES

Is this configuration correct (Yes/No) [Y]?
```

5. If the configuration is correct, type **y** and press **Enter**.

Starting BrxGMAN

Perform the following steps to start the BrxGMAN software.

The setup script prompts you to select a task.

```
The installation procedure allows you to install:

(1) Configure BrxGMAN Software.
(2) Configure BrxGMI Software.
(3) Configure BrxPU21 Software.
(4) Configure BrxGMAN Software.
(5) Start BrxGMAN Software.
(6) Start BrxPU21 Software
(7) Stop BrxGMAN Software
(8) Stop BrxPU21 Software
(9) Show BrxGMAN Software
(10) Show BrxPU21 Software

(q) Exit

Enter selection [q] 5
```

1. Type **5** to start the BrxGMAN and press **Enter**.
2. Type the following command to start the Graphical Manager and configure SNA LU6.2 definitions:

```
# ./brxgmi.sh
```

Refer to the Brixton documentation for additional information about configuring the SCO system for Brixton SNA connectivity.

Sample Brixton BrxPU2.1 Configuration

Connect:Direct for UNIX supports platforms running Brixton SNA 4.1 Server for LU6.2 connectivity. The following sample displays a sample Brixton 4.1 SNA definition for a token ring-attached workstation. This file template is provided in the directory *d_dir/etc*. The VTAM resource names correspond to the samples given in this appendix:

```
// Brixton BrxPU2.1 SNA Server Sample Configuration - Connect:Direct for UNIX//
CP
NAME = CDUPU01
NQ_CP_NAME = CDUNET.CDUPU01
;
LU
COMMENT = "LOCAL ILU"
NAME = CDULU01
LUTYPE = 6.2
PACING = 0
SESS_LMT = 8
;
TRLINE
COMMENT = "NCP Token Interface"
NAME = NCPTIC
SOURCE_ADDRESS = X'400050000000'
LAN_RATE = RING_16Mbs
;
PU2
COMMENT = "VTAM PU"
NAME = CDUPU01
LINK_NAME = NCPTIC
MAXDATA = 2057
ROLE = Negotiable
TERMINID = X'05700004'
ALS_CONNECT = Active
LMT_RES = No
ACTPU_SUPPRESS = No
RMTTERMINID = X'05700004'
RMTNQ_CP_NAME = CDUNET.HOSTCP
RMTMACADDR = X'400050000004'
;
PTNR_LU
NAME = NDMAPP4
LOC_LU_NAME = CDULU01
INIT_TYPE = INITIATE_OR_QUEUE
;
```

Continued

Continued

```

MODE
NAME = NDM624K
PTNR_LU_NAME = NDMAPP4
DLC_NAME = CDUPU01
SND_MAX_RU_LB = 8
RCV_MAX_RU_LB = 8
PREF_SND_RU = 4096
PREF_RCV_RU = 4096
LCL_MAX_SESS_LMT = 8
MIN_CW_SESS = 4
MIN_CL_SESS = 4
CW_AUTOACT_LMT = 4
AUTOINIT_SL = Yes
;

TP
TP_NAME = NNV2DTF
LOC_LU_NAME = CDULU01
CONV_TYPE = BASIC
SYNC_LVL = CONFIRM
PIP = NO
PRIVILEGE = NONE
;

```

Note: The LU SESS_LMT must be 2 greater than the MODE LCL_MAX_SESS_LMT.

AS400 and NetWare definitions include the following in the DLC directive:

```
RMTNQ_CP_NAME=CDUNET.CP_NAME //Rmt Network Qualified Name
```

After running the Brixton configuration for the AS400 connection, change the AS400 device description to match the **Mode_Name** defined in the Brixton configuration.

SunLink SNA 9.1 for Sun Solaris Configuration Requirements

For SunLink SNA support, use the following procedure to install and configure the SunLink SUNWpu2.1 SNA server software:

- ◆ For SunLink SNA support, configure the following SunLink software packages: SUNWlu62, SUNWgmi, SUNWgman, and SUNWpu21.

Product	Description
SUNWgman	SNA Gateway Manager
SUNWgmi	SNA Graphical Management Interface
SUNWlu62	SNA Logical Unit Type 6.2
SUNWpu21	SNA PU2.1 Server

- ◆ Connect:Direct for UNIX requires that you configure SUNWgman, SUNWgmi, and SUNWpu21 packages.
- ◆ The SUNWgmi (Graphical Management Interface) generates a working configuration that can be altered to match your needs.

Note: This is not an SNA configuration.

1. Type the following commands to run the PU2.1 setup program:

```
# cd /opt/SUNWPU21
```

```
# ./sunsetup
```


The following screen displays a list of tasks:

```
The installation procedure allows you to install:
```

- (1) Configure GMAN Software.
- (2) Configure GMI Software.
- (3) Configure PU21 Software.
- (4) Start GMAN Software.
- (5) Start PU21 Software
- (6) Stop GMAN Software
- (7) Stop PU21 Software
- (8) Show GMAN Configuration
- (9) Show GMI Configuration
- (10) Show PU21 configuration

```
(q) Exit
```

```
Enter selection [q] 1
```

2. Type **1** to configure the SUNWgman software.

The following screen prompts you to change the root directory:

```
The SUNWgman configuration file directory root is currently set to /opt/SUNWgman.
Do you want to change it (Yes/No) [N]?
```

3. Type **n** and press **Enter**.

The setup script prompts you to change the DNS server configuration.

```
The SUNWgman is configured for a site that runs a main DNS server. In this mode,
client systems must be configured to use this system directly to resolve lookups
for resources in the SunLink domain.
```

```
Do you want to change this setting (Yes/No) [N]?
```

4. Type **n** and press **Enter**.

The setup script prompts you to change the DNS domain name.

```
The DNS domain name is currently set to stercomm.com.
Do you want to change it (Yes/No) [N]?
```

5. Type **n** and press **Enter**.

The setup script prompts you to change the startup option.

