Installing and Administering HP OSI Transport Services

Edition 6

32070-90030
HP 9000 Networking
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.

Contents

1. HP OTS/9000 Resources

HP-UX Manual Reference Pages 18

Logging Messages 20
- Link Subsystems 21
- OTS Subsystems 21

OSI Transport Services Documentation 22

Contacting Your HP Representative 23

HP OTS/9000 25
- OTS/9000 Components 26

The OSI/RFC1006 Stack 28

How HP OTS/9000 Establishes a Connection 29

Supported Services and Functionality 30
- ACSE/Presentation Functionality 30
- Session Functionality 31
- Transport Functionality 32

How OTS/9000 Finds a Remote End System 33

How OTS/9000 Uses Network Identifiers 37

How OTS/9000 Uses the X.25 Network 38
- Using Protocol Identifiers (PIDs) and Subaddresses 39

Addressing Concepts 40

Network Layer 44

Structure of NSAP Addresses 47
- The Syntax of an NSAP Address 48
- The Initial Domain Part 48
- The Domain Specific Part 49
- The Privately Allocated Part 50

Contents

Current NSAP Allocation Formats 54
ANSI Format 54
AFNOR Format 55
United States GOSIP 55
United Kingdom GOSIP 57
MAP/TOP 3.0. 58

Building Temporary Administrative Prefixes. 60
Use an International Telephone Number 60
Use an X.121 Address 61
Use the ISO Local Format 62

A Recommended PAP Structure 63
Network Identifiers (Network ID) 64

General Recommendations for NSAP Addresses 65

Non-standard NSAP Formats for Use in OTS 66

2. Planning Your Network

Planning Your Network 68

Determine the Services Required 69
X.400 Service 69
CMIS Service. 69
FTAM Services 70
APRI Service 70
High Availability Service 71
XTI Service 71

Determine the Vendors Involved 72

General LAN Questions 74

General X.25 Questions 75

Determine the Network Structure 77

Contents

Determine the Addressing Scheme 78
Network Address 78
Application Addresses 79
Naming Hierarchies 79

Gather and Distribute Configuration Information 81

3. Gathering Configuration Information

A Map to the Data Gathering Process 84
About Worksheets 84

Using the Remote System Worksheet 86
General Information 86
Application Addresses 86
Subnetwork Addresses 87
X.25 Subnetwork Information 87
LAN Subnetwork Information 88
Network Addresses (NSAPs) 89
RFC1006 NSAP and IP Address 89
RFC1006 Addressing Considerations 90

Remote System Worksheet 91

Using the Local Parameter Worksheet 93
Local Worksheet Organization 93
General Considerations 93
Local Parameter Worksheet Fields 94
The Next Steps 97

Local Parameter Worksheet 98

4. Installing HP OTS/9000

Installing HP OTS/9000 102

Hardware and Software Requirements 103

Contents

Hardware 103
Software 103

Installation Procedures 105

If Not On HP-UX 10. 30 106

To Add a New Link to HP OTS/9000 for Series 700/800 107

Installing HP OTS/9000 Software 108
Installing and Upgrading HP OTS/9000 from HP-UX 10.01 or Later 110
Installing and Upgrading HP OTS/9000 from HP-UX 9.x 110
Upgrade to HP-UX 10.01 Required. 111
Upgrade from HP-UX 9.x to 10.01 112

De-installing HP OTS/9000 115

5. Configuring and Verifying HP OTS/9000

Configuring and Verifying HP OTS/9000 118
HP OTS/9000 Configuration. 118
Overview of HP OTS/9000 Configuration 120

To Configure HP OTS/9000 122

To Configure RFC1006 123

To Add HP OTS/9000 CLNS Over 802.3 or FDDI LAN 124

To Add HP OTS/9000 CLNS Over X.25 125

To Add HP OTS/9000 CONS Over X.25 126

To Add HP OTS/9000 Destination System 127
An Outgoing Subnetwork Name Example. 128

To Add an HP OTS/9000 Route 129

To Start HP OTS/9000 130

Contents

To Update HP OTS/9000 131

To Verify HP OTS/9000 Configuration 132

6. HP OTS/9000 Configuration Files

About the Configuration Files. 134
- OTS Files 134
- Related Files 134

Configuration Files and the config_parms.txt File 136
- Steps for Changing Parameter Values 137

Multiple Configuration Sets 138

To Create A New File Set 139
- Multiple Configuration Diagram 141
  - Checking OSI_CONFIG Current Value 141
  - How the OTS Nodal Management Tools Use OSI_CONFIG 141

Glossary

Contents

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

Preface

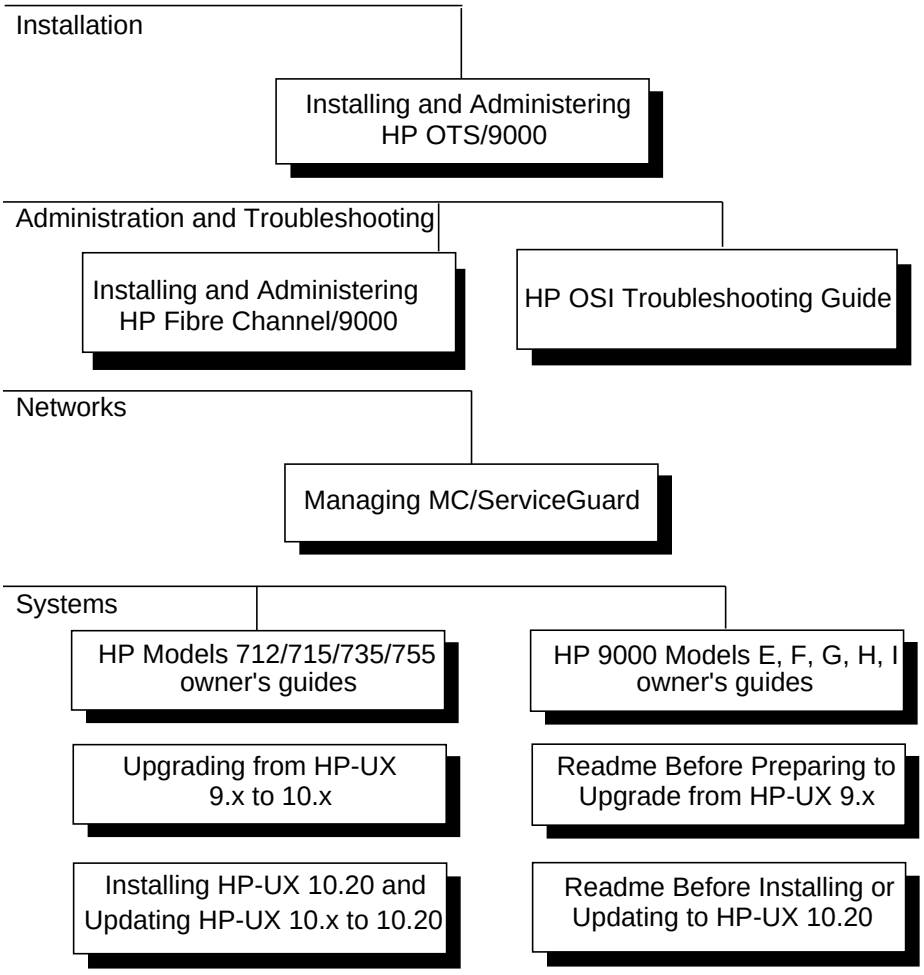
This booklet describes how to plan, install, and configure the HP OSI Transport Services product. It is divided into six chapters, which provide the following information:

Chapter 1	"HP OTS /9000 Resources" introduces OTS, provides OSI concepts, and references other useful tools for installing, configuring, and maintaining OTS software.
Chapter 2	"Installing OTS/9000" describes how to install OTS/9000 and RFC1006.
Chapter 3	"Planning Your Network" describes how you determine services required, network structure, and vendors involved.
Chapter 4	"Gathering Configuration Information" tells you what information you need to collect so you can configure your network.
Chapter 5	"Configuring and Verifying HP OTS/9000" describes how to configure your system to run either OTS/9000 or RFC1006 and how to add these over various links. It also covers starting, updating, and verifying your configuration.
Chapter 6	"HP OTS /9000 Configuration Files" describes the OTS files used to configure the product.
Glossary	"Glossary" defines OTS and other network-related terms.

HP OTS/9000 Documentation Map

The following documentation map is intended to be a general guideline to the manuals containing information related to HP OTS/9000.

Figure 1



1 HP OTS/9000 Resources

This chapter provides OTS concepts, network examples, and additional tools for installing, configuring, and maintaining HP OTS/9000.

HP-UX Manual Reference Pages

While installing, configuring, or troubleshooting OTS/9000, you may need to refer to any of the following online manual reference pages (man pages) for useful HP-UX operating system or OTS commands. To display a man page, include `/opt/ots/man` in your MANPATH shell variable, then type the following at the system prompt:

```
man <command name>
```

- *osiadmin(1M)*, the OSI Administration program, gives you access to the various configuration, administration, and diagnostic tools to setup and maintain OTS/ 9000.
- *osiconf(1M)*, and interactive configuration tool, allows you to verify and modify configuration information between OTS and FTAM.
- *osiconfchk(1M)* allows you to verify the correctness of configuration files prior to actually starting the OSI stack.
- *osidiag(1M)* initializes all the FDDI network interfaces on a system and connects to the FDDI network.
- *osiping(1M)* sends a CLNP echo request to specified network hosts for testing and debugging. (Only versions of HP OTS/9000 at C.05.02 and later respond to *osiping*.)
- *osistart(1M)* allows you to start OSI services, such as FTAM and X.400.
- *osistop(1M)* allows you to stop OSI services, such as FTAM and X.400.
- *otsaddes(1M)* adds a single end system entry to the specified subnet.
- *otsaddis(1M)* adds a single intermediate system entry to the specified subnetwork.
- *otsaddnsap(1M)* adds a local NSAP to OTS configuration.
- *otsaddroute(1M)* adds a single route entry for the specified subnetwork.
- *otsdeles(1M)* deletes the specified end system entry.
- *otsdelis(1M)* deletes the specified intermediate system entry.
- *otsdelnsap(1M)* deletes a local NSAP from OTS configuration.

- *otsdelroute(1M)* deletes the specified route entry.
- *otsshowes(1M)* displays all end system entries for the specified subnetwork.
- *otsshowis(1M)* displays all intermediate system entries for the specified subnetwork.
- *otsshownsaps(1M)* provides the NSAPs configured for a given network service.
- *otsshowroute(1M)* displays all route entries for the specified subnetwork.
- *otsstart(1M)* starts the protocol subsystems and the CONS and CLNS parts of the network layer.
- *otsstat(1M)* shows if OTS/9000 is running and whether the OTS/9000 subsystem can successfully communicate with the X.25 and LAN software.
- *otsupdate(1)* incorporates the configuration changes you've made to "dynamic" parameters while OTS/9000 is running.

Logging Messages

HP OTS/9000 uses the *nettl(1M)* logging and tracing facility supplied with HP-UX. See the *nettl(1M)* manual (man) page for information on using the command line interface.

NOTE

All log message cause and action statements are now online and can be viewed with any ASCII text editor. The OTS cause and action statement file is `/opt/ots/doc/ots_messages.txt`.

Listed below are some example commands.

- To examine the log file:

  ```
  netfmt -file /var/adm/nettl.LOG00 -t 50
  ```

  Note the message number, then search the `messages.txt` message file for a description of the problem and possible solutions. A sample OTS log message is shown below.

  ```
  **************************HP OSI MGMT**********************
  Timestamp        :Mon Dec 16PST 1996  03:40:10.555252
  Process ID       :750                 Subsystem   :TRANSPORT
  User ID (UID)    :0                   Log Class   :DISASTER
  Device ID        :1                   Path ID     :0
  Connection ID    :0                   Log Instance:0
  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

  <1317> OTS driver encountered a lobe error on interface unit
  <1>. The error code is <-1>; reset or reboot.
  ```

- To check network logging and tracing status:

  ```
  nettl  -status
  ```

- To start all OTS transport and session tracing to the file */var/adm/tracefile*:

  ```
  nettl -traceon all hdrin hdrout pduin pduout -entity
  transport session -file /var/adm/tracefile
  ```

- To stop OTS tracing:

  ```
  nettl -traceoff -entity transport session
  ```

- To format the OTS trace file into the file */var/adm/traceout:*

  ```
  netfmt -file /usr/adm/tracefile.TRC0 > /var/adm/
  traceout
  ```

Link Subsystems

Use the following link subsystem names when logging and tracing OTS/9000:

- NS_LS_DRIVER - This is the IEEE 802.3 LAN link.
- FDDI - This is the FDDI LAN link.
- SX25L2 - This is the level 2 high performance X.25 link tracing subsystem.
- SX25L3 - This is the level 3 high performance X.25 link tracing subsystem.

OTS Subsystems

Use the following subsystem names when logging and tracing OTS/9000:

- Network - This is the Network layer entity of the OTS stack. This subsystem includes both the Connection-Oriented (CONS) and Connectionless (CLNS) Network Service entities.
- Transport - This is the Transport layer entity. Some CLNS logged errors may also appear under this entity.
- Session - This is the Session layer entity.
- ACSE_PRES - This is the ACSE/Presentation entity.
- OTS - This corresponds to non-layer specific tasks performed while managing the various stack entities, for example, communication between the OTS stack and user space, communication between the OTS stack and network devices, and other administrative tasks, such as buffer management.

OSI Transport Services Documentation

There are two manuals provided with the HP OTS/9000 product:

- *Installing and Administering OSI Transport Services* (the OTS manual). This manual provides information specific to OTS/9000. It covers:
  - Installation
  - Network planning
  - Gathering configuration data
  - Configuring and verifying
- *OSI Troubleshooting Guide* (the OSI manual). This manual contains information relevant to the whole OSI stack.
  - Interoperability Testing
  - Troubleshooting
  - OSI/OTS Tools

The chapters in *Installing and Administering OSI Transport Services* are in the suggested order to best configure OTS on your system. When you have finished verifying your configuration, go to the *OSI Troubleshooting Guide* for information on testing your Interoperability.

In addition to the two printed manuals that come with the OTS product, Hewlett-Packard provides a compressed printable electronic file, `/opt/ots/doc/ots_addendum.ps.Z`, that contains OTS concepts, example network topologies, configuration parameters, and error message cause and action information. Uncompress the file with the HP-UX `uncompress` command, then print the resulting `/opt/ots/doc/ots_addendum.ps` file.

The error message information is also contained in the file `/opt/ots/doc/ots_messages.txt`, and the configuration parameter information is also contained in the file `/opt/ots/doc/ots_config_parms.txt`.These files are not compressed.

The files are located in the */opt/ots/doc* directory.

Contacting Your HP Representative

If you have no service contract with HP, you may follow the procedure described below, but you will be billed accordingly for time and materials.

If you have a service contract with HP, document the problem as a Service Request (SR) and forward it to your HP representative. Include the following information where applicable:

- A characterization of the problem. Describe the events leading up to and including the problem. Attempt to describe the source and symptoms of the problem.

  Your characterization should include: HP-UX and OTS commands; communication subsystem commands; job streams; result codes and messages; and data that can reproduce the problem. You should also provide a network map with the host name, IP/Internet address, and station address of each system connected with the HP system.

  Illustrate as clearly as possible the context of any message(s). Prepare copies of information displayed at the system console and user terminal.

- Obtain the version, update, and fix information for all software. To check the version of your kernel, execute *uname -r*.

  This allows HP to determine if the problem is already known, and if the correct software is installed at your site.

- Prepare copies of the */etc/hosts* and */etc/rc.config.d/netconf* files.

- Run the verification command, *swverify*, and record the output.

- Record all error messages and numbers that appear at the user terminal and the system console.

- Save all network log files. Make sure that ERROR and DISASTER log classes are enabled when log files are collected. Prepare the formatted output and a copy of the log file for your HP representative to further analyze.

- Prepare a listing of the HP-UX I/O configuration you are using for your HP representative to further analyze. Use the *ioscan(1M)* command to help collect this information.

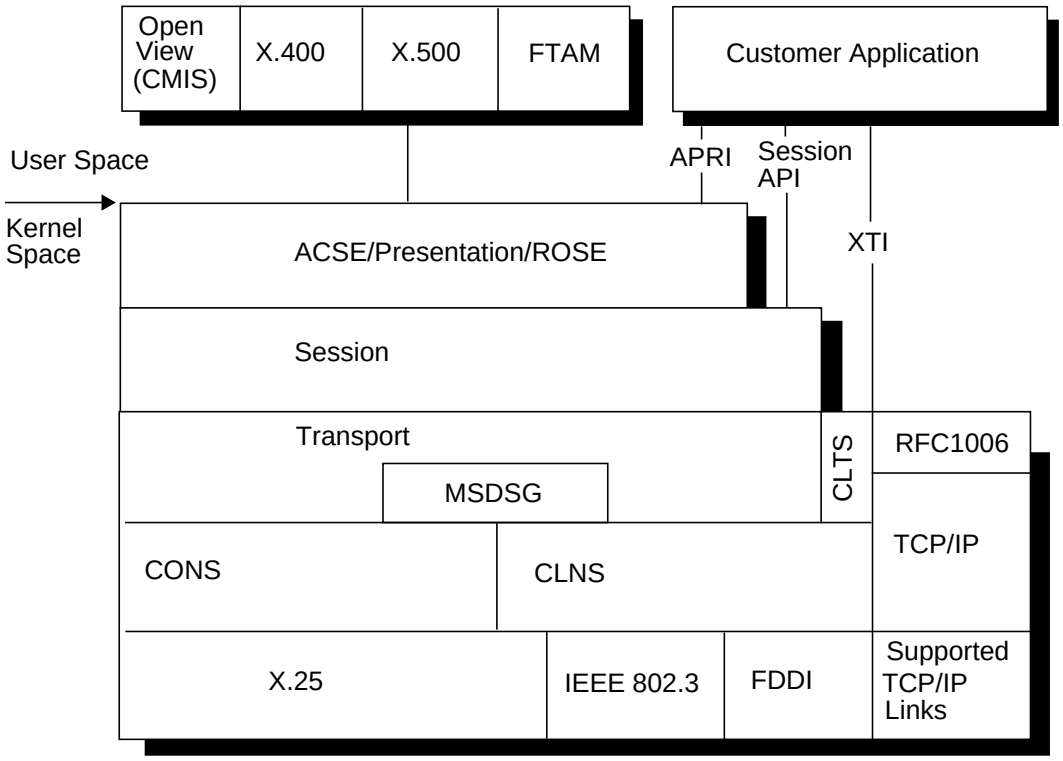
- Try to determine the general area within the software where you think the problem exists. Refer to the appropriate reference manual and follow the guidelines on gathering information for that product.
- Document your interim, or “workaround,” solution. The cause of the problem can sometimes be found by comparing the circumstances in which it occurs with the circumstances in which it does not occur.
- Create copies of any Internet or OTS/9000 link trace files that were active when the problem occurred for your HP representative to further analyze.
- **In the event of a system failure, a full memory dump must be taken.** Use the HP-UX utility *savecore* to save a core dump. Send the output to your HP representative.

HP OTS/9000

HP OSI Transport Services/9000 (OTS/9000) networking software provides the Network, Transport, Session, Presentation, ROSE, and ACSE layers of the OSI reference model. OTS/9000 also provides OSI network layer services over the X.25/9000, FDDI/9000, or LAN/9000 link. These layers supply the necessary foundation to run OSI services, such as FTAM and X.400, as well as CMIP, which is part of the HP OpenView product. OTS/9000 provides several application programmatic interfaces to allow developers to write custom applications (XTI and APRI). In addition, OTS/9000 provides RFC1006 functionality. This feature allows running OSI services such as X.400 over TCP/IP connections using any link supported by TCP/IP. OTS/9000 is the main component of HP's OSI product solutions, which include:

- X.400 (Message Handling Services)
- FTAM (File Transfer, Access and Management)
- CMIS (Common Management Information Service)
- APRI (ACSE/Presentation and ROSE Interface)
- Session API (Session Layer Application Programmatic Interface)
- XTI (X/Open Transport Interface)
- IEEE 802.3 (Local Area Network)
- FDDI (Fiber Distributed Data Interface)
- X.25 WAN (Wide Area Network)

Figure 1-1



OTS/9000 Components

OTS/9000 resides in the kernel and is accessed through the streams facility. OTS consists of the following components:

- ACSE (Association Control Service Element)
- ROSE (Remote Operation Service Element)
- Presentation (OSI Presentation Layer)
- Session (OSI Session Layer)
- Transport (OSI Transport Layer)
- CLTS (Connectionless Transport Service)

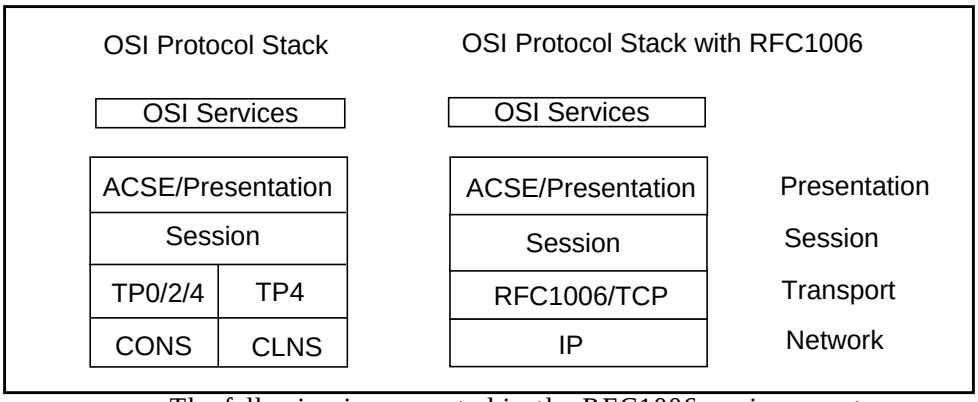
- MSDSG (Multi-System Distributed System Gateway)
- RFC1006 (OSI Transport Class 0 over TCP Specification)
- CONS (Connection Oriented Network Service)
- CLNS (Connectionless Network Service)

The OSI/RFC1006 Stack

RFC1006 allows OSI services, for example X.400, to run over TCP connections. RFC1006 provides the OSI Transport Protocol (TP) class 0 over TCP. RFC1006 does not, by itself, support OSI services. The upper layers of the OSI stack provided by OTS are still required.

