HP OSI Troubleshooting Guide

HP 9000 Networking

Edition 6

32070-90031

E0597

Printed in: United States

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Copyright Notices.

Trademark Notices

Contents

1. Interoperability Testing

Testing FTAM Interoperability 12
FTAM Interoperability Testing 12
FTAM Pre-Test Checklist 13
FTAM Interoperability Testing 14
FTAM Connectivity Test 14
FTAM File Transfer Test 15
Interpreting FTAM Errors 16
Testing APRI Interoperability 18
APRI Pretest Checklist 19
Running APRI Tests (Client Mode) 20
Running APRI Tests (Server Mode) 21
Interpreting APRI Errors 22
Testing Session Interoperability 24
Session Pre-Test Checklist 25
Running Session Tests (Client Mode) 26
Running Session Tests (Server Mode) 27
Interpreting Session Errors 28
Testing Transport Interoperability 30
Transport Pre-Test Checklist 31
Running Transport Tests 32
Interpreting Transport Errors 33
Testing LAN (802.3 or FDDI) Interoperability 34
LAN Pre-Test Checklist 35

Contents

Running LAN Tests 36
Interpreting LAN Errors 37
Testing X.25 Interoperability. 39
X.25 Pre-Test Checklist 40
Running X.25 Tests 41
Interpreting X.25 Errors 42
Reason and Refuse Codes 44
Protocol Reason Codes 44
Session Refuse Codes 51
To Create A Result File 52

2. Problem Solving

Basic Steps 54
Interpreting Errors 55
Checking System Status 56
Status Check 1 56
Status Check 2 56
Status Check 3 56
Status Check 4 57
Status Check 5 57
Running Verification Tests 58
Link Verification 58
OTS Transport Verification 59
Service Verification 59
Collecting Troubleshooting Data. 61
Tracing and Logging through `/opt/ots/bin/osidiag` 62
Tracing and Logging User Applications 63

Contents

Common Configuration Mistakes 65
ots_dests Common Mistakes 65
ots_subnets Common Mistakes 65
ots_parms Common Mistakes 66
local_app Common Mistakes 66
remote_app Common Mistakes 66

Common Logged Errors 67

Submitting Problem Information to HP 70

3. Using OSI and OTS Tools

OSIADMIN 72

Managing Your Configuration 74
Using osiconf 74
Using osiconfchk 74

OSI Diagnostics 76

Starting and Stopping OSI 78
osistart Command 78
Stopping OSI 79
osistat Command 79

Starting OTS: otsstart 80
Syntax 80
Example 80
Recovering from otsstart Failure 81

Checking OTS Status: otsstat 82
Syntax 82
Example 1 83
Example 2 83
Example 3 83

Contents

Updating OTS: `otsupdate` 84

Dynamic Routing Commands 85
End System Commands 85
Intermediate System Commands. 86
ES/IS Parameters 87
Route Commands 89
Route Command Parameters 90
Route Command Options 91
NSAP Commands 91

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. the manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Edition 1	June 1989
Edition 2	April 1991
Edition 3	March 1992
Edition 4	January 1995
Edition 5	July 1996
Edition 6	May 1997

1 Interoperability Testing

Processes for verifying and troubleshooting communication between your local HP node and another node on the network.

Testing FTAM Interoperability

Use the following procedures to test FTAM Interoperability.

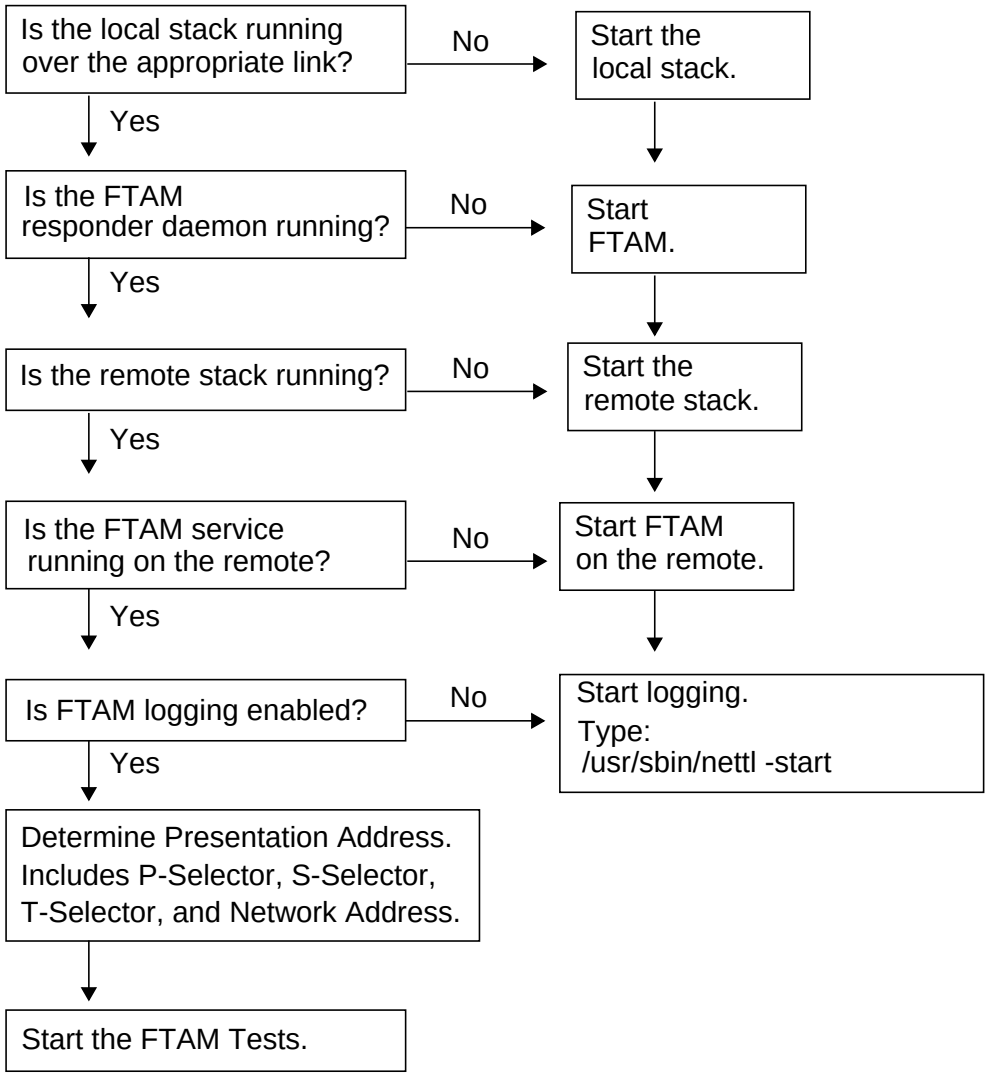
FTAM Interoperability Testing

1. Log on as root.
2. Perform the pre-test checklist.
3. Create a result file.
4. Perform FTAM tests.
5. If `osidiag` cannot find a default local application title, perform "Specifying Application Titles."
6. Interpret errors.

FTAM Pre-Test Checklist

Check the following before attempting to run the FTAM tests.

Figure 1-1 FTAM Pre-Test Checklist



FTAM Interoperability Testing

This procedure invokes FTAM through `osidiag` to provide as much information as possible about errors that might occur.

FTAM Connectivity Test

The steps below describe how to test FTAM connectivity between the local and remote node.

1. From root, type `osidiag` and select "FTAM TESTS."
2. Create a result file.
3. Select "Connect" from the FTAM menu.
4. Enter Initiator Identification (your login information for the remote node).
   - Change ID field from local login name to remote unless login on remote is the same.
   - Enter initiator password associated with remote login.
5. Press `Done`.
6. Enter Presentation Address for remote node.
7. Go to the "FTAM File Transfer Test" on page 15.

FTAM File Transfer Test

After a successful FTAM connect test. Follow the steps below to do an FTAM file transfer.

1. From the FTAM menu, create a new result file.
2. Select “Low Level Transfer.”
3. The initiator ID parameters are displayed.
   a. Leave first ID set to local login.
   b. Set first password to your local password.
   c. Leave second set unchanged.
   d. Press Done.
4. Leave source Presentation address unchanged. Press Done.
5. Leave destination address unchanged. Press Done.
6. If your system has a “message of the day” configured, leave the source and destination file names unchanged. If your system does not have a “message of the day” configured, overwrite the source file name with a valid name.
7. Check “TEST STATUS” near the end of the report.

   If the status is “PASSED,” FTAM verification is complete.

   If the status is “FAILED,” see “Interpreting FTAM Errors” on page 16, make your corrections, then re-run this test.

Interpreting FTAM Errors

Table 1-1 may help you to find what caused your FTAM test to fail.

1. Check the field labeled “Diagnostic”.

   If this field is present, look for a text string labeled “further details” for the cause.

2. Look at the line after “FAILED”. The operation that failed is listed.

Table 1-1 FTAM Call Errors

FTAM Call	Reason	Corrective Action
`ft_aeactivation()`	FTAM not correctly installed.	Run `swverify` on the FTAM fileset to verify that all components are installed.
	OTS stack not up.	Run the Status operation under Session or Transport to verify.
`ft_connect()`	Incorrect address specified.	Recheck the value of the Presentation address specified and the value configured for the remote.
	Incorrect User ID.	Check user name and password, usually corresponds to the remote.
	Remote stack not up.	Recheck stack.
	Responder not running.	Repeat the verification described in the pre-test section.
	Lower Layer Problem.	Go back to the step you were on and continue.
`ft_select()`	Incorrect source file name.	Check the source file name and correct.

FTAM Call	Reason	Corrective Action
`ft_create()`	Permission problem or incorrect directories were specified in the path for the destination file name.	Check the permissions and the directories specified.
`ft_sdata()`	Transfer file too large. (Error code 101 Buffer too large error).	Rerun the test with a smaller file or use the High Level Transfer test.
`ft_xxx()`	Uncommon points of error; or, if an abort indication is received, the remote went down for some reason.	Check the remote stack and FTAM responder if an abort indication is indicated.