```
The BrxGMAN product is not set to startup automatically each time your system
reboots.
Do you want to change it (Yes/No) [N]?
```

6. Type **n** and press **Enter**.

The following message prompts you to verify the SUNWgman configuration.

```
The SUNWgman can be configured as follows:
  Installation directory           /opt/SUNWgman
  Working directory                /opt/SUNWgman
  Configuration file directory root /opt/SUNWgman
  SunLink DNS configuration        SUNWgman is primary DNS server
  Full DNS domain name             csg.stercomm.com
  Run startup script at boot       NO

Is this configuration correct (Yes/No) [Y]?
```

7. Do one of the following:

- ◆ If the configuration is correct, type **y** and press **Enter**.
- ◆ If necessary, type new parameters for each option. Type **y** and press **Enter**.

The following screen is displayed:

```
The installation procedure allows you to install:

(1) Configure GMAN Software.
(2) Configure GMI Software.
(3) Configure PU21 Software.
(4) Start GMAN Software.
(5) Start PU21 Software
(6) Stop GMAN Software
(7) Stop PU21 Software
(8) Show GMAN Configuration
(9) Show GMI Configuration
(10) Show PU21 configuration

(q) Exit

Enter selection [q] 2
```

8. To configure the SUNWgmi software, type **2**. The following message prompts you to change the current Help browser.

```
The SUNWgman help browser is currently set to mosaic.
Do you want to change it (Yes/No) [N]?
```

9. Type **n** and press **Enter**. The script prompts you to change the working directory.

```
The SUNWgman working directory is currently set to /opt/SUNWgman.
Do you want to change it (Yes/No) [N]?
```

10. Type **n** and press **Enter**. The script prompts you to verify the configuration.

```

The SUNWgman can be configured as follows:
  Installation directory           /opt/SUNWgman
  Working directory                /opt/SUNWgman
  Help browser type                mosaic
  Help browser pathname/image     mosaic
  Xterm command path              /usr/bin/X11/xterm

Is this configuration correct (Yes/No) [Y]?

```

11. Do one of the following:

- ◆ If the configuration is correct, type **y** and press **Enter**.
- ◆ If necessary, type new parameters for each option. Type **y** and press **Enter**.

The setup script prompts you to select a task:

```

The installation procedure allows you to install:

(1) Configure GMAN Software.
(2) Configure GMI Software.
(3) Configure PU21 Software.
(4) Start GMAN Software.
(5) Start PU21 Software
(6) Stop GMAN Software
(7) Stop PU21 Software
(8) Show GMAN Configuration
(9) Show GMI COnfiguration
(10) Show PU21 configuration

(q) Exit

Enter selection [q] 3

```

12. Type **3** to configure SUNWpu21 and press **Enter**. The setup script prompts you to change the working directory.

```

The SUNWpu21 working directory is currently set to /opt/SUNWpu21.
Do you want to change it (Yes/No) [N]?

```

13. Type **n** and press **Enter**. The setup script prompts you to change the root directory.

```

The SUNWpu21 configuration file directory root is currently set to /opt/SUNWpu21.
Do you want to change it (Yes/No) [N]?

```

14. Type **n** and press **Enter**. The setup script prompts you to change the startup setting.

```

The SUNWpu21 product is not set to startup automatically each time
your system reboots.
Do you want to change it (Yes/No) [N]?

```

15. Type **n** and press **Enter**. The setup script prompts you to verify the configuration.

```
The SUNWpu21 can be configured as follows:
  Installation directory           /opt/SUNWpu21
  Working directory                /opt/SUNWpu21
  Configuration file directory root /opt/SUNWpu21
  Run startup script at boot      YES

Is this configuration correct (Yes/No) [Y]?
```

16. Do one of the following:

- ◆ If the configuration is correct, type **y** and press **Enter**.
- ◆ If necessary, type new parameters for each option. Type **y** and press **Enter**.

The setup script prompts you to select a task.

```
The installation procedure allows you to install:

(1) Configure GMAN Software.
(2) Configure GMI Software.
(3) Configure PU21 Software.
(4) Start GMAN Software.
(5) Start PU21 Software
(6) Stop GMAN Software
(7) Stop PU21 Software
(8) Show GMAN Configuration
(9) Show GMI Configuration
(10) Show PU21 configuration

(q) Exit

Enter selection [q] 4
```

17. Type **4** to start the SUNWgman.

18. Type the following command to start the Graphical Manager and configure SNA LU6.2 definitions.

```
# ./sungmi.sh
```

Sample MVS Definitions for an LU6.2 Connection

This section provides samples of the MVS NCP and VTAM definitions required for LU6.2 connectivity between Connect:Direct for UNIX and Connect:Direct OS/390. A sample Connect:Direct OS/390 network map definition is also included.

Token Ring 3174-R Gateway Controller Configuration

The following figure displays sample line, PU, and LU definitions used by VTAM to define a token ring 3174-R gateway controller for an LU6.2 connection:

```

*****
*       REAL 3174 CONTROLLER, FUNCTIONS AS THE GATEWAY CONTROLLER
*****
D1IRR1  PU ADDR=01,
        DATMODE=HALF,
        MAXDATA=521,
        MAXOUT=7,
        PACING=2,
        PUDR=YES,
        DLOGMOD=SNX32702,
        MODETAB=DALLMTAB,
        USSTAB=LSUSSTAB,
        SSCPFM=USSSCS,
        PUTYPE=2,
        DISCNT=(NO),
        SECNET=NO,
        VPACING=4,
        XID=YES,
        ISTATUS=ACTIVE