The graphic below shows the OSI protocol stack with and without RFC1006. The RFC1006 replaces the OSI transport connections with TCP connections. All upper layer APIs are identical between RFC1006 and pure OSI protocol stacks.

Figure 1-2



The following is supported in the RFC1006 environment:

- Supported OSI Services: X.400, X.500, FTAM, CMIS
- Supported OTS APIs: XTI, Session API, APRI
- Supported links: Any link that TCP/IP supports

How HP OTS/9000 Establishes a Connection

Establishing a connection between local and remote systems involves the following:

- Higher-layer applications, such as FTAM and X.400, require address information and NSAP values. The addresses determine the peer entity at each layer of the stack. See “Addressing” in the “Resources” chapter of this manual.
- A user-created application uses the stream `/dev/osipi` or `/dev/ositpi` for primitive requests. The application registers with OTS using its local address.
- Upon successful registration, the application sends a connect request to the remote system.
  - If the remote is connected through CONS, OTS/9000 looks up its X.121 address in the OTS configuration and sends a call packet.
  - If the system is attached to an 802.3 or FDDI LAN, OTS/9000 uses the ES-IS protocol to determine the Media Access Control (MAC) address for the destination NSAP.
- After the remote address is determined, OTS/9000 normally issues the connect request to establish a connection if the type of network service used is a Connection-Oriented Network Service (CONS). This is provided on X.25 networks.
- If another network service type, Connectionless Network Service (CLNS), is used, it differs only in that there are no network layer connections established. OTS/9000 provides CLNS over FDDI, IEEE 802.3 LANs and X.25.

Supported Services and Functionality

The OTS/9000 product includes the following:

- ACSE/Presentation services (ISO 8649 and ISO 8822)
- ROSE Service (ISO 9072-1, CCITT X.219)
- OSI Session protocol and services (ISO 8326, 8327; CCITT X.215, X.225, T.62)
- OSI Transport protocol and services (ISO 8072, 8073, 8602; CCITT X.214, X.224 and T.70 for Teletex terminals)
- OSI Network services: CONS over X.25; CLNS over X.25, FDDI and IEEE 802.3 LANs; ES/IS routing (ISO 8348 , 8473, 8878, 9542)
- RFC1006 - OSI Services over TCP/IP
- Multi-System Distributed System Gateway (MSDSG) - OSI Services over TCP/ IP (ISO/IEC TR10172)
- X/Open Transport Interface (XPG.4) (For more information, refer to the *XTI Programmer's Reference Guide*)
- APRI (ACSE/Presentation and ROSE Interface) - see the *ACSE/Presentation and ROSE* manual

ACSE/Presentation Functionality

The ACSE/Presentation and ROSE Interface (APRI) provides a programmatic interface to the Association Control Service Element (ACSE), Remote Operation Service Element (ROSE) and Presentation layer protocols.

The ACSE/Presentation interface enables two or more application processes on the same or different computers to:

- establish an association (connection) with another application process
- exchange (send and receive) information
- shutdown the association (connection)

Using ROSE with ACSE/Presentation provides the request/reply service that is useful in building distributed applications. ROSE cannot be used independently of the ACSE/Presentation interface.

Session Functionality

The Session layer provides cooperating applications with a standard protocol to organize and synchronously exchange user data, and to map user-oriented Session addresses to network-oriented Transport addresses. The Session layer corresponds to layer 5 of the OSI reference model.

OTS/9000 offers the following Session functionality:

- Session Protocol Version 1 and Version 2 with extended concatenation for half/ full duplex and minor synchronization functional units. The Session version is negotiated at connection establishment. It defaults to Version 1 when either side is unaware of the negotiation or when Version 1 is proposed by one side.

NOTE While Version 2 allows extended user data on calls that were not allowed with Version 1, OTS/9000 limits extended user data size to 10 Kilobytes maximum per Session primitive.

- Infinite Session service data unit (SSDU) size for normal and typed data.
- The following functional units:
  - Kernel
  - Half-duplex
  - Duplex
  - Expedited data
  - Typed data
  - Minor synchronize
  - Major synchronize
  - Resynchronize
  - Activity management
  - Capability data
  - Exceptions

OTS/9000 does not support negotiated release or symmetric synchronization through the Session API.

Transport Functionality

The Transport layer corresponds to layer 4 of the OSI reference model. As with the Session layer, the Transport layer provides cooperating applications with a standard protocol to organize and exchange user data. Unlike Session, the Transport is implemented with a greater knowledge of the underlying network configuration. Therefore, its definition involves details hidden from the Session layer entity.

The level of Transport sophistication and capabilities are divided into classes of operation, 0 through 4. OTS/9000 implements the following:

- An application using the Connectionless Network Service (CLNS) must use TP (Transport) class 4.
- An application using the Connection-Oriented Network Service (CONS) can use TP classes 0, 2, or 4.
- OTS supports Transport (TP) classes 0, 2, and 4 over CONS/X.25 and TP class 4 over a CLNS IEEE 802.3 or FDDI LAN and CLNS/X.25.
- TP 0 is the only alternate class OTS supports.

When an administrator configures a class parameter for CONS communications, they can force the use of class 0 only or offer a preferred multiplexing class (TP 2 or TP 4). On the connect request, the transport user can select the preferred class, with or without class 0 as an alternative, or simply select class 0. For example, if an application requests an alternate class of 0 and multiplexing, OTS/9000 may propose TP 2 with an alternate of TP 0 and send the connect request. If the remote does not allow TP 2, TP 0 is used to make the connection.

How OTS/9000 Finds a Remote End System

After a brief review of what an end system and an intermediate system are, this section describes how routing information is obtained and provided, and how OTS/9000 uses it.

A system can act as an end system or as an intermediate system. OTS can function only as an ES.

- An end system (ES) initiates or responds to a communication (it supports layers 1 through 7).
- An intermediate system (IS) forwards communication traffic across subnetworks (it supports layers 1 through 3).
- Routing means establishing a path across the subnetwork(s) and intermediate system(s) so that data is exchanged between end systems. Normally, an ES communicates directly with another ES. That is, they are connected to the same subnetwork. If the local ES cannot directly reach the remote ES, the local ES makes the first “hop” to an IS. The IS determines the best path to the remote ES.

OTS/9000 can function as:

- An ES connected to a single subnetwork.
- An ES connected to multiple subnetworks. OTS/9000 is capable of choosing different routes for sending a PDU, but it does not forward PDUs.

OTS/9000 does not function as an IS.

Routing information can be provided dynamically through the ES-IS protocol, or it can be provided statically through the osiadmin configuration screens. Remote LAN systems that support the ES-IS protocol periodically multicast their NSAP and MAC addresses. By default, OTS/9000 records these addresses in a routing table. These dynamic table entries are discarded after a period of time specified by the remote system. Static table entries, that do not time-out, can be configured using osiadmin. When the routing table is full, any new dynamic routing information is ignored.

The maximum number of routing entries (by type of subnetwork) is as follows:

	CONS/X.25	CLNS/X.25	CLNS/802.3 or FDDI LAN
Number of ES entries	430 (default), 2550 (maximum)*	325 (default), 999 (maximum)	250 (default), 999 (maximum)
Number of IS entries	430 (default), 2550 (maximum)*	15 (default), 999 (maximum)	15 (default), 999 (maximum)

* Total number of routing ES and IS entries across all CONS/X.25 subnetworks. This value is configurable. (ots_parms: cons_max_route_entries)

The CLNS numbers are per subnetwork and are also configurable (ots_subnets: snet_max_es_entries, snet_max_is_entries).

Static routes can be configured in osiadmin using the destination system's configuration by specifying the NSAP to Physical Address mapping of remote system(s) or a Network ID that identifies a whole class of remote NSAPs (by prefix).

When OTS/9000 needs to communicate to a remote ES, it uses the following algorithm to route PDUs:

	IF	THEN
1	The destination NSAP belongs to an ES known through static configuration or dynamic addition through the ES-IS protocol or the otsaddes command	OTS/9000 sends the PDU directly to the specified remote ES
2	The network ID of the destination NSAP matches a local LAN network ID configured in the osiadmin LAN Subnetwork screen.	OTS/9000 will send the PDU to the first IS on the subnetwork, if known. Otherwise, it will multicast the NSAP by using the Query Config function of the ES/IS protocol. If the NSAP is multicasted, the remote ES will usually respond with dynamic route information to avoid subsequent multicasting.
3	The network ID of the destination NSAP matches a route network ID that was configured using osiadmin routes configuration or the dynamic routing command otsaddroute	OTS/9000 sends the PDU to the corresponding IS
4	OTS has exhausted all other means of sending an outbound packet to its destination, and the snet_query_subnet parameter is set to yes	OTS/9000 sends the PDU to all CLNP subnets that have the snet_query_subnet parameter set. If there is an IS on the subnet, the PDU is sent to the IS: otherwise, the packet is sent to the subnet using Query Configuration.

NOTE In all cases, if multiple Network IDs match, the longest match is chosen, but local LAN Network IDs are always chosen over Network IDs configured as routes.

How OTS/9000 Uses Network Identifiers

OTS/9000 will always check to see if it has a Destination system entry (either dynamically or statically created) for a given NSAP first. If no such entry exists, it will try to determine which subnetwork the destination may be reached on. This is accomplished using the Network ID field on the LAN (802.3 or FDDI) subnetwork configuration screens. If the destination can be reached on the LAN subnetwork, (the Network ID is matched) OTS will either send the packet to an IS on the LAN, or, if no IS is present, use the Query configuration function to resolve the route.

If OTS cannot determine the outgoing subnetwork, it then looks at the configured routes to see if the destination NSAP matches one of the configured Network IDs (the front portion of the NSAP matches the Network ID). If a Network ID matches, the configured IS is used to route information to the destination NSAP. Since Network IDs vary in length, OTS will check them using a longest-length-first search order. For instance, if two route entries have been created, 4901 and 490101, and the NSAP OTS is trying to route to is 4901010001, the route associated with the Network ID 490101 will be selected.

More precisely, Network IDs are checked using a most-1-bits-in-mask search. The route entries with the greatest number of 1s in their route_id_mask are considered first. Since the default is to set the mask to a string of Fs as long as the Network ID, this results in a longest-length-first search. However, if you edit the ots_routes file directly and create custom masks, you must keep the actual search algorithm in mind.

How OTS/9000 Uses the X.25 Network

OTS/9000 supports the Connection-Oriented Network Service (CONS) and Connectionless Network Service (CLNS) over the X.25 network. The main objectives of X.25 are:

- forming the control and data packets
- exchanging these packets
- establishing and supervising virtual circuits

OTS/9000 is primarily concerned with the virtual circuit (VC) objective, leaving the other objectives to the X.25 product.

When a connection is to be established, a virtual circuit is established at the network layers. “Virtual”' implies that it is not necessary for a dedicated connection to exist between systems, but that a logical association be made through a network based on the source and destination addresses of the two systems. This does not mean that there cannot be dedicated circuits. X.25 allows both permanent virtual circuits (PVC) and switched virtual circuits (SVC), with the distinction based on how long the association is valid. A PVC maintains a permanent association. An SVC maintains the association only for the current connection call.

NOTE OTS/9000 supports only SVCs.

System addresses are based on the X.121 standard which uses a sequence of 15 deecimal digits (0-9) that includes a subaddress of 0 to 5 digits. When configuring local system addresses (in ots_subnets), the system address is constructed by concatenating the X.121 address from the X.25 configuration with the subaddress specified by the snet_x25_subaddress parameter. The physical address specified by the dest_phys_address parameter in X.25 ots_dests entries is a system address and contains both the X.25 address and the subaddress.

Null subaddresses can be used for both CONS and CLNS X.25 subnetwork switches that do not support subaddressing. Subaddresses are unique on a particular link and cannot be shared by different X.25 applications. (See the *HP OTS Addendum* for information on the `snet_x25_subaddress` parameter for defining null subaddresses.)

OTS/9000 uses the X.25 address to configure a logical mapping of the NSAP. For X.25 implementations using the 1984 specification or later, the NSAP is passed in the Extended Address (EA) facilities field in the X.25 call packets, if configured; the NSAP is the calling address. If the X.25 switch or X.25 network does not support the 1984 X.25 protocol, or the extended address facility is not configured, OTS/9000 will use the X.25 address as the calling address.

X.25 offers several connection management facilities. OTS/9000 can be configured to support the Reverse Charge (through osiadmin) and Closed User Group (through customization) facilities. Refer to the HP X.25 documentation for a description of these facilities.

Using Protocol Identifiers (PIDs) and Subaddresses

A single X.25 link is capable of supporting many applications, including OTS. Different applications, including multiple attachments to the same link by OTS, are differentiated from each other by the use of subaddresses and Protocol Identifiers (PIDs).

If the underlying X.25 subnetwork supports subaddressing, the easiest way to differentiate applications is to assign each one a unique subaddress without regard to PIDs. However, if subaddressing is not supported or not desired, the NULL subaddress must be used. If NULL subaddressing is used, then unique PIDs must be assigned to differentiate each application.

By default, OTS does not use a PID for X.25 subnetworks (it uses a NULL PID). This allows for the greatest degree of interoperability with remote OSI systems. If differentiation by PID is required, then OTS must be configured to use the standard OSI PIDs.

To configure OTS to use the standard OSI PID, use an editor to modify the active ots_subnets file. Change the snet_bind_by_pid parameter for the affected subnetwork(s) to yes (1). This change will take effect the next time the stack is started. Other related parameters are dest_pid in the ots_dests file and tpcons_null_pid in the ots_parms file.

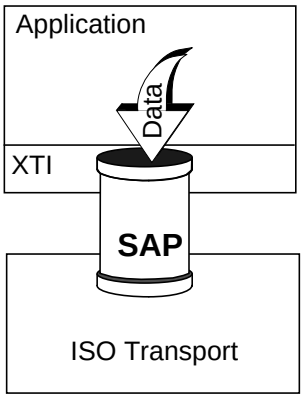
Addressing Concepts

SAP - A SAP, or Service Access Point , is a “pipe” between two OSI layers that allows one layer to obtain a set of services from another layer. The services obtained vary from layer to layer, but are usually management functions, such as connection establishment and termination, and data transfer functions. For instance, a SAP between an application and the OSI Transport is a “pipe” the application uses to open connections, for example, send/receive data using the OSI Transport service.

A SAP is similar to a Berkeley socket. A BSD (Berkeley Software Distribution) socket is a “pipe” between an application and TCP or UDP used to create connections and send/receive data.

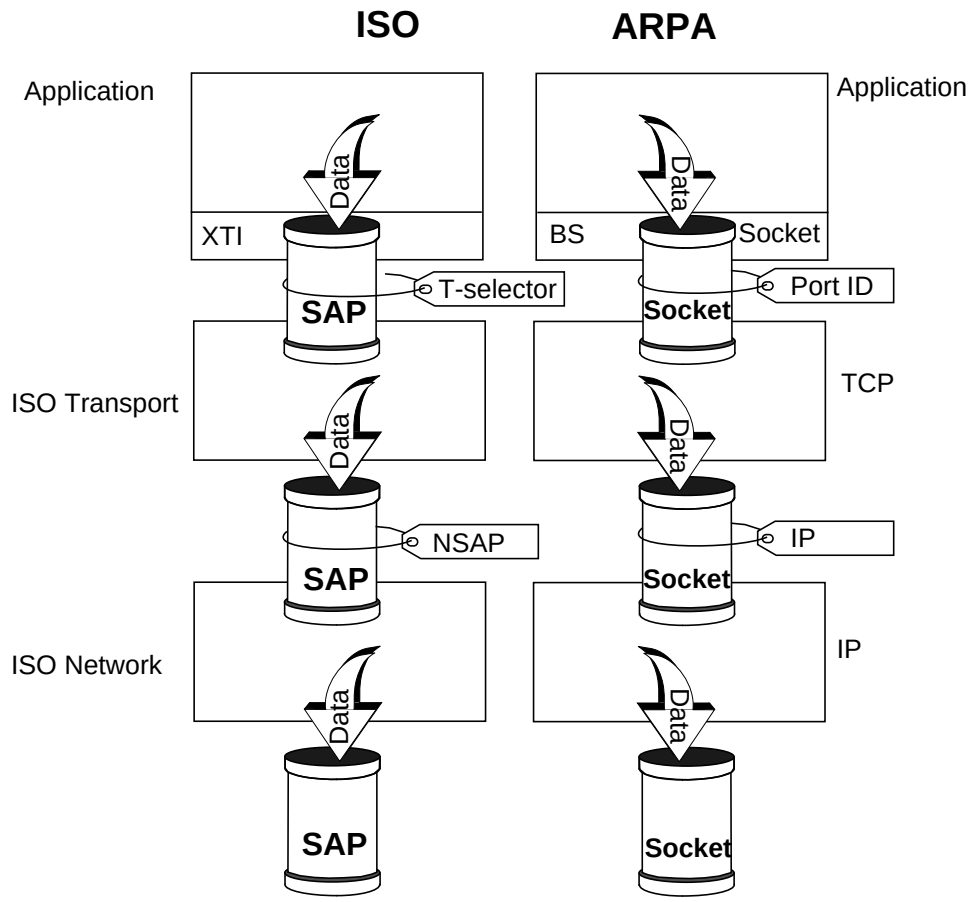
SAPs may be created between any adjacent layers in the ISO protocol suite. These SAP “pipes” can then be connected together to form a whole “conduit” through the protocol stack that allows a user to send data to, and receive data from, a remote system.

Figure 1-3



In the ARPA protocol suite, “conduits” through a protocol stack are relatively simple. They consist of a layer 4 (TCP or UDP) SAP (socket), and an IP SAP. The situation is more complex in ISO because “conduits” can extend from layer 3 up to layer 7, so several SAPs may be required to build a complete “conduit” for an ISO application.

Figure 1-4



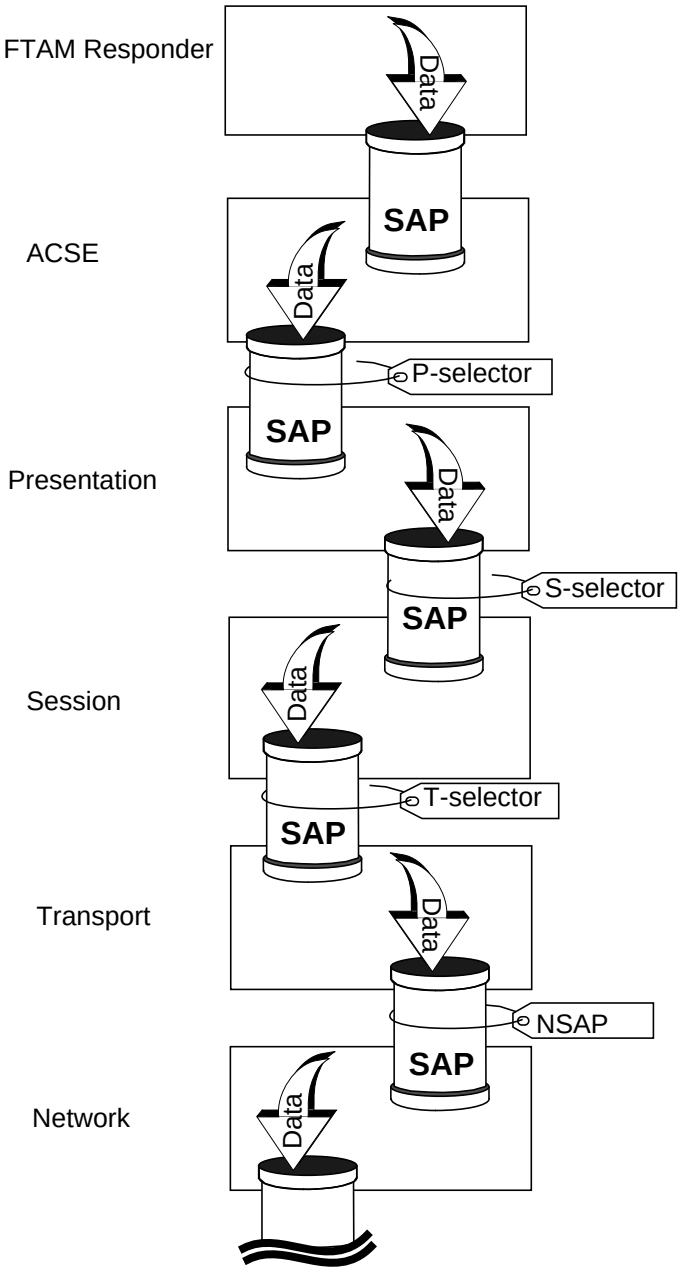
Selector - A selector is a sequence of octets (bytes) used to identify a SAP. Using the BSD socket analogy, a SAP is the socket, a selector is the two octet Port ID that is bound (using *bind()*) to the socket. When a selector identifies a specific SAP at a specific layer, it is referred to as either a P-selector, S-selector, or T-selector, so it is clear which layer the selector is associated with.

