# TransNav Product Overview Guide

## Contents

### Section 1 Overview and Features

- Chapter 1
  - Overview .................................................. 1-1
- Chapter 2
  - Network Management Features .......................... 1-7
- Chapter 3
  - User Interfaces .......................................... 1-13

### Section 2 Management System Planning

- Chapter 1
  - TransNav Management System Requirements .......... 2-1
- Chapter 2
  - TransNav Management System Planning ............... 2-9
- Chapter 3
  - IP Address Planning .................................... 2-13
- Chapter 4
  - Network Time Protocol (NTP) Sources ............... 2-25

### Index

- Index-1
SECTION 1 OVERVIEW AND FEATURES

Contents

Chapter 1 Overview
What Is the TransNav Management System? ........................................ 1-1
TransNav Software Architecture .................................................. 1-2
Client Workstation Application ................................................... 1-3
Management Server Application .................................................. 1-3
Node Agent Application ............................................................. 1-4
TransNav Management System Features ......................................... 1-4
Interoperability with Third-party Management Systems ..................... 1-4
Autodiscovery and Pre-provisioning ............................................. 1-4
Simultaneous Users ..................................................................... 1-4
Scalability .................................................................................. 1-5
Reliability, Availability, and Serviceability (RAS) ................................ 1-5

Chapter 2 Network Management Features
Fault and Event Management ......................................................... 1-7
Alarm Data .................................................................................. 1-7
Data Sequence ............................................................................ 1-7
Flexible Filtering ......................................................................... 1-8
Flexible Scoping ......................................................................... 1-8
Sorting ........................................................................................ 1-8
Clearing Alarms .......................................................................... 1-8
Configuration Management .......................................................... 1-8
Equipment Configuration ............................................................. 1-8
Pre-provisioning .......................................................................... 1-9
Service Provisioning ...................................................................... 1-9
Secondary Server Support ............................................................. 1-9
Accounting Management ............................................................. 1-10
Performance Management ............................................................ 1-10
Role-based Access Control ............................................................ 1-10
Domain Users .............................................................................. 1-10
Node Users ................................................................................ 1-10
Node Administration ..................................................................... 1-10
System Log Collection and Storage .............................................. 1-11
Report Generation ........................................................................ 1-11
General Reports ......................................................................... 1-11
Data Set Snapshots ..................................................................... 1-12
Chapter 3
User Interfaces

Access to User Interfaces ........................................... 1-13
Graphical User Interfaces .......................................... 1-15
   TransNav Server GUI ........................................... 1-15
   Node-level GUI .................................................. 1-15
Map View ............................................................... 1-15
Shelf View .............................................................. 1-17
Command Line Interface ............................................ 1-18
Domain Level CLI ...................................................... 1-18
Node Level CLI ........................................................ 1-18
TL1 Interface ........................................................... 1-18
Chapter 1
Overview

Introduction

This chapter describes the TransNav management system:
- What Is the TransNav Management System?, page 1-1
- TransNav Software Architecture, page 1-2
- Client Workstation Application, page 1-3
- Management Server Application, page 1-3
- Node Agent Application, page 1-4
- TransNav Management System Features, page 1-4

Note: The TransNav and TN-Xpert management system applications can co-exist and be run independently on a single workstation. The TransNav management system allows you to access the Traverse and TE-100 products, while the TN-Xpert management system application allows you to access the TE-206 nodes. Currently, the TE-206 nodes must be installed using the TN-Xpert management system and have an IP address assigned. The TE-206 nodes can then be discovered on the TransNav management system. For details on the TN-Xpert management system, see the TransNav Xpert Installation Guide and the TransNav Xpert Users Guide.

What Is the TransNav Management System?

The TransNav management system is an advanced element and subnetwork management system designed for comprehensive management of the Traverse network consisting of Traverse, TraverseEdge, and TransAccess products. The Java™-based software smoothly integrates into existing automated and manual operations support system (OSS) infrastructure.

The multi-level management architecture applies the latest distributed and evolvable technologies. These features enable you to create and deploy profitable new services, as well as transition gracefully to a more dynamic and data-centric, multi-service optical transport network.