*
*                                         COAX PORTS
D1IRR102 LU LOCADDR=2, ISTATUS=ACTIVE
D1IRR103 LU LOCADDR=3, ISTATUS=ACTIVE
D1IRR104 LU LOCADDR=4, ISTATUS=ACTIVE
D1IRR105 LU LOCADDR=5, ISTATUS=ACTIVE
D1IRR106 LU LOCADDR=6, ISTATUS=INACTIVE
D1IRR107 LU LOCADDR=7, ISTATUS=INACTIVE
D1IRR108 LU LOCADDR=8, ISTATUS=INACTIVE
D1IRR109 LU LOCADDR=9, ISTATUS=INACTIVE
*
*   FOR LU6.2 ILU
CDULU01 LU LOCADDR=0, DLOGMOD=NDM621K, RESSCB=5, ISTATUS=ACTIVE
CDULU02 LU LOCADDR=0, DLOGMOD=NDM621K, RESSCB=5, ISTATUS=ACTIVE
CDULU03 LU LOCADDR=0, DLOGMOD=NDM621K, RESSCB=5, ISTATUS=ACTIVE
CDULU04 LU LOCADDR=0, DLOGMOD=NDM621K, RESSCB=5, ISTATUS=ACTIVE
*

```

```

*****
*      DOWNSTREAM PU OFF OF THE REAL 3174 GATEWAY CONTROLLER      *
*      INDEPENDENT LU6.2                                          *
*****
CDUPU01  PU ADDR=02,
          DATMODE=HALF,
          MAXDATA=521,
          MAXOUT=7,
          PACING=2,
          PUDR=YES,
          DLOGMOD=SNX32702,
          MODETAB=DALLMTAB,
          USSTAB=LSUSSTAB,
          SSCPFM=USSSCS,
          PUTYPE=2,
          DISCNT=(NO),
          SECNET=YES,
          VPACING=4,
          ISTATUS=ACTIVE
*
DISPLAY2 LU LOCADDR=2, ISTATUS=ACTIVE
DISPLAY3 LU LOCADDR=3, ISTATUS=ACTIVE

```

The 3174-R token ring gateway requires that the RS/6000 token ring adapter address match the address configured in the 3174-R.

Token Ring 3745 Token Ring Interface Coupler (TIC) Configuration

The following figure displays sample line, PU, and LU definitions used by VTAM to define a token ring TIC for an LU6.2 connection:

```

M1IRGPGP GROUP ECLTYPE=PHYSICAL          PHYSICAL GROUP
* NTRI PHYSICAL LINE DEFINITION
M1IRG  LINE  ADDRESS=(1088,FULL),        LAN                *
          LOCADD=400076543210,          'SOFT' ADDRESS FOR TIC *
          MAXTSL=4060,                  RANGE 265 TO 16732     *
          OWNER=SA01,                   MVS OWNS THIS LINE    *
          NPACOLL=YES,                  NPM                   *
          PORTADD=0,                    WHERE ACRS3LGP POINTS TO *
          RCVBUFC=1440,                 RANGE 6*BFRS TO 4095  *
          ADAPTER=TIC2,                 TIC2                  *
          TRSPEED=4,                   SPEED OF LAN          *
          SPAN=(8000)                   NETVIEW OPERAND
M1IRG1  PU   SPAN=(8000)
M1IRG100 LU  ISTATUS=INACTIVE,          IBM RECOMMENDED       *
          SPAN=(8000)                   NETVIEW OPERAND
M1IRGLGP GROUP ECLTYPE=LOGICAL,         LOGICAL GROUP         *
          CALL=INOUT,                   ALLOW DIAL IN AND DIAL OUT *
          NPACOLL=YES,                  NPM                   *
          OWNER=SA01,                   MVS OWNS THIS LINE GROUP *
          PHYPORT=0,                   POINTS TO ACRS3 LINE PORTADD *
          SPAN=(8000),                 NETVIEW OPERAND      *
          TYPE=NCP                      NETWORK CONTROL MODE
M1IRGT00 LINE AUTOCOPY=(35,M1IRGT01,D)
M1IRGP00 PU  NEXT=(M1IRGP01,D)
          ENDAUTO
*****
*          TOKEN RING NTRI SWITCHED SNA DEFINITION          *
*****
M1T2001 VBUILD TYPE=SWNET
CDUPU01  PU  ADDR=01,                    *
          PUTYPE=2,                      *
          DISCNT=NO,                     *
          MAXOUT=7,                      *
          PASSLIM=7,                     *
          ISTATUS=ACTIVE,                 *
          IDBLK=071,                     *
          IDNUM=43210,                   *
          SSCPFM=USSSCS,                 *
          MODETAB=DALLMTAB,              *
          USSTAB=LSUSSTAB,               *
          DLOGMOD=NDM621K
CDULU01  LU  LOCADDR=0,DLOGMOD=NDM621K,RESSCB=5
    
```

VTAM Application Definition

The following figure shows a VTAM application (APPL) definition for an LU6.2 connection between Connect:Direct OS/390 and Connect:Direct for UNIX:

```

NDMAPP4 APPL ACBNAME=NDMAPP4,          VTAM APPLICATION ID      *
      APPC=YES,                        ENABLE TO RUN LU6.2 SESSIONS *
      AUTH=(ACQ,NOCNM,NOPASS,NOPO,NOTSO,VPACE), APPROXIMATE # OF CONCURRENT SESS *
      EAS=6,                            MODE TABLE NAME        *
      MODETAB=NDMTAB,                  NO UNBIND IN SCIP EXIT  *
      SONSCIP=NO,                      NO SRB PROCESSING       *
      SRBEXIT=NO,                      RECEIVE PACING OF 7     *
      VPACING=7,                       MODE TABLE ENTRY       *
      DLOGMOD=NDMLOGM,                 PARALLEL SESSIONS CAN BE USED *
      PARSESS=YES,                     # OF CONCURRENT LU6.2 SESSIONS *
      DSESLIM=8,                       # OF LOCAL CONTENTION WINNERS *
      DMINWNL=4,                       # OF REMOTE CONTENTION WINNERS *
      DMINWNR=4,                       # OF AUTOMATIC LU6.2 SESSIONS *
      AUTOSSES=4,                      ALLOW CNOS TO DRAIN SESSIONS *
      DDRAINL=ALLOW,                   DEF RESPONSIBILITY FOR LOCAL CNOS*
      DRESPL=ALLOW,
      VTAMFRR=NO

```

VTAM Logmode Table Entries

The following figure displays a sample mode table entry for an LU6.2 connection using a 1-K RU.