NOTE Because of the relationship between SAPs and selectors, the terms are sometimes used synonymously. If the term SAP (for example, PSAP, SSAP, TSAP) appears in HP documentation, it should be taken to mean the selector (that is, P-selector, S-selector, T-selector) representing the SAP.

Address - An address is a sequence of selectors, plus at least one NSAP (network service access point), that identifies an entire "conduit" through a protocol stack. For instance, in the case of FTAM, the address of its "conduit" includes the presentation, session, transport, and network layers. Its address is therefore: a P-selector, S-selector, T-selector, and one or more NSAPs. This address is commonly called a presentation address (P-address) since it defines a "conduit" whose top-most layer is presentation. More than one NSAP may be included in a P-address because the system may be reachable on more than one network (for example, a system that is accessible via both a CONS network and a CLNS network). This situation is similar to an ARPA system that is connected to more than one IP network and therefore has more than one IP address.

Applications access SAP "conduits" by using a programmatic interface. An example of a programmatic interface is X/Open's Transport Interface (XTI), that gives applications the ability to communicate with remote systems using the OSI Transport layer. The application tells the programmatic interface which "conduit" to use by passing an address to the appropriate interface procedure call. In the case of XTI, the address of the "conduit" a local application wishes to listen on is passed during the t_bind() procedure call. If the local application wishes to communicate with a remote application, it passes the remote application's address to XTI during the t_connect() procedure call.

Figure 1-5 FTAM Presentation Address



Network Layer

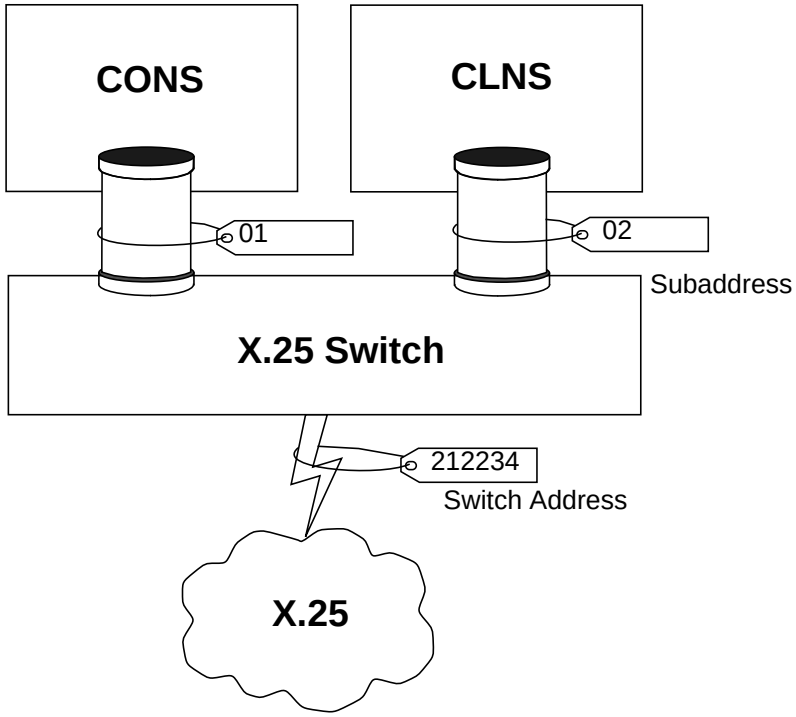
Unlike the ARPA protocol suite that only has a single network protocol (IP), ISO has defined two network layer services: CONS (Connection-Oriented Network Service) and CLNS (Connectionless Network Service). OTS supports CONS over the X.25 protocol, and CLNS over the X.25 and 802.3/ FDDI protocols. The OTS programmatic interfaces, such as XTI, are designed to allow applications to communicate over either network service. The choice of which service (CONS or CLNS) to use is made in one of two ways. The first way is by OTS automatically examining the destination address and determining over which network service this address may best be reached. The second way to use the HP-UX bind command to specifically identify one service or the other.

The OSI protocol suite communicates with other systems over physical subnetworks. Examples of physical subnetwork types are X.25 and 802.3. An address as defined above is used by the OSI protocol suite to route information up from, and down to, the network layer. It is the job of the network layer to route information to destination NSAPs over the proper subnetwork. This is called network routing.

Network routing is accomplished by associating a destination NSAP with its point of attachment on a physical subnetwork, that is, the point on a physical subnetwork where that NSAP may be reached. An NSAP's point of attachment onto a subnetwork is identified by a subnetwork address.

On an X.25 subnetwork, a point of attachment is identified by an X.121 address. An X.121 address is one to 15 digits in length and has two parts: the switch address portion, and the subaddress portion. The switch address tells the X.25 protocol which switch on the subnetwork is the destination. The subaddress portion tells the switch which entity above X.25 is to receive the sent information.

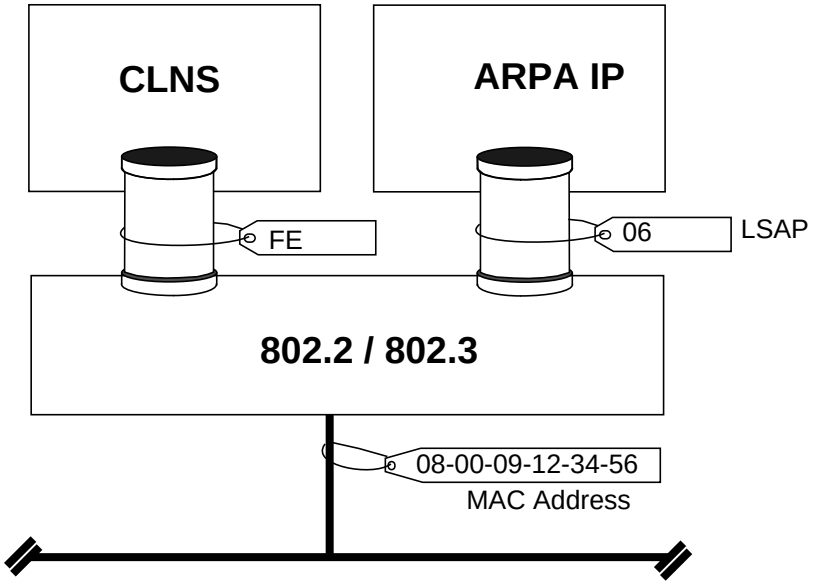
Figure 1-6



In this example, two X.121 addresses have been defined: the subnetwork address for the CONS entity is 21223401, and the subnetwork address for the CLNS entity is 21223402.

NOTE Although the use of subaddresses is the recommended method to identify different X.25 users, some switches and X.25 networks do not support its use. If this is the case for your installation, see the Installing and Administering OSI Transport Services manual for more information.

Figure 1-7



On an 802.3 subnetwork, a point of attachment is identified by an IEEE MAC address. Instead of configured subaddress portions, the 802.3 protocol uses embedded, well known LSAP (Link Service Access Point) values for the CLNS and ARPA IP entities.

The network layer obtains its routing information in one of two ways: automatically using the ISO End System to Intermediate System Routing Protocol (ES-IS), or from statically configured tables entered by using the OTS Destination System and Routes configuration screens in osiadmin.

Structure of NSAP Addresses

A Network Service Access Point address (NSAP) is the ISO-defined Internet Address. It is used to identify real systems unambiguously on a network. NSAPs are used by OTS/9000 in much the same way as ARPA Internet addresses are used by TCP/IP.

There are several documents that may help you better understand this section. Among them are:

- ISO 7498/AD3, Information Processing Systems - Open Systems Interconnections - Addendum to the OSI Reference Model Covering Naming and Addressing
- ISO 8348/AD2, Information Processing Systems - Data Communications - Addendum to the Network Service Definition Covering Network Layer Addressing
- ISO 9542, Information Processing Systems - Data Communications - End System to Intermediate System Routing Exchange Protocol for Use in Conjunction With the Protocol for the Provision of the Connectionless-mode Network Service [ES-IS Protocol]
- ISO 10589, Information Processing Systems - Data Communications - Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol [IS-IS Protocol]

These documents, as well as many others, are available for a small fee from:

Omnicom, Inc. 115 Park Street, SE Vienna, Va 22180-4607 USA
Telephone: (USA) 703 281-1135

Omnicom International, Ltd. 17 Park Place Sevenage, Herts. SG1 1DU UK Telephone: (UK) 44 438 742424

Other documents describing specific addressing formats are mentioned in their respective sections.

The structure for NSAP addresses discussed here has been formulated to meet the following objectives:

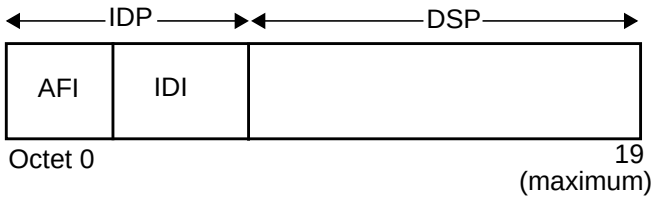
- Provide a framework so that HP can recommend a management strategy.

- Take into account the needs of different network types (individual or "small," sophisticated or "big," and intermediate).
- Facilitate efficient routing in private networks.
- Provide a strategy that takes advantage of dynamic routing protocols such as ES-IS and the emerging IS-IS protocols.
- Minimize the risk of re-structuring, due to present lack of universally accepted standards for NSAP structures.
- Minimize the risk of re-allocation of values, due to present lack of administrative authorities.
- Propose a method for automatic allocation of unique NSAP addresses.

The Syntax of an NSAP Address

An NSAP, as defined by ISO, has several characteristics. It may be one to twenty octets (bytes) in length. It is composed of two parts: the Initial Domain Part (IDP) and the Domain Specific Part (DSP). The DSP may also be partitioned into several fields. These fields and their sizes are defined by the authority that controls the IDP.

Figure 1-8



The Initial Domain Part

The IDP portion of an NSAP declares which national or international group owns the right to manage an NSAP space. This group is called an authority. Examples of authorities that presently manage NSAP spaces are AFNOR, ANSI and NIST. They have been given, by ISO, specific IDP values that they control and have the right to use for the distribution of NSAP addresses. As an example, NIST has been given the IDP value 470005 for use within the U.S. GOSIP networks. Therefore, any NSAP

that begins with this value is ultimately under the control of NIST. NIST also owns the right to define how the DSP portion of its NSAP space is to be formatted and used.

The IDP contains two fields. The authority and format identifier (AFI) field identifies the type of address used in the DSP. The initial domain identifier (IDI) field identifies which domain the DSP part belongs to.

NOTE In this section, all numeric values are represented as hexadecimal digits unless otherwise specified.

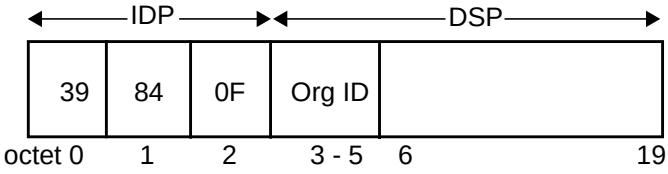
The Domain Specific Part

The purpose of the DSP is to

- allow authorities to further delegate control of NSAP addresses
- uniquely identify a real open system unambiguously on the network
- provide information that may be used to facilitate the routing of data on concatenated subnetworks

This is accomplished by dividing the DSP into a number of fields, each with its own meaning. As an example, consider the format defined by ANSI:

Figure 1-9



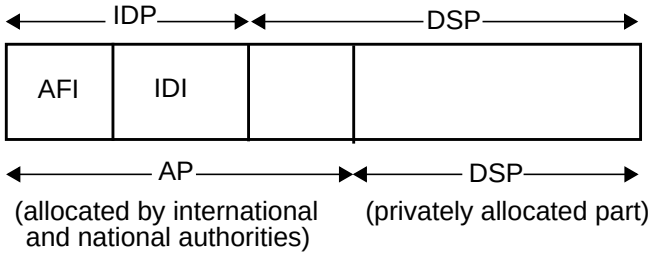
The AFI value of 39 indicates that the IDI portion will be a Data Country Code (DCC), and the DSP will be encoded in binary. The value 840 (padded with F) is the DCC for the United States.

ANSI has defined the first three octets of the DSP to contain an Organization Identifier (Org Id). This number, assigned by ANSI, allows other organizations to control a subset of ANSI's NSAP space. ANSI has left the rest of the DSP undefined so that the organization will have the ability to define its own address structure. For instance, if Joe's Grommet Shop petitions ANSI for an Org Id value and is assigned the value 010101 (three octets), then Joe's Grommet Shop controls the prefix

39840F010101. Any NSAP that begins with this value is under the control of Joe's Grommet Shop. Joe's Grommet Shop may also define the format for the rest of the DSP to suit their needs.

The fields of an NSAP create a hierarchy where each field further divides the NSAP space into smaller, more manageable spaces. Also, the leftmost portion of an NSAP deals with the administration of NSAP spaces, not specifically with the identification of real systems. In the above example, the leftmost part of the NSAP space is "publicly" administered, that is, administered by national and international standards bodies, whereas the right part is left up to private organizations to define and use. For convenience, these two parts will be called the administrative prefix (AP), and the privately allocated part (PAP).

Figure 1-10



This separation between what a network administrator is given and what the administrator controls is very important. It is the key to understanding how an NSAP space is managed. Also, some companies may have several different APs, or may start with one AP and have to migrate over to a different one at some point in time. Only through careful management of the PAP can a network administrator minimize the problems that this may cause.

The Privately Allocated Part

Whereas the AP is used to administer NSAP spaces, the PAP is used to define a routing strategy. The two portions, when combined together, yield a unique NSAP for a given system.

The ISO model of routing contains the following levels:

Subnetwork - A subnetwork is an autonomous collection of equipment and medias used to interconnect systems. Examples of types of subnetworks are: IEEE 802.3 LANs and X.25 PDNs.

Area - An area is a group of end systems and intermediate systems interconnected by one or more subnetworks. They have been grouped together by way of an autonomous routing mechanism. An autonomous routing mechanism is either a set of statically configured intermediate systems, or a set of intermediate systems that support a dynamic routing protocol, such as the ISO IS-IS protocol.

Routing Domain - A Routing Domain is also a group of end systems and intermediate systems interconnected by one or more subnetworks. They have been grouped together by way of some routing or security policy defined by the network administrator. Typically, a number of areas are grouped together to form a routing domain.

An area may be composed of one or more subnetworks. The criteria for grouping subnetworks into areas can be based upon topology, reachability, and network traffic. The criteria for grouping areas into routing domains is based upon policy. For instance, a company might want to create an area for their factory, and area for their product design lab and put them in the same routing domain. However, the company may choose to create a separate routing domain for their accounting and payroll departments.

To facilitate routing strategy, a network administrator will often define the PAP to contain one or more of the following fields:

- Routing Domain Identifier
- Area Identifier
- Subnetwork Identifier
- End System Identifier

The order they are listed here is the order, left to right, in which they would be defined in a PAP.

Other fields that often find their way into the PAP are:

Version Number or DSP Format Identifier - The purpose of these fields is to allow a network administrator to redefine the PAP structure at a later point in time, or allow the network administrator to define several PAP formats. Each format would be identified by a different value in the Version Number or DSP Format Identifier field.

Reserved field - This is simply a portion of the PAP that is not in use, but has been reserved in case it is needed some time in the future. If the network administrator defines a PAP with a reserved field, a default value (usually all 00s) should be defined that the reserved field is always set to.

NSAP selector - A one octet field at the rightmost portion of the PAP. It identifies the entity attached to the network layer. In OTS the entity is always the transport protocol. HP recommends that the NSAP selector be set to 01.

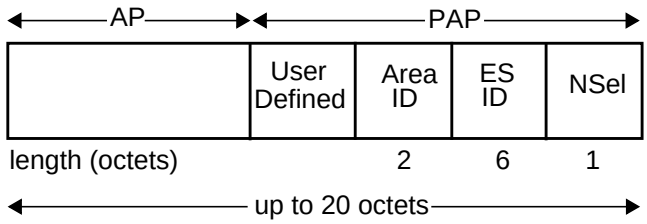
The section on current allocation formats, and the section on recommended PAP structures show examples of how these fields are used to manage NSAP spaces and routing topologies.

ISO IS-IS Routing protocol - ISO is in the process of defining a protocol standard for a dynamic Intermediate System to Intermediate System routing protocol, known as the IS-IS protocol. This protocol, when complete, will allow Intermediate Systems (the ISO term for network layer routers) to automatically route traffic between each other across concatenated subnetworks and areas. It will not, however, automate routing traffic between routing domains. This will still require static configuration of route information.

Though the protocol is still in development, ISO has defined a format for the rightmost portion of the DSP to be used by the IS-IS protocol for its automated routing. Network administrators should use this format whenever possible so that it is easier to support the IS-IS protocol once it becomes available.

The format defined by ISO is the following:

Figure 1-11



Area ID	A two octet field containing a unique ID for the area on which the NSAP resides.
ES ID	A six octet value, unique within the Area, which identifies the end system.
NSel	A one octet value. The recommended value is 01.

This format is commonly called the 2/6/1 structure because of the sizes of the three defined fields.

This is the format that NSAP addresses should obey in order to get the most use out of the automated routing protocols. See the section “A Recommended PAP Structure” later in this chapter for a possible PAP structure that network administrators may use to define NSAP formats. This recommended structure is compatible with the IS-IS protocol format.

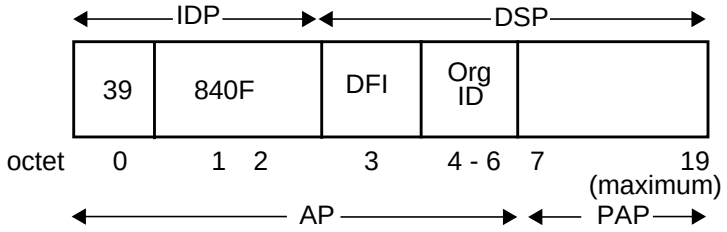
Current NSAP Allocation Formats

This section shows a number of examples for existing NSAP allocation formats. Other standards organizations may have additional formats that customers may want to use. Customers can contact standards organizations within their home country to obtain more information.

NOTE HP recommends that customers use the binary format for NSAPs. Therefore, only this format is discussed here.

ANSI Format

Figure 1-12



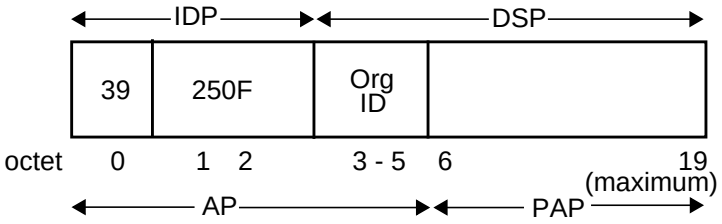
ANSI is the standards body that controls the United States Data Country Code (DCC) 840. They have defined the first three octets of the DSP to be an Organization Identifier, leaving the other 14 octets (the PAP) to be defined by each controlling organization. ANSI may be reached at the following address:

American National Standards Institute 1430 Broadway New York, New York, 10018, USA Telephone: (USA) 212 642-4932

NOTE ANSI defines a recommended PAP structure for their NSAP space. Its syntax may be obtained by writing to the above address.