The TransNav management system consists of an integrated set of software components that reside on the server(s), the client workstations, and individual nodes.

- Client Workstation Application, page 1-3. Provides the user interface for managing the network. The TransNav management system supports a graphical user interface (GUI), a command line interface (CLI), and a TL1 interface.
- Management Server Application, page 1-3. Communicates with the nodes and the servers, as well as provides classical element management FCAPS functionality (fault, configuration, accounting, performance, and security), policy
management, reporting, and system administration. For networks that include TraverseEdge 206 nodes, the TransNav management system supports a WebCraft GUI interface to manage the TE-206 nodes.

- **Node Agent Application**, page 1-4. Resides on the control card and maintains a persistent database of management information for specific nodes. It also controls the flow of information between the management server and specific nodes.

The TransNav management system is an all Java-based, highly-integrated system that uses the identical architecture on the Traverse network nodes and the management server(s). The architecture leverages the Java Dynamic Management Kit (JDMK) and implementation of Java Management Extensions (JMX) to provide an efficient client-server architecture.

Communication between the client application and the server uses the Java Remote Method Invocation (RMI) system over TCP/IP. The client can also communicate to the server via http/https. The server communicates to the client either via RMI over TCP/IP or in the case of the TE-206, via TL1 commands over a telnet session.

Information flows southbound — from the user on the client workstation, to the Session Manager, to the application server, to the Traverse Node Gateway Client inside the
management server, and finally down to the Traverse Node Gateway Agent embedded in the node – via RMI over TCP/IP.

**Client Workstation Application**

The client workstation application provides the user interface for managing the network. The TransNav management system supports GUI, CLI, TL1, and SNMP. See Figure 1-1 TransNav Software Architecture for a graphical representation of the client workstation application.

For Traverse nodes, the client workstation application communicates with the session manager on the management server. Download the Node-level GUI application from the management server, or simply telnet to the management server, to access the CLI or TL1 interfaces. Using a GUI interface, users can access the EMS server or a specified node. Access levels depend on the security levels specified for each user. For TE-206 nodes, the WebCraft GUI is included when the TransNav server GUI application is downloaded.

**Management Server Application**

The management server application communicates with nodes and provides classical element management FCAPS functionality (fault, configuration, accounting, performance, and security), as well as policy management, reporting, and system administration. See Figure 1-1 TransNav Software Architecture for a graphical representation of the management server application.

Security management, logging, and external interfaces to upstream applications are all implemented in the upper level session management component on the management server. These functions are implemented as a JDMK server and are responsible for servicing both the GUI client applet and the northbound interfaces. Enhanced security is achieved using Functional Groups to provide RBAC (Role-based Access Control) functionality.

A separate SMNP agent, also implemented as a JDMK server, supports SNMP traps (fault management) for simplified version control. The SNMP agent works with the fault management application card.

The agent on the node passes node-level data to the management server via RMI over TCP/IP. On the management server, the Node Gateway Controller receives the information and pre-processes it. The Node Gateway Controller then passes the pre-processed information to the management functions within the application server.

The application server is responsible for persistence at the server side and, to this end, manages the entire interface with the underlying SQL database.

Each TransNav management system supports up to eight servers; one server is designated as the Primary server, the remaining servers are designated as Secondary servers. The Primary server actively manages the network. The Secondary servers passively view the network but cannot perform any management operations that would change the state of the network. Any Secondary server can be promoted to the Primary server role in case of failure or maintenance. The switch in server roles requires some degree of user intervention.
Node Agent Application

Each node has a redundant control card with a persistent relational database management system that records provisioning, alarm, maintenance, and diagnostic information for the node. See Figure 1-1 TransNav Software Architecture for a graphical representation of the node agent application.

Each control card uses Java agents (M-Beans [management beans]) to communicate with Java applications on the management server and synchronize data between the server and the nodes it manages.

TransNav Management System Features

The TransNav management system provides comprehensive management for both the nodes and for the connections between nodes through the Intelligent Control Plane. This specifically includes efficient integration of management plane and control plane functions, and policy-based management.