```

* LU6.2 LOGMODE
*
NDM621K  MODEENT LOGMODE=NDM621K,          *
      TYPE=1,                             *
      COS=NJE,                             *
      FMPROF=X'13',                        *
      TS_PROF=X'07',                       *
      PRIPROT=X'B0',                      *
      SECPROT=X'B0',                      *
      COMPROT=X'D0B1',                    *
      RUSIZES=X'8787', 1K SEND AND RECV RUSIZE *
      PSERVIC=X'06020000000000000000300'

```

The following figure displays a sample mode table entry for an LU6.2 connection using a 4-K RU:

```

* LU6.2 LOGMODE
*
NDM624K  MODEENT LOGMODE=NDM624K,          *
      TYPE=1,                             *
      COS=NJE,                             *
      FMPROF=X'13',                        *
      TS_PROF=X'07',                       *
      PRIPROT=X'B0',                      *
      SECPROT=X'B0',                      *
      COMPROT=X'D0B1',                    *
      RUSIZES=X'8989', 4K SEND AND RECV RUSIZE *
      PSERVIC=X'06020000000000000000300'

```


NTRI Switched Major Node Definition

The following figure displays a sample token ring NTRI switched SNA definition for an LU6.2 connection between Connect:Direct OS/390 and Connect:Direct for UNIX:

```

*
CDUPU    VBUILD TYPE=SWNET
*
CDUPU01  PU      ADDR=01,                X
          PUTYPE=2,                       X
          IDBLK=071,                      X
          IDNUM=54321,                    X
          SSCPFM=USSSCS,                  X
          MODETAB=DALLMTAB,              X
          USSTAB=RSUSSTAB,              X
          DLOGMOD=NDM621K

```

ILU CDRSC Definitions

The following figure displays a sample VTAM 3.4 CDRSC definition for independent LUs used between Connect:Direct OS/390 and Connect:Direct for UNIX:

```

CDULU    VBUILD TYPE=CDRSC
*
CDULU01  CDRSC  ISTATUS=ACTIVE,          X
               ALSLIST=CDUPU01,        ADJ LINK STATION      X
               MODETAB=DALLMTAB,        LOGON MODE TABLE     X
               DLOGMOD=NDM621K,         LOGON MODE TABLE ENTRY X
               RESSCB=5                  SESSION CONTROL BLOCKS
*
CDULU02  CDRSC  ISTATUS=ACTIVE,          X
               ALSLIST=CDUPU01,        ADJ LINK STATION      X
               MODETAB=DALLMTAB,        LOGON MODE TABLE     X
               DLOGMOD=NDM624K,         LOGON MODE TABLE ENTRY X
               RESSCB=5                  SESSION CONTROL BLOCKS
*
CDULU03  CDRSC  ISTATUS=ACTIVE,          X
               ALSLIST=CDUPU01,        ADJ LINK STATION      X
               MODETAB=DALLMTAB,        LOGON MODE TABLE     X
               DLOGMOD=NDM621K,         LOGON MODE TABLE ENTRY X
               RESSCB=5                  SESSION CONTROL BLOCKS
*
CDULU04  CDRSC  ISTATUS=ACTIVE,          X
               ALSLIST=CDUPU01,        ADJ LINK STATION      X
               MODETAB=DALLMTAB,        LOGON MODE TABLE     X
               DLOGMOD=NDM622K,         LOGON MODE TABLE ENTRY X
               RESSCB=5                  SESSION CONTROL BLOCKS

```

Connect:Direct Remote Node Entry

The following figure displays a sample UNIX remote node definition for the Connect:Direct OS/390 network map. You must specify an LU6.2 logmode entry:

```
ADJACENT.NODE=(PARSESS=(6, 2) -
  (UNIX.LU62.DALLAS, CDULU01, , LU62) -
  LOGMODE=NDM621K -
  ENVIRONMENT=UNIX)
```

Special Considerations

This section identifies special considerations when configuring LU6.2 connections.

Required Changes to the File Specified with the comm.info Parameter

This information applies to the following operating systems:

- ◆ HP SNA
- ◆ SNAP-IX

After you install Connect:Direct for UNIX, the file pointed to by the **comm.info** parameter (default name **host11**) is located in the same directory as the configuration files. This file includes communications information for the SNA configuration.

In order to configure an LU6.2 connection, modify the values for **local_lu**, **remote_lu**, and **mode**. These names must correspond to the names defined in the SNA package. The **local_lu** field is a required field. The following figure displays the contents of the **host11** file:

```
comm.info:\
:local_lu=LOCAL_LU:\
:remote_lu=REMOTE_LU:\
:mode=HOSTMODE:
```

The following figure displays values for **lu** and **mode** that correspond to the sample MVS definitions for an LU6.2 connection as illustrated in *Token Ring 3174-R Gateway Controller Configuration* on page 93.

```
comm.info:\
:local_lu=CDULU01:\
:remote_lu=NDMAPP4:\
:mode=NDM624K:
```

Obtaining Traces for the Brixton LU6.2 API and SunLink P2P

The **trace comm** command also provides Brixton LU6.2 API and SunLink P2P tracing control.

To activate the Brixton LU6.2 API and SunLink P2P traces, type the following command:

```
trace comm level=2|3|4
```

To deactivate the Brixton and SunLink traces, type the following command:

```
trace comm level=0|1
```

Trace files are created in the directory where Connect:Direct for UNIX is started. Refer to the Brixton documentation and the SunLink documentation for additional details.

Stopping Connect:Direct on SNA Systems

When running Connect:Direct for UNIX with the LU6.2 on an HP SNA, AT&T Global Information Solutions SNA, or Brixton SNA system, you must issue the following command to stop Connect:Direct:

```
Direct> stop force;
```

Connectivity Between RS/6000 and AS/400 Systems

To configure RS/6000 to AS/400 connections, run the **cdsnacfg** script on the RS/6000. You must then modify the default AIX SNA Server/6000 configuration to allow the automatic AS/400 configuration to build the appropriate connections.

To modify the default AIX SNA Server/6000 configuration, type the following commands. PUNAME is the PU name typed in the **cdsnacfg** script.