AFNOR Format

Figure 1-13

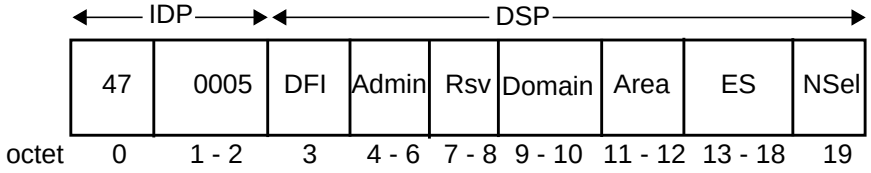


AFNOR (Association Francaise de NORmalisation) is the standards body that controls the French Data Country Code (DCC) 250. Like ANSI, they have defined the first three octets of the DSP to be an Organization Identifier, leaving the other 14 octets (the PAP) to be defined by each controlling organization. AFNOR describes their addressing format in its document, X 60-000. AFNOR may be reached at the following address:

AFNOR Tour Europe - Cedex 7 F-92049 PARIS LA DEFENSE (FRANCE) Telephone: +33 1 42 91 55 55

United States GOSIP

Figure 1-14



DFI	DSP Format Identifier. This is used to specify the structure, semantics and administration requirements for the remainder of the DSP. Currently, only one DSP Format exists. This field is similar in function to a Version field.
Admin	This field functions in much the same way as the Org ID field in the ANSI format. It is an Administration authority identifier. The values for this field are under the control of NIST.
Rsv	Two octets are reserved for future expansion.
Domain	The Routing Domain this NSAP resides in. Routing Domain values are determined by the authority identified by the Admin field.
Area	The Area number this NSAP resides in. Area values are determined by the authority identified by the Admin field.
ES	A number, unique within the area, that identifies the end system. End System identifiers are determined by the network administrator
NSel	This field identifies the Network Service user. U.S. GOSIP recommends this value be set to 01 for the Transport protocol.

The United States GOSIP format, whose administration authority is NIST, is to be used by United States Government agencies for their OSI networks. NIST will also assign NSAPs from their NSAP space to non-government organizations upon request.

This format is a good example of how the various PAP fields may be used to create a well defined NSAP space that can evolve over time. U.S. GOSIP has taken a domain/area approach to routing and has defined the entire structure of the DSP. Because of this, they have also added some fields that will allow their structure to change over time, namely the DFI and Rsv fields.

To obtain more information about the U.S. GOSIP NSAP structure, contact:

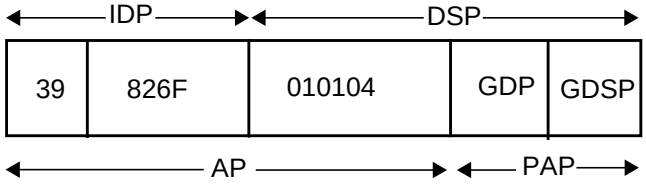
Telecommunications Customer Requirements Office U. S. General Services Administration IRMS Office of Telecommunications Services 18th & F Sts. N.W. Washington, D. C., 20405

A more complete discussion of this addressing format may be found in *U.S. Government OSI Profile Specification Version 2*.

This document is produced by the National Institute of Standards and Technology, USA (NIST). It should be available through Omnicom or NIST.

United Kingdom GOSIP

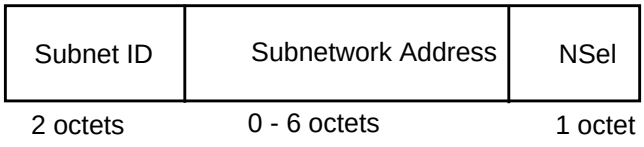
Figure 1-15



GDP	Government Domain Part (one octet)
GDSP	Government Domain Specific Part (up to 11 octets)

The United Kingdom GOSIP program, like ANSI, has chosen the Data Country Code format for their IDP. GDP values are provided by the Central Computer and Telecommunications Agency (CCTA), and functions in a similar fashion as U.S. GOSIP's Admin field. The GDSP is undefined and is left up to the controlling organization (identified by the GDP) as to its structure. U.K. GOSIP recommends that the following fields be defined as the rightmost portion of the GDSP:

Figure 1-16



The Subnetwork Identifier may identify a physical subnetwork, or an area. The Subnetwork Address field may contain a real subnetwork address, such as a MAC or X.121 address, or a virtual end system identifier that uniquely identifies the end system for the specified Subnet ID. HP recommends that the NSel field be set to 01.

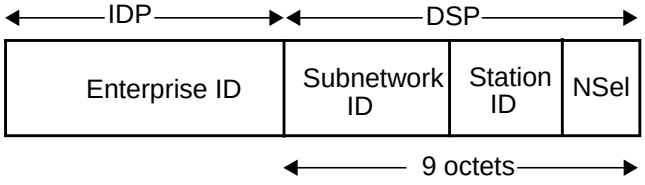
A more complete discussion of this addressing format may be found in *U.K. Government OSI Profile Specification Version 3.1* and *Procedure for Obtaining a U.K. Government Domain Part (GDP) under the ISO DCC Addressing Scheme.*

These documents are produced by the Central Computer and Telecommunications Agency, UK. They should be available through Omnicom International, Ltd. or CCTA.

GOSIP Project Office CCTA Riverwalk House 157/161 Millbank LONDON SW1P 4RT UK

MAP/TOP 3.0

Figure 1-17



Enterprise ID	The AP portion of the NSAP. It includes the AFI, IDI and, if necessary, an Org ID.
Subnetwork ID	A portion that uniquely identifies the Subnetwork on the Enterprise.
Station ID	A portion that uniquely identifies an end system on the subnetwork
NSel	The field that identifies the entity above the network layer.

Unlike ANSI and AFNOR, which defined an AP and left the PAP undefined, MAP/TOP has defined a general format for the PAP portion. Their PAP may be used with any valid AP.

MAP/TOP has decided to use subnetworks as their level of routing rather than areas. This is more in line with present ARPA routing procedures than the upcoming ISO routing protocols. MAP/TOP does recommend that the customary 2/6/1 field lengths be used for the PAP portion to allow easy migration to area-based routing in the future.

A more complete discussion of this addressing format may be found in *Manufacturing Automation Protocol Specification, Version 3.0*, available from the MAP/TOP users group:

North American MAP/TOP Users Group ITRC P.O. Box 1157 Ann Arbor, MI 48106 USA

Building Temporary Administrative Prefixes

In many cases, the examples above will not fit the needs of many users. This is because they are not government organizations, the company does not reside in a country which has an NSAP authority, or the company does not wish to pay the registration fees required to obtain an NSAP space.

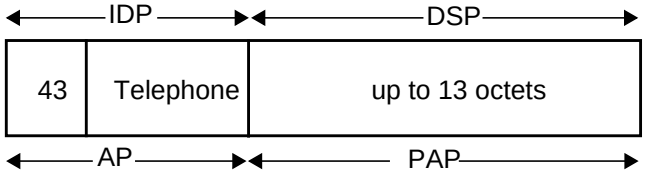
In cases like these, a network administrator can create a temporary Administrative Prefix that their company may use as an interim solution until a more permanent AP becomes available. The network administrator must be sure to create a PAP format that can easily be migrated to the permanent NSAP space, once it becomes available.

The first two methods described create a unique NSAP space, and the NSAP addresses may be used on open networks (that is, networks connected to a public network). The last method, Local Format, does not guarantee a unique NSAP space and should only be used when connectivity to OSI networks outside the customer's network is not required.

Use an International Telephone Number

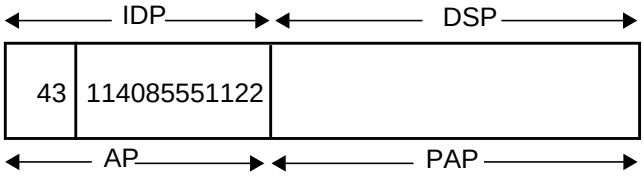
ISO allows NSAP spaces to be built that have an International Telephone Number as their IDI value. This is known as the E.163 format. The AFI code to use is 43. The telephone number is encoded as Binary Coded Decimal (BCD) into the IDI. Up to 12 digits may be used. Any unused digits should be set to F (hexadecimal). The DSP portion, and therefore the PAP, may be up to 13 octets in length.

Figure 1-18



As an example, suppose Joe's Grommet Shop decides not to obtain an ANSI Org Id at this time. Instead, they use the E.163 format. The network administrator decides to use the International Telephone Number of their customer order department for the IDI value.

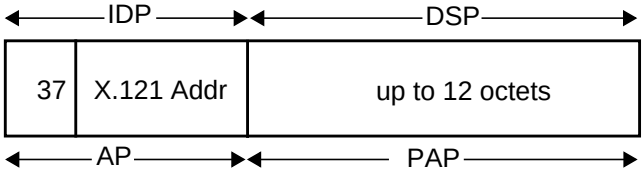
Figure 1-19



Use an X.121 Address

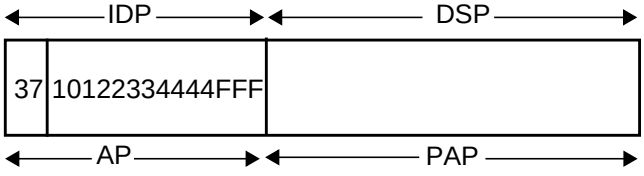
Another option is to use an X.121 address as the IDI value. The AFI for this format is 37. The IDI is up to 14 BCD encoded digits, with any extras padded with F. The DSP, and therefore the PAP, may be up to 12 octets in length. Note that the X.121 address is only used to uniquely identify the customer's AP. It does not have any routing significance in this example.

Figure 1-20



For instance, Joe's Grommet shop decides to use one of its public X.121 address for the IDI value.

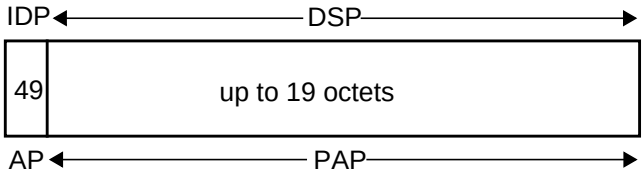
Figure 1-21



Use the ISO Local Format

ISO defines a format known as the Local format. HP recommends that you do not use this format because it can result in non-unique NSAP values. They should only be used for pilot networks or for diagnostic purposes on networks that are isolated, that is, not connected to any public networks.

Figure 1-22



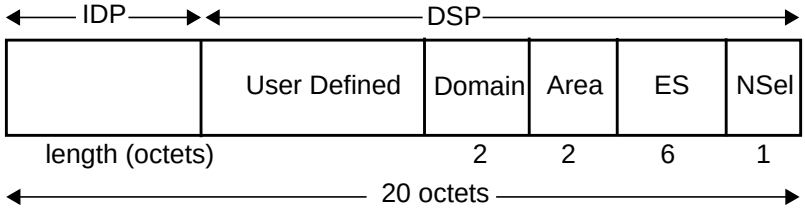
When using Local Format it is especially important to create and manage the PAP portion in a way that can be easily migrated to another AP in the future.

A Recommended PAP Structure

Here is an example of a PAP structure that may either be used with a current allocation format that allows the PAP to be defined (such as ANSI), or with a temporary AP.

The last portion of the PAP should have the following structure:

Figure 1-23



User Defined	A unique, user defined number.
Domain ID	A two octet field containing a unique ID for the routing domain on which the NSAP resides.
Area ID	A two octet field containing a unique ID for the area on which the NSAP resides.
ES ID	A six octet value, unique within the area, that identifies the end system. Possible values that may go here are: If the NSAP is to be used over 802.3, the MAC address may be used. If the NSAP is to be used over X.25, and the X.121 address space is 12 digits or less, the X.121 address may be used. The X.121 address is entered as BCD digits, two digits per octet. If the X.121 address has an odd length, pad the last octet with F.
NSel	A one octet value. The recommended value for OTS is 01.

The above PAP allocation follows the structure used by the IS-IS protocol. It allows areas to be created that contain multiple subnetworks.

The User Defined portion may be comprised of one or more of the following fields:

- A version or DSP format identifier. This allows the format of the PAP to be redefined at some later point in time. These fields are usually two octets in length, but any size may be chosen. For most NSAP spaces, one octet will often be sufficient.
- A reserved field. It is often a good idea to reserve a few octets of space for future use.

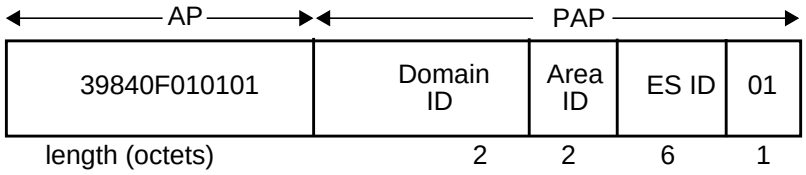
If any of these fields are used, they should be defined in the order, left to right in the PAP, as they are listed above.

Network Identifiers (Network ID)

Because of the hierarchical definition of NSAP formats, a prefix portion of an NSAP may be used to identify a group of systems that reside in the same routing domain, the same area, or the same subnetwork. This prefix portion is called an “NSAP Prefix,” or a “Network ID.”

As an example, suppose Joe’s Grommet Shop, whose AP value is 39840F010101, decides to use the Recommendation 1 format for its PAP.

Figure 1-24



It has two areas in routing domain 0000 that are assigned Area ID values: 0001 and 0002. The corresponding Network IDs for these areas are: 39840F01010100000001 and 39840F01010100000002.

Network IDs may be used in OTS to simplify the configuration of routing information. Rather than configuring a route to every remote system, OTS allows network administrators to configure a route to a distant routing domain, area, or subnetwork by using its Network ID. It also allows local subnetworks to have their Network IDs configured to help the routing protocols with local network traffic.

General Recommendations for NSAP Addresses

Here is a list of recommendations by HP for the allocation of NSAPs for use with OTS:

- Use an Administrative Prefix obtained from a national or international authority if at all possible. An authority does not have to reside in the same country as the petitioning organization (for example, a company in Spain could petition AFNOR for an Organization Identifier).
- If the Local Format is to be used, the network must be completely isolated from public network traffic. If a customer needs a temporary AP, they should use a International Telephone Number, or the X.121 format.
- Use the binary AFI value whenever possible.
- If using a temporary AP, limit the length of the PAP to 14 octets or less. This will allow the PAP to fit into the space allowed by a national or international authority's AP in the future.
- If using an AP allocated by an international or national authority, define all 20 octets of the NSAP, even if this means allocating a reserved field.
- Define and manage the PAP address structure independent of the AP. This will make managing multiple AP values, or migrating between AP values easier. This especially includes the following fields:

  Area ID Routing Domain ID Subnet ID

  All the above fields should be unique regardless of AP value, even if the authorities administering the APs have defined the full DSP. For instance, if a network administrator is managing a MAP network and a U.S. GOSIP network, the values used in the Subnet ID fields for the MAP network NSAP addresses should not be reused in the Area ID values in the U.S. GOSIP NSAP addresses.
- All fields should be defined to fall on octet boundaries, that is, they should always contain an even number of hexadecimal digits.
- To be compatible with the ISO IS-IS Routing Protocol, the last three fields of the PAP should conform to the 2/6/1 format.

Non-standard NSAP Formats for Use in OTS

If the CONS network being used supports the 1984 X.25 Extended Address facility, the NSAPs configured should conform to the above recommendations.

If the CONS network being used is version 1980, or does not support the Extended Address facility, use the X.121 address of the system's attachment point onto the X.25 network in place of an NSAP.

For subnetworks that use the Null Subset of CLNP, the subnetwork address, either MAC or X.121, of the system's point of attachment onto the subnetwork should be used in place of an NSAP.

2 Planning Your Network

The process you should use to successfully bring up a new OSI network or add to an existing OSI network

Planning Your Network

This chapter describes the process you should use to successfully bring up a new OSI network or add to an existing OSI network.

The following steps should be taken to get your OSI network up and running:

Task	Action	Chapter
1	Determine the services required	this chapter
2	Determine the vendors involved	this chapter
3	Determine the network structure	this chapter
4	Determine your addressing scheme	this chapter
5	Gather and distribute configuration information	"Gathering Configuration Information"
6	Install software	"Installing OTS/9000"
7	Configure systems	"Configuring and Verifying OTS/9000"
8	Start up systems (if needed)	"Configuring and Verifying OTS/9000"
9	Perform local verification	"Configuring and Verifying OTS/9000"
10	Perform interoperability tests	*OSI Troubleshooting Guide*

Determine the Services Required

The first step in planning your network is to identify what communication problems you are trying to solve and what OSI service or services best address your needs. This section describes each service provided by Hewlett-Packard and when it may be appropriate for meeting your communication needs.

X.400 Service

Type of Service	Use if:
Message Handling (Electronic Mail)	You require electronic messaging between users of the OSI network

- Allows encapsulation of electronic information and reliably deliver it to one or more destination users.
- Messages are transferred in a store and forward manner, not real-time.

CMIS Service

Type of Service	Use if:
Management of “managed objects”	You want distributed management of nodes and other network resources.

- Can enable and disable network resources.
- Can view and change configurable values.
- Can register for notification of exceptional events.

- Can act as a requestor of operations against a resource (a manager), or only as a responder to such requests (an agent), or both.
- Provides a programmatic interface to CMIS, which allows you to write applications acting as either a requestor or a responder.

FTAM Services

Type of Service	Use if:
File Transfer	You wish to move or manage files across an OSI network.

- Allows transfer of files across an OSI network.
- Provides facilities to create, delete, and modify files on a remote node.
- Has both a programmatic and interactive interface.

APRI Service

Type of Service	Use if:
General interprocess communication mechanism	You are porting layer 7 protocols to the HP platform, developing specialized layer 7 applications, or remote operation applications.

- Provides you with the ability to implement your own OSI application layer protocols, or custom applications.
- Provides Abstract Syntax Notation One (ASN.1) context negotiation.
- ROSE provides remote operation capabilities to invoke operations on the remote and receive status on completion. This service runs on top of the service provided by ACSE and Presentation.

High Availability Service

Type of Service	Use if:
Create and manage highly available clusters	You wish to create and manage highly available enterprise clusters of HP9000 Series 800 computers using the HP MC/ServiceGuard product.

- Allows you to group programs in “packages” which run on particular nodes.
- Monitors the health of your SPU, LAN cards, and application “packages” on each node.
- See the HP OTS/9000 Addendum for more information on configuring and using HP MC/ServiceGuard with HP OTS/9000.

XTI Service

Type of Service	Use if:
Transport layer interface	You are porting existing IPC applications that run over non-OSI networks and for achieving high performance as a result of low protocol overhead.

- Provides a very simple set of functions, for example, connect, send data (normal and expedited) and disconnect.
- Building blocks that provide a basic and low overhead access to performing interprocess communication over an OSI network.
- Makes your application source code portable between platforms following the standard.

Determine the Vendors Involved

Another factor in determining the ultimate layout of your network is the equipment various vendors use to communicate.

Not all vendors provide every OSI service. A given vendor may only provide some subset of functionality for a given layer. For example, HP does not currently provide the Virtual Terminal service. Another vendor may not provide X.500. Or another vendor may provide a Network Management Agent, but have no facilities to manage the resources local to that node.

When planning your network, you need to take such factors into consideration. Listed below is a checklist of items you should investigate to help ensure your success.

- Does the vendor provide this service?

  If you wish to communicate with a piece of equipment, it must support the service. Access to mid-stack layers (Session, Transport) cannot be assumed just because a vendor provides a seven layer stack.

- Does this service coexist with other facilities I want to use on this node?

  Determine what effects installing this product has on the other operations of your system. Especially check on its coexistence with other non-OSI networking services you may be using.

- What version of this service is provided?

  Some standards are evolving. For example, Session provides both Version 1 and Version 2. Verify that the version supported is acceptable to all nodes of communication you intend to use.

- What functional units of this service are provided?

  Many OSI implementations are a subset of the full service. You should understand what facilities you require from this service and ensure that each vendor supports those.

- What lower layer protocols does this product use? What versions are these? Can I use it over the link I want?

Verify that the underlying layers are compatible. The primary considerations are Session version and functional units, Transport Layer class, Network Layer protocol and link type. For more detailed questions about the links used, see "General LAN Questions" and "General X.25 Questions."

- What is the interface to this product? Is it standardized? Does it meet my needs?

  The interfaces to the OSI services can be broadly broken into two categories:

  - interactive, where you type commands, or select choices from a menu
  - programmatic, where you develop your own program (typically in C) using a set of OSI library commands

  Support of a standard interface will increase the portability of your applications and make the transition from one platform to another simpler.

- What level of conformance or interoperability testing has been achieved by this product?

  Conformance testing indicates that an implementation has successfully passed a suite of tests against a reference OSI implementation. Such testing improves the chances that the implementation is correct and that it will interoperate with other conformant systems.

  Interoperability testing is a direct test between two vendors' implementations.

- Who will install, configure and test this product?

  If you will not be doing the entire installation yourself, you should coordinate with the other individuals involved. HP provides a remote system worksheet that you can use to gather information for these other systems. See chapter 4.

General LAN Questions

- Is ES/IS (end system/intermediate system) protocol supported?