The TransNav management system features include:

- **Interoperability with Third-party Management Systems**, page 1-4
- **Autodiscovery and Pre-provisioning**, page 1-4
- **Simultaneous Users**, page 1-4
- **Scalability**, page 1-5
- **Reliability, Availability, and Serviceability (RAS)**, page 1-5

Interoperability with Third-party Management Systems

The TransNav management system supports other telecommunications management network layer functions at the network management layer, the service management layer, and the business management layer through a variety of northbound interfaces.

The management system provides options to support the following interfaces:

- Forwarding of SNMP traps to SNMP network management systems for integrated higher-layer fault management
- Domain-level and node-level CLI via scripts
- TL1 alarm and performance management forwarding from the management server
- TL1 equipment and protection group configuration and test access

Autodiscovery and Pre-provisioning

Each node uses a process called *autodiscovery* to learn the addresses of all equipment in its control plane domain. Commission the node using the CLI and enter the host name or IP address of the gateway node(s). The management system then discovers and manages all the nodes in the domain without requiring any other preprovisioned information.

The TransNav management system supports *preprovisioning* which allows provisioning functions independent of service activation. The effectiveness of preprovisioning depends upon effective traffic engineering to ensure network capacity is available upon activation. Upon installation, a node is discovered automatically and the management server forwards the preprovisioned information to the node.

**Note:** TraverseEdge 206 nodes must be manually activated from the TransNav server GUI and cannot be preprovisioned.

Simultaneous Users

The number of simultaneous users of user sessions is configurable on the server (MaxNoOfUserSessions). The default is 20 simultaneous users. The management...
system does not restrict the number of simultaneous users either by software licensing or system configuration parameters. Customer usage patterns may allow more simultaneous users with reasonable response time than specified.

One GUI session, one CLI session, or one TL1 session counts as a simultaneous user. Up to 10 simultaneous users can log into a node-level CLI session.

### Scalability

Force10 works with customers to specify configurations to support the scalability required. The TransNav management system supports:

- 1 to 8 TransNav servers. One server is designated the Primary server, the remaining servers are Secondary servers.
- Up to 200 Traverse nodes or TE-206 nodes and simultaneous users for servers, based on specific user behaviors, by:
  - Selecting a multi-processor server with the potential capacity to support the estimated maximum requirements, and the addition of CPUs, memory, and disk capacity as needed.
  - Distributing various components of the management system over multiple servers.

### Reliability, Availability, and Serviceability (RAS)

Force10 works closely with customers to configure hardware and software to achieve desired levels of high availability for their Sun Solaris server-based TransNav system deployments. This includes supporting secondary network operation centers for disaster recovery. Our goal is to achieve exceptional service reliability and availability in a cost-effective manner.
Chapter 2
Network Management Features

Introduction
The TransNav management system provides classical element management functionality (FCAPS—fault, configuration, accounting, performance, and security), plus policy management, reporting, and system administration.

- Fault and Event Management, page 2-7
- Configuration Management, page 2-8
- Secondary Server Support, page 2-9
- Accounting Management, page 2-10
- Performance Management, page 2-10
- Role-based Access Control, page 2-10
- Node Administration, page 2-10
- System Log Collection and Storage, page 2-11
- Report Generation, page 2-11

Fault and Event Management
The TransNav management system graphical user interface (GUI) enables each technician to open multiple Alarm windows. The number of windows is limited only by effective use of the workstation’s screen area and the client workstation system resources, such as memory and CPU load.

If technicians have their nodes grouped, clicking a node group in the navigation tree or clicking a node group map displays only the alarms associated with that node group. This includes nodes and node groups within the parent-level node group.

In the GUI, windows and dialog boxes have the following characteristics:

Alarm Data
The system provides a count of the number of outstanding alarms by severity level. This information is available at a network level as well as for each individual node.

Data Sequence
Each user can specify the sequence in which data fields will appear for each window.
Flexible Filtering
The user can determine what data appears in the selected fields for each separate Alarm window.

Flexible Scoping
The user can determine which nodes and equipment appear in the selected fields for each separate Alarm window.