```
chснаobj -t'sna_dlc_token_ring' -b 'no' trdlc11
chснаobj -t'link_station' -w'token_ring' -y 'trdlc11' -a 'no' PUNAME
```

AIX SNA Error Messages

AIX SNA return codes are documented in the *AIX SNA Server/6000: Transaction Program Reference* or in the file `/usr/include/luxsna.h`.

Connect:Direct for UNIX Manual Pages

Connect:Direct provides manual pages for the following topics:

- ◆ Process Manager and server (cdpmgr)
- ◆ Translation Table Generator (ndmxt)
- ◆ Message Manager (ndmmsg)

As system administrator, you have the option of combining Connect:Direct manual pages with UNIX manual pages. This chapter describes how to access Connect:Direct manual pages and identifies the commands that display specific manual pages.

Setting Up Connect:Direct for UNIX Manual Pages

The UNIX operating system organizes all Help into manual (man) pages. For syntax and a description of a UNIX command, type the following command, where *command* is the UNIX command.

```
% man command
```

Combining Manual Pages

Most UNIX systems store online manual pages in /usr/man/man1. Connect:Direct stores its manual pages in *d_dir*/ndm/man1, where *d_dir* is the path name to the Connect:Direct installation directory. To combine the manual pages, type the following command to copy the Connect:Direct manual pages into the UNIX manual pages directory:

```
% cp d_dir/ndm/man1/*.1 /usr/man/man1
```

Note: You must have write privileges to the directory /usr/man/man1 to perform this command.

You can also use symbolic links instead of copying the files. Refer to UNIX manual pages for information on using the UNIX **ln** command to create symbolic links.

Displaying Connect:Direct Manual Pages

Type the following command to access Connect:Direct manual pages that you combined with UNIX manual pages, where *command* can be **cdpmgr**, **ndmxlt**, or **ndmmsg**:

```
% man command
```

Accessing Connect:Direct Manual Pages

The following sections show the commands to display Connect:Direct manual pages on various platforms.

Using MANPATH in the Bourne Shell

On an HP 9000 system, you must set the environment variable, MANPATH, in order to locate the Connect:Direct manual pages.

Note: The value used for setting MANPATH is the typical value used in UNIX systems. Your system can have other localized manual pages that need to be included in the search path. Changing MANPATH is a function of the system administrator.

Type the following command to access Connect:Direct manual pages on a HP9000 using the B shell, where *command* can be **cdpmgr**, **ndmxlt**, or **ndmmsg**:

```
$ MANPATH=/usr/man:/usr/contrib/man:d_dir/ndm/man1
$ export MANPATH
$ man command
```

Using MANPATH in the C Shell

On an HP 9000 system, set the environment variable, MANPATH, in order to locate the Connect:Direct manual pages.

Note: The value used for setting MANPATH is the typical value used in UNIX systems. Your system can have other localized manual pages that need to be included in the search path. Changing MANPATH is a function of the system administrator.

Type the following command to access Connect:Direct manual pages on a HP9000 using the C shell, where *command* can be **cdpmgr**, **ndmxlt**, or **ndmmsg**:

```
% setenv MANPATH /usr/man:/usr/contrib/man:d_dir/ndm/man1
% man command
```

Accessing Manual Pages on an IBM RISC System/6000 or Sun SPARC Platform Using BSDI

Type the following command to access Connect:Direct manual pages on IBM RISC System/6000, or Sun SPARC running the Solaris operating system, if the system is using the BSD version of the **man** command (/usr/ucb/man). The *command* can be **cdpmgr**, **ndmxlt**, or **ndmmsg**.