  Most systems today support the ES/IS protocol. This protocol allows systems to dynamically maintain information about the NSAP to MAC address mapping for systems on a LAN. By using this protocol, a great deal of configuration can be avoided.

- Can this system behave as an IS?

  An intermediate system is capable of forwarding traffic from one subnetwork to an IS on another subnetwork. This system should support both the ES/IS and IS/IS protocols. HP systems do not behave as an IS.

- Will this subnetwork use the NULL subset of CLNS?

  The NULL subset of CLNS is used for systems that are on an isolated LAN network. When NULL subnetting is used, no traffic can be forwarded via routers.

  The benefit of the NULL subnet is reduced protocol packet size (on the order of 40 bytes per packet).

  The drawback is the inability to communicate outside the subnetwork.

- Is your LAN link configured for IEEE 802.3?

  If you want to configure OTS CLNS over 802.3, you must use SAM to configure your LAN link to use IEEE 802.3.

General X.25 Questions

- Is ISO 8878 behavior supported?

  ISO 8878 defines how X.25 is to be used to provide CONS. Among other features:

  - It defines a mechanism for conveying NSAPs in 1984 and 1988 X.25 CALL packets. OTS supports full 8878 by default.
  - Defines a “special” mechanism, called SNDCP, which simulates this behavior on 1980 X.25 networks. Many OSI implementations do not support the SNDCP behavior.

  The configurable parameter, “snet_allow_iso8878”, in the file “ots_subnets” controls whether or not OTS will use the SNDCP when communicating over 1980 X.25.

- What versions of X.25 will be used?

  There are three versions of X.25 support: X.25 ‘80,’84, and ‘88. Each is effectively a superset of the previous. Sending X.25 ‘84 traffic to an X.25 ‘80 system may result in connection refusal. It is important to understand what systems support which protocol. OTS by default sends X.25 ‘84 packets and receives both X.25 ‘80 and ‘84.

- What level of X.25 switch or PDN should I use?

  If your switch or Public Data Network only supports X.25 ‘80, then systems connected through it must use X.25 ‘80. Otherwise ‘80, ‘84, and ‘88 are acceptable.

- Is subaddressing supported?

  HP recommends use of subaddressing in order to share the same physical card with various services. If subaddressing is not supported, then you will be restricted to configuring a single CONS and a single CLNS network through each card. For a discussion of the parameter see “snet_bind_by_pid” in the “ots_parms”.

- Are Protocol ID values used?

  If the remote can accept calls using the NULL PID, then you can safely set the “tpcons_null_pid” parameter. OTS by default sends the PID. The parameter “tpcons_null_pid”, in the file “ots_parms” can override this behavior.

By default, OTS will also accept call packets with either the OSI or NULL PID values. Setting the “snet_bind_by_pid” parameter in the “ots_subnets” file will prevent OTS from accepting CALL requests using the NULL. If set, OTS will refuse calls with a PID other than the OSI standard PID.

- What Network layer protocols will be used (CONS, CLNS)?

  The Connectionless Network Service (CLNS) has the advantage in that it can be used with routers and does not require the gateway facility provided by MSDSG in order to interconnect with CLNS/LAN subnetworks. However, CLNS does present more overhead because each packet sent contains addressing information, and Transport Class 4 must be used.

  The Connection-Oriented Network Service (CONS) is currently more widely used than CLNS/X.25.

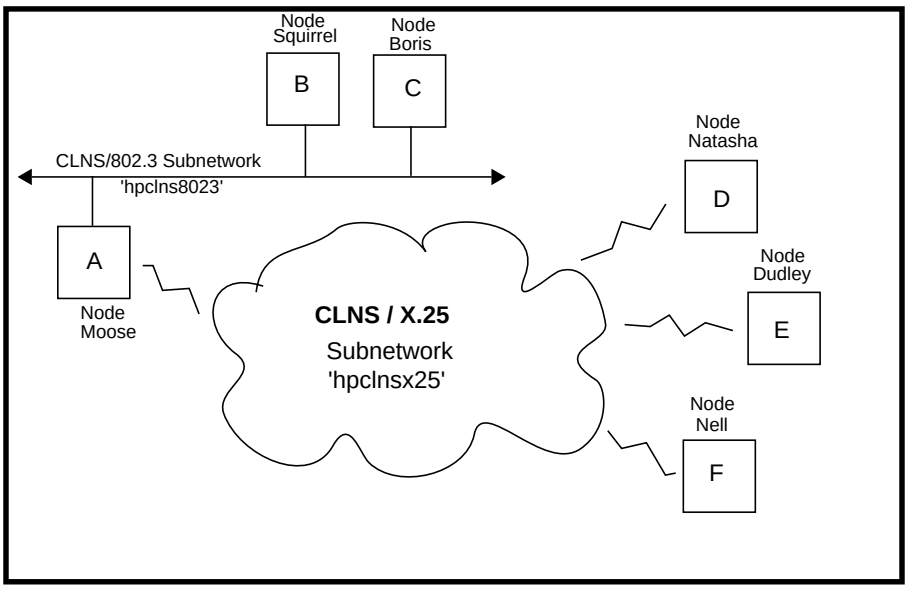
Determine the Network Structure

At this point, you have identified the nodes and the services you will be using for your network. The next step is to draw a network map to visualize the structure of your network.

If this is an addition to an existing network, update the existing network map, otherwise, follow these steps to draw your map. A simple example of a network map is shown below.

- Identify the subnetworks and nodes in your network.
- Assign unique names to each node and subnetwork and other pieces of network equipment.
- Draw the subnetworks, using lines for LANs and clouds for X.25.
- Place each node on the subnetworks you've drawn.
- Place any other pieces of network equipment on the diagram (for example, routers, repeaters, X.25 switches, and analyzers).
- Identify any non-OSI nodes or network equipment that may be sharing the network.

Figure 2-1



NOTE Information beyond the node name, such as X.25 subaddresses, network addresses, and applications, can be kept separately by making copies of the "Remote System Worksheet." See chapter 4, "Gathering Configuration Information."

Determine the Addressing Scheme

Network Address

At this point, you have determined the layout of your network. Now develop an addressing scheme that facilitates routing in your existing network, as well as future expansion.

Most network address formats allow you to segment your network into routing domains and areas. Examine your network map and consider:

- Areas should be defined as groups of subnets that are connected and have common bandwidth capabilities. For example, if you have two LAN subnetworks connected by an Intermediate System, you may consider them to be in the same area.
- Do not assign the same area ID to subnets that are connected to one another, but differ in bandwidth (for example, an X.25 subnetwork and a LAN subnetwork, or two LANs connected via a modem link).
- Areas should not contain more than 10,000 nodes. This is dictated by the IS to IS protocol.
- The assignment of domain identifiers is largely a policy decision. Any number of areas may be assigned to a single domain. However, a limitation of 10,000 areas per domain is a good rule.

  You may assign a single domain ID to your entire network unless the following criteria are true.

  - Any area that is isolated from another area should have a different Domain ID.
  - If, for security reasons, you wish to distinguish between traffic in different areas, you should assign different domain IDs to those areas. For example, could assign "Finance" and "Research" different domains.

After you have done the partition into domains and areas, you can then assign an appropriate network address prefix for each node, and the full address can be completed by using each node's End System address.

Application Addresses

You may also want to dictate the selector values to be used for the upper layer addresses. (Note that HP OSI services use default addresses. For instance, FTAM uses 0x0001 (hex) for P-, S-, and T- selectors. X.400 uses blank (null) P- and S- selectors and 4D4853 (hex) as the T-selector. Refer to the appropriate product manuals to see what, if any, default addresses are used.)

If you wish to change the default addresses, you might assign all FTAM responders to have the P-, S- and T-selectors of 0x0010. For an XTI application you are developing, you may want all initiators to use T-selectors 0x0020 and all responders to use T-selectors of 0x0021.

You have a wide array of addresses to choose from. The selectors may fall in the following range:

P-selector: 0 to 16 bytes

S-selector: 0 to 16 bytes

T-selector: 0 to 32 bytes

Remember that the longer or more complicated you make your selector values, the more room you leave for error during configuration.

NOTE Some government profiles may dictate the selector values for certain services (for example, U.S. GOSIP for FTAM and X.400).

Naming Hierarchies

If you are using FTAM o r X.500, you will use Directory Distinguished Names (DDNs) in some capacity. These are hierarchical names, for example, "/C=us/O=hp/OU=hpnode1/AP=mms/AE=demo_prog".

At this time, you should define what components of the naming hierarchy you plan to use and define conventions for assigning values to each component.

As an example, you might decide that the Country attribute will not be used, the Organization attribute will always be your company's name in all lower case, and the Organization Unit will correspond to the node name given on the network map in all lower case.

See the discussion of naming in the configuration manuals for the respective services for more information about what attribute classes are available and which ones are required.

Gather and Distribute Configuration Information

Now that you have determined the network topology and addressing scheme for your network, you are ready to compile the configuration information required for each system so that they may communicate with one another.

HP has provided a worksheet for gathering information about each node on the network. It is contained in chapter 4, “Gathering Configuration Information.”

After performing the data gathering steps, you will be able to configure your HP system to communicate with each system on your network. The worksheet will also be useful for other vendors' network administrators.

3 Gathering Configuration Information

A discussion on collecting information to configure local nodes.

A Map to the Data Gathering Process

Before starting your data gathering, see chapter 3, “Planning Your Network.”

Once your network is planned:

- Make copies of the Remote System Worksheet, one for your local node and others to distribute to the other nodes on the network.
- Make copies of your completed local node Remote System Worksheet to distribute to each of the other nodes you will communicate with. This allows the other network administrators to configure your new node on their systems.
- Distribute the Remote System Worksheets and a copy of your Remote System Worksheet to those other network nodes. If one person administers all the nodes, you must still have one worksheet filled out for each node.
- Fill out the parts of your Local Parameter Worksheet that you can while waiting for the information from the other nodes. Fill in the remainder of the information you need on your Local Parameter Worksheets from information you gather from the remote nodes.
- Collect all the worksheets into a packet. This packet will contain all the information you need to configure your new node. You should also save this packet for reference when modifying any of your network parameters.

Once you have all this information gathered, you are ready to configure your network. Chapter 5, “Configuring and Verifying HP OTS/9000” contains instructions for configuration and verification. If you have not yet installed OTS, see chapter 2, “Installing HP OTS/9000” for installation instructions before starting your configuration.

About Worksheets

There are two worksheets for you to use:

- **Remote System Worksheet**. This worksheet is designed to help you gather network information both for your node and other nodes on the network with which you wish to communicate. Since the remote

nodes need to know information about your local node, it is advisable to fill out a Remote System Worksheet for you node and send a copy of it along with blank worksheets to the remote nodes.

- **Local Parameter Worksheet**. This worksheet is designed to help you collect the information you need to configure your local node. One of these worksheets is needed for every subnetwork you configure. Use the Remote System Worksheet information you collect from other nodes. Both worksheets are needed to complete your configuration.

When you have all the worksheets completed, you are ready to start configuration. Some sections on these worksheets may not apply to your network or are optional entries.

Using the Remote System Worksheet

The Remote System Worksheet should be filled out for every OSI system you intend to connect to. This INCLUDES your local node.

This worksheet represents parts of the OSI stack. The information is broken into six different sections. These six sections (described below) should be filled out by the network administrator for each remote node.

General Information

This contains basic information about the remote system.

Node Name	What the system is called (uxnode1, hpnode2, etc.). This name should match the name given to the system on network maps.
Vendor/Type	The manufacturer and model number (for example, HP9000/J200) .
Routing Information	Indicates whether this node acts as an End System (final destination for traffic), an Intermediate System (router), or Both.

Application Addresses

List all the remote applications you will communicate with.

Application Name	What the application is (FTAM responder, Net Management Agent, etc.).
P-, S-, T-Selectors	Upper layer addresses for the application. If the program runs over Transport, only the T-selector should be specified. For Session and X.400, specify only the S- and T-selectors. For all other applications, the P-, S-, and T-selectors should be used. Indicate a NULL selector value by using “NULL.”

Subnetwork Addresses

The subnetwork information is typically transparent to the end user, because the Network Layer (CONS or CLNS) determines this information from the NSAP. In some cases, this mapping must be configured on the system which is why this information is requested.

If you have multiple X.25 or LAN cards, use additional worksheets.

NSel	The Network layer selector (typically 0x01). This field may be left blank if it is not explicitly configured on the remote.
CONS/CLNS/X.25 Subaddr	Indicate what (if any) subaddresses are used by these services over X.25. If subaddressing is not used then use “NULL.”
X.121	Provide the X.121 address of the remote system.
802.3/FDDI MAC	This is the Media Access Control (MAC) layer address of the remote LAN card. These are always 6 bytes long and should be specified in hexadecimal.

X.25 Subnetwork Information

This box contains other X.25 configuration items that are important to know to achieve successful interoperability.

ISO 8878 Support	This indicates whether the remote supports the use of the X.25 extended addressing facility, as prescribed by ISO 8878 (Use of X.25 to provide CONS). Systems that do not use this facility should have their NSAP match their X.25 address (X.121 + Subaddress).
Accept Reverse Charging	If true, the vendor allows the call charges to be billed “collect.” Typically this is set to “N”.
X.25 Standard	This indicates which X.25 capabilities are supported by the system. The 1984 standard provides more facilities than the 1980 standard. At least one must be circled. (Circle all that apply or will be allowed by the X.25 service).

LAN Subnetwork Information

This box indicates what subset of the CLNS protocol is supported.

CLNP Subset	U.S. GOSIP requires the use of the Full subset, with NULL CLNP packets being discarded. This is the default for HP systems. The NULL subset is used only when all destination OSI nodes are physically connected via the same LAN. It provides low overhead at the cost of internetworking. It also requires that the NSAP match the MAC address of the system. Non-segmenting and Full subset (accept NULL) are less frequently used, but are supported by HP.
ES/IS Supported	Indicates whether this node supports the End System/ Intermediate System protocol. With this protocol, subnetwork addressing information is done dynamically. Therefore, other systems on the network do not need to statically configure this addressing information.

Network Addresses (NSAPs)

The last items you should provide are the Network Addresses (sometimes referred to as NSAPs) that are used to access this system.

The full NSAP should be specified here if the remote configures the Network Address in components (IDP, DSP), or does not include the NSEL. These values should all be concatenated and written in the appropriate field.

RFC1006 NSAP and IP Address

OSI uses NSAP network addresses. TCP/IP uses IP addresses. Since the OSI networking layer is replaced by TCP/IP, the special RFC1006 NSAP must be used in any OSI dialog between systems.

The RFC1006 NSAP has:

- a specific header with an IP address, for example, RFC1006 NSAP is 540072872203
- optionally a TCP port ID appended to it

Therefore, an OSI service running over TCP must specify a destination NSAP using the RFC1006 NSAP structure.

The IP address of 123.55.77.5 is encoded in the RFC1006 NSAP as a string of digits using three digits corresponding to one octet of the IP address.

IP Address of:	Encoded in NSAP as:
123.55.77.5	123055077005

If the default port (102) is not used, the TCP port number is encoded as 5 digits followed by “F”.

The complete RFC1006 NSAP with an optional port number of 103 is shown below. If you use the standard port of 102 you omit the port number from the end of the NSAP.

Address Header	IP Address	Port # (optional)
540072872203	123055077005	00103F

If you use the standard NSAP address header, but an invalid IP address, the NSAP address is unreachable.

RFC1006 Addressing Considerations

- When addressing a remote, always use the remote's IP address to construct the destination NSAP.
- Applications must bind to the RFC1006 NSAP with the IP address as configured in osiadmin whether you are connecting to remote via that address or not. You can also use a wildcard NSAP for the local address.

Remote System Worksheet

A blank Remote System Worksheet is shown below (in the next two graphics). You can print it and use it for your actual worksheet.

General Information

Node Name	
Vendor/Type	
Routing Info (Check one): ES_____ IS_____ Both _____	

Application Addresses

Appl Name	Service	P-selector	S-selector	T-selector

Subnetwork Addresses

NSel	
CONS Subaddr	
CLNS Subaddr	
X.121	
802.3 MAC	
FDDI MAC	

LAN/X.25 Subnetwork Information

X.25 Subnet information	LAN Subnet Information
ISO 8878 Support (y/n):	CLNP Subset (check one): NULL____ Non-segmenting____ Full ____
Accept Reverse Charging (y/n):	ES/IS Supported (y/n):
X.25 standard (check one): 1980____ 1984____ 1988 ____	

NSAPs

Include NODE if used as part of the NSAP	
NSAP of 802.3	
NSAP of FDDI	
NSAP of CONS/X.25	
NSAP of CLNS/X.25	
NSAP for RFC1006	

Using the Local Parameter Worksheet

Fill out a Local Parameter Worksheet for each subnetwork. Some of the information you collected on the Remote System Worksheet will be repeated here.

Local Worksheet Organization

Information on the Local Parameter Worksheet is organized as follows:

General subnetwork information	Lines 1 through 4
X.25 information	Lines 5 and 6
LAN information	Lines 7 and 8
Routing information	Line 9

The configuration instructions in chapter 5, “Configuring and Verifying OTS/9000” use the line numbers on this worksheet for easy reference.

General Considerations

A subnetwork is either a Local Area Network segment, or an X.25 Network to which your local node is attached.

If it is a LAN, each card connected to the LAN constitutes an OTS subnetwork. You may have a maximum of two LAN subnetworks.

For X.25, if you have multiple cards connected to the same X.25 network (for increased connections, throughput, or redundancy), you will typically want to group these cards into a single OTS subnetwork.

You also have the option of using the same X.25 card in more than one OTS subnetwork. This allows your system to listen on different network addresses, or if you want to use both CLNS and CONS over this card.

Local Parameter Worksheet Fields

The following information describes each field on the Local Parameter Worksheet.

Subnetwork Name	OTS uses a symbolic name you define to refer to each subnetwork. Use a name that is meaningful to you (for example, fddilan, site_8023, transpac).
Local NSAP	This value defines the NSAP (network address) that other systems on the network will use when establishing connections to your system. The value should be expressed as an even number of hexadecimal digits.
Local Network ID	This value is used in making routing decisions for addresses that have not been explicitly configured, and that do not broadcast End System Hellos. It is some initial set of digits of the NSAP that form a prefix for all systems reachable over this subnetwork. For example, if you have a Local Network ID of 0x490001, then this subnetwork is used for reaching the system with the address 0x490001223344 (assuming that no explicit configuration for this address exists). The use of this parameter is optional.
SubnetworkType	Specify what network service and link type you will use for this subnetwork.

X.25	If this subnetwork uses the X.25 link, then regardless of whether CONS or CLNS is used, you must provide the information requested. Specifically, indicate all the X.25 cards being used and a subaddress value (or the keyword NULL). At least one subaddress/programmatic access pair is required. Each card is identified by its programmatic access name. The programmatic access name is determined by the X.25 link configuration. The subaddress you provide is appended to the configured X.121 address. This defines the SNPA address that calling entities must specify to reach OTS. X.25 configuration files typically reside in /etc/x25. Run `x25stat -d <x25 device file> -c` to view the currently configured values for the corresponding device file that is running. The System Administrator Manager utility (SAM) can also be used to view the X.25 configuration.
CONS/X.25	Specify all of the X.25 facilities that you wish to use over this subnetwork. ISO 8878 Support - If true, this results in the use of the X.25 extended addressing facility, as described by ISO 8878 (use of X.25 to provide CONS). If you do not use this facility, your NSAP should match the X.25 address (X.121 + subaddress). X.25 Standard - This indicates which X.25 standard versions are supported by the system. At least one of these must be specified. The most flexibility is afforded by enabling all facilities supported by the network.

Device Interface Name	For LAN-based subnetworks, you need to provide the device interface name for the card. This is not necessarily the same as the device file name. Typically, the interface name will be “lanx” where x is the logical unit number or the select code. To view existing LAN card interface names, run the utility lanscan(1M). The encapsulation method must be IEEE802.3 to allow OSI to run over an 802.3 LAN. To determine if you have IEEE, type `lanconfig lan`*X*, where “*X*” is the LAN interface you wish to use. If the output does not show “IEEE”, edit the `/etc/rc.config.d/netconf` file and add “ieee” to the LANCONFIG_ARGS[0] entry.
CLNP Subset	U.S. GOSIP requires the use of the full subset with NULL packets being discarded. This is the default. The NULL subset is used only when all destination OSI nodes are physically connected via the same LAN. It provides low overhead at the cost of internetworking. It also requires that the NSAP match the MAC address of the LAN card. Non-segmenting and Full subset (accept NULL) are less frequently used, but are supported by HP.
Routing Information	These describe how to reach systems that are not directly connected to your subnetworks, and require a router. For simple networks, you may not require any route entries. You can specify the route for specific destinations by using the full remote NSAP. Otherwise, you can specify a route for a set of destinations by using a Network ID (or prefix) that is common to all remote systems reachable through this route. You must also specify the NSAP of the Intermediate System that will act as the router for the destinations.