Sorting
When a column heading (e.g., “severity”) is selected, the Alarm window is sorted by that category.

Clearing Alarms
Only a node clears alarms. Alarms received by the management system are automatically marked as cleared and added to the display. The user can also set the retention duration of cleared alarm messages in the server alarm database and the alarm display.

Graphical buttons and a context menu provide the following options:
- Acknowledge the alarm.
- Select a detailed alarm view that allows the user to view alarm details in addition to adding comments.
- Set filters that allow the user to include or exclude alarms from specific sources from being displayed in the Alarm window.
- Open a new Alarm window.

Configuration Management
Use the TransNav management system for all configuration management requirements:
- Equipment Configuration, page 2-8
- Pre-provisioning, page 2-9
- Service Provisioning, page 2-9
- Secondary Server Support, page 2-9
- Report Generation, page 2-11

Equipment Configuration
After a node is installed and activated, it discovers its specific components and forwards that information to the management system. The system, in turn, populates its databases and builds the graphical representation of the equipment. The Intelligent Control Plane automatically discovers the network and forwards that information to the management plane which creates the network topology map.

Use node-level CLI for initial system commissioning. For detailed information, see the Traverse Installation and Commissioning Guide, Section 11—Node Start-up and Commissioning Procedures, Chapter 1—“Node Start-up and Commissioning,” page 11-1.

The TransNav management system supports Telcordia CLEI™ (Common Language® Equipment Identifier) codes per GR-485-CORE. These are encoded on individual cards.
Pre-provisioning

The TransNav management system supports complete pre-provisioning of all nodes. Pre-provisioning facilitates rapid turn-up of new nodes and node expansions as well as support for planning and equipment capital control. Pre-provisioning of customer services enables the service provider to efficiently schedule provisioning work independent of service activation.

The TransNav management system stores the parameters of the service request and sends them to the Intelligent Control Plane upon activation. If the TransNav management system cannot complete activation, it provides appropriate alarms including insight into the nature of the inability to complete provisioning and activation of the service. The effectiveness of pre-provisioning depends upon effective traffic engineering to ensure that network capacity is available upon activation.

Service Provisioning

The TransNav management system provides end-to-end provisioning of services and requires minimal input from the user. Alternatively, you can set the constraints (each hop and time slot) of a service. You can provision a service using any of the following methods:
- Graphical user interface
- Script language (typical for batch provisioning)
- Domain-level CLI interface

Secondary Server Support

The Traverse management system supports one Primary server and up to seven Secondary servers in the network. The Primary server actively manages the network, while the Secondary servers passively view the network but do not perform any management operations that would change the network. If the Primary server fails or is scheduled for maintenance, any Secondary server can be manually changed to take the Primary server role.

Critical information on the Secondary servers is synchronized with the network elements automatically in real time. This includes current provisioning, service state, alarm and event information from the Traverse nodes. To synchronize PM data, Domain user login profiles, user references and roles, customer records, alarm acknowledgement and annotations, reports, report templates and schedules, the Primary server database must be exported and then imported to the Secondary server database. Depending on the network size, the import process takes between one and five minutes.

Manual synchronization should be performed on a Secondary server database before it is promoted to a Primary server role. For detailed information on promoting a Secondary server, see the TransNav Management System Server Guide, Section 2—Management Server Procedures, Chapter 3—“Server Administration Procedures,” or the TransNav Management System CLI Guide, Chapter 2—“CLI Quick Reference.”
Accounting Management

Accounting data for all services is based primarily on performance management data and transmitted from the nodes to the management system. Using this data, the service provider can track service levels and ensure that traffic complies with service level agreements (SLAs). SLA monitoring enables the service provider to create a billing opportunity and to charge a premium for the guaranteed level of service.

Performance Management

Nodes collect performance management data and forward it to the Primary management server to store in the database. The data is processed in two ways:

- The service provider’s management system administrator can set threshold crossing alert limits. The threshold crossing alert appears as an event on the GUI Events tab.
- The TransNav management system on the Primary server provides basic reports. The data can be exported for analysis and graphical presentation by software applications such as Microsoft Excel.