Testing APRI Interoperability

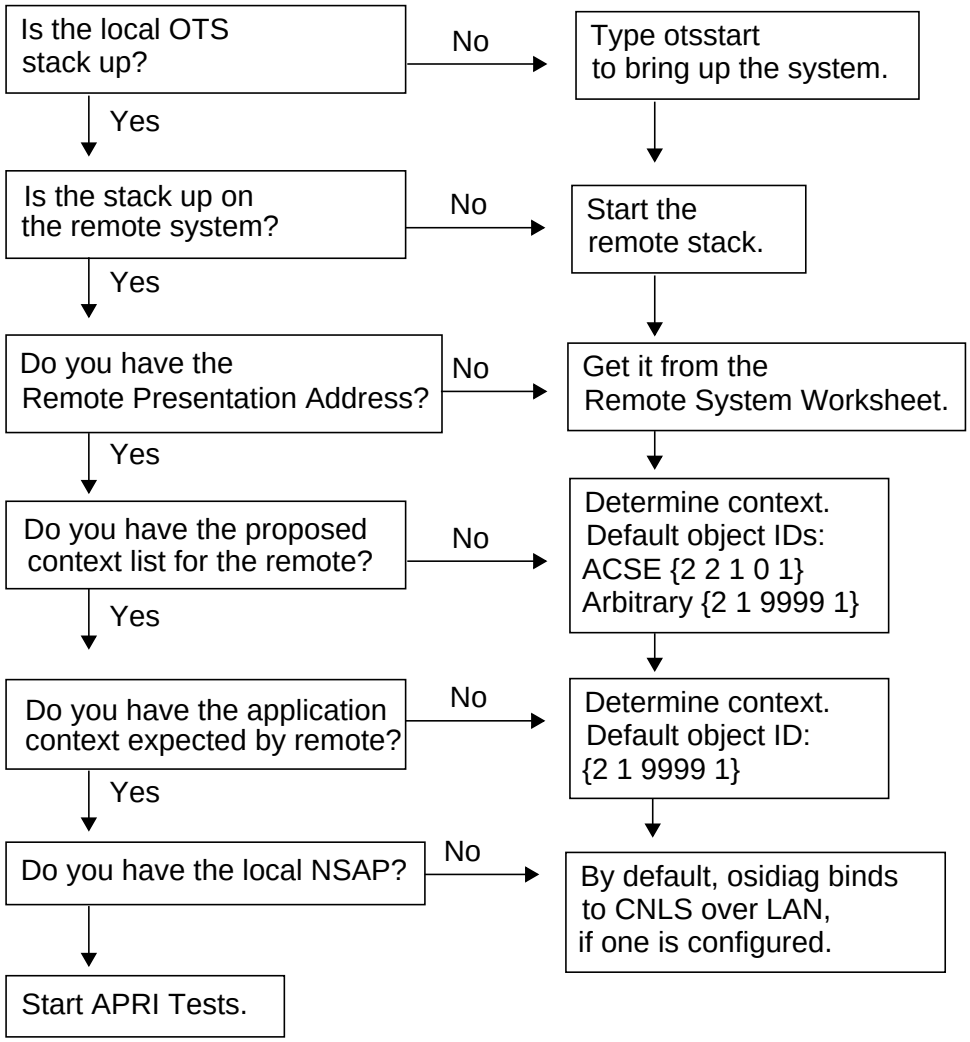
The steps below describe how to test the ACSE/Presentation and ROSE (APRI) layer connectivity between the local and remote node. Use this only if you are developing APRI programs and wish to verify connectivity at this layer.

1. Log on as root.
2. Perform the pre-test checklist.
3. Perform APRI test - Client Mode.
4. Perform APRI test - Server Mode (optional).
5. If `osidiag` cannot find a default local application title, perform "Specifying Application Titles."
6. Interpret errors.

APRI Pretest Checklist

Check the following before attempting the APRI Interoperability tests.

Figure 1-2 APRI Pre-Test Checklist



Running APRI Tests (Client Mode)

The following steps verify APRI connectivity and interoperability with a remote node.

If the remote is not capable of receiving connections, or you want to test the remote's ability to establish connections, follow the instructions in "Running APRI Tests (Server Mode)" on page 21.

1. From root, type `/opt/ots/bin/osidiag` and select "ACSE/Presentation or ROSE Tests."
2. Create a result file.
3. Make sure a server application is running on the remote. Then, select "Connect" from the Test Case menu.
4. Enter Presentation Address when prompted.

NOTE `osidiag` will display the local address by default. The default P, S, and T selectors are given in ASCII surrounded by double quotes. If the address you must use is specified in hexadecimal rather than ASCII, then omit the double quotes (for example, 22003176).

5. Enter Proposed Contexts when prompted.
6. Enter Application Context when prompted.
7. For ROSE only: Enter the context identifiers when prompted.
8. Check the "TEST STATUS" near the end of the report.

   If the status is "PASSED," you have successfully communicated with the remote node and are finished with this section.

   If the status is "FAILED," see "Interpreting APRI Errors" on page 22, and find problem.

   If you find the error, rerun this test.

   If you cannot find the error, enable tracing. See "Tracing and Logging through /opt/ots/bin/osidiag" on page 62 for more information.
9. Go to the APRI Tests (Server Mode). (Optional)

Running APRI Tests (Server Mode)

If the remote is not capable of receiving connections, or you want to test the remote's ability to establish connections, follow these instructions.

1. From root, type `/opt/ots/bin/osidiag -w 300` (the `-w 300` allows 300 seconds to get the client ready once the server is started), and select "ACSE/Presentation or ROSE Tests."
2. Create a result file.
3. Select "Server..." from the Test Case menu.
4. For ROSE only: Enter the Presentation context identifiers to be used as ROSE contexts.
5. For ROSE only: Leave the autorespond to ROSE default set to "Y".
6. Generate the connection from the client side via the remote application. Follow steps in the APRI Tests (Client Mode) if an HP system.
7. Check the "TEST STATUS" near the end of the report.

   If the status is "PASSED," you have successfully communicated with the remote node and are finished with this section.

   If the status is "FAILED," see "Interpreting APRI Errors" on page 22, and find the problem.

   If you find the error, rerun the server test and rerun the client test on the remote to connect to this server.

   If you cannot find the error, enable tracing on the local node. See "Tracing and Logging through /opt/ots/bin/osidiag" on page 62 for more information.

Interpreting APRI Errors

Table 1-2 describes possible errors and corrective actions if an error occurs during a call to APRI.

Table 1-2 APRI Call Errors

APRI Call	Reason	Corrective Action
`ap_open()`	Incorrect installation or OTS stack is not up.	Run `otsstat` to see if OTS stack is up. Run `otsstart` to start OTS stack.
`ap_set_env()`	Incorrect address specified. (parameter *ap_my_psap*)	Recheck the value of *ap_my_psap*.
`ap_poll()`	Time out (`osidiag` defaults to 30 seconds for indication or confirmation).	Increase time if needed.
	Unanticipated primitive (`osidiag` received an indication it did not expect.)	Check `osidiag` display immediately after the call to `ap_poll()`.
`ap_rcv(A_PABORT_IND)`	Incorrect remote address.	Recheck remote address; check that local NSAP is on same subnet as the destination system.
`ap_rcv(A_ABORT_IND)`	The application on top of the Presentation layer detected some problem. An abort may also be sent by the HP provider if the specified address is valid, but no process is currently accepting connections.	Examine the output of the remote application for further information as to why the abort was sent.

APRI Call	Reason	Corrective Action
`ap_rcv(A_ASSOC_CNF)`	Your connect request arrived at the remote, but the remote did not like one of your proposed values or it is not available to service connections. The confirmation carries three pieces of information: the result, the source (if rejected), and a diagnostic code.	Examine the diagnostic code for the course of action.
`ro_bind()`	The values you specified are not compatible with those negotiated.	Verify that the values for *ap_p_ctx_list* and *rose_pci_list* are consistent.

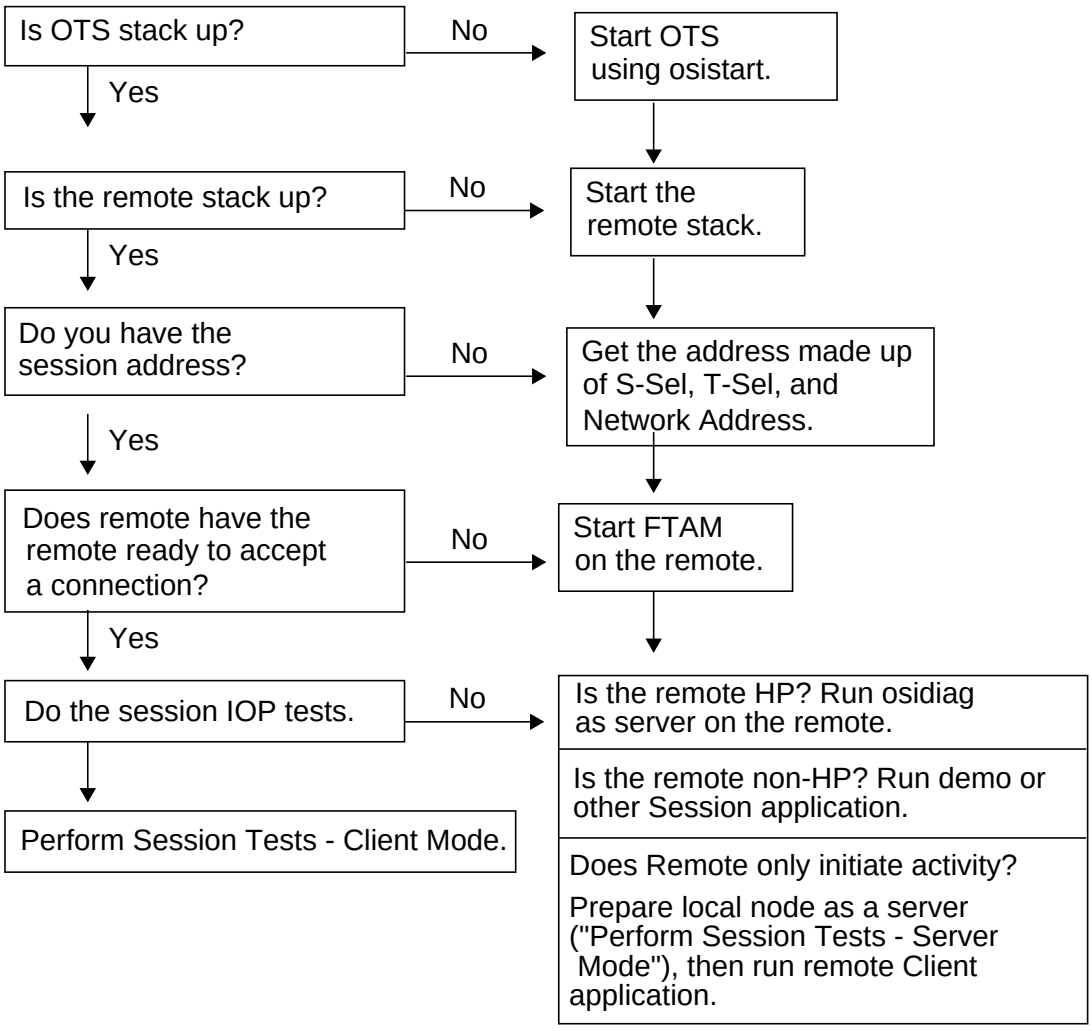
Testing Session Interoperability

The steps below describe how to test the session layer connectivity between the local and remote node. Use this only if you are developing session programs and wish to verify connectivity at this layer.

1. Log on as root.
2. Perform the pre-test checklist.
3. Perform Session tests - Client Mode.
4. Perform Session tests - Server Mode (optional).
5. If `osidiag` cannot find a default local application title, perform "Specifying Application Titles."
6. Interpret errors.

Session Pre-Test Checklist

Figure 1-3 Session Pre-Test Checklist



Running Session Tests (Client Mode)

Normally you use this list of steps to verify connectivity and interoperability with a remote node. If the remote is not capable of receiving connections, or you wish to test the remote's ability to establish connections, follow the instructions in "Running APRI Tests (Server Mode)" on page 21.

1. From root, type `/opt/ots/bin/osidiag` and select "Session Tests."
2. Create a result file.
3. Make sure a server application is running on the remote, then: Select "Connect" from the Test Case menu.
4. Enter the destination Session Address when prompted. NOTE: `osidiag` will display the local address by default.
5. Check the "TEST STATUS" near the end of the report.

   If the status is "PASSED," you have successfully communicated with the remote node and are finished with this section.

   If the status is "FAILED," see "Interpreting Session Errors" on page 28 to find the problem.

   If you find the error, rerun this test.

   If you cannot find the error, enable tracing. See "Tracing and Logging through /opt/ots/bin/osidiag" on page 62.
6. Go to "Running APRI Tests (Server Mode)" on page 21 (Optional).

Running Session Tests (Server Mode)

If the remote is not capable of receiving connections, or you wish to test the remote's ability to establish connections, follow these instructions.