The Next Steps

- Collect all Remote System Worksheets.
- Collect Local Parameter Worksheet for each subnetwork.
- Install OTS, if not already done.
- Start configuring OTS.

Local Parameter Worksheet

Use this worksheet (shown in the next two graphics) to collect information you will need to configure your local network node parameters. One worksheet is required for each subnetwork.

1. Subnetwork name: _____
2. Local NSAP: _____
3. Local Network ID (optional): _____
4. Subnetwork type (check one):
   CLNS over LAN (802.3) _____ CONS over X.25 _____
   CLNS over LAN (FDDI) _____ CLNS over X.25 _____
   RFC1006 _____
5. X.25 (Matching Pairs Required)

X.25 Sub Address	X.25 Programmatic Access Name

6. CONS/X.25 (check all that apply):
   ISO 8878 _____ X.25 1980 _____ X.25 1984 _____ X.25 1988 _____
7. Device Interface Name (LAN only) _____
   Example: lan0
8. CLNP Subset (CLNS only) (check one):
   Null _____ NON-Segmenting _____ Full (Accept Null) _____
   Full (Discard Null) _____ (Default)

9. Routing information

Supply the full NSAP or a network ID (NSAP Prefix common to a group of destination NSAPs), and the NSAP of the intermediate system that will act as the router for the specified destinations.

Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)
Network ID or NSAP
Primary Route (NSAP of IS)

4 Installing HP OTS/9000

This chapter contains the step-by-step instructions for installing HP OTS/9000.

Installing HP OTS/9000

HP software, including HP OTS/9000, is installed using the *swinstall* program. If you're installing software for the entire OSI stack, you should have already installed and configured any link products (for example, LAN or X.25) for your network. If the procedures to install the link components have not been completed, please complete them before proceeding with configuration.

More installation information can be found in the individual link product manuals. Be sure to follow and complete all installation procedures before beginning HP OTS/9000 network node configuration procedures.

If you are installing HP OTS/9000 over the LAN LINK product, verify that the LAN product is LAN or configured to run with the IEEE protocol enabled. To do this, look at the `/etc/rc.config.d/netconf` file. For each LAN interface (lan0, lan1, etc.), the parameter LANCONFIG_ARGS, defined in that file, specifies the protocol enabled. For example, for LAN interface lan0, the following lines may be present:

```
INTERFACE_NAME[0]=lan0
IP_ADDRESS[0]=”12.34.456.789”
SUBNET_MASK[0]=”255.255.255.0”
BROADCAST_ADDRESS[0]=
LANCONFIG_ARGS[0]=”ether ieee”
```

For HP OTS/9000 to function over a particular interface, the LANCONFIG_ARGS parameter should include “ieee” for that interface.

Hardware and Software Requirements

Before installing or updating HP OTS/9000 (version C.07.00), you must have the following hardware and software components installed and operational.

Hardware

You must have the following hardware installed and operational.

- HP9000 Series 800. Supported Series 800s include (but are not necessarily limited to):
  - Models D, E, F, G, H, I and J systems; comparable business servers
  - Models 8 35, 840, 845, 855, 859
- HP9000 Series 700 - 712, 715, 735, 755
- Install/update media hardware such as:
  - CD-ROM drive
  - DDS tape drive
- 16 MB RAM
- 18.2 MB free disk space
- Networking link adapters, for example, an HP LAN/9000 card

Software

HP-UX operating system:

- Series 700/800:

  You must have HP-UX 10.30 or greater on your system before using *swinstall* to load the OTS product. If you are currently running an older version of HP-UX, you must update to HP-UX 10. 30 before installing the OTS product.

- Networking link products, for example, HP LAN/9000, HP FDDI/9000, and HP X.25 products (and TCP/IP if you're using the RFC1006 component of HP OTS/ 9000).

Installation Procedures

This section outlines the procedure for installing HP OTS/9000 on HP-UX release 10.30 using the SD utility *swinstall*. These instructions are for a new installation of OTS or on an existing 9.0 system on which HP-UX 10.x has been cold-installed. Either a LAN, FDDI, or X.25 link must also be installed and configured.

Ensure that the following products have been installed correctly on the system:

- HP-UX operating system
- Networking
  - IEEE 802.3 LAN and
  - X.25 or
  - FDDI

To do this, check the following SDU log files for errors or warnings: `/var/adm/sw/swinstall.log` and `/var/adm/sw/swagent.log`.

If Not On HP-UX 10. 30

If you already have an HP-UX 9.x system running HP OTS/9000 and would be installing 10.30 or later on your system, you will need to backup your configuration and data files before cold-installing 10.x on your system.

The configuration files for HP OTS/9000 on a 9.x system reside in the directory `/etc/net/osi/conf`. Backup all the files in this directory before installing 10.30.

1. Install HP-UX 10.x on your system. See the manual *Upgrading from HP-UX 9.x to 10.x* for detailed instructions.
2. After installing HP-UX 10.30, restore all the HP OTS/9000 configuration files from the backup. These configuration files may be restored to their 9.x location, `/etc/net/osi/conf`.
3. Now install HP OTS/9000 on the 10.30 system. When the system reboots after installation, the configuration files will be moved to `/etc/opt/ots/conf` and will be converted to the 10.30 format. The 9.x directory `/etc/net/osi` will be removed upon completion of the installation.

To Add a New Link to HP OTS/9000 for Series 700/800

If you want to add a new type of link to your system after the OTS product has been installed, and you have not configured your system for that type of link, follow these instructions. For example, your kernel is configured for LAN links only and you want to add an X.25 link.

1. Install new link product using *swinstall* and follow the instructions provided for installation and configuration of that particular link product.
2. Reinstall HP OTS/9000 using *swinstall*. This will run all the necessary installation scripts which will add the appropriate OTS driver for the new link into the system file, recompile the kernel, install the new kernel, and reboot the system. In *swinstall*, select the “reinstall” option to be true.

Installing HP OTS/9000 Software

NOTE If your system is running HP-UX 10.01 or later, follow the instructions in "Installing and Upgrading HP OTS/9000 from HP-UX 10.01 or Later." If your system is running HP-UX 9.x, follow the instructions in "Installing and Upgrading HP OTS/9000 from HP-UX 9.x."

On HP-UX 10.x systems, HP OTS/9000 is installed using the Software Distribution utility *swinstall(1M)*. For detailed information on using *swinstall* and other SD utilities, refer to the online manpage and the manual *HP Openview Software Distributor Administrator's Guide*, part number J2325-90001.

CAUTION Before installing HP OTS/9000, make sure you've installed and configured all link products you want to use and you've read and performed the steps described in the chapters "Planning Your Network" and "Gathering Configuration Information" in the *Installing and Administering HP OSI Transport Services/9000* manual. If you are installing HP OTS/9000 over the IEEE 802.3/Ethernet LAN LINK product, use the `lanconfig(1M)` command to make sure that the LAN product is configured to run with the IEEE protocol enabled. If you install HP X.25 link after you have installed HP OSI Transport Services/9000, you must reinstall OTS/9000 in order for OTS to operate over the new X.25 link. You will also need to add the new link to OTS configuration. Refer to the chapter "Configuring and Verifying OTS/9000" in this manual.

1. Log in as `root`.
2. Load the software media into the appropriate drive.
3. Run the *swinstall(1M)* program to install the software using the command: `/usr/sbin/swinstall`.
4. Change the default Source Host Name, if necessary, then enter the mount point of the drive in the Source Depot Path field. Activate the `OK` button to return to the Software Selection Window.
5. Highlight the *OSI Trnspt Srvcs* software.
6. Choose Mark for Install from the "Actions" menu to choose the product to be installed.

When you mark the HP OTS/9000 software for installation you may see the following error message:

```
The software “32070A,r=C.xx.xx,a=HP-
UX_B.10.xx_800,v=HP” refers to a bundle or to a
product, subproduct or filesets within a bundle. The
software specified was selected but there were
problems selecting software that depends on it. The
messages below show which items experienced these
difficulties: The software “OTS9000,r=C.xx.xx,a=HP-
UX_B.10.xx_800,v=HP” was marked but the following
requisites could not be resolved: OS-Core.CORE-KRN
```

This error may be ignored, as the OS-Core.CORE-KRN fileset has already been installed successfully on the system.

When you mark an OTS fileset for installation, other filesets that may be required for operation are automatically marked for installation. When you mark either of the OTS-KRN or OTS-RUN filesets, the other fileset is automatically marked for installation. When you mark the PRG filesets, the OTS-KRN and OTS-RUN filesets are automatically marked for installation. When you mark the ROSE-PRG fileset, the APLI-PRG, OTS-KRN, and OTS-RUN filesets are automatically marked for installation. (Marking man page filesets does not cause any other filesets to be automatically marked.) This feature ensures that filesets required for an operational OTS are installed. You can disable the feature if needed by setting the autoselect_dependencies parameter to “false”; you can then mark individual filesets to be installed.

7. Choose Install from the “Actions” menu to begin product installation and open the Install Analysis Window.
8. Activate the OK button in the Install Analysis Window, when the Status field displays a Ready message.
9. Activate the YES button at the Confirmation Window to confirm that you want to install the software.

   `swinstall` loads the fileset, runs the control scripts for the filesets, and builds the kernel. Estimated time for processing: 3 to 5 minutes. View the Install Window to read processing data while the software is being installed. When the Status field indicates Ready, the Note Window opens.

10. Activate the OK button on the Note Window to reboot. The user interface disappears and the system reboots.
11. Once the system comes back up, log in as `root` and view the `/var/adm/sw/swagent.log` and `/var/adm/sw/swinstall.log` files to view any error or warning messages that may have occurred during the installation.
12. If this is a new installation, go to the chapter "Configuring and Verifying OTS/ 9000" in this manual.
13. Perform the verification steps described in the chapter "Configuring and Verifying OTS/9000" in this manual. You are done when you can successfully perform the verification steps.

Installing and Upgrading HP OTS/9000 from HP-UX 10.01 or Later

You must upgrade the operating system to the latest version of HP-UX before installing the latest version of HP OTS/9000. After you have upgraded HP-UX, upgrade HP OTS/9000 from the 10.01-compatible version (C.05.01 or C.05.02) by installing the latest version of the HP OTS/9000 software onto the system using *swinstall(1M)*.

Refer to "Installing HP OTS/9000 Software" in this document for OTS installation instructions.

Installing and Upgrading HP OTS/9000 from HP-UX 9.x

CAUTION

If you intend to upgrade your HP-UX operating system from a 9.x version, please note the following BEFORE continuing with the installation/upgrade process:

In order to upgrade to the latest version of HP-UX, you must first upgrade to HP-UX 10.01. During the upgrade from HP-UX 9.x to HP-UX 10.01, the `/etc/netlinkrc` file is transitioned to the appropriate `/etc/rc.config.d/*` files. If you upgrade your operating system before the rest of your networking products, you may receive a failure on startup for the network (the *HP-UX Start-up in progress* list, the *Configure LAN interfaces* item shown during system boot). This may be due to an attempt to configure a non-existent link (one of your networking products needs to be upgraded to the 10.01 version.)

Continue with the upgrade. If, after upgrading your networking products, you still receive a startup failure for networking, use the lanscan command to verify the configuration in SAM and view the `/etc/rc.log` file for any failure statements.

Also note the following:

- Upgrade to HP-UX operating system version 10.01 and then to the latest version of HP-UX ONLY when compatible networking products are available. Upgrading the operating system without compatible networking products will cause the loss of network functionality. To recover that functionality, upgrade the appropriate networking products.
- Upgrade the HP-UX operating system before installing any new networking products.
- Upgrade your existing networking products at the same time you upgrade the HP-UX operating system.
- Upgrade the link products (for example, HP LAN/9000 or HP FDDI/9000) before upgrading HP OTS/9000.
- DO NOT move or reposition any network adapter cards before or during the upgrade process.
- Stop all applications running over the network before starting the upgrade process.
- Note that device interface names may change to reflect your upgraded system.

- If problems arise during the upgrade process, check the following files: `/etc/rc.log`, `/var/adm/sw/snoop.log`, `/var/adm/sw/swagent.log`.

Upgrade to HP-UX 10.01 Required

You cannot upgrade your system from HP-UX 9.x to the latest version directly; you must first upgrade to HP-UX 10.01 and then to the latest version. At a high level, the process is:

1. Upgrade HP-UX 9.x to 10.01. Also upgrade applications to 10.01; this includes upgrading OTS C.04.xx to C.05.02. Refer to “Upgrade from HP-UX 9.x to 10.01” in this document.

2. Upgrade HP-UX 10.01 to the latest version. Also upgrade applications to the latest versions; this includes upgrading OTS C.05.02 to the latest version. Refer to "Installing and Upgrading HP OTS/9000 from HP-UX 10.01" in this document.

Upgrade from HP-UX 9.x to 10.01

Use the Upgrading from HP-UX 9.x to 10.x manual as the guide to upgrade HP-UX 9.x to 10.01. After you have upgraded HP-UX to 10.01, upgrade HP OTS/9000 to the 10.01-compatible version (OTS version C.05.02) using `swinstall(1M)`. The 9.x to 10.01 upgrade of HP OTS/9000 occurs when you install the 10.01-compatible version of HP OTS/9000. Follow steps 1 through 10 described in "Installing HP OTS/9000 Software" in this chapter to run `swinstall` and install and upgrade OTS/9000.

The following actions are performed by the HP OTS/9000 control script while running `swinstall(1M)`:

1. All 9.x product files, except the configuration files are deleted from their 9.x locations.
2. The 10.01 HP OTS/9000 product is installed on the system.
3. After the installation is complete, the product configuration files are copied from their 9.x location (`/etc/net/osi/conf`) to their 10.x location (`/etc/opt/ots/conf`). These files are then converted to the format required for HP OTS/ 9000 which is compatible with HP-UX 10.01.
4. During the LAN product upgrade, the LAN interface names may be modified. The HP OTS/9000 upgrade process will get the new interface name and replace the old interface name with the new interface name in the file /etc/opt/ots/ conf/ots_subnets. If problems are encountered, while converting the HP- UX 9.x interface names to the HP-UX 10.x interface names, an error message is printed in the log file `/var/adm/sw/swagent.log`. If there is an error, the file `/etc/opt/ots/conf/ots_subnets` may not be correct for the LAN configuration on the HP-UX 10.01 system. You will have to make the necessary corrections manually in the `ots_subnets` file before starting HP OTS/9000.

   The following line in the `ots_subnets` file may be modified during the upgrade:

   ```
   snet_if_name <lan interface name>
   ```

<*lan interface name*> will be modified depending on the conversions that happen during the LAN link upgrade.

5. If you have HP OTS/9000 configured over X.25 prior to the upgrade, the HP OTS/9000 upgrade may not include the driver required for running HP OTS/9000 over X.25 in the kernel. HP OTS/9000 may have to be reinstalled after the system has been upgraded and after making sure that the X.25 product has been installed and configured. The following WARNING message will be printed in the log file `/var/adm/sw/swagent.log` if the driver required for OTS to operate over X.25 has not been configured in the kernel:

   ```
   Warning: OTS X.25 device driver not configured in
   kernel. Reinstall OTS9000 after making sure X.25 is
   installed and configured.
   ```

6. After the installation completes, transition links will be created for the product files. For example:

   On an HP-UX 9.x system, the file `otsstart` was located in `/usr/bin/otsstart`. On an HP-UX 10.x system, this file will be located in `/opt/ots/bin/otsstart`. After the transition links are created, `/usr/bin/otsstart` will be linked to `/opt/ots/bin/otsstart`:

   ```
   /usr/bin/otsstart -> /opt/ots/bin/otsstart
   ```

After you have installed and upgraded OTS/9000 to the 10.01-compatible version, perform the following steps to verify your configuration:

1. Run the `lanscan` command and record the Network Interface Name and Unit for any LAN or FDDI network interfaces that OTS/9000 uses.
2. Run `osiadmin`.
3. Check the OTS Subnetwork configuration for any LAN or FDDI interface names.
4. Verify that the device interface name is the same as the `lanscan` output.
5. If you are using RFC1006, go to the RFC1006 Configuration screen and verify that the IP address configured is valid.

6. Modify any entries to correct configuration discrepancies. Save the changes and exit osiadmin, reboot your system, and perform the verification steps described in the chapter “Configuring and Verifying HP OTS/9000” in this manual. You are done when you can successfully perform the verification steps.

De-installing HP OTS/9000

On HP-UX 10.x systems, HP OTS/9000 can be de-installed using the Software Distribution utility *swremove(1M)*. All HP OTS/9000 filesets, including the kernel fileset OTS-KRN, are now removable. *swremove* will remove the filesets, regenerate the kernel, then reboot the system. For detailed information on using *swremove* and other SD utilities, refer to the online manpage and the manual *HP Openview Software Distributor Administrator's Guide*, part number J2325-90001.

5 Configuring and Verifying HP OTS/9000

This chapter contains step-by-step instructions for configuring and verifying HP OTS/9000.

Configuring and Verifying HP OTS/9000

At this point you should have completed the following tasks. Don't go on until they have been successfully completed:

- configured all links using SAM
- collected all the Remote Parameter Worksheets
- filled out Local Parameter Worksheets
- verified installation of link layer and OTS
- verified installation of all applicable software
- verified correct kernel configuration

Now you are ready to start the HP OTS/9000 configuration.

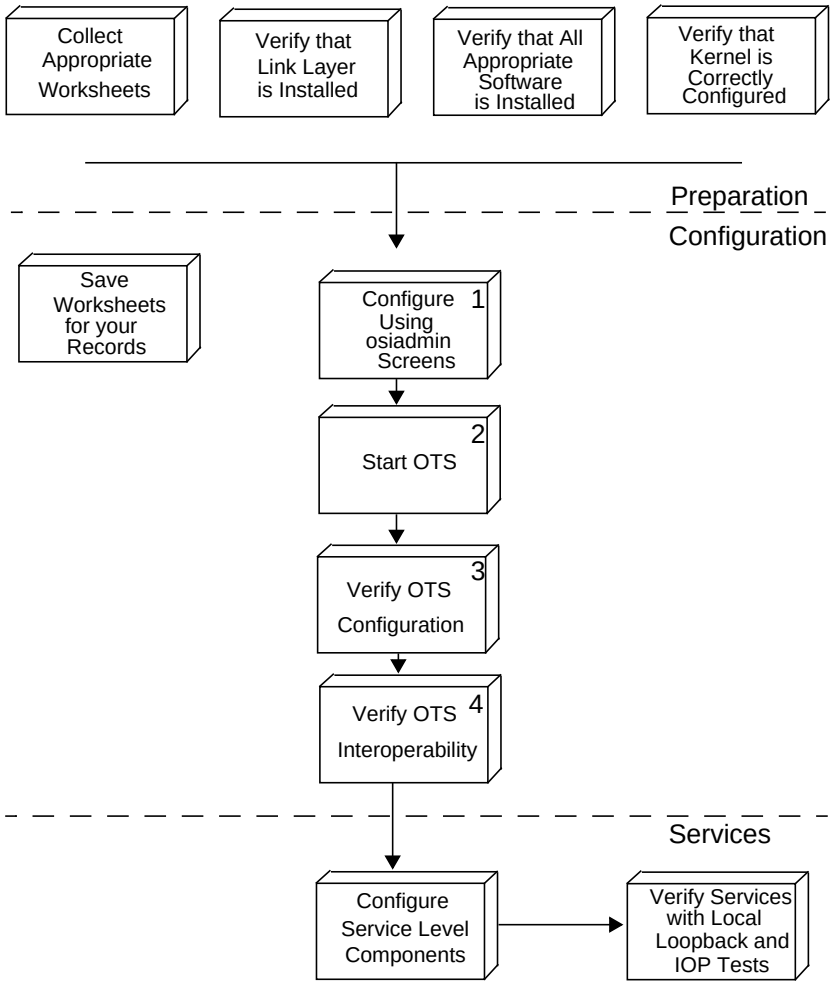
HP OTS/9000 Configuration

Configuration consists of using a combination of programs that apply to different software products in the OSI stack. The *osiadmin* program provides a single entry point to these programs which simplifies the configuration process. Configuration of all links using osiadmin or SAM is recommended. This causes the appropriate link configuration to be added to the `/etc/rc.config.d/netconf` file. If these commands are not present in this file, osiadmin cannot recognize the link as valid.

To have full connectivity with other nodes on the network, the rest of the network also needs to know your local configuration data. Fill in a Remote System Worksheet for your local node so you can communicate this information to the rest of the network.

The figure on the following page shows the flow of the configuration and verification process. Note that before starting OTS configuration, you must have all the applicable software installed (HP LAN /9000, HP X.25/9000, HP OTS/9000). When you have collected the worksheets from all the other network nodes with which you wish to communicate, you can start your configuration.