Role-based Access Control

Security management enables the network administrator to create and manage user accounts with specific access privileges.

Access control on the management system is through a combination of functional groups and access groups for domain users, and through access groups for node users.

Domain Users

A domain user can only belong to one functional group at a time. With the exception of administrators, functional groups are user-defined combinations of pre-defined access groups and specific nodes. Domain users in a functional group who have Administrator roles can access all of the system resources, including user management. They assign access privileges of other domain users to a set of system features (access groups) and resources (nodes) with user-defined functional groups. Security applies to both the GUI and the CLI. For more information on domain security, see the TransNav Management System GUI Guide, Section 2—Administrative Tasks, Chapter 1—“Managing Server Security,” page 2-1.

Node Users

The management system has several pre-defined access groups for node users. Any node user can be in one or more access groups. Within the access groups, access is cumulative; a user who is in two access groups has the privileges of both access groups. See the TransNav Management System GUI Guide, Section 2—Administrative Tasks, Chapter 2—“Managing Node Security,” page 2-11 for more information on node security.

Node Administration

The TransNav management system provides the following capabilities to support efficient remote administration of nodes:

- Software management and administration
  The GUI interface allows users to view an entire network, a group of nodes, or a specific node. Groups of nodes can be set up in a hierarchical fashion, and can be associated with specific geographical maps that coincide with each node group.
• Synchronization of the node and management system databases
  The management system database is a superset of each node’s database and eliminates the need for remote backup and restore of the node itself. The database on each node is synchronized with the management server database, based on user-defined policies.
• Equipment alarm and event history analysis
• Remote restore of the database on the node for disaster recovery in the event of:
  – A failure of both control cards or a major central office (CO) catastrophe.
  – A major, unpredictable service provider network failure that creates uncertainty about the general state of node databases.

The TransNav management system has a local persistent database on the fault-protected control cards that protects against a single control card failure. A major advantage of the Intelligent Control Plane automatic mesh service setup and restoration mechanism is to maintain service connectivity.

<table>
<thead>
<tr>
<th>System Log Collection and Storage</th>
<th>The TransNav management system collects a broad array of information that is stored in the server database for reporting and analysis.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The following list represents data that can be extracted from the server database:</td>
</tr>
<tr>
<td></td>
<td>• All user actions from the domain-level GUI or CLI or through the node-level CLI.</td>
</tr>
<tr>
<td></td>
<td>• Alarm and event history including performance management threshold crossing alerts:</td>
</tr>
<tr>
<td></td>
<td>– Equipment configuration history</td>
</tr>
<tr>
<td></td>
<td>– Node equipment alarm log</td>
</tr>
<tr>
<td></td>
<td>• Security logs:</td>
</tr>
<tr>
<td></td>
<td>– User list denoting each user’s profile</td>
</tr>
<tr>
<td></td>
<td>– Sign-on/sign-off log</td>
</tr>
<tr>
<td></td>
<td>– Failed log-on attempts</td>
</tr>
<tr>
<td></td>
<td>• Performance management data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Report Generation</th>
<th>You can print or export all reports as text-formatted comma delimited files.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Reports</td>
<td>The TransNav management system allows you to schedule or execute on demand a set of pre-defined reports. These reports include functions and data such as:</td>
</tr>
<tr>
<td></td>
<td>• Equipment inventory</td>
</tr>
<tr>
<td></td>
<td>• Historical alarms</td>
</tr>
<tr>
<td></td>
<td>• Historical events</td>
</tr>
<tr>
<td></td>
<td>• Performance monitoring and management</td>
</tr>
<tr>
<td></td>
<td>• Resource availability</td>
</tr>
<tr>
<td></td>
<td>• Service availability</td>
</tr>
<tr>
<td></td>
<td>• Domain service</td>
</tr>
<tr>
<td></td>
<td>You can set reports to be created once, hourly, daily, weekly, and monthly.</td>
</tr>
</tbody>
</table>
Data Set Snapshots

The TransNav management system also provides a simple form of reporting that produces a file based on a set of information that is currently displayed in the GUI. For example, the GUI displays active alarms in a dialog box. The set of active alarms is a data set; the windowing capability of the GUI presents as much of this data set as possible in the display’s dialog box, allowing you to scroll to view more of the data set. The TransNav management system allows you to print, or save to a file, any data that the system can display in a dialog box.