1. From root, type `/opt/ots/bin/osidiag -w 300` (the `-w 300` allows 300 seconds to get the client ready once the server is started), and select “Session Tests”.
2. Create a result file.
3. Select “Server...” from the Test Case menu.
4. Generate the connection from the client side via the remote application. Follow steps in “Running APRI Tests (Client Mode)” on page 20, if an HP system.
5. Check the “TEST STATUS” near the end of the report. If the status is “PASSED,” you have successfully communicated with the remote node and are finished with this section.

   If the staus is “FAILED,” see “Interpreting Session Errors” on page 28.

   If you find the error, rerun the server test, then rerun the client test on remote to connect to this server.

   If you cannot find the error, enable tracing on the local node. See “Tracing and Logging through /opt/ots/bin/osidiag” on page 62.

Interpreting Session Errors

Table 1-3 describes possible errors and corrective actions. The list is sorted by the name of the function producing the error. The names are displayed by `osidiag` on the line immediately after the test status.

Table 1-3 Session Call Errors

Session Call	Reason	Corrective Action
`osi_init()`	Usually lack of available swap space.	Add swap space as necessary.
`osi_rgr_rq()` `osi_rgr_cf()`	Possibly stack is not up. Another application is already listening on this address or has requested exclusive access to this address.	Check to see if stack is up. See if another applications is using this address or has exclusive access.
`osi_get_event()`	Two common errors: 1. Time out - `osidiag` only waits 30 seconds by default. May indicate that the remote is not sending any response to your request. 2. Unanticipated primitive - `osidiag` received an indication that it did not expect.	Verify that the remote is indeed performing its end of the dialog. If the timeout is too short, it may be changed under the utilities menu. The name of the indication will be displayed immediately after the call to `osi_get_event()`.
`ses_pabort_id()`	Used to decode an incoming provider abort indication. For more information see “Protocol Reason Codes” on page 44. The reason code appears in the middle of the `osidiag` output.	Check the reason code and correct accordingly.

Session Call	Reason	Corrective Action
`ses_uabort_id()`	Used to decode incoming abort indication. Indicates the application on top of the Session layer detected some problem.	Examine the output of the remote application for further information as to why the abort was sent.
`ses_connect_rf()`	Called to decode a refusal to connection request. Indicates that your connect request arrived at the remote, but remote did not like one of your proposed values or it is not available to service connections. The refuse code is displayed in the middle of the `osidiag` output.	Check the remote to see if it is available to service connections. Also check your proposed values. For more information on disconnect codes and suggested actions, See “Interpreting Transport Errors” on page 33.

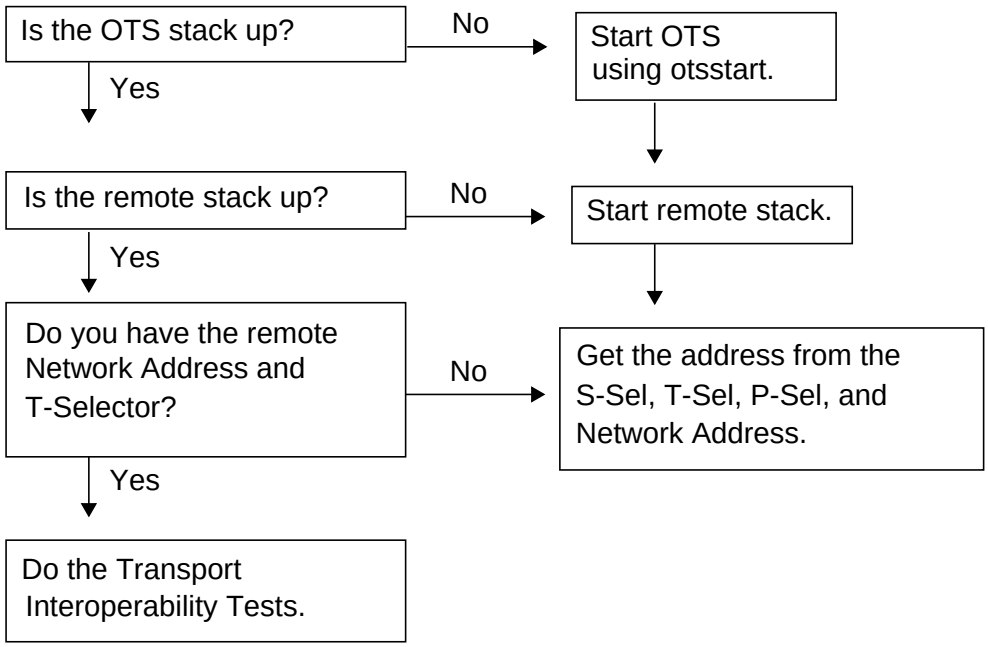
Testing Transport Interoperability

The steps below describe how to test Transport layer connectivity between the local and remote node.

1. Log on as root.
2. Perform the pre-test checklist.
3. Perform Transport tests.
4. If `osidiag` reports “FAILED”, see “Interpreting Transport Errors” on page 33.

Transport Pre-Test Checklist

Figure 1-4 Transport Pre-Test Checklist



Running Transport Tests

1. From root, type `/opt/ots/bin/osidiag` and select “Transport Tests.”
2. Create a result file.
3. Make sure a server application is running on the remote, then select “Connect” from the Transport Tests menu.
4. Enter the destination Transport Selector and Network Address when prompted. NOTE: `osidiag` will display the local address by default. The default P, S, and T selectors are given in ASCII surrounded by double quotes. If the address you must use is specified in hexadecimal rather than ASCII, then omit the double quotes (for example, 22003176). If you are testing RFC1006 interoperability, enter the RFC1006 NSAP for the remote system.
5. Check the “TEST STATUS” near the end of the report.

   If the status is “PASSED,” you have successfully communicated with the remote node and are finished with this section.

   If the status is “FAILED,” see “Interpreting Transport Errors” on page 33 to find the problem.

   If you find the error, rerun this test.

   If you cannot find the error, enable tracing. See “Tracing and Logging through /opt/ots/bin/osidiag” on page 62.

Interpreting Transport Errors

The following are possible situations you may currently find yourself in.

Transport problem corrected.

If you have made a change that corrected your Transport problem, then return to the Service Layer test that originally failed and try again.

Configuration or other change required.

If the corrective action in the following sections require you to change a configuration parameter or make some other change, then do so and rerun the Transport test.

Problem persists.

If you have been unsuccessful in correcting the problem, gather the information you have collected to provide to your HP support representative.

Table 1-4 Transport Call Errors

Error	Reason	Action
`t_open()`	The stack is most likely not up.	Run status operation under Transport menu.
`t_bind()`	Failed to associate an address with the transport endpoint. Likely a parameter error. Link supporting this address went down.	Verify that the parameter *tp_my_tsap* is set to "`diagt`" or "`diagt.`*NSAP*" where NSAP is valid local address. Run status operation under Transport menu.
`t_rcvdis()`	Called to decode a disconnect indication.	Check online error messages.
`t_look()`	Remote stack does not respond for default time.	Check to see if one node is configured as NULL internet and other is not. Check for incorrect remote network address.

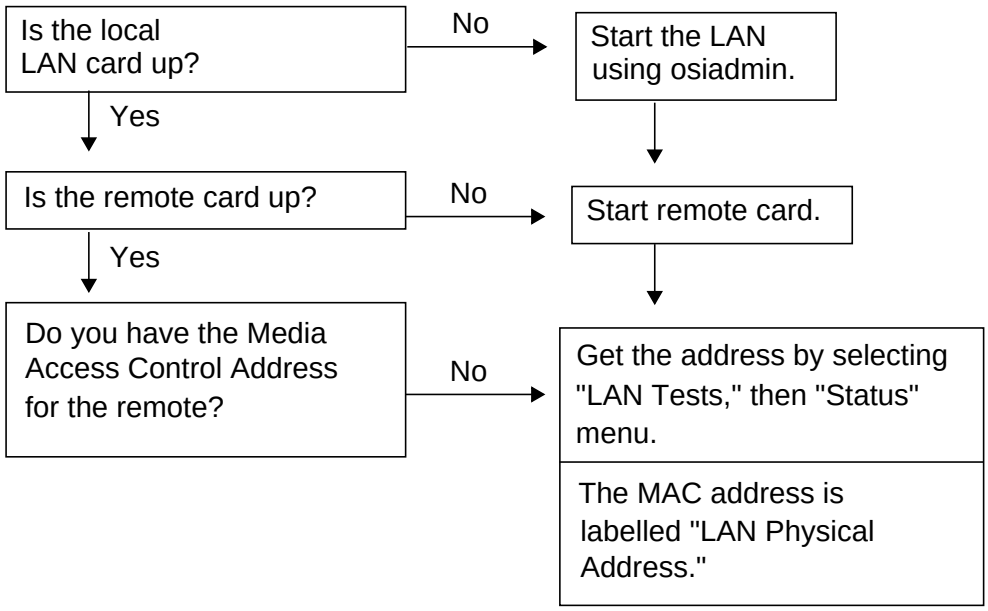
Testing LAN (802.3 or FDDI) Interoperability

The steps below describe how to test connectivity at the Link level (either 802.3 or FDDI LAN) between the local and remote node.

1. Log on as root.
2. Perform the pre-test checklist.
3. Perform LAN test.
4. If `osidiag` reports “FAILED,” see “Interpreting LAN Errors” on page 37.

LAN Pre-Test Checklist

Figure 1-5 LAN Pre-Test Checklist



Running LAN Tests

1. From root, type `/opt/ots/bin/osidiag` and select “LAN Tests.”
2. Create a result file.
3. Select “Test Frames.”
4. Enter the interface name to issue the test from (lan0, lan1, etc.). The default from the `ots_subnets` file can be used unless you have multiple I/O Cards.
5. Enter the value previously retrieved for the remote MAC address in hexadecimal (always 6 bytes - 12 hex digits). Do *not* include the leading “0x” if present.
6. If the test status field says “PASSED,” proceed to “Testing Transport Interoperability” on page 30.

   If the test status field says “FAILED,” see “Interpreting LAN Errors” on page 37.

Interpreting LAN Errors

The following are possible situations you may currently find yourself in.

LAN problem corrected.

If you have made a change that corrected your LAN problem, then proceed to the OTS layer tests.

Configuration change required.

If the corrective action in the following sections require you to change a configuration parameter, then do so and rerun the LAN test.

Problem persists.

If you have been unsuccessful in correcting the problem, gather the information you have collected to provide to your HP support representative.

Table 1-5 LAN Errors

Error	Reason	Action
LAN Interface Name	The “interface name” is extracted from the OTS subnet configuration. If the device is not open, it may have the wrong value configured (or no value).	Check the parameter `lanX_if_name` from the top of the `osidiag` output and verify that this interface exists using the lanscan command.
`open()`	Opens the DLPI stream device. Device file `/dev/dlpi` may not exist.	Create device file using `mkdev`(1M) command.
`getmsg (DL_BIND_ACK)`	Used to set up various options for LAN access. Possible errors: *Setting SSAP. Sets Link Service Access Point. Will fail if it is currently in use by another osidiag process or by OTS.	If OTS is running, make sure OTS will not be started when the system comes up and reboot the system to perform this command.

Error	Reason	Action
`getmsg (DL_TEST_CON)` `getmsg (DL_UNITDATA_ACK)`	Receives information from the remote either on Receive or Test Frame operation. Usually means time out.	Check MAC address specified, and cabling between the two systems. If neither is true, check to see if remote supports IEEE 802.3 TEST frames.
`putmsg (DL_TEST_REQ)`	The local system is not configured to use IEEE packets.	Check and correct as necessary using the lanconfig(1M) command.
`putmsg (DL_UNITDATA_REQ)`	Data exceeds maximum MTU size for LAN.	Use “status” in LAN Test menu to determine MTU size.