Figure 5-1 OTS Configuration



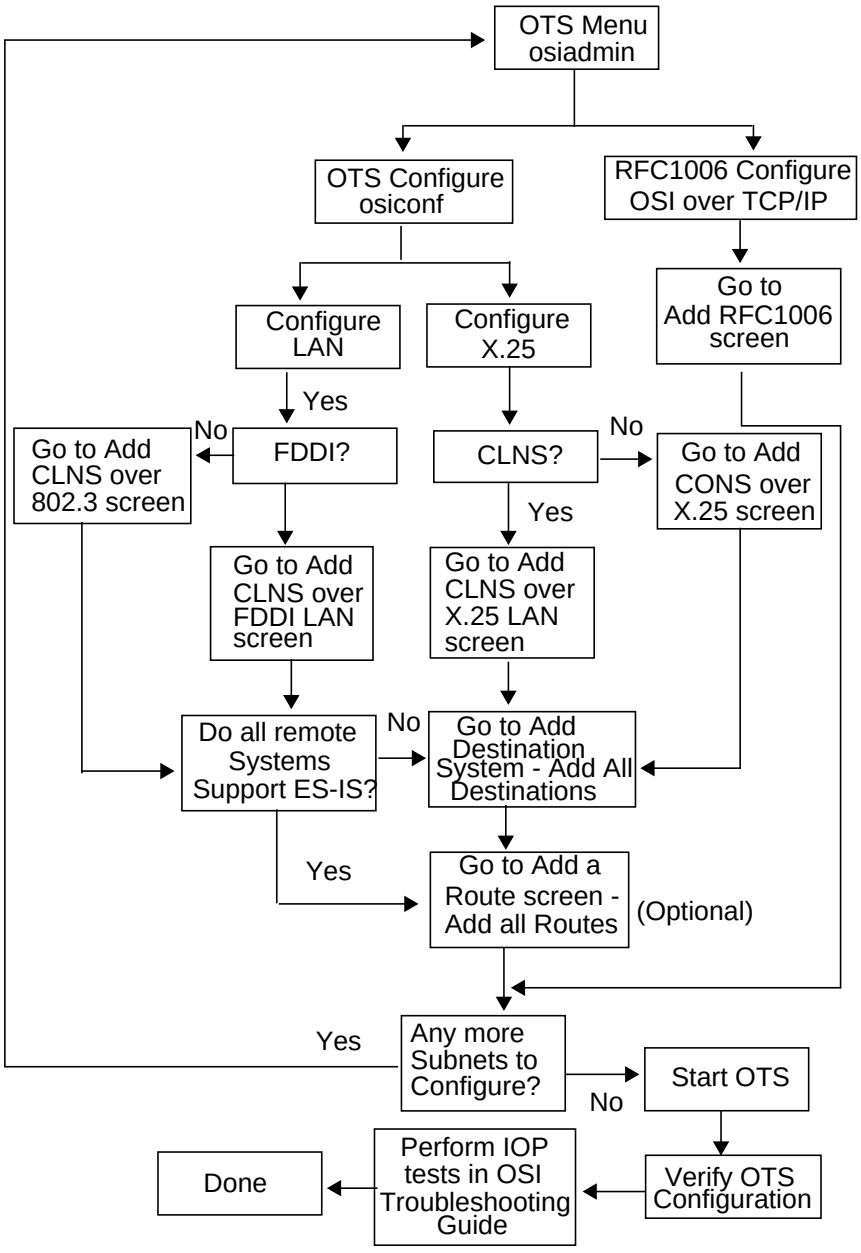
Overview of HP OTS/9000 Configuration

- Start configuration by adding `/opt/ots/bin` and `/opt/ots/man` to your system path. This will save you some typing later.
- Run the osiadmin program. This program calls up the osiconf program to do the OTS configuration tasks. When configuration is complete, you return to osiadmin. See "Finding Your Way Through OTS Configuration" for which configuration screens you'll use.
- Start OTS for the first time.
- Perform the Local Loopback tests as the first test. It verifies configuration of the local node through the link layer of the OSI stack.
- Perform the OTS Interoperability (IOP) tests (for Transport and Session) next. This test verifies the connectivity of your local node to other nodes on the network. It will confirm the interoperability of your configuration up to this point. Refer to "Interoperability Testing" in the *OSI Troubleshooting Guide*.
- When the IOP test completes successfully, you can add the services layer to your network.
- After a successful services installation and verification, start the service level IOP tests. Installation and configuration of the services is described in the manual for each service.

To complete the following configuration instructions, refer to the worksheets you filled out (see the chapter, "Gathering Configuration Information"). The Remote System Worksheet supplies you with information about the nodes with which you wish to connect. The Local Parameter Worksheet will supply you with information about your local subnetworks. You should have a Local Parameter Worksheet for each subnetwork that the local node will attach to.

The tasks listed in this chapter are more or less in the order you will do them.

Figure 5-2 Finding Your Way Through OTS Configuration



To Configure HP OTS/9000

1. Log in as `root`, then add `/opt/ots/bin` and `/opt/ots/man` to your system path.
2. At the system prompt, type `osiadmin`, then press [return].
3. Highlight “OTS” and press “Select Item” or [return].
4. Highlight “Configure OTS” and press “Select Item” or [return].
5. Select the configuration mode and the file set (or accept the defaults shown) and press “Done.” (For the first time you configure, you should always select the defaults.) Press the space bar if a warning message appears on the screen.
6. Under Subnetworks, select “Configure” and press “Select Item” or [return].
7. On the Subnetwork Configuration screen, select “ADD” after one of the four configuration options and press “Select Item” or [return].
   - If you want to configure CLNS over 802.3 or FDDI, go to the section “To Add OTS/9000 CLNS Over 802.3 LAN or FDDI LAN.”
   - If you want to configure CLNS over X.25, go to the section “To Add OTS/ 9000 CLNS Over X.25.”
   - If you want to configure CONS over X.25, go to the section “To Add OTS/ 9000 CONS Over X.25.”
8. Proceed to the tasks that apply to your network configuration.
9. Look at the OTS Configuration flowchart to determine the next task you should perform.

To Configure RFC1006

RFC1006 is configured using the osiadmin tool. HP OTS /9000 does not have to be configured. TCP/IP and the appropriate links must already be configured. You will need your local IP Address for step 5.

1. Type osiadmin to start the configuration. The first screen presented to you is the osiadmin Main Menu.
2. Select “OTS” since the RFC1006 is part of the OTS product.
3. Select “Configure OSI over TCP (RFC1006)” from the OTS menu. When the “Set Configuration Mode” menu appears, accept the defaults (restart mode) and Press “Done”. Press the space bar if a warning message appears on the screen.
4. Select “Add...” from the RFC1006 Configuration menu.
5. Enter an IP Address for your local system on the Add RFC1006 Subnetwork menu. Accept the defaults for other entries.
6. Press **f4** to “Perform Task”. This completes the configuration task.
7. Look at the OTS Configuration flowchart to determine the next task you should perform.

To Add HP OTS/9000 CLNS Over 802.3 or FDDI LAN

1. Under CLNS over 802.3 or CLNS over FDDI LAN, highlight “Add” and press “Select Item” or [return]. If you selected 802.3, the CLNS over 802.3 screen appears. If you selected FDDI, the CLNS over FDDI screen appears.
2. Enter the following parameters from your Local Parameter Worksheet for this subnetwork.
   a. Enter the Subnetwork Name from line 1.
   b. Enter the Network ID from line 3. (Optional NSAP prefix common to a group of destination NSAPs.)
   c. Enter the Local Network Address (NSAP) from line 2.
   d. Enter Device Interface Name from line 7.
   e. Enter CLNP Subset from line 8.
3. Press “Perform Task” **f4**. You will see a pop-up screen displaying “Task completed....”.
4. Press space bar to continue.
5. Press “Previous Menu” **f8** to return to OTS Configuration Menu.
6. Look at the OTS Configuration flowchart to determine the next task you should perform.

Perform these tasks for each CLNS over 802.3 or FDDI LAN. The line numbers above refer to those on the worksheet.

The CLNP subset defaults to 3 for NIST compliance. The other nodes on the network must be at the same subset level. If NULL (0) is selected, the NSAP has to be the same as the physical address to pass verification testing.

To Add HP OTS/9000 CLNS Over X.25

1. Under CLNS over X.25 highlight “Add” and press “Select Item” or [return].
2. Enter the following parameters from your Local Parameter Worksheet for this subnetwork.
   a. Enter the Subnetwork Name from line 1.
   b. Enter a Network ID, if applicable, from line 3.
   c. Enter Local Network Address (NSAP) from line 2.
   d. Enter Subaddress and X.25 Programmatic Access Name from line 5. (At least one pair is required.)
3. Press “Perform Task” **f4**. You will see a pop-up screen displaying “Task completed...”
4. Press space bar to continue.
5. Press “Previous Menu” **f8** to return to OTS Configuration Menu.
6. Look at the OTS Configuration flowchart to determine the next task you should perform.

Perform these tasks for each CLNS over X.25 subnetwork. The line numbers above refer to those on the worksheet.

To Add HP OTS/9000 CONS Over X.25

1. Under CONS over X.25 highlight “Add” and press “Select Item” or [return].
2. Enter the following parameters from your Local Parameter Worksheet for this subnetwork.
   a. Enter the Subnetwork Name from line 1.
   b. Enter Local Network Address (NSAP) from line 2.
   c. Enter Y(es) for each applicable Subnetwork Standard from line 6. (ISO 8878 must be Y or N. At least one of the following must be Y: X.25 1980, X.25 1984, or X.25 1988.)
   d. Enter Subaddress and X.25 Programmatic Access Name from line 5. (At least one pair is required.)
3. Press “Perform Task” **f4**. You will see a pop-up screen displaying “Task completed...”
4. Press space bar to continue.
5. Press “Previous Menu” **f8** to return to OTS Configuration Menu.
6. Look at the OTS Configuration flowchart to determine the next task you should perform.

Perform these tasks for each CONS over X.25 subnetwork. The line numbers above refer to those on the worksheet.

To Add HP OTS/9000 Destination System

1. Select “Add” under Destination Systems on the OTS Configuration menu.
2. Enter the following parameters from your Remote System Worksheet. (One for each remote node to be configured.)
   a. Network Address (NSAP of destination system from the NSAPs box).
   b. Physical Address (If X.25, use the combination of any X.121 address concatenated with the subaddress. If LAN, use the MAC address from the Subnetwork Address box.)
   c. Enter Outgoing Subnetwork Name from line 1 of the Local Parameter Worksheet for the subnetwork reachable from this remote system.
   d. Enter the type of remote system as either End System (0), Intermediate System (1), or Both (2) from the General Information Box.
   e. If an X.25 system, enter either Y(es) or N(o) for Accept Reverse Charging from the X.25 Subnet Information Box. (This field is disabled if the subnetwork is not X.25.)
3. Press “Perform Task” **f4**. You will see a pop-up screen displaying “Task completed...”
4. Press space bar to continue. This returns you to the OTS Configuration Menu.
5. If this node is an Intermediate System, you may want to add a route that uses this IS. (Optional)
6. Look at the OTS Configuration flowchart to determine the next task you should perform.

OTS needs this information to communicate with specific peer systems. Complete this task once for each remote node to be configured. It is necessary for all directly connected systems except those supporting the ES-IS protocol.

An Outgoing Subnetwork Name Example

If you named your X.25 CLNS subnetwork “x25clns” and this is the configuration for a remote reachable over X.25 CLNS, enter “x25clns” as the outgoing subnetwork name.

To Add an HP OTS/9000 Route

1. Select “Add” under Routes on the OTS Configuration menu.
2. Enter the following parameters from your Local Parameter Worksheet for this subnetwork.
   a. Enter Network ID or Network Address (NSAP) from line 9.
   b. Enter Outgoing Subnetwork Name from line 1.
   c. Enter Primary Route NSAP from line 9.
3. Press “Perform Task” **f4**. You will see a pop-up screen displaying “Task completed...”
4. Press space bar to continue, returns you to the OTS Configuration Menu.
5. Look at the OTS Configuration flowchart to determine the next task you should perform.

OTS needs this information to communicate with peer end systems that are not directly connected to this system, but are reachable through an intermediate system. Sets of systems may be specified if they have a common prefix portion of their NSAP (that is, network ID), and are reachable through a common intermediate system. There is no need to enter this information if all peer end systems are directly connected.

The DEFAULT route is used when the destination is not directly reachable and no other route has been specified for the destination NetID/NSAP.

To Start HP OTS/9000

1. Press “Exit Task” **f8** until you are back on the OTS Menu.
2. Highlight “Start OTS” and press “Select Item” or [return]. This takes a few moments. You will see messages flashing on your screen as OTS verifies that the links are running and then starts itself.
3. Press [return] to continue.

NOTE

You only need to use the start option after initial configuration. OTS is automatically started by `/sbin/rcz.d/s380ots` when booting up the system after this first start. To avoid OTS from starting automatically upon bootup, edit the `/etc/rc.config.d/ots` file. Modify the `OTSSTART` statement to read “OTSSTART = off”. The next time the system is rebooted, OTS will not start automatically.

4. Look at the OTS Configuration flowchart to determine the next task you should perform.

To Update HP OTS/9000

1. Press “Exit Task” **f8** until you are back on the OTS Menu.
2. Highlight “Update OTS” and press “Select Item” or [return]. This takes a few moments. You will see messages flashing on your screen as OTS verifies that the links are running and then updates.
3. Press [return] to continue.

You may update HP OTS/9000 if:

- HP OTS/9000 is already running AND
- Only dynamic parameters have been changed since the stack was started. See the `config_parms.txt` file online or print the `ots_addendum.ps` file for a complete list of Dynamic/Non-dynamic parameters.

To Verify HP OTS/9000 Configuration

1. Make sure the stack is started.
2. From the OTS menu in osiadmin, highlight “Test Connectivity” and press “Select Item” or [return].
3. Highlight “Transport Tests” on the OSI Diagnostics main menu and press “Select Item”.
4. Highlight “Loopback” on the Transport Test Cases Menu and press “Select Item” or [return]. A window titled “Transport Destination TSAP” will appear. It displays the field for the Transport Selector (a default value) and Network Address (what you just configured).

   If you are verifying RFC1006 configuration, enter the local RFC1006 NSAP in the “Network Address” field.
5. Press “Done” **f4**. The screen will be filled with a report showing various values. At the end will be a line called “Test Status” which should say PASSED. If the test did not pass, refer to “Troubleshooting Basics” chapter 2 in the *OSI Troubleshooting Guide*.
6. Press [return] to clear the screen. You can repeat the above steps for all of your local subnetworks. Just change the NSAP at the “Transport Destination TSAP” screen to another of your local NSAPs.
7. Press “Previous Menu” **f8**.
8. Press “Exit to OSIADMIN” **f8** to return to osiadmin screens.
9. To verify OTS interoperability (IOP), refer to chapter 1 in the *OSI Troubleshooting Guide*.

6 HP OTS/9000 Configuration Files

This chapter describes the HP OTS/9000 configuration files.

About the Configuration Files

The OTS/9000 configuration files are standard ASCII files. For a new installation, they are copied from /opt/ots/newconfig to /etc/opt/ots/conf. This is accomplished when *swinstall* runs during the installation. You can reset the configuration to its original (installed) condition by copying the needed files from opt/ots/newconfig. This erases prior configuration and customization.

The following configuration files are used by the OTS product:

OTS Files

ots_subnets	Local subnetworks parameters
ots_dests	Destination System parameters
ots_routes	Routing parameters
ots_parms	Protocol layer parameters
ots_genrl	Miscellaneous parameters
ap_user_app	Local Address for APRI X.410 Mode Applications (Reserved for future use.)

Related Files

local_app	FTAM/MMS local application parameters
remote_app	FTAM/MMS remote responders parameters

Related files are not necessary for the OTS product. They are only used when the related product has been installed. You can change these files using any text editor.

The following shows an example of the configuration file format.

```
#####################################################################
#             OTS Route Parameters                                  #
#                                                                   #
# Note: Changes made by editing this file will not take             #
#       effect until the OTS stack is restarted or                  #
#       updated.                                                    #
#####################################################################
#
#@(#) C.07.00
```

```
#
#-------------------------------------------------------
1
# Guidelines:
#
# The4 parameters route_id, route_id_mask,route_out_subnet,
# & route_primary are grouped together, route_id must appear
# first in each group.
#
# The DEFAULT ROUTE is configured by setting route_id and
# route_id_mask as follows:
#     route_id             00        # hexadecimal number
#     route_id_mask        00        # hexadecimal bitmask
#-------------------------------------------------------
2
#-------------------------------------------------------
# parameter | current | Additional user information and/or
# name     | value  |minimum/ maximum / factory default
#-------------------------------------------------------

#-------------------------------------------------------
# route example: To use this example, remove the comment
# characters and change the parameters with regard to the
# guidelines above.
#-------------------------------------------------------
3

4  # route_id             4311     # hexadecimal number
   # route_id_mask        FFFF     # hexadecimal bitmask
   # route_out_subnet     test8023snet
   # route_primary 43114085551212000000000010800090026f0201
   #                       # The NSAP of the destination IS
   #                       # (1st hop) for this route id
```

1. The guidelines section contains important information to help you understand and configure the parameters.
2. The parameters are in the form: `parameter_name value`
3. Anything after “#" is a comment. Comments are a useful guide to the file. Erasing them is not recommended.
4. Some parameters comprise a record and must appear in the order given. Do not change the order of single parameters or parameter groups.

Configuration Files and the config_parms.txt File

The most efficient way to configure HP OTS/9000 is by using the worksheets in chapter 4, "Gathering Configuration Information," of this manual and the *osiadmin* facility. Using these will enable you to configure the minimum set of parameters. If you are accustomed to configuring your communications software using ASCII configuration files directly, you can use this chapter and the information in the file `/opt/ots/doc/config_parms.txt` to configure HP OTS/9000 the same way. Using the parameters described in the `config_parms.txt` file requires an in-depth knowledge of OSI networking. The configuration files described in the `config_parms.txt` file are located in the `/etc/opt/ots/conf` directory.

NOTE

The `config_parms.txt` file is an ASCII text file that you can use to search for OTS parameter information using any text editor. This information is also contained in the compressed file `/opt/ots/doc/ots_addendum.ps.Z`. Use the HP-UX uncompress command to uncompress the file, then print the resulting `ots_addendum.ps` file.

The config_parms.txt file provides the following information about OTS parameters:

- The parameter description
- The file format
- The unit type
- The range
- The default
- The osiadmin status
- The dynamic status
- The osiconf/osiadmin screen name
- The osiconf/osiadmin field name

NOTE Although you can change the configuration files while HP OTS/9000 is running, only parameters that are listed as being dynamic can be changed without requiring a system reboot. The otsupdate command must be used to invoke these dynamic changes. See the section “To Update HP OTS/9000” in chapter 5 for more information.

Steps for Changing Parameter Values

1. Make the changes you need to the parameters described in the config_parms.txt file.
2. Read “Running osiconfchk” in chapter 5 of the *OSI Troubleshooting Guide* for information on how to verify that the parameter values are valid.
3. Update or restart the system depending upon what types of parameters are changed.

Multiple Configuration Sets

The nodal management tools can work with configuration files sets residing in directories other than the default directory /etc/opt/ots/conf. This is limited to the creation and management of files sets on the local node only.

There is no limit to the number of sets that can exist, but each file set must contain a complete set of configuration files. Each configuration file set is identified by the directory where the configuration files exist. Only one set can be active at any time. The OSI_CONFIG environment variable tells the OTS commands which directory to find the active configuration files. If OSI_CONFIG is not set, the active configuration files are assumed to be in the default directory.

NOTE The active file set will reflect the configuration of the running stack/services ONLY if the OSI_CONFIG environment variable has not been set or reset since the stack/ services were started.