Note: This is different from the “screen capture” function of the client workstation’s operating system that captures only the data set information that is visible in the dialog box.
Chapter 3
User Interfaces

Introduction
The TransNav management system supports the following user interfaces:

- Access to User Interfaces, page 1-13
- Graphical User Interfaces, page 1-15
- Command Line Interface, page 1-18
- TL1 Interface, page 1-18

Access to User Interfaces
The following table lists the different access methods you can use to connect to a TransNav management server or a specific Traverse node.

Table 1-1 Accessing the TransNav Management System

<table>
<thead>
<tr>
<th>Management System Interface</th>
<th>Access Method</th>
</tr>
</thead>
</table>
| TransNav GUI                | • Installed client application (recommended)  
|                             | • Local connection to node and remote connection (DCC bytes) to a management server  
|                             | • Installed application on a Citrix server  |
| TransNav CLI                | • Telnet to a management server  
|                             | • Local connection to node and remote connection (DCC bytes) to a management server  |
| TransNav TL1                | • Local connection to the management system and telnet to a node  |
| Node-level GUI              | • Installed client application (required to view GUI)  
|                             | • Local connection to specific node  |
| Node CLI                    | • Local connection to the node  
|                             | • Local connection to the node and remote login to a different node in the domain  |
| Node TL1                    | • Telnet to the management system and connect to a node  
|                             | • Local connection to the node  |
Two GUIs are available to access the Traverse platform - the TransNav server GUI and the Node-level GUI. Users can only see those nodes to which they have security access rights.

**TransNav Server GUI**

The TransNav server GUI allows domain-level personnel to perform a wide range of provisioning and monitoring tasks for a single node, groups of nodes, or a network of nodes attached to a specific server. There are two main views in the TransNav server GUI:

- Map View
- Shelf View

See the *TransNav Management System GUI Guide* for detailed descriptions of the TransNav server GUI features. See the *TransNav Management System Server Guide* for information on saving background images.

**Node-level GUI**

The Node-level GUI allows technicians at a remote location and locally, using a craft port, to perform monitoring and maintenance tasks for a single node.

The Node-level GUI provides a Shelf View of specific node. Map View is not available.

For information about the Node-level GUI, see the *Traverse Node-level GUI Guide*.

**Map View**

Available only from the server GUI, Map View displays all of the node groups and discovered nodes for a server when you first start the server GUI. From Map View, you can see and manage all the nodes, node groups, links between the nodes, and network services. The graphic area displays a background image (usually a map of physical locations of the nodes) and icons representing the nodes. This initial background image is the Network Map view. Each node group can have a different background image associated with it; this is the Group Map.

Each domain user can group the nodes to which they have access in order to more easily manage their areas of responsibility. They can also add node groups within
existing node groups. The node groups appear in the server network navigation tree.

The menu bar is context-sensitive. Commands display as available (highlighted) or unavailable (grayed out), depending on the selected object. The server network alarm summary tree gives you visibility at a glance to network alarms. If you select a node group, only alarms associated with that node group display.

The network navigation tree shows you the node groups and node networks attached to the server in an outline format in alphanumeric order. Node groups display first, then nodes. In Map View, clicking a node group or a node displays the node group or node name on the top and bottom bars of the window. To view the nodes in a node group, double-click the Group icon in Map View or expand the node group in the navigation tree. In Shelf View, right-clicking a node in the navigation tree or double-clicking the node in Map View to display a graphical representation of the node and related information; you can see which object (card or port) you have selected by the white rectangle around the object and the name that displays on the top and bottom bars of the window.

The context-sensitive tabs provide server, node group, or node information on alarms, events, configuration information, protection, services, and service groups.