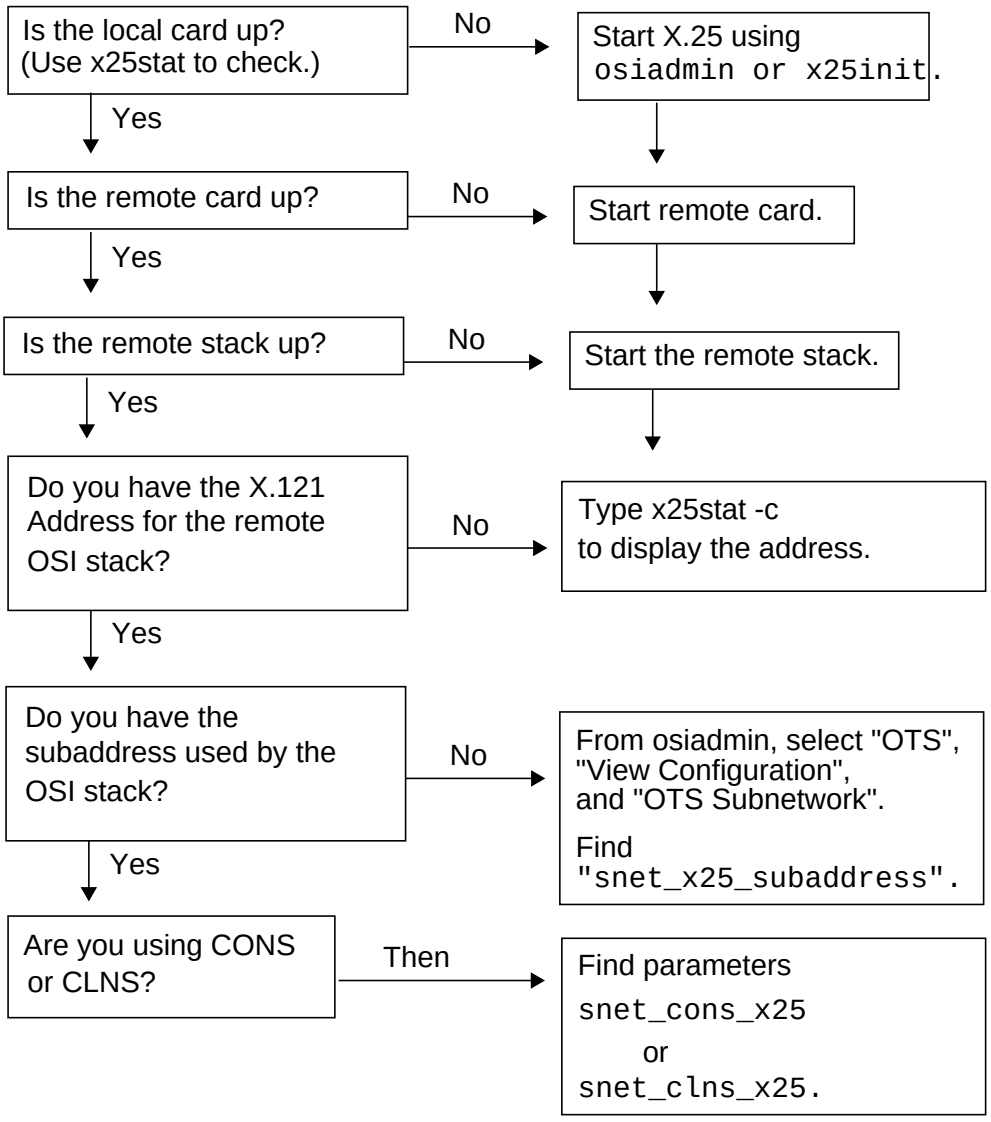
Testing X.25 Interoperability

The steps below describe how to test connectivity at the Network Layer for nodes connected via X.25.

1. Log on as root.
2. Perform the pre-test checklist.
3. Perform X.25 test.
4. If `osidiag` reports “FAILED,” see “Interpreting X.25 Errors” on page 42.

X.25 Pre-Test Checklist

Figure 1-6 X.25 Pre-Test Checklist



Running X.25 Tests

1. From root, type `osidiag` and select “WAN X.25Tests.”
2. Create a result file.
3. Select “Connect.”
4. Enter the value for the remote X.121 address. This value is both the address for the remote card and any subaddress concatenated into a single decimal number.
5. Leave the X.25 Interface name unchanged.
6. For CONS change the protocol ID to the value 03010100. For CLNS, change the protocol ID to 81. Press Done.
7. If the test status field says “PASSED,” proceed to “Testing Transport Interoperability” on page 30.

   If the test status field says “FAILED,” see “Interpreting X.25 Errors” on page 42.

Interpreting X.25 Errors

The following are possible situations you may currently find yourself in.

X.25 problem corrected.

If you have made a change that corrected your X.25 problem, then proceed to the Transport layer tests.

Configuration change required.

If the corrective action in the following sections require you to change a configuration parameter, then do so and rerun the X.25 test.

Problem persists.

If you have been unsuccessful in correcting the problem, gather the information you have collected to provide to your HP support representative.

Table 1-6 X.25 Errors

Error	Reason	Action
`socket()`	X.25 is not installed on your system.	Install X.25.
`bind()`	If OTS is running, osidiag is not able to bind to the same X.121 address the stack is using.	If supported by a switch, try binding to a different subaddress or the NULL subaddress.
`connect()`	Invalid programmatic access name.	Use default or leave blank. Can also verify the value by issuing the “Status...” operation through the X.25 Tests.

Error	Reason	Action
`recv(*00B*)`	Errors related to the receipt of an unexpected CLEAR or RESET packet.	Some common diagnostics: (0) No additional information - may indicate that the request was delivered to the remote, but it was rejected by the OSI stack. Check Protocol ID. (67) Call setup problem; Invalid called address. Check addresses of the remote and correct. (231) Connection Rejection - NSAP Unreachable. Check the Protocol ID and subaddress.

Reason and Refuse Codes

Protocol Reason Codes

The following are reason codes that may be logged or returned to your program.

Session Provider Abort Reason Code

The value passed back to Session programs by the `ses_pabort_id()` routine.

Transport Disconnect Reason Code

The value passed back to XTI program by the `t_rcvdis()` routine.

ASCE/Presentation DCNX_KO Log Message

The value shown in the second low order byte of the Cause field (`f3` in Cause = 0x0001f3ff).

Session S_REJECT Log Message

The value shown in the second low order byte of the Cause field (`f3` in Cause = 0x0001f3ff).

Transport T_REJECT Log Message

The value shown in the second low order byte of the Cause field (`f3` in Cause = 0x0001f3ff).

Network N_REJECT Log Message

The value shown in the second low order byte of the Org/Reas field (the “08” in Org/Reas = 0108).

Table 1-7 shows the reason code value, its meaning, and possible corrective actions.

Table 1-7 Reason and Refuse Codes

Code	Meaning	Action
(0)	Normal disconnect Specified address may be correct, but there is no process listening for a connection.	Verify that OSI services are up in the remote. Verify that the T-selector is specified.

Code	Meaning	Action
(0x01)	Provider N-Disconnect (Transient) Previously active network connection was abruptly disconnected. Congestion at TSAP Some vendor's equipment may indicate that the application above transport is not capable of receiving any more connections.	The X.25 card or the switch may have gone down. Check the remote for any further logged information.
(0x02)	Provider N-Disconnect (Permanent) Previously active network connection was abruptly disconnected. Transport User Not Attached to TSAP Indicates that the address specified is valid, but that no process capable of receiving connections is active.	The X.25 card or the switch may have gone down. Verify that server is active on remote.
(0x03)	Provider N_Reject (Transient) Network connection could not be established. Address Unknown Address specified was incorrect.	Check the NSAP and T-selector.
(0x04)	Provider N_Reject (Permanent) Request to establish a network connection was rejected.	Check for facility rejection, non-use of fast select, reverse charge failure, switch or PDN out of order.
(0x05)	Provider N_Reject (QOS unavail/ Transient) QOS negotiation failed for this connection.	
(0x06)	Provider N_Reject (QOS unavail/ Permanent) QOS negotiation failed for this connection.	
(0x07)	N-Reject (NSAP unreachable/ Transient) Network connection could not be established because there were not enough VCs or resources available.	Use `x25stat` to examine the state of the network card. Check log file for OTS messages.

Code	Meaning	Action
(0x08)	N-Reject (NSAP unreachable/ Permanent) Network connection could not be established because the X.121 address was incorrect.	Use `osiadmin` or `otsshowes` to examine the configured X.121 address for this NSAP. Verify if remote is up and listening on the configured address.
(0x09)	N-Reset from NS Provider (No Reason) Network connection was reset.	No recognized diagnostic is provided.
(0x0a)	N-Reset from NS Provider (Congestion) Network connection was reset.	X.25 diagnostic indicates provider was a problem.
(0x0b)	N_Reject (Address Unknown) No destination or route entry exists for the given NSAP. Network connection cannot be established.	Use `osiadmin` or `otsaddes` to configure the destination system.
(0x12)	Disconnect for NS User Remote Transport layer encountered a failure and abruptly released the network connection.	
(0x14)	User N_Reject (Transient) The remote Transport layer refused this network connection request.	
(0x15)	User N_Reject (Permanent) The remote Transport layer refused this network connection request.	
(0x16)	User N_Reject (QOS unavail/ Transient) QOS negotiation failure	
(0x17)	User N_Reject (QOS unavail/ Permanent) QOS negotiation failure	
(0x18)	N_Reject ((Unrecognized NS-user- data)	

Code	Meaning	Action
(0x1a)	Network Reset from NS User (Resynch) Network connection was reset.	X.25 diagnostic indicates resynchronization was requested.
(0x20)	Undefined reason, unknown origin Indicates some X.25 problem.	Check for down card on local or remote, switch, or facilities negotiation.
(0x21)	Invalid Parameter (OTS Kernel) An encoded parameter is invalid.	Check for NSAPs that are too large or missing.
(0x22)	External Protocol Error (OTS Kernel) Failure decoding facility information.	An error should be logged describing the protocol error.
(0x23)	Invalid Internal State (OTS Kernel) A network primitive was received or is to be sent in an unexpected state.	An error should be logged describing the protocol error.
(0x24)	Facility or Data Field Overflow (OTS Kernel) Processing of the facility fields indicated failure	An error should be logged describing the protocol error.
(0x41)	X.25 Facility Requested not Allowed The configured X.25 facilities do not match those of the provider.	Determine the facilities available and reconfigure OTS and X.25 to use the appropriate set.
(0x42)	Could not Access X.121 Address of Remote The X.121 address mapped to the NSAP you specified is incorrect or the remote system is down.	Reset the remote system or reconfigure the OTS routing table appropriately.
(0x81)	Remote Transport Entity Congestion at Connect Time Indicates that no problems were detected with the Transport layer, but user of service may have sent an abort or other higher level error.	