```
% man -M d_dir/ndm command
```


A

Application Programming Interface (API)

An application that enables End User Applications (EUAs) and the Connect:Direct Command Line Interface (CLI) to interact with the Connect:Direct software.

C

Client

The program that executes commands sent by the CLI/API and sends the results back to the CLI/API. Carries out the Connect:Direct authentication procedure in conjunction with API to determine access to Connect:Direct. Interacts with the PMGR when executing commands.

Command Line Interface (CLI)

A program available to submit Connect:Direct Processes and commands from a command line environment.

Command Manager (CMGR)

The program that executes commands sent by the API and sends the results back to the API. In conjunction with the API, the CMGR carries out the Connect:Direct authentication procedure, which determines if the user name and password are authorized to access the system. CMGR interacts with the PMGR when required by command execution.

Connect Control Center

A centralized management system that provides operations personnel with continuous enterprise-wide business activity monitoring capabilities for Connect:Direct z/OS, UNIX, and Windows servers. It manages multiple Connect:Direct servers to suspend, release, and delete Processes, stops Connect:Direct servers, and views detailed statistics on running or completed Processes. It monitors service levels to view Connect:Direct processing across Connect:Direct z/OS, UNIX, and Windows servers within your network and retrieve information about active and completed

Processes. It receives notification of data delivery events that occur or do not occur as scheduled and defines rules that, based on processing criteria, can generate an alert, send an e-mail notification, generate a Simple Network Management Protocol (SNMP) trap to an Enterprise Management System (EMS), or run a system command. It monitors for alerts, such as a server failure or a Process not starting on time.

Connect:Direct

The family of data transfer software products that distributes information and manages production activities among multiple data centers.

Connect:Direct Browser User Interface

As an alternative to submitting Connect:Direct commands through the command line interface, you can use the Connect:Direct Browser User Interface to create, submit, and monitor Processes from an Internet browser, such as Microsoft Internet Explorer or Netscape Navigator. You can also use the Connect:Direct Browser to perform Connect:Direct system administration tasks, such as viewing and changing the network map or initialization parameters, if you have the appropriate Connect:Direct authority.

Connect:Direct for UNIX

The UNIX implementation of the Connect:Direct product.

Connect:Direct Node

Any computer/workstation running Connect:Direct.

Connect:Direct Process

A series of statements, which can be predefined and stored in a directory, submitted through the API to initiate Connect:Direct for UNIX activity. Examples of Process functions are copying files and running jobs.

D

daemon

The long-running process that provides a service to a client. The PMGR is the Connect:Direct for UNIX daemon.

Diagnostic Commands

Connect:Direct commands that assist in the diagnosis of Connect:Direct software problems.

E

End User Application (EUA)

An application program developed by an end user to accomplish a particular task.

Execution Queue

A logical queue in the TCQ. A Process in the Execution Queue can be transferring data to or from a remote Connect:Direct node or it can be waiting for a connection to the remote Connect:Direct node before it can perform its tasks.

F

File Agent

An application program and component of Connect:Direct. It scans specified directories searching for the presence of a file. When a file appears in a watched directory, Connect:Direct either submits a Process or performs the action specified by the rules for the file.

H

Hold Queue

A logical queue in the TCQ. Processes in the Hold Queue are waiting for operator intervention before they move to the Wait Queue for scheduling.

M

Monitoring Commands

Connect:Direct commands that allow you to display information from the statistics file and the TCQ about Connect:Direct Process execution results.

O

Operational Control Commands

Connect:Direct commands that allow you to submit a Process, change specific characteristics of a Process in the TCQ, remove executing and nonexecuting Processes from the TCQ, and stop Connect:Direct.

P

Process Manager (PMGR)

The long-running Connect:Direct server that initializes the Connect:Direct software, accepts connection requests from Connect:Direct APIs and remote Connect:Direct nodes, creates Command Managers and Session Managers, accepts requests from Command Managers and Session Managers where centralized Connect:Direct functions are required, and terminates Connect:Direct software execution.

PNODE (Primary Node)

The Connect:Direct node on which the Process is being executed. The primary node is also called the controlling or source node, but is not always the sending node because PNODE can be the receiver. Every Process has one PNODE and one SNODE. The submitter of a Process is always the PNODE. If defined in the **netmap.cfg** file, the PNODE name can be 1–16 characters long. If not defined in the **netmap.cfg** file, the PNODE name can be 1–256 alphanumeric characters long.

S

Session

A connection between two Connect:Direct nodes.

Session Manager (SMGR)

Responsible for creating or completing a connection with a remote Connect:Direct node and carrying out the Connect:Direct work to be performed.

SNODE (Secondary Node)

The Connect:Direct node that interacts with the Primary node (PNODE) during Process execution. The Secondary node (SNODE) also can be referred to as the participating, target, or destination node. Every Process has one PNODE and one SNODE. The secondary node is the node participating in Process execution initiated by another node (PNODE). If defined in the **netmap.cfg** file, the SNODE name can be 1–16 characters long. If not defined in the **netmap.cfg** file, the SNODE name can be 1–256 alphanumeric characters long.

T

TCQ Status Value

A two-letter code assigned to a Process by Connect:Direct when the Process is placed on the TCQ. The status of a Process can be examined with a **select process** command.

TCQ (Transmission Control Queue)

A queue that holds all Processes that are submitted to Connect:Direct for UNIX. TCQ contains the following four logical queues:

- ◆ EXECUTION
- ◆ WAIT
- ◆ TIMER
- ◆ HOLD

Timer Queue

A logical queue in the TCQ. Processes on the Timer Queue are waiting for a start time before they move to the Wait Queue for scheduling.

W**Wait Queue**

A logical queue in the TCQ. Processes on the Wait Queue are waiting on a connection to or from the remote Connect:Direct node.

A

- Accessing manual pages 101
- AIX SNA
 - configuration script for Connect:Direct for UNIX 74
 - creating the transaction program profile name 73
 - requirements 73
- API, description 9
- APPC requirements for LU6.2 connectivity 72

B

- Brixton SNA
 - for SUN Solaris support 81

C

- Changing file ownership and permissions 38
- CLI, description 9
- CLI/API configuration file
 - creating 36
 - worksheet 68
- CLI/API, creating a configuration file 36
- Client authentication key file
 - worksheet 70
- Cluster environments 24
 - high-availability and load-balancing 24
 - limitations
 - load-balancing 25
 - preparing to install on 23
 - supported
 - high-availability 24