To Create A New File Set

To create and activate a new file set, use the following sequence of commands as an example.

```
$ mkdir /tmp/myconfig
$ cp /usr/opt/ots/newconfig/ * /tmp/myconfig
$ ls /tmp/myconfig
ap_user_app local_app
ots_genrl ots_subnets  o ts-parms remote_app
ftam_parms ots_dests ots_routes
$ OSI_CONFIG=/tmp/myconfig
$ export OSI_CONFIG
$ osiadmin
```

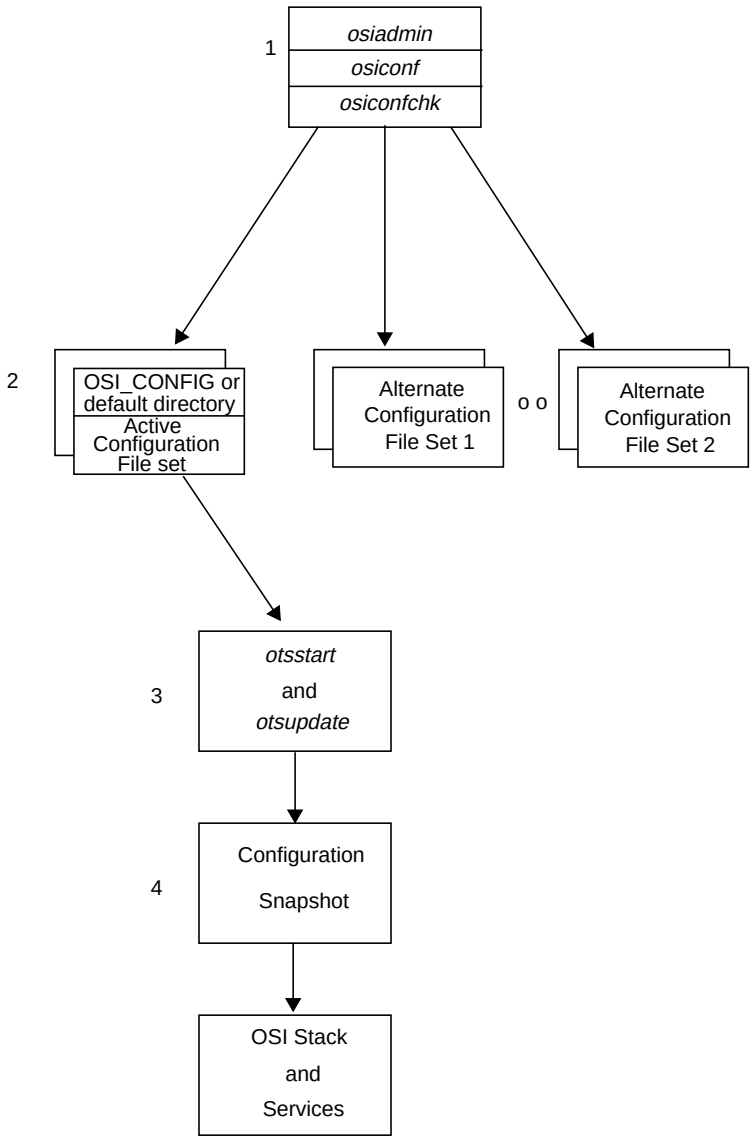
From osiadmin you can modify the new active file sets.

When you run the OTS in this environment, the nodal management tools will use the configuration files in /tmp/myconfig directory. Once the environment variable is set, no further action is required. All of the nodal management tools are programmed to look for this environment variable.

NOTE Be careful when altering the OSI_CONFIG environment variable. While the OTS tools recognize the OSI_CONFIG environment variable immediately, the OTS stack will not use the configuration files referenced by OSI_CONFIG until the stack is updated or the system rebooted. When rebooting, be sure that OSI_CONFIG is defined properly in the boot environment.

OTS tools can now manipulate any file set, active or alternate, that resides on the local node. (An alternate file set is any file set that is not active.) The following diagram shows the interaction of OTS tools and the files sets.

Figure 6-1 Multiple Configuration Sets



Multiple Configuration Diagram

The following numbers refer to “Multiple Configuration Sets.”

1. The OTS tools (osiadmin, osiconf, osiconfchk), by default, manipulate the active configuration file set. They can also manipulate alternate configuration files sets which are not active.
2. The active configuration files set can reside in any directory. By default it is located in /etc/opt/ots/conf directory unless the OSI_CONFIG environment variable is set, in which case the active configuration file set is specified by this variable.
3. The otsstart/otsupdate tools provide the startup/dynamic reconfiguration functions of OTS. These tools retrieve configuration information from the active file set, either the default directory or the directory referenced by OSI_CONFIG.
4. The configuration snapshot contains encoded copies of the current configuration files as they were at the last time oststart or otsupdate was successfully executed. The running stack or services consult these binary files for configuration information. These files are only updated when the next restart/update takes place. This means that the ASCII files can be changed without affecting the running software.

Checking OSI_CONFIG Current Value

To check the value in the OSI_CONFIG environmental variable use:

```
$ env | grep OSI_CONFIG
```

If this variable is not set, you will just see your system prompt.

How the OTS Nodal Management Tools Use OSI_CONFIG

osiadmin	Will view active configuration files sets for OTS and FTAM based on the value in the OSI_CONFIG environment variable.
osiconf	Provides a menu-driven screen interface to create or modify OTS configuration information. osiconf defaults to the active file set based on the value in OSI_CONFIG environment variable. osiconf will also allow you to specify the directory of an alternate file set

where is may read or write configuration information. This means that you can also select a file set that is not active and configure it.

To select an alternate file set, enter the directory into the “Configuration File Set Path” field on the “Set Configuration Mode” pop-up screen. When working with an alternate file set, osiconf will prompt you to enable or disable the local parameter checks. These checks verify the parameter values against the configuration of the current node. You should disable local checks when editing the configuration of another machine node.

osiconfchk — Provides quick verification of OTS configuration information. If defaults to the active file set based on the value in OSI_CONFIG environment variable.

Also allows you to verify any OTS configuration file set by specifying the directory of an alternate file set for it to read. You specify the location of the configuration files you want to work with by using the -D option. This setting is independent of /etc/opt/ots/conf or the value of OSI_CONFIG. If using an alternate file set, you may wish to suppress the local checks by using the -l option. Refer to the osiconfchk man page for more information.

Glossary

ACSE/Presentation and ROSE Interface See APRI

Advanced Research Projects Agency See ARPA

ANSI The American National Standards Institute that publishes standards for use by national industries.

API A set of functions enabling an application program to interact with and control network operations and resources.

application program interface See API

APRI An application program interface to the OSI presentation.

argument The part of a command line that identifies what (file, directory, etc.) is to be acted upon.

ARPA The Advanced Research Projects Agency. A U.S. government research agency that was instrumental in developing and using the original ARPA services on the ARPANET.

backbone The principal network segment to which all nodes are connected, or to which other segments are connected.

BAS This subset is used with basic X.400 application and Session version 1.

basic activity subset See BAS

basic combined subset See BCS

basic synchronized subset See BSS

BCS This subset is used with basic FTAM applications and Session version 2.

boot To start up your system, loading it into the computer memory.

bridge A device that connects different LANs.

BSS This subset is used with advanced user application and advanced FTAM usage.

bypass A mechanism to avoid sending data to a faulty device or portion of the network.

Glossary

CCITT Consultative Committee for International Telegraphy and Telephony. An international organization of communication carriers.

CLNP subset Indicates the LAN subnetwork information.

CLNS Connectionless-oriented network services.

common management information service (CMIS)

The interface for development of network management applications.

CONS Connection-oriented network services.

command A word or phrase that you type at the system prompt to carry out an action when you press the ENTER key.

connection-oriented network services See CONS

connectionless-oriented network services See CLNS

Consultative Committee for International Telegraphy and Telephony See CCITT

configure To set up your computer system so that the computer and all peripheral devices can work together. If the computer is part of a network, this includes loading the appropriate software and establishing the necessary connections.

configuration The arrangement of a computer system or network as defined by the nature, number, and the chief characteristics of its functional units. More specifically, the term configuration may refer to a hardware configuration or a software configuration.

cug Closed user group. An X.25 user facility that allows a predetermined group of users to contact and be contacted by members of the group alone.

daemon A software process that runs continuously and provides services on request.

distributed system A computer system in which computing, storage, and other resources are dispersed throughout several or many locations.

Glossary

Ethernet A 10 Mb/s LAN, developed by Digital Equipment Corporation, Intel, and Xerox Corporation, upon which the IEEE 802.3 network is based.

FDDI A specification for a fiber-optic ring network featuring a link speed of 100 Mb/s and fault tolerant capabilities.

fiber distributed data interface See FDDI

fileset Describes the logical, defined set of files on an update or installation tape.

file transfer, access, and management See FTAM

file transfer protocol See FTP

FTAM Provides the capability to manipulate data files locally and at remote nodes.

FTP The file transfer protocol that is traditionally used in ARPA networks. The ftp command uses the FTP protocol.

gateway A node that connects two or more networks together and routes packets between those networks.

GOSIP Government OSI Profile. An OSI-based network protocol used by governments (for example, the United States and United Kingdom).

heterogeneous network A network composed of dissimilar host computers, such as those of different manufacturers. See homogeneous network for contrast.

homogeneous network A network composed of similar host computers, such as those of one model or one manufacturer. See heterogeneous network for contrast.

IEEE The Electronics Engineers. A national association, whose activities include publishing standards applicable to various electronic technologies.

IEEE 802.3 network A 10-megabit-per-second LAN, described by the ANSI/IEEE 802.3 Standard for Local Area Networks, that uses a CSMA/CD network access method.

IOP Interoperability procedures used to verify that nodes can communicate over the network.

Glossary

ISO The International Standards Organization that created a network model identifying the seven commonly-used protocol levels for networking.

kernel The part of the HP-UX operating system that is an executable piece of code responsible for managing the computer's resources.

LAN A data communications system that allows a number of independent devices to communicate with each other.

LLC (logical link control) The ANSI FDDI standard that provides a common protocol between the MAC function in the data link layer and the network layer.

Local Area Network See LAN

local network The network to which a node is directly attached.

local network ID Some initial set of digits of the NSAP that form a prefix for all systems reachable over this subnetwork.

MAC The ANSI FDDI standard that defines the data link layer function responsible for the scheduling, routing and delivery of frames on and off the FDDI ring.

manufacturing message specification See MMS

media access control See MAC

MMS Provides the capability to control and coordinate programmatic factory floor devices involved in manufacturing.

network address See NSAP

network administrator An individual responsible for network administration, for example, organizing network domains and issuing node names.

network architecture The set of principles, including the organization of functions and the description of data formats and procedures, that governs the design and implementation of a user-application network.

node Any point in a network where services are provided or communications channels are interconnected. A node could be a workstation or a server processor.

Glossary

NSAP A unique value that defines a system's address for use when establishing network connections among various systems.

open system interconnection

See OSI

OSI Open System Interconnection reference model defined by the International Standards Organization (ISO). It establishes a data communication architectural model for networks.

OTS HP's term for the OSI transport services.

packet A sequence of binary digits that is transmitted as a unit in a computer network. A packet usually contains control information plus data.

PID A unique identification number assigned to all processes by the operating system.

port A software access point for data entry or exit to a network controller.

process identifier See PID

protocol A specification for transferring information between computers on a network.

redundancy Duplication of service. Networks can provide redundancy to increase the probability that communications can continue despite various failures.

remote Not directly connected or processed at another location.

RFC1006 Allows OSI communication over TCP/IP connections as described in RFC1006 and RFC1277.

routing node A node that is able to transmit packets between similar networks. A node that transmits packets between dissimilar networks is called a gateway.

SAP Service access points between network layers.

selector A sequence of octets (bytes) used to identify a SAP; referred to as p-selector, s-selector, and t-selector to identify the OSI layer association.

service access point See SAP

Glossary

SAS A station in an FDDI network that connects to only one of the two FDDI network rings. An SAS must attach to the network through a concentrator.

session interface An application program interface to the OSI session layer.

single attachment station See SAS

SMT The ANSI FDDI standard which manages connections with the ring as well as station and ring configuration.

station management See SMT

subnetwork A group of computers that are a part of a larger network and whose IP address includes a subnetwork number.

system administrator The person who oversees system maintenance and computer operation.

topology The physical and logical geometry governing placement of nodes in a computer network. Also, the layout of the transmission medium for a network.

X/open transport interface See XTI

XTI An application program interface to the OSI transport layer.

X.21 Defines the interface between a computer and a public data network where the access to the network is made over synchronous digital lines.

X.25 Defines the interface between a computer and a packet switching network.

X.400 The interface for electronic messaging applications over a network.

X.500 A distributed directory interface allowing different vendors to store and access information on different systems.

Index

Symbols

/dev/osipi, 29
/etc/net/osi/conf, 134
/etc/net/osi/conf/template, 134

Numerics

1984 X.25, 30

A

ACSE/Presentation layer
  functionality, 30
adding
  a destination system, 127
  a route, 129
  CLNS over 802.3 LAN, 124
  CLNS over X.25, 125
  CONS over X.25, 126
  new link to OTS - series 800, 107
addresses
  extended, 39
  system, 38
addressing, 42
  determining the scheme, 78
  planning application, 79
administrative prefix
  AP, 50
AFI, 49
AFNOR format NSAP, 55
ANSI format NSAP, 54
AP, 50
  temporary, 60
  using an X.121 address, 61
  using telephone numbers, 60
  using the ISO local format, 62
application addresses, planning, 79
area, 51
authority and format identifier
  AFI, 49

B

BSD socket, 40

C

CCITT
  1980, 30
  X.214, 30
  X.215, 30
  X.219, 30
  X.224, 30
  X.225, 30
check value
  OSI_CONFIG, 141
CLNS, 44
  adding over 802.3 LAN, 124
  adding over X.25, 125
  over X.25, 38
closed user group, 39
CMIS, planning, 70
concepts, 40
conduits, 40
configuration
  file format, 134
  OTS overview, 118, 120
  RFC1006, 123
  verifying OTS, 132
configuration data
  planning, 81
configuration files
  about, 134
  resetting, 134
Connectionless Network Service
  CLNS, 44
Connection-Oriented Network Service
  CONS, 44
connections
  establishing, 29, 38
  management facilities, 39
CONS, 44
  adding over X.25, 126
  over X.25, 38
create OTS config info, 141
customizing steps, 137

D

data gathering process, 84
DDN, 79
destination system
  adding, 127
DFI, 56
directory distinguished name
  DDN, 79
DIS 8473, 30
documentation
  related Fibre Channel, 15
domain specific part
  DSP, 49
DSP, 49
  format identifier, 51

E

end system, 33
  how OTS finds a remote, 33
end system to intermediate system
  ES-IS, 46
Enterprise ID, 58
ES
  end system, 33
ES-IS, 46
establishing connections, 29
example of RFC1006 NSAP, 89
extended address, 39

F

Fibre Channel
  related documentation, 15
files
  about the configuration, 134
  format, configuration, 134
FTAM
  planning, 70
functionality

Index

ACSE/Presentation layer, 30
session layer, 31
transport, 32

G

GOSIP
United Kingdom, 57
United States NSAP, 56
Government Open Systems Interconnection Profile
GOSIP, 56

H

hardware requirements, 103
how OTS/9000 uses X.25, 38
how to
add a destination system, 127
add a route, 129
add CLNS over 802.3 LAN, 124
add CLNS over X.25, 125
add CONS over X.25, 126
configure OTS, 122
configure RFC1006, 123
start OTS, 130
update OTS, 131
upgrade OTS from HP-UX 10.x, 110
verify OTS configuration, 132

I

IDI, 49
IEEE 802.3, 30
installing over, 108
IEEE MAC address
MAC address, 46
initial domain identifier
IDI, 49
initial domain part, 48
installation
if not 10.0, 106
scenarios, 105
intermediate system, 33
intermediate system to intermediate system
IS-IS, 52
IP Address
RFC1006, 89
IS
intermediate system, 33
IS-IS, 52
ISO
8072, 30
8073, 30
8326, 30
8327, 30
8348, 30
8602, 30
8649, 30
8822, 30
8878, 30
9072-1, 30
9542, 30
ISO/IEC TR10172, 30

L

LAN
general questions, 74
planning, 74
LAN link, 108
lanconfig(1M), 108
link service access point
LSAP, 46
local parameter worksheet, 98
considerations, 93
organization, 93
LSAP, 46

M

MAC address, 46
manpage
osiadmin, 18
osiconf, 18
osiconfchk, 18
osidiag, 18
osistart, 18
osistop, 18
otsaddes, 18
otsaddis, 18
otsaddnsap, 18
otsaddroute, 18
otsdeles, 18, 19
otsdelis, 18
otsdelnsap, 18
otsdshownsap, 19
otsshowes, 19
otsshowis, 19
otsshowroute, 19
otsstart, 19
otsstat, 19
otsupdate, 19
manual reference page, see manpage, 18
MAP/TOP 3.0, 59
maximum routing entries, 34
MC/ServiceGuard
planning, 71
medium access control
MAC address, 46
multiple configuration sets, 138

N

naming hierarchies, planning, 79
network
determining the structure, 77
ID, 64
identifiers,how OTS/9000 uses, 37
layer, 44
planning your, 68
routing, 33
network routing, 44
non-standard NSAP, 66
North American MAP/TOP Users Group, 59
NSAP

Index

additional reference documents, 47
addresses, 47
AFNOR format, 55
allocation formats, 54
ANSI format, 54
domain specific part, 49
example of RFC1006, 89
initial domain part, 48
non-standard, 66
recommendations, 65
RFC1006, 89
selector, 52
syntax, 48
United Kingdom GOSIP, 57
United States GOSIP, 56
with CLNP, 66
with CONS, 66
NSel, 58, 63
null X.25 subaddresses, 38

O

Omicom, Inc., 47
OSI products, 25
OSI stack, 28
RFC1006, 28
OSI_CONFIG, 138
check value of, 141
osiadmin, 141
manpage, 18
osiadmin static routing information, 33
osiconf, 141
manpage, 18
osiconfchk, 142
manpage, 18
osidiag
manpage, 18
osistart
manpage, 18
osistop
manpage, 18
OTS/9000
about CLNS, 38
about CONS, 38
ACSE/Presentation, 30
configuring, 122
configuring overview, 120
establishing a connection, 29
how it uses Network Identifiers, 37
how it uses X.25, 38
parameters, 136
performance, 26
routing, 33
session functionality, 31
software components, 26
standards supported, 30
starting, 130
transport functionality, 32
updating, 131
otsaddes
manpage, 18
otsaddis
manpage, 18
otsaddnsap
manpage, 18
otsaddroute
manpage, 18
otsdeles
manpage, 18
otsdelis
manpage, 18
otsdelnsap
manpage, 18
otsdelroute
manpage, 19
otsdshownsap
manpage, 19
otsshowes
manpage, 19
otsshowis
manpage, 19
otsshowroute
manpage, 19
otsstart
manpage, 19
otsstat
manpage, 19
otsupdate
manpage, 19
overview
OTS configuration, 118
planning your network, 68

P

P-address, 42
PAP, 50
recommended structure, 63
parameters, 136
OTS, 136
OTS related, 136
permanent virtual circuit, 38
physical subnetwork types, 44
PID
protocol identifiers, 39
pipe, 40
planning
application addresses, 79
CMIS, 70
determining addressing scheme, 78
determining network structure, 77
FTAM, 70
gather and distribute configuration data, 81
LAN, 74
MC/ServiceGuard, 71
naming hierarchies, 79
network, 68
network address, 78
overview, 68
required services, 69
vendors, 72
X.25, 75
X.400, 69

Index

XTI, 71
Port ID, 41
presentation address
P-address, 42
presentation selector
P-selector, 41
privately allocated part
PAP, 50
protocol identifiers, 39
P-selector, 41
PVC
permanent virtual circuit, 38

R

recommended PAP structure, 63
remote end system
how OTS finds a, 33
remote system worksheet, 91
application addresses, 86
general information, 86
LAN subnetwork, 88
NSAPs, 89
subnetwork addresses, 87
using, 86
X.25 subnetwork, 87
requirements
hardware, 103
software, 103
reserved field, 52
reverse charge, 39
RFC1006
example NSAP, 89
IP Address, 89
NSAP, 89
NSAP structure, 89
route
adding, 129
routing
domain, 51
maximum entries, 34
network, 33, 44
table, 33

S

SAP, 40
screens
Add a Route, 129
Add CLNS over 802.3, 124
Add CLNS over FDDI, 125
Add CLNS over X.25, 126
Add CONS over X.25, 126
Add Destination, 129
OTS menu, 130
Subnetwork Configuration, 124
selectors, 41
service access point
SAP, 40
session layer functionality, 31
session selector
S-selector, 41
session service data unit, 31
socket
BSD socket, 40
software requirements, 103
SSDU
session service data unit, 31
S-selector, 41
standards supported, 30
starting
OTS/9000, 130
stopping
OTS/9000, 130
subnetwork, 50
types, 44
supported standards, 30
SVC
switched virtual circuit, 38
swinstall, 108, 115
switched virtual circuit, 38
system addresses, 38

T

T.62, 30
T.70, 30
temporary administrative prefixes, 60
transport layer functionality, 32
transport selector
T-selector, 41
troubleshooting
contacting HP representative, 23
T-selector, 41

U

United Kingdom GOSIP NSAP, 57
United States GOSIP NSAP, 56
updating OTS configuration, 131
upgrading, 108
from HP-UX 10.01, 110
using local parameter worksheet, 93

V

variable
OSI_CONFIG, 138
VC
virtual circuit, 38
vendors, planning, 72
verifying
OTS configuration, 132
OTS configuration information, 142
version number, 51
view active file set, 141
virtual circuit, 38
permanent, 38
switched, 38

W

worksheet
about the, 84
local parameter, 98
packets, 84
remote system, 91

using local parameter, 93
using remote system, 86

X

X.121 address, 44
X.25
establishing connections, 38
general questions, 75
installed over OTS, 108
null subaddresses, 38
planning, 75
X.400
planning, 69
XPG.4, 30
XTI
planning, 71