Code	Meaning	Action
(0x82)	Connection Negotiation Failed May be a problem with the classes specified (transport over CONS error).	Check to see if remote only uses class 0. If so you might reconfigure the local stack to force class 0.
(0x83)	Duplicate Source Reference for Same NSAP This is a protocol error.	The caller must generate a unique reference number for each connection it forms.
(0x84)	Mismatched References Either a protocol error, or may indicate that the remote stack was taken down and brought back up while existing connections remained.	Check the state of the remote stack.
(0x85)	Protocol Error	Check any logged information on the remote side. Also verify the stack was not being brought up at the time.
(0x88)	Connection Request Refused on this Network Connection The level of multiplexing configured for the local node may not be compatible with that on the remote.	On HP systems, examine the Transport over CONS parameters `tpcons_max_con_mux_in` and `tpcons_max_con_mux_out` and change if max out exceeds max in.
(0x8A)	Header or Parameter Length Invalid Indicates a protocol error.	Check log information on remote.
(0xE4)	X.25 Network Error or Network Down	Run `x25stat` to determine the status of the X.25 link. May need to restart X.25 or reset other X.25 hardware.

Code	Meaning	Action
(0xE7)	Problem Accessing X.25 Subaddress of Remote Subaddress portion of X.121 from the OTS routing table is incorrect or the remote is not up.	Correct the routing table or bring up the remote.
(0xE8)	NSAP not Configured Network address portion of the address specified is not configured in the routing table. (Not usually LAN)	Configure remote X.25 using `osiadmin`.
(0xF0)	Protocol Error Detected by Remote's Transport Remote encountered an error decoding one o the Transport PDUs sent by us.	Generate a trace and contact your HP support representative.
(0xF1)	Protocol Error Detected by Remote's Session Remote encountered an error decoding one of the Session PDUs sent by us.	Generate a trace and contact your HP support representative.
(0xF3)	Invalid Address or Permanent Transport Error Usually returned when an invalid T- selector or Network Address is given. Could also get when remote stack is not running or the remote's X.121 address is not associated with its NSAP.	Use `osiconf` to associate X.121 address with NSAP.
(0xF4)	Invalid Address or Permanent Session Error	Check address specified, and state of remote stack to ensure it is running.
(0xF6)	X.25 Unavailable or Transient Transport Error	Verify that X.25 is up by running `x25stat` operation.
(0xF7)	Transient Session Error	Verify status of remote stack.

Code	Meaning	Action
(0xF9)	Protocol Error Detected by Local Transport Error encountered decoding a PDU sent by the remote Transport entity.	Generate a trace and contact your HP support representative.
(0xFA)	Protocol Error Detected by Local Session Error encountered decoding a PDU sent by the remote Transport entity.	Generate a trace and contact your HP support representative.
(0xFC)	Insufficient Resources for Local Transport Stack experiencing resource problems.	Examine other OTS processes running. Contact HP support representative if condition persists.
(0xFD)	Insufficient Resources for Local Session Stack experiencing resource problems.	Examine other OTS processes running. Contact HP support representative if condition persists.
(0xFE)	Insufficient Resources for Local ACSE/Presentation Stack experiencing resource problems.	Examine other OTS processes running. Are you near the 448 connection limit? Contact HP support representative if condition persists.
(0xFF)	Local User Error Usually caused by overriding parameter default values, Could result from trying to run an operation in the wrong state.	Check parameters values you changed.
(01-EF X.25 F0-FF Transport	Code Unknown An unrecognized error code was received.	Examine documentation of other vendor for disconnect reason codes. If X.25 range, run an X.25 connection test, the diagnostic information may be helpful.

Session Refuse Codes

Table 1-8 describes the meanings defined by ISO 8327 for the reason codes carried on a negative Session connect confirmation. These values are logged after `S_CONNECT_Resp` (Negative) message, and on return from the `ses_connect_rf()` library call.

Table 1-8 Session Refuse Codes

Code	Meaning
0	Reason not specified.
1	Rejection by called Session service user due to temporary congestion.
2	Rejection by called Session service user. The following octets may be used for up to 512 octets of user data.
81	SSAP identifier unknown.
82	Session service user not attached to SSAP.
83	SBM congestion at connect time.
84	Proposed protocol versions not supported.

To Create A Result File

Use the following steps to create a result file. It can be reached from several `osiadmin` menus.

1. Select “Utilities” from a services menu.
2. Select “Open Result File”.
3. Enter the name of your file (for example, `/tmp/ftam.res`).
4. Press `Done`.
5. Press the space bar when a message appears showing the file was opened.

   If the message shows an error, check the name you specified.
6. Press `Previous Menu`.

2 Problem Solving

Information and procedures for identifying and troubleshooting problems that you may encounter using Hewlett-Packard's OSI products.

Basic Steps

NOTE

If the problem you encounter occurs only when communicating with another system, see Chapter 1, “Interoperability Testing,” on page 11.

1. Interpret the initial error. To find more information about the specific error, see “Interpreting Errors” on page 55.
2. Determine the status of components. Make sure all the OSI product components are up and running. See “Checking System Status” on page 56.
3. Verify operation. If all components report that they are up and the problem persists, verify the ability of the link (X.25, 802.3 or FDDI), the stack, and the specific service you are using to communicate. See “Running Verification Tests” on page 58.
4. Gather more information. If the information from the basic verification test was insufficient to diagnose the problem, then you can get additional information through Hewlett-Packard’s tracing and logging facilities. See “Collecting Troubleshooting Data” on page 61.
5. Validate configuration. If you have not already done so, run `osiconfchk` to validate the configuration. For a description of this tool, see Chapter 3, “Using OSI and OTS Tools,” on page 71. Also check the possible problems listed in “Common Configuration Mistakes” on page 65.
6. Validate installation. If the system behavior is still not correct, check that your software installation has not been corrupted. The tool `swverify`(1M) performs this task.
7. Submit information to HP. If you were not successful in diagnosing and correcting the problem, contact your HP support representative. See “Submitting Problem Information to HP” on page 70.

Interpreting Errors

This section describes where you should look to find more information about an error you encountered. Table 2-1 gives the places where you may encounter errors and how to interpret them.

Table 2-1 Interpreting Errors

Where	Action
`osidiag`	You will find a description of how to interpret errors at the end of each section in Chapter 1, "Interoperability Testing," on page 11.
`nettl` log files	Many errors contain detailed text describing the problem. Some common logged errors are described at the end of this chapter.
User applications	Errors received in applications you write are passed back through return codes. You may want to use the API tracing facility for the interface. The `nettl` log file many also contain information. You could also increase the logging level and reproduce the problem. See "Tracing and Logging through `/opt/ots/bin/osidiag`" on page 62.
FTAM Interactive Commands	These errors are described in the *HP FTAM/9000 User's Guide* and the *HP FTAM/9000 Reference Manual*.
X.400 Commands	Refer to the *Managing X.400—Administrator's Guide*.
OSI/OTS Administrative Commands	These errors are produced from commands like `otsstart` and `osiconfchk`. Descriptions of these errors can be found online. Also look in the log files in `/var/opt/ots`.
System Panics	Panics occur when an irrecoverable error is detected by the HP-UX operating system. At reboot after a panic, a copy of the state of the system will be saved by savecore. See `/etc/rc.config.d/savecore`. You may need to create a special directory for `savecore` to actually save the image to disk. Interpreting panics is done by your HP support representative or the factory.

Checking System Status

There are several tools that allow you to check if the links, stack, and services are up and running. Perform the following steps to verify that your local system is up.

Status Check 1

1. Run `otsstat` to verify the status of OTS and its attachment to the underlying links.
2. If status says "RUNNING," go to Status Check 2.
3. If status says "NOT RUNNING," start the stack using `otsstart` or `osiadmin`.

   If still "NOT RUNNING," run `osiconfchk`. This indicates a configuration problem.

Status Check 2

1. If one or more LAN cards are configured, run `lanscan` to show status of all LAN cards on the system.
2. If net interface state shows "DOWN," the card is disabled. Restart the card by running `osiadmin` or `ifconfig`. If the card is still down after starting it, check for hardware or cabling problems.
3. If OTS still shows link is "DOWN" while `lanscan` shows it as up, verify that the configured interface name shown by `otsstat` matches that shown by `lanscan`.

Status Check 3

1. If one or more X.25 cards, run `x25stat`, against each card's device file name.
2. If the message says "not currently active," start the card using `osiadmin` or `x25init`.
3. If the message says "Level 2 is DOWN," there is a communication problem between the card and the switch. Check the cabling and the configuration of the device the X.25 card is connected to.

Status Check 4

1. If you are using the FTAM Service, run `osistat` to verify that the shared memory segment is present and to display the number of currently active FTAM applications. See Chapter 3, “Using OSI and OTS Tools,” on page 71, for more information on `osistat`.
2. If you are using FTAM, then the count of “Active FTAM responder service providers” should be one or more. If not, then run `osiadmin` or `osistart` to start FTAM.
3. If `osistat` indicates that it is “Unable to access the shared- memory segment” formatting, you may need to regenerate the kernel to increase the available amount of shared memory or semaphores.

Status Check 5

1. If you are running X.400, then type `/opt/x400/bin/x4stat` to display the X.400 processes that are enabled.
2. If the process status of any component displayed is “not running!” then issue the command `x4start`.
3. Use the *Managing X.400—Administrator's Guide* if problems persist.

Running Verification Tests

The verification strategy described here follows a bottom up approach. It first checks the ability of the links to communicate, then the OTS Transport Layer, and last the desired service.

All the verification tests use `osidiag`. Testing the X.400 services may alternatively be performed through `x4admin` or the X.400 tools described in *Managing X.400—Administrator's Guide*.

`osidiag` may be invoked directly from the command line, or through `osiadmin` by selecting "Test Connectivity->" for the appropriate layer.

NOTE Hewlett-Packard strongly recommends that you run these verification tests even if the problem you are troubleshooting is seen through a user-written application. If the verification tests fail, then there is a general network problem that you should correct. If these tests pass, then the problem is related to your program's behavior. For a description on how to further analyze program-specific problems, see "Collecting Troubleshooting Data" on page 61.

Link Verification

For X.25

1. For X.25, run the "Loopback..." test under `osidiag`'s "X.25 Test Cases."
2. If you have multiple X.25 cards, run this test under `osiadmin`, so that `osidiag` will use the correct default values.
3. If OTS is not configured to use subaddressing, you will not be able to run this test when OTS is running. The error you see is "Address already in use." Try running the "Connect..." test instead, making sure the Protocol ID field is blank and not "dx25."
4. If you encounter errors, see "Interpreting X.25 Errors" on page 42.

For LAN

1. For LAN, run the "Test Frames..." test under `osidiag`'s "LAN Test Cases."

2. If you have multiple LAN cards, run this test under `osiadmin`, so that `osidiag` will use the correct default values
3. If you encounter errors, see “Interpreting LAN Errors” on page 37.

OTS Transport Verification

To verify OTS Transport, do the following:

1. Go to “Transport Tests-” under `osidiag` and select the “Loopback...” test.
2. Overwrite the Network Address if you want to test a subnetwork other than the default. By default, `osidiag` will run over the first LAN subnet configured. If no LAN is configured, then it will run over the first WAN subnet configured.
3. If you encounter errors, see “Interpreting Transport Errors” on page 33.

Run this test for each subnetwork you have configured. The subnetwork used is determined indirectly by the network address you specify in step 2.

The other network address values can be found on your Local Configuration Worksheets. Alternatively, you can find the other local addresses by doing the following:

1. Select the “Status...” test from the “Transport Test Cases” menu.
2. Look for fields labeled `snet_local_net_address`. These are the local network addresses you have configured for your subnetworks.

Service Verification

The verification steps for the X.400 and FTAM products are given in more detail in the respective “Installing and Configuring” manuals. The general steps for service verification are outlined below.

1. From `osidiag`, select the service to test. Or from `osiadmin`, select “Test Connectivity...” in the menu for the service to test.
2. Select the “Loopback” test from the menu. For FTAM, use “Connect” instead of loopback.