 - load-balancing 24
 - server 25
 - SNODE 25

CMGR, description 8

- Command
 - cdinst 28, 43
 - change process 14

- delete process 14
- flush process 14
- for TCQ 14
- select process 14
- select statistics 14
- setting up environment variable NDMAPICFG 49
- setting up environment variable NDMAPICFG, from C shell 49
- starting the Connect:Direct for UNIX server 49
- stop 14
- stop force 50
- stopping Connect:Direct LU6.2
 - HP SNA system 50
- submit 14
- trace 14

Command line interface, overview 9

Command manager, overview 8

- Configuration requirements
 - for IBM HACMP 48
 - in a SunCluster 2.2 environment 47, 48
 - in a SunCluster 3.0 environment 47

Configured Security Functions 55, 56

Connect Control Center 105

- Connect:Direct
 - concepts 12
 - defining initialization parameters file 32

Creating a strong access control list file 37

Customization worksheet 62

Customizing, user authorization information file 34

D

Defining high-availability settings 46

- Definition
 - local node 12
 - remote node 12

- Description
 - API 9
 - CLI 9

CMGR 8
network map 14
PMGR 7
SMGR 8
TCQ 13
user authorization 15

E

Environment variables, setting up 49

F

File

CLI/API configuration file 36
client authentication key file 37
initialization parameters file 32
network map file 33
server authentication key file 36
user authorization information file 34

H

High-availability, defining settings 46

I

IBM AIX SNA support

configuration script for Connect:Direct for UNIX 74
creating the transaction program profile name 73
requirements 73

IBM HACMP, configuration requirements 48

Initialization parameters file

customizing 32

Installation

configuration types 23
Connect:Direct for UNIX 23
verifying 49

Installing Connect:Direct on the Linux S/390 operating system 26

L

limitations

high-availability 24

Link types, for LU6.2 connectivity 72

Linux for S/390 operating system, installing on 26

Local node

definition of 12
in network map 14

Local Node Security Feature Definition Worksheet 55

LU6.2 connectivity

APPC requirements 72
configuration requirements 72
configuring 46
configuring SNA support 92
creating a remote node information record 33
for AIX SNA support 73
for Brixton SNA for Sun Solaris support 81
link types 72
recommended pacing values 72
recommended RU sizes 72
supported connections 71

M

Manual pages

combining 101
displaying combined manual pages 102
displaying on AT&T GIS systems using BSD 103
displaying on HP9000 using Bourne shell 102
displaying on HP9000 using C shell 102
displaying on IBM RISC/6000 103
displaying on SUN Sparc 103

max.age, parameter 17

N

Network map file

creating a remote node information record 33
description 14
worksheet 69

P

Pacing values, for LU6.2 connectivity 72

PMGR, description 7

Process restart, overview 16

Process statements, listed 13

Process, samples 17

R

Remote node

definition of 12
in network map 14

Remote node information record
 creating 19
 worksheet 69
 RU sizes for LU6.2 connectivity 72

S

Sample MVS definitions for LU6.2 connections
 ILU CDRSC definitions 97
 NTRI switched major node definition 97
 Token Ring 3174-R Gateway Controller
 Configuration 93
 Token Ring 3745 Token Ring Interface Coupler (TIC)
 Configuration 95
 VTAM application definition 96
 VTAM logmode table entries 96

Samples
 MVS definitions 92
 Processes 17
 shell scripts 18

Security
 client authentication key file 37
 client authentication key file worksheet 70
 customizing the user authorization information file 34
 server authentication key file 36
 server authentication key file worksheet 70

Server authentication key file
 created 36
 worksheet 70

Session manager, overview 8

Setting environment variables, NDMAPICFG 49

Shell script, samples 18

SMGR, description 8

SNA LU6.2 connectivity
 APPC requirements 72
 configuration requirements 72
 configuring SNA support 92
 creating a remote node information record 33
 for Brixton SNA for SUN Solaris support 81
 recommended pacing values 72
 recommended RU sizes 72
 sample Brixton BrxPU2.1 configuration 86
 supported connections 71

Special considerations, connectivity between RS/6000
 and AS/400 systems 99

Sterling Control Center 10

Stopping Connect:Direct, SNA systems 99

Strong access control file, creating 37

Suncluster 2.2, configuration 47, 48

SunCluster 3.0 environment, additional configuration
 requirements 47

T

TCQ, description 13

Terminating a procedure 27

Transaction program profile name, for AIX SNA
 support 73

U

User authorization information file
 customizing 34
 description 15
 Worksheet 63

V

Verifying, the installation 49

W

Worksheet
 client authentication key file 70
 Customization worksheet 62
 Installation 62
 installation worksheet 62
 network map remote node information file 69
 server authentication key file 70
 User authorization information file 63

Worksheets
 local node definition 55

Copyright © 1999-2006
Sterling Commerce, Inc.
ALL RIGHTS RESERVED

STERLING COMMERCE SOFTWARE

TRADE SECRET NOTICE

THE CONNECT:DIRECT(c) UNIX Version 3.8 SOFTWARE ("STERLING COMMERCE SOFTWARE") IS THE CONFIDENTIAL AND TRADE SECRET PROPERTY OF STERLING COMMERCE, INC., ITS AFFILIATED COMPANIES OR ITS OR THEIR LICENSORS, AND IS PROVIDED UNDER THE TERMS OF A LICENSE AGREEMENT. NO DUPLICATION OR DISCLOSURE WITHOUT PRIOR WRITTEN PERMISSION. RESTRICTED RIGHTS.

This documentation was prepared to assist licensed users of the Sterling Commerce Connect:Direct Select software. The Sterling Commerce Software, the related documentation and the information and know-how it contains, is proprietary and confidential and constitutes valuable trade secrets of Sterling Commerce, Inc., its affiliated companies or its or their licensors (collectively "Sterling Commerce"), and may not be used for any unauthorized purpose or disclosed to others without the prior written permission of Sterling Commerce. The Sterling Commerce Software and the information and know-how it contains have been provided pursuant to a license agreement which contains prohibitions against and/or restrictions on its copying, modification and use. Duplication, in whole or in part, if and when permitted, shall bear this notice and the Sterling Commerce, Inc. copyright legend.

Portions of the Sterling Commerce Software may include products, or may be distributed on the same storage media with products, ("Third Party Software") offered by third parties ("Third Party Licensors"). Sterling Commerce Software may include Third Party Software covered by the following copyrights: Copyright © 1997-2005 Certicom Corp.
Copyright © 1999-2004 Hewlett-Packard Development Company. Copyright © IBM Corporation, 1996-2005.
Copyright © 1995-2005 Jean-loup Gailly and Mark Adler. Copyright © 1998-2005 The OpenSSL Project.
Copyright © 1996, 2004 Oracle. Copyright © 1992-2004 SNMP Research International, Inc.
Copyright © 1995-2005 Sun Microsystems, Inc. All rights reserved by all listed parties.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com). This product includes software the copying and distribution of which is done with the permission of SNMP Research International, Inc. This product contains Runtime Modules of IBM(r) 32-bit SDK for AIX(tm), JAVA(tm) 2 Technology Edition, Version 5 Copyright © IBM Corporation, 1996-2005.