Double-click a node group to display the node groups and nodes associated with it. Click a node to display node-specific information. Click anywhere on the map to display network information specific to the server.
Shelf View

Shelf View displays all of the cards in a node and their associated ports. From the Node-level GUI, this is the only view available. Available features are specific to maintenance tasks performed at the node level. Domain level users can use the TransNav server GUI to perform tasks at the network level. From the TransNav server GUI, you can navigate to Shelf View in the following ways:

- Click the node in Map View, then select **Show Shelf View** from the **View** menu.
- Double-click the node in Map View.
- Right-click a node in Map View and select **Show Shelf View**.
- Right-click a node name in the Navigation Tree and select **Show Shelf View**.

![Figure 1-3 Shelf View](image)

The menu bar is context-sensitive. Commands are displayed as available (highlighted) or unavailable (grayed out), depending on the selected object.

You can see which object you have selected by the white rectangle around the object in the graphic and the name displayed on the top and bottom bars of the window.

Context-sensitive tabs (in the bottom half of the screen) provide information on alarms, events, configuration information, protection, and services. In Shelf View, these tabs provide single node, card, or port information. Click a card to display card-specific information. Click a port to display port-specific information. Click an external clock to display external clock timing information.
A shortcut menu also exists for Shelf View. For more information about the EMS server GUI features, see the TransNav Management System GUI Guide, Section 1—Installation and Overview, Chapter 4—“General Description of EMS Server GUI,” page 1-34. For information about the Node-level GUI features, see the Traverse Node-level GUI Guide, Chapter 1—“Node-Level GUI General Description,” Traverse Node-Level Shelf View.

### Command Line Interface

You can also access the TransNav management system using a command line interface (CLI). The CLI has these features:

- **Command line editing**: Use backspace and cursor keys to edit the current line and to call up previous lines for re-editing and re-submission.
- **Hierarchical command modes**: Organization of commands into modes with increasingly narrow problem domain scope.
- **Context-sensitive help**: Request a list of commands for the current context and arguments for the current command, with brief explanations of each command.
- **Command completion**: Enter a command or argument’s left-most substring and view a list of possible allowable completions. Abbreviate any command or argument to its left-most unique substring (for many commands, one character).
- **Context-sensitive prompt**: The prompt for each command displays the current command mode.

You can access a single node or a network of nodes using the CLI.

See the TransNav Management System CLI Guide for detailed information on the command line interface.

### Domain Level CLI

Use domain-level commands from the TransNav management server to perform network commissioning, provisioning, synchronizing, and monitoring tasks. Domain-level commands affect multiple nodes in a network and include:

- Setting the gateway node
- Configuring network links
- Creating performance monitoring templates and alarm profiles
- Creating protection rings and services
- Generating reports

Accessing the domain-level CLI also gives you access to the node-level CLI through the `node` command.

### Node Level CLI

Use node-level CLI commands to perform commissioning, provisioning, or monitoring tasks on any node on the network. Node-level commands affect only one node in the network.

### TL1 Interface

The TransNav management system supports a TL1 interface to the management servers and to individual nodes. Currently, the TransNav management system supports a subset of TL1 commands.

Force10 supports these node and network management tasks through the TL1 interface:

- Fault and performance management (including test access and report generation)
• Equipment configuration and management
• Protection group configuration and management
• Security management

For information on TL1 and how to use the TL1 interface, see the TransNav Management System TL1 Guide.
SECTION 2 MANAGEMENT SYSTEM PLANNING

Contents

Chapter 1 TransNav Management System Requirements
Management System Deployment ........................................ 2-2
TransNav Network Management ........................................ 2-2
Intelligent Control Plane .................................................. 2-2
Control Plane Domain ..................................................... 2-3
Management Gateway Nodes ........................................... 2-3
Sun Solaris Platform for TransNav Management Server ............ 2-3
Windows Platform for TransNav Management Server ............... 2-4
TransNav GUI Application ............................................... 2-5
Node-level GUI Application Requirements ............................ 2-7

Chapter 2 TransNav Management System Planning
Recommended Procedure to Create a Network ......................... 2-9