3. Use the default configured values that `osidiag` presents. For more information about a parameter, press the “Help” key when in the field in question.
4. If you encounter errors, see “Interpreting Errors” for the specific layer in Chapter 1, “Interoperability Testing,” on page 11.

Collecting Troubleshooting Data

If the information already given was not sufficient to isolate and correct the problem, use the tracing and logging facilities to gather more information.

The method you use to gather tracing and logging information will depend on the error that is produced. Table 2-2 lists the possible methods.

Table 2-2 Troubleshooting Methods

Type of Error	Troubleshooting Method
`osidiag`	If the problem is reported during a run of `osidiag`, then use the tracing and logging utilities provided by `osidiag`. This procedure is described in the section "Tracing and Logging through `/opt/ots/bin/osidiag`" on page 62.
X.400	If the problem occurs through an X.400 application, then follow the tracing procedures described in the *Managing X.400—Administrator's Guide*.
User Application	If the problem occurs through a user-written application, then there are two facilities that can give you further information. This procedure is described in the section "Tracing and Logging User Applications" on page 63.

Tracing and Logging through /opt/ots/bin/osidiag

osidiag (located in the /opt/ots/bin directory) provides the ability to automatically capture nettl trace and log information and append it to the output for a test operation. osidiag also allows you to copy the results displayed to the screen to a result file. The following steps describe how to enable both facilities through osidiag.

1. Invoke osidiag either directly or through osiadmin and go to the Utilities menu.
2. Select "Open Result File" and enter a file to save the results of the test operation (for example, /tmp/ftam.res). The file specified will be overwritten if it already exists.
3. Select "Tracing and Logging."
4. Enable logging for OTS, by placing a "Y" after its name in the pop-up window. Enable tracing for the layer being tested and the layer below. So, for FTAM you would enable FTAM and ACSE/Presentation. For Transport, you would enable Transport and Network. Use the "Help" facility for more information about a particular flag. Press Done on the Trace and Log screen after setting the appropriate fields to "Y."
5. Use the default values presented for the log and trace levels by pressing Done on these screens, and then exit the Utilities menu.
6. Now rerun the test you are gathering information for. The results of the logging and tracing will be displayed on your screen as well as copied to the file you specified in step 2.

To analyze the errors logged, see "Common Logged Errors" on page 67.

The trace information produced may be useful to your HP support representative. Interpreting traces requires a good understanding of the various OSI protocol internals. Some information on trace interpretation is given at the end of the "Session," "OTS," "X.25," and "LAN" sections of Chapter 1 "Interoperability Testing".

Tracing and Logging User Applications

Two facilities exist to provide more data about the behavior and errors encountered by your application, API tracing and nettl.

API Tracing — This facility allows you to trace the calls your application makes to the Application Programmatic Interface. The mechanism to perform API tracing is described in the programmer's guide for the service you are using.

nettl — The nettl command allows you to enable logging and tracing in the OTS stack as well as for the FTAM service. The syntax of the nettl and netfmt commands is given in the nettl(1M) and netfmt(1M) man pages.

Hewlett-Packard recommends that you enable warning and error logging for stack components at and below the service you are using. Table 2-3 shows the entities on which you should enable logging for gathering information.

Table 2-3 Logging and Tracing Entities

Service/Layer	Entities to Log
X.400*	X.400 Logging facilities + OTS entities + Link entity
FTAM	FTAM_VFS FTAM_USER FTAM_INIT FTAM_RESP + ULA entities + OTS entities + Link entity
APRI	ACSE_PRES + OTS entities + Link entity
OTS	SESSION TRANSPORT NETWORK OTS
LAN 802.3	NS_LS_DRIVER
X.25	SX 25 L2, SX25L3 (Level 2 and 3 link tracing)

Service/Layer	Entities to Log
FDDI	`FDDI`

* The tracing and logging of X.400-specific components can be done through `x4admin`, and is described in the *Managing X.400—Administrator's Guide*. Tracing and logging of OTS and the link is still performed through `nettl` for X.400.

Tracing is only recommended if you have a good understanding of the protocol internals. When used, it is useful to trace at the layer your application uses and one level below.

For instance, to trace an FTAM application, you might enable tracing for the FTAM entities and ACSE/Presentation. To trace an XTI application, you might enable Transport and Network tracing. The kind of tracing will usually be PDU In, PDU Out, Header In, and Header Out.

To analyze the errors logged, see "Common Logged Errors" on page 67.

Common Configuration Mistakes

The following list describes some common configuration errors that may result in failure during verification. The errors are grouped by the configuration file that contains them.

See the "OTS and Related Parameters" chapter in the OSI Transport Services manual for detailed information about all the parameters.

ots_dests Common Mistakes

- Mistyped `dest_net_address` or the `dest_phys_address`, will cause a fail in your attempt to connect.
- Destination entries must be made in order for loopback to work over both CONS and CLNS/X.25. Be sure to include any X.25 subaddress when specifying the physical address.
- Destination entries must be made in order for loopback to work over CLNS/ LAN when CLNP Subset 0 is used. In other cases, destination entries for LAN should be avoided.
- Specifying the incorrect outgoing subnetwork for a destination, will cause a fail to connect.
- When specifying reverse charging for X.25, the remote must be configured to accept it. Otherwise, it will reject your connection.

ots_subnets Common Mistakes

- Mistyping your local address will cause the remote systems to be unsuccessful in connecting with you.
- Incorrect CLNP subset for LAN. This can prevent interoperability with other systems on the LAN. See the parameter `snet_clnp_subset`.
- LAN-based networks with a large number of nodes (over 200), should have the parameter `snet_max_es_entries` increased. Not doing so can result in failure to establish connections with other systems.

- Incorrect interface name. Specifying an interface name that is not configured will result in warnings, but OTS will still start. If `otsstat` indicates any links are “NOT RUNNING,” verify these names.

`ots_parms` Common Mistakes

- If close to the limit of connections available (448 over LAN, 4096 over X.25) through OTS, the `ses_reuse_tp_con` flag may hold open connections you need to recycle.
- If using CONS/X.25, ensure that the Transport class OTS requests is acceptable to the remote. The `tpcons_pref_mux_class` parameter determines whether you use class 2 or 4. The parameter `tpcons_tp0_only` forces class 0.
- Some vendors do not accept the OSI Transport protocol ID carried on X.25 connection requests. This can be disabled with `tpcons_null_pid`.

`local_app` Common Mistakes

- Setting the maximum invocations, or inbound associations too low can result in your failing to receive or create connections with remote FTAM applications.
- If you manually edit these files rather than using `osiadmin`, you should be sure that all FTAM application titles match the `ftam_ddn_lookup_path` parameter.

`remote_app` Common Mistakes

- Mistyping a remote application title or alias for FTAM will result in your connection failing.
- Mistyping a remote presentation address for FTAM will result in your connection failing.

Common Logged Errors

The following list describes some of the more common errors logged by OTS that you can encounter. These errors are sorted by the subsystem name and the message ID as it appears in the log.

Table 2-4 Subsystem OTS

Error	Description
[9600] High Access Method ERROR	Indicates an error in the streams interface between user programs and the OTS stack in the kernel. One common problem is attempting a bind operation to an invalid network address or SAP. Verify the local address used on your test and try again.
[9800] x25 ERROR	Indicates that the X.25 card has not been started or has gone down. Use `otsstat` and `x25stat` (or their equivalents under `osidiag`) to view the status of X.25. Restart X.25 if necessary under `osiadmin`.

Table 2-5 Subsystem ACSE_PRES

Error	Description
[6010] P_DCNX_KO	Indicates that the presentation layer is releasing the connection after some error was encountered. Examine the log or user application for other errors.
[6011] PST_LOG	Indicates a problem found by the presentation layer in the OTS stack. This may indicate a protocol error, or an ASN.1 encoding issue. Examine the packets sent in the trace output.

Table 2-6 Subsystem SESSION

Error	Description
[5008] S_REJECT	Indicates that a session connection was not successfully established. If the log does not show a `T_REJECT` error, this indicates that the problem was at the session layer. If a `T_REJECT` error is logged, then the `S_REJECT` is just a propagation of a Transport (or lower) layer problem.

Error	Description
[5010] S_DCNX_KO	This error is logged after the Session layer has successfully established a connection, but is releasing the connection in some error state. Examine the log or user application for other errors.

Table 2-7 Subsystem TRANSPORT

Error	Description
[4103] Protocol Error	Indicates a protocol error was detected at this layer. You should verify that both sides are using correct combinations of Class, Alternate Class, Flow Control and Expedited Data. If problem persists, ensure that you have both Transport and Network layer traces of the dialog, and contact your HP support representative.
[4108] T_REJECT	Indicates that the Transport connection was not successfully established. Examine the log for other errors (such as routing problems, or network layer problems). If no other logged errors appear, the problem may be that no process is listening at the address you specified. Verify the remote address given as well as what addresses are available at the remote.
[4113] Routing	Indicates that CLNS was unable to determine the NSAP/ MAC address translation for the destination Network Address given. Possible problems are: mistyped address, remote is not up, remote does not support ES/IS, the remote's destination configuration (ots_dests) is incorrect.
[4115] Processing Error	This error usually appears in conjunction with a protocol error. It may give more information about what was not liked with the PDU.

NOTE Transport errors will have message IDs that begin with either 41*xx* or 40*xx*, depending on whether you are running over CLNS or CONS respectively. The statements shown below apply as well to the 40*xx* errors.

Table 2-8 Subsystem NETWORK

Error	Description
[3003] N_REJECT	Indicates the X.25 connection could not be established with the remote. Possible problems are that the NSAP/X.121 address mapping for this remote is incorrect. Facility negotiation failed with X.25 (for example, Reverse Charging, X.25 '80/'84). The remote stack or card may not be enabled. The remote system may not be able to accept anymore X.25 connections.
[300 5] N_ DCNX_KO	This error is logged after the Network layer has successfully established a connection, but is releasing the connection in some error state. Examine the reason code for more details.
[3014] N_ERROR	This may provide more detailed information for why the network connection was rejected. Errors regarding route resolution mean that your destination address configuration is in error.

Submitting Problem Information to HP

The following items will be very useful in having HP Support diagnose problems with your OSI products.

- Result Files - The output created for all your runs of `osidiag`. Examples of the recommended file names are `/tmp/ftam.res` and `/tmp/tran.res`.
- OTS Configuration Files - The contents of the following files in `/etc/opt/ots/conf`:

`local_app`	For FTAM problems only.
`ots_dests`	For nodes running over X.25 or NULL internet.
`ots_parms`	In all cases.
`ots_routes`	In all cases.
`ots_subnets`	In all cases.
`remote_app`	For FTAM only.

- X.400 Configuration Report. If you are using X.400 and experience problems, type the following:

  ```
  /opt/x400/bin/x4dump
  ```

  A file called `/tmp/x4dump.sh` is created which can be e-mailed or put on tape.
- X.25 Configuration Report. If you are using X.25 and experience problems, type the following:

  ```
  /opt/x25/bin/x25stat -c /tmp/x25.cnf
  ```

  Print the resulting file.
- LAN Configuration Report. If you are using LAN (802.3 or FDDI) and experience problems, type the following:

  ```
  /usr/sbin/lanscan /tmp/lan.cnf
  ```

  Print the resulting file.

3 Using OSI and OTS Tools

The software tools you'll use to configure, maintain, and troubleshoot your HP OSI products.