As and when provided to any governmental entity, government contractor or subcontractor subject to the FARs, the Sterling Commerce Software is provided with RESTRICTED RIGHTS under Title 48 CFR 52.227-19. Further, as and when provided to any governmental entity, government contractor or subcontractor subject to DFARS, the Sterling Commerce Software is provided pursuant to the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation. Those portions of the Sterling Commerce Software which include, or are distributed on the same storage media with, the Third Party Software where use, duplication, or disclosure by the United States government or a government contractor or subcontractor, are provided with RESTRICTED RIGHTS as set forth in the Third Party Licensor's product specific terms.

References in this manual to Sterling Commerce products, programs, or services do not imply that Sterling Commerce intends to make these available in all countries in which Sterling Commerce operates.

Printed in the United States of America

WARRANTY DISCLAIMER

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as described in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Ster-

ling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

As set forth in the README file located at [insert file locator path here] ("Read Me file"), certain of the Third Party Licensors assert specific terms with respect to their respective products. Such terms shall only apply as to the specific Third Party Licensor product and not to those portions of the product derived from other Third Party Licensor products or to the Sterling Commerce Software as a whole. Except as otherwise described in the README file, the Third Party Software is provided 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. FURTHER, IF YOU ARE LOCATED OR ACCESSING THIS SOFTWARE IN THE UNITED STATES, ANY EXPRESS OR IMPLIED WARRANTY REGARDING TITLE OR NON-INFRINGEMENT ARE DISCLAIMED. Additionally, certain Third Party Licensor product terms and information are set out below. Such terms shall only apply as to the specific Third Party Licensor product and not to those portions of the product derived from other Third Party Licensor products or to the Sterling Commerce Software as a whole.

HEWLETT PACKARD

The Sterling Commerce Software is distributed on the same storage media as the Hewlett-Packard Software which contains Java Runtime Environment 1.4.2 for Tru64 and 1.5 HP-UX PA-RISC and HP-UX Integrity, Copyright © 1999-2004 Hewlett-Packard Development Company (collectively the "HP JRE Software"). All Rights Reserved. Additional license information is located at <Connect:Direct install dir>\jre\LICENSE [INSERT DIRECTORY LOCATION FOR EACH PRODUCT] and applies only to the HP JRE Software and not to the Sterling Commerce Software or to any other Third Party Software.

If the HP JRE Software is licensed for use in the performance of a U.S. government prime contract or subcontract, you agree that, consistent with FAR 12.211 and 12.212, commercial computer software, computer software documentation and technical data for commercial items are licensed under HP's standard commercial license.

You will only find the JRE license information for the HP JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on a HEWLETT PACKARD system.

IBM

The Sterling Commerce Software is distributed on the same storage media as the IBM software which contains Java Runtime Environment 1.5 for AIX and Linux zSeries, Copyright © 1998-2005 IBM Corporation (collectively "IBM JRE Software"). All Rights Reserved. Additional license information is located at <Connect:Direct install dir>\jre\LICENSE [INSERT DIRECTORY LOCATION FOR EACH PRODUCT] and applies only to the IBM JRE Software and not to the Sterling Commerce Software or to any other Third Party Software.

U.S. Government Users Restricted Rights- Use, duplication or disclosure restricted by the GSA ADP Schedule Contract with the IBM Corporation.

You will only find the JRE license information for the IBM JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on an IBM system.

OPENSSL SOFTWARE

The Sterling Commerce Software includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>), ("OpenSSL Software"). The OpenSSL Software is subject to the following license terms:

Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright

notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to

endorse or promote products derived from this software without prior written permission. For written permission, please contact
openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following

acknowledgment:

"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

ORACLE CORPORATION

The Sterling Commerce Software is distributed with or on the same storage media as the Oracle Help for Java Software provided by Oracle Corporation, Copyright (c) 1996, 2004 Oracle Corporation ("Oracle Software"). The License relating to the Oracle Software is included in the directory file located at: [INSERT FILE NAME/LINK]. Such license applies only to the Oracle Software which is the subject of such directory and does not apply to the Sterling Commerce Software or to any other Third Party Software.

Restricted Rights

The Oracle Software is provided under restricted rights. If you are (or if you distribute a license to) the United States government, the Oracle Software, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

SUN MICROSYSTEMS

SUN, Sun Microsystems, Solaris, Java, Jini, Forte and iPlanet and all related trademarks,

service marks logos and other brand designations that are referred to or displayed in the Sterling Commerce Software or the related documentation are trademarks or registered trademarks of Sun Microsystems, Inc.

The Sterling Commerce Software is distributed on the same storage media as the JAVA (tm) 2 Runtime Environment (J2RE) Standard Edition, Version 1.5 for Solaris-Sparc, Solaris-i586 and Linux-i586, Copyright © 1999-2006 Sun Microsystems, Inc. (collectively "Sun JRE Software"). All Rights Reserved. The license terms for the Sun JRE Software are located at <Connect:Direct install dir>\jre\LICENSE [INSERT DIRECTORY FOR ALL THREE PRODUCTS]. The Sun JRE Software includes the following notice: "Additional copyright notices and license terms applicable to portions of the Sun JRE Software are set forth in the THIRDPARTYLICENSE-README.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Sun JRE Software in this distribution."

The Sun JRE Software license terms for also require the inclusion of the following notice:
"This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/ico4j/>."

If [Sun JRE] Software is being acquired by or on behalf of the U.S> Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in [Sun JRE] Software and accompanying documentation will be only as set forth in this agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

You will only find the JRE license information for Sun JRE Software in the specified directory if the Sterling Software and Third Party Software are installed

on a SUN system.

SUN MICROSYSTEMS (Java Help 1.1.3 Authoring Tool))

The Sterling Commerce Software is distributed on the same storage media as the jh.jar and jhall.jar software (together, the "Sun Software"). Use of the Sun Software is subject to a license which can be found at http://java.sun.com/products/javahelp/download_binary.html#download.

ZLIB SOFTWARE

All source code, binaries, documentation and other files distributed with the zlib 1.1.3 Software are subject to the following license terms, and are held under the following copyright notice, unless otherwise noted within the individual files.

zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be

appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly
jloup@gzip.org

Mark Adler
madler@alumni.caltech.edu

CDunix 3.8 readme_v1