Chapter 3 IP Address Planning
IP Addresses in a TransNav Network .................................... 2-13
IP Addressing Guidelines ................................................ 2-15
IP Networks and Proxy ARP ............................................. 2-15
In-Band Management with Static Routes ............................. 2-15
Out-of-Band Management with Static Routes ......................... 2-16
Out-of-Band Management with no DCC Connectivity .............. 2-16
TraverseEdge 50 and TransAccess Mux ............................... 2-16
Quality of Service ....................................................... 2-17
Proxy ARP ............................................................... 2-18
In-Band Management with Static Routes ............................. 2-19
In-Band Management with Router and Static Routes ............... 2-20
In-Band Management of CPEs Over EOP Links ...................... 2-21
Out-of-Band Management with Static Routes ......................... 2-23

Chapter 4 Network Time Protocol (NTP) Sources
NTP Sources in a Traverse Network .................................... 2-25
Daylight Saving Time .................................................... 2-25
NTP Sources on a Ring Topology ....................................... 2-26
NTP Sources on a Linear Chain Topology ............................. 2-26
Chapter 1
TransNav Management System Requirements

Introduction

The TransNav management system software package contains both server and client workstation applications. The server functions communicate with the nodes and maintain a database of topology, configuration, fault, and performance data for all nodes in the network. The client workstation application provides the user interface for managing the network.

Note: The TransNav and TN-Xpert management system applications can co-exist and be run independently on a single workstation. The TransNav management system allows you to access the Traverse and TE-100 products, while the TN-Xpert management system application allows you to access the TE-206 nodes. Currently, the TE-206 nodes must be installed using the TN-Xpert management system and have an IP address assigned. The TE-206 nodes can then be discovered on the TransNav management system. For details on the TN-Xpert management system, see the TransNav Xpert Installation Guide and the TransNav Xpert Users Guide.

For information on installing the TN-Xpert application, see the TransNav Xpert Installation Guide.

Use the requirements listed in the following sections to help you determine the management system requirements for your network.

- Management System Deployment, page 2-2
- TransNav Network Management, page 2-2
- Sun Solaris Platform for TransNav Management Server, page 2-3
- Windows Platform for TransNav Management Server, page 2-4
- TransNav GUI Application, page 2-5
TransNav Product Overview Guide, Section 2: Management System Planning

Management System Deployment

The TransNav management system software package contains server applications, client workstation applications, and agent applications that reside on the node.

![Management System Deployment Diagram]

Each TransNav management system supports up to eight servers; one server is designated as the Primary server, the remaining servers are designated as Secondary servers. The Primary server actively manages the network. The Secondary servers passively view the network but cannot perform any management operations that would change the state of the network. Any Secondary server can be promoted to the Primary server role in case of failure or maintenance. The switch in server roles requires some degree of user intervention.

The server applications communicate with the nodes and maintain a database of topology, configuration, fault, and performance data for all nodes. The client workstation application provides the user interface for managing the network (GUI or CLI). The agent application resides on the node control card and maintains a persistent database of management information for the node. It also controls the flow of information between the management server and the node itself.

In addition to the management system applications, the TransNav management system uses the following Traverse software components:

**Intelligent Control Plane**

An Intelligent Control Plane is a logical set of connections between TransNav-managed network elements through which those network elements exchange control and management information. This control and management information can be carried either in-band or out-of-band.

- See Chapter 3—“IP Address Planning,” Quality of Service, page 2-17 for an example and description of IP quality of service routing protocol.
- See Chapter 3—“IP Address Planning,” Proxy ARP, page 2-18 for information on using the proxy address resolution protocol.
- See Chapter 3—“IP Address Planning,” In-Band Management with Static Routes, page 2-19 for an example and a detailed description.
- See Chapter 3—“IP Address Planning,” Out-of-Band Management with Static Routes, page 2-23 for an example and a detailed description.
Control Plane Domain

A control plane domain is a set of nodes completely interconnected by the intelligent control plane. One TransNav management system can manage up to 200 nodes in a single control plane domain.

Domain management includes tasks such as:
- Setting the gateway node
- Configuring network links
- Creating performance monitoring templates and alarm profiles
- Creating protection rings and services
- Generating reports

Management Gateway Nodes