OSIADMIN

The `osiadmin` (OSI Administration) program gives you access to the various configuration, administration, and diagnostic tools you need to set up and maintain your HP OSI products. `osiadmin` acts as an umbrella for these tools, providing you with a single, easy way to configure, start, stop, and test each product.

Table 3-1 shows the HP OSI products, administration functions, and software tools called by `osiadmin`.

Table 3-1 `osiadmin` Functions

Product	Function	Tool
LAN	configure	SAM (System Administration Manager)
	start	`ifconfig`
	stop	`ifconfig`
	test	`osidiag`
X.25	configure	SAM
	start	`x25init`
	stop	`x25stop`
	view	`x25stat`
	test	`osidiag`
OTS	configure	`osiconf`
	start	`otsstart`
	view	`osiadmin`
	test	`osidiag`
	update	`otsupdate`

RFC1006	configure	osiconf
	start	otsstart
	view	osiadmin
	test	osidiag
FTAM	configure	osiconf
	start	ftam_resp
	stop	ftam_resp
	view	osiadmin
	test	osidiag
X.400	configure	x4admin
	start	x4start
	stop	x4stop
	view	x4configprint
	test	osidiag
	administer	x4admin

Managing Your Configuration

Using `osiconf`

The `osiconf` program is an interactive configuration tool you can use to do the following:

- Verify that your configuration information has been entered with the proper syntax and range, and that it is consistent between OTS and FTAM.
- Modify the OTS and FTAM configuration files.

`osiconf` is most commonly used through `osiadmin`, but it may be started alone. `osiconf` has two "modes:"

update/dynamic — Only dynamic parameters can be modified. Changes take effect when you run `otsupdate`. When dynamic changes take effect, they are applied to the running OTS or FTAM.

restart — Can modify all parameters in this mode. Changes take effect when `otsstart` is run (if this is the initial configuration), or when you reboot (if you've changed an existing configuration).

For more information, refer to the online HP-UX man page for `osiconf`.

Using `osiconfchk`

The `osiconfchk` program is a configuration verification tool that allows you to verify the correctness of configuration files prior to actually starting the stack. Checks are performed to ensure that all required information is present, that parameters are of the proper syntax and range, and that information is consistent across configuration files.

NOTE For X.400, `osiconfchk` checks only those parameters that are also configured in OTS. The `osiconfchk` program does not verify the correctness of the X.400 configuration.

The directory where the configuration files may be found is specified by setting the environment variable `OSI_CONFIG`. If `OSI_CONFIG` is not set, `/etc/opt/ots/conf` is searched as the default location.

Running `osiconfchk`

Follow these steps to run the `osiconfchk` program:

1. Login as root.
2. Type `osiconfchk`. For details on the options and variables, refer to the HP-UX online man pages for `osiconfchk`.
3. If there are no parameter problems, the root prompt re-appears.

Troubleshooting Using `osiconfchk`

If `osiconfchk` finds problems with the configuration parameters, it displays the file the problem was in, the line of the file, and the actual parameter at fault. The example below shows a sample output of `osiconfchk` errors.

```
/etc/opt/ots/conf/local_app

Line 26:
->ae_local_paddr 7874693.0001.0001 # p-, s-, and t_selector
An even number of hexadecimal digits is required.  (CHK023)
```

First line	Configuration file name from X.25, OTS, FTAM, or X400.
Line number	This is the line number from the file.
Next line	The actual parameter name and value of the parameter.
Last line	A statement of what `osiconfchk` found wrong with the parameter.

Compare this display with the parameter value on the appropriate worksheet to be sure it was entered correctly.

Read the problem descriptions and take the recommended actions to correct the configuration problems.

OSI Diagnostics

The `osidiag` (OSI Diagnostic) program allows you to verify that the OSI services provided by the HP network node are operational. You'll use `osidiag` throughout the remote interoperability procedures. It can also be used as a layer troubleshooting aid in determining the functionality of the suspect component. You can start `osidiag` from within `osiadmin` or directly from the HP-UX system prompt.

Table 3-2 shows the components of the OSI stack and the tests provided by `osidiag`.

Table 3-2 Tests Provided by `osidiag`

Component	Test
FTAM Initiator	Tests the communication between HP's FTAM Initiator and the specified remote responder.
X.400	Four tests are available for X.400: • The RTS connection tests provide verification of HP's ability to establish or receive connections at the RTS layer. • The User Agent connection test verifies HP's ability to send an X.400 message and receive a delivery confirmation from the remote node. In order to provide more feedback to the user, this test will track message activity as the message transfers from one X.400 process to another. • The RTS loopback test does a local loopback test to verify that the RTS can communicate with OTS.
ACSE/ Presentation	Allows you to create or receive ACSE/Presentation connections and send data.
ROSE	Allows you to create or receive connections over ACSE/ Presentation /ROSE and issue and receive operation invocations.

Component	Test
Session	Provides verification of HP's ability to establish or receive connections at the session layer. Data, expedited data, and some of the activity management primitives may also be sent on this connection.
Transport	Provides verification of HP's ability to establish or receive connections at the transport layer. Data, and expedited data may also be sent on this connection. Please read that follows this table.
X.25	Allows an X.25 connection to be established and brought down verifying layer 3 connectivity with the remote node. Card status and statistical information can also be reported.
LAN (802.3/ FDDI)	Uses the 802.3 Test Frames to determine if there is layer 2 connectivity. Card status may also be reported.

NOTE

An entity must be running on the remote node, capable of receiving (or initiating) a session or transport level connection. For the HP node, `osidiag` provides the capability to both establish and receive the connection. However, some vendors may not have exposed access to this layer or the functionality provided by `osidiag`. In that case, the test desired may have to be run manually (without `osidiag`).

With `osidiag`, you can automatically start tracing and logging while running diagnostic tests at a specified layer of the stack. By designating a "Result File," you can store a duplicate of the information displayed while the test case is running. This file can be useful in relaying problem information if consulting help is requested. For more information on `osidiag`, see the online manpage.

Starting and Stopping OSI

Occasionally, while configuring, verifying, or troubleshooting any of the OSI products, you'll need to start or stop the OSI products. Use the commands described here.

`osistart` Command

Execute the `osistart` command from the system prompt. Use it to start services, such as FTAM and X.400 along with the OTS component and whatever links are being used. Issue the `osistart` command with no options.

You can start the services separately by using the `-s` option. This also starts the OTS and link components (if necessary). For example:

```
osistart -s x400
```

For more details on the `osistart` command and its options, refer to the HP-UX online man pages.

NOTE If you make OTS configuration changes via `osiadmin` to start OTS automatically, OTS/9000 is automatically started when the system is booted. Thus, OTS is usually up and will rarely (if ever) be started by `osistart`. See “OSIADMIN” on page 72 for the list of tools that `osistart` uses to start the OSI stack. If you don’t make the configuration changes using `osiadmin`, you must use `otsstart` manually to start OTS.

Stopping OSI

To stop the OSI stack, you must shutdown your system. After initial installation of OTS/9000, the OSI stack will start automatically after rebooting. If you do not want it to start automatically, edit the `/etc/rc.config.d/ots` file and change the value of `otsstart` to "off."

`osistat` Command

Super-users can use the `osistat` command to get the status of various aspects of OSI service products, for example:

- active service providers
- aborts sent
- aborts received
- connections established

Executed from the system prompt, the `osistat` command with no option prints global service provider process (SPP) statistics for FTAM. With the `-m` option, `osistat` prints memory buffer statistics without SPP statistics.

Starting OTS: otsstart

This section tells you how to start OTS/9000 directly from the HP-UX shell command line. See the section "To Start OTS/9000," in chapter 5 of the OSI Transport Services manual, for how to start OTS/9000 from `osiadmin`.

`otsstart` starts the protocol subsystems, and the CONS and CLNS parts of the network layer. This command requires super-user capability.

Before executing `otsstart`, make sure the following are true:

- The OTS/9000 subsystem is configured.
- The X.25 software is configured and started, if used.
- The LAN link is running, if used.
- No X.25 layer 3 applications (that is, `x25server`, `x29server`) are running, if null subaddressing is used.

Syntax

```
otsstart
path: /opt/ots/bin
```

OTS/9000 can only be started once per system boot-up. Subsequent invocations of `otsstart` have no effect. To check whether OTS/9000 is running, see `otsstat` later in this chapter.

Example

The following example shows `otsstart` executed when OTS detects a problem with the LAN card and the X.25 cards:

```
Startup log:

OTS:     running
lan0:    NOT RUNNING
telenet: NOT RUNNING
telenet1:DOWN
```

1. Check to make sure that `lan0` LAN and the `telenet` and `telenet1` X.25 links are running and properly configured. X.25 may be:

   `NOT RUNNING` not configured or not started

`DOWN`	not configured, but level 2 is down

2. Next, make sure that OTS is properly configured to use these links.
3. Finally, make sure that no other applications are conflicting with OTS's use of these links.

Recovering from `otsstart` Failure

In most cases, when `otsstart` fails, you will need to change the configuration before trying to start OTS/9000 again. Use the error messages from `otsstart` and `osiconfchk` as a guide for making changes.

If an error is reported before “Starting OTS”, fix the configuration and try again. If the error occurs after “startup log:”, you'll have to fix the error and reboot.

Checking OTS Status: `otsstat`

If connectivity problems occur, one of the first actions to take is to find out whether OTS/9000 and the network services are running. The `otsstat` command tells you if OTS/9000 is running and whether the OTS/9000 subsystem can successfully communicate with the X.25 and LAN software. The X.25 status is reported in terms of each card's programmatic access name. The LAN status is reported in terms of the LAN interface name.

LAN status may be "running" or "NOT RUNNING."

X.25 status may be:

`running`

`NOT RUNNING` not configured or not started

`DOWN` level 2 is not running

If the OTS/9000 subsystem is running, but X.25 or LAN is DOWN or NOT RUNNING, do the following:

1. Verify the X.25 network service is operational. If not, restart X.25.
2. Verify the LAN card is accessible. For example, perform a LAN loopback test.
3. If the OTS status still reports the X.25 or LAN as down, reboot.
4. Run `osidiag` to verify OTS/9000 can communicate over the X.25 link and/or over the LAN.

It is possible for OTS/9000 to be running after a network service (for example, X.25) has been stopped. The result is that applications (for example, X.400) will not be able to communicate over OTS/9000, if that particular network service is required.

Syntax

```
otsstat
path: /opt/ots/bin
```

Example 1

The following example shows the output of `otsstat` when OTS/9000 is running and can properly communicate with X.25 and with LAN. The programmatic access name for the X.25 card is `telenet`. The interface name for the LAN is `lan0`.

```
/opt/ots/bin/otsstat

OTS:       running
lan0:      running
telenet:   running
```

NOTE The `otsstat` command does not include the status of the X.25 and LAN network services. To check their status, use the `x25stat` and `lanscan` commands.

Example 2

The following example shows the output of `otsstat` when the OTS/9000 subsystem is not running:

```
/opt/ots/bin/otsstat

OTS:    NOT RUNNING
```

Example 3

The following example shows the output of `otsstat` when OTS/9000 is running, cannot properly communicate with the X.25 link software, but can communicate with LAN.

```
/opt/ots/bin/otsstat

OTS:      running
lan0:     running
telenet:  DOWN
```

Updating OTS: `otsupdate`

Chapter 5 of the OSI Transport Services manual describes many OTS configuration parameters as being “dynamic.” This means that you may change the values of these parameters and have them take effect while OTS/9000 is up and running. Non-dynamic parameters take effect only after the system has been rebooted.

After changing dynamic parameters with `osiadmin` or any ASCII editor, use the `otsupdate` command to cause the changes to take effect. If you've changed a non-dynamic parameter, the update process will not allow any updates to occur. The update process is very sensitive to the changing of non-dynamic parameters. For example, deleting and re-adding a local subnetwork (even with exactly the same values) could cause the update process to fail.

NOTE

If changing parameters with `osiadmin`, you can restrict your updates to dynamic parameters only by setting the update mode to dynamic (D).

In general, parameters dealing with protocol layer operation (for example, timers), and parameters dealing with remote addressing (for example, destinations and routes) can be updated using `otsupdate`.

For additional information, see the manpage for `otsupdate`.

Dynamic Routing Commands

Dynamic routing commands provide an alternative to using `otsupdate`. Use of these commands may be more efficient than using `otsupdate` when the information is small and restricted to routing information.

OTS routing information is contained in the Routing Information Base (RIB). The information contained in this database can be changed using a set of user commands.

Use these commands to:

- View the current RIB entries.
- Dynamically update the stack's RIB.
- Make changes to the local configuration file.

You can change or view routing information for:

- End Systems
- Intermediate Systems
- Routes
- NSAPs

End System Commands

End systems are nodes directly reachable from the local node.

otsaddes

ADD: Adds a single end system entry to the specified subnet. Now also supports per-destination protocol identifiers (PIDs).

`otsaddes` *`es_nsap subnet_name es_phys_addr`* [*`options`*]

[*`options`*]= `-C`*`cug`*`, -f|F, -r|R, -s|S, -t|T, -w, -x|X`

otsdeles

DELETE: Deletes the specified end system entry.

`otsdeles` *`es_nsap subnet_name`* `[-w]`

otsshowes

VIEW: Displays all end system entries for the specified subnetwork.

`otsshowes` *subnet_name*

Intermediate System Commands

Intermediate systems are nodes directly reachable from the local node that function as inter-network or intra-network routers.

otsaddis

ADD: Adds a single intermediate system entry to the specified subnetwork.

`otsaddis` *is_nsap subnet_name is_phys_addr* [*options*]

[*options*] = -C, -f|F, -r|R, -s|S, -t|T, -w, -x|X

otsdelis

DELETE: Deletes the specified intermediate system entry.

`otsdelis` *is_nsap subnet_name* [-w]

otsshowis

VIEW: Displays all intermediate system entries for the specified subnetwork.

`otsshowis` *subnet_name*

ES/IS Parameters

Table 3-3 ES/IS Command Parameters

Argument	ots_dests Parameter	Description
es_nsap	dest_net_address	Specifies the end system's NSAP
is_nsap	dest_net_address	Specifies the intermediate system's NSAP
subnet_name	dest_out_subnet	The symbolic name for the outgoing subnetwork to which this end system is attached. This name must have been previously configured before OTS startup.
es_phys_addr	dest_phys_address	The physical point of attachment to the subnetwork. This will be a X.121 address for X.25 or a MAC address for 802.3/FDDI subnets.
is_phys_addr	dest_phys_address	The physical point of attachment to the subnetwork. This will be a X.121 address for X.25 or a MAC address for 802.3/FDDI subnets.

Table 3-4 ES/IS Command Options

Option	Description
`-r`	Reverse Charge Request off. Specifying this option prohibits outgoing calls from requesting reverse charging. This is the default.
`-R`	Reverse Charge Request on. Specifying this option makes outgoing calls request reverse charging.
`-x`*N*	X.25 level of service. `N`=[0-3]. 0 is X.25 ISO 8878 1 is X.25/ 1980 2 is X.25/ 1984 3 is X.25/ 1988 Specifying this option turns off support for the service specified by `N`. The default is to have all possible levels of service supported. Only those levels supported by the subnetwork are valid. See the file `ots_subnets` for related parameters.
`-X`*N*	X.25 level of service. *N*=[0-3]. 0 is X.25 ISO 8878 1 is X.25/ 1980 2 is X.25/ 1984 3 is X.25/ 1988 Specifying this option turns on support for the service specified by *N*. The default is to have all possible levels of service supported. Only those levels supported by the subnetwork are valid. See the file `ots_subnets` for related parameters.
`-f`	Flow control off. Specifying this option disallows flow control parameters (packet size/window size) to be negotiated. This is the default.
`-F`	Flow control on. Specifying this option allows flow control parameters (packet size/window size) to be negotiated.

Option	Description
`-P` *pid*	Specifying this option causes a destination protocol identifier (PID) to be configured for this destination. This value is specified as 2 to 16 hexadecimal digits (must be an even number of digits) or the word “NULL” (without the quotes). If you use a hexadecimal value, this value is used as the destination PID on connection requests to the end system. If the PID is configured “NULL”, the NULL PID is used, This option is only valid for end systems connected over CONS/X.25. If no option is specified, OTS chooses the destination PID. Refer to the `dest_pid` parameter.
`-s`	Fast Select off. Specifying this options disallows user data to be sent with call set-up and clear packets. This is the default.
`-S`	Fast Select off. Specifying this options allows user data to be sent with call set-up and clear packets.
`-t`	Throughput Class Negotiation off. Specifying this option disallows throughput class to be negotiated. This is the default.
`-T`	Throughput Class Negotiation on. Specifying this option allows throughput class to be negotiated.
`-w`	Write this action (add or delete) to the `ots_dests` configuration file. Default is no write.
`-C`*cug*	Closed User Group. *cug* specifies the closed user group to which this end system belongs. *cug* is four decimal digits long, padded on the left with zeros.

NOTE The X.25 parameters (for example, flow control, fast select, etc.) can only take effect if the X.25 card configuration allow the parameters to be negotiated.

Route Commands

Routes specify paths to nodes that can be reached via an intermediate system. A route may specify such a path for a single system by using a full NSAP, or groups of NSAPs by using their Network ID. (A Network ID is an NSAP prefix common to a group of destination NSAPs that can all be reached through the same intermediate system.)

otsaddroute

ADD: Adds a single route entry for the specified subnetwork.

`otsaddroute` *net_id subnet_name is_nsap* `[-m`*Mask*`] [-w]`

otsdelroute

DELETE: Deletes the specified route entry.

`otsdelroute` *net_id subnet_name* `[-m`*Mask*`] [-w]`

otsshowroute

VIEW: Displays all route entries for the specified subnetwork.

`otsshowroute` *subnet_name*

Route Command Parameters

Table 3-5 Dynamic Route Commands

Argument	ots_routes Parameter	Description
net_id	route_id	Specifies the end systems NSAP or network ID. If this value is the full length end-system NSAP, then this route entry will send information for this particular destination through the specified intermediate system (is_nsap). If this value is a prefix of an NSAP, then it is used to specify a group of systems, all having this common NSAP prefix.
subnet_name	route_out_subnet	The symbolic name for the outgoing subnetwork to which the intermediate system is attached. This name must have been previously configured before OTS startup.
is_nsap	route_primary	Specifies the intermediate system NSAP. Information destined for the end system will be sent through this system.

Route Command Options

Table 3-6 Route Command Options

Argument	Description
`-w`	Write this action (add or delete) to the `ots_routes` configuration file making the change permanent. The default is no write.
`-m`*Mask*	Network ID mask. *Mask* is a bit mask, specified in hex digits. It specifies how may bits in the network ID are significant when resolving addresses. For instance, with *Mask* of FFF8, the first 15 bits will be used when matching the route entry to the destination NSAP. If no `-m` option is specified, a mask of *N* F's will be used, where *N* is the number of hex digits in the NSAP/network ID.

NSAP Commands

Network Service Access Point (NSAP) addresses are used to identify real systems unambiguously on a network. Dynamic NSAPs are used for high availability clusters running the MC/ServiceGuard product, which automatically shares NSAPs when a node or its network communications fail. Use the following commands to add, delete, and show dynamic NSAPs for local CONS/CLNS subnetworks. See the manpages for these commands for more information.

`otsaddnsap`

ADD: Adds a local NSAP to OTS configuration for a specified network service.

`otsaddnsap` *service nsapvalue* `[silent]`

The `silent` option means the added NSAP is never broadcast in the ESH packet.

`otsdelnsap`

DELETE: Deletes a local NSAP from OTS configuration. The default/main NSAP configured via `osiadmin` cannot be deleted with `otsdelnsap`.

`otsdelnsap (`*nsapvalue*`)`

otsshownsaps

VIEW: Shows local NSAPs configured for a specified network service.

```
otsshownsaps
```

Index

A

ACSE/Presentation, 76
adding
  end systems, 85
  intermediate systems, 86
  route entries, 90
APRI
  interpreting interoperability errors, 22
  pretest checklist, 19
  running client mode tests, 20
  running serbver mode tests, 21
  testing interoperability, 18

C

collecting troubleshooting data, 61
commands, dynamic routing, 85
common configuration mistakes, 65
common logged errors, 67
configuration
  common mistakes, 65
  local_app, 66
  managing using osiconf, 74
  remote_app, 66
  updating, 84
creating result file, 52

D

deleting
  end systems, 85
  intermediate systems, 86
  route entries, 90
determining OTS status, 82
dynamic routing
  parameters, 90, 91
  route commands, 89
Dynamic routing commands
  end system, 85
  intermediate system, 86
  otsaddes, 85
  otsaddis, 86
  otsaddroute, 90
  otsdeles, 85
  otsdelis, 86
  otsdelroute, 90
  otsshowes, 86
  otsshowis, 86
  otsshowroute, 90
dynamic routing commands, 85

E

end system, dynamic routing commands, 85
errors
  common logged, 67
  interpreting troubleshooting, 55
ES/IS command parameters, 87
examples
  otsstart, 80
  otsstat, 83

I

intermediate system, dynamic routing commands, 86
IOP
  using osiadmin, 72

L

local_app, 66
logging user applications, 63

O

Open Systems Interconnection (OSI), 78
OSI
  starting and stopping, 78
osiadmin, using for IOP, 72
osiconf
  dynamic mode, 74
  managing configuration, 74
  restart mode, 74
osiconfchk, 74
osidiag, tracing and logging through, 62
osistart, 78
osistat, 79
osistop, 79
OTS/9000
  determining status of, 82
  starting, 80
  updating, 84
otsaddes, 85
otsaddis, 86
otsaddroute, 90
otsdeles, 85
otsdelis, 86
otsdelroute, 90
otsshowes, 86
otsshowis, 86
otsshowroute, 90
otsstart, 80
  examples, 80
  failure recovery, 81
  syntax, 80
otsstat, 82
  examples, 83
  failure recovery, 82
  syntax, 82
otsupdate, 84

P

parameters
  dynamic routing, 90, 91
  ES/IS command, 87
problem information, submitting to HP, 70
problem solving, basic steps, 54
protocol reason codes, 44

R

reason codes, 44
recovering otsstart failure, 81

Index

refuse codes, 51
remote_app, 66
result file, creating, 52
RIB, 85
route command, 89
routing information base, see RIB, 85
routing, dynamic, 85

S

session refuse codes, 51
starting
  OSI, 78
  OTS/9000, 80
status
  checking system, 56
  OTS/9000, 82
stopping
  OSI, 78
submitting problem information to HP, 70

T

tracing user applications, 63
troubleshooting
  basic steps, 54
  checking system status, 56
  collecting data, 61
  common logged errors, 67
  interpreting errors, 55
  running verification tests, 58
  using osidiag, 62

U

updating OTS configuration, 84
user applications
  tracing and logging, 63

V

verification, running the tests, 58
verifying
  links for troubleshooting, 58
  OTS for troubleshooting, 59
  services for troubleshooting, 59
viewing
  end systems, 86
  intermediate systems, 86
  route entries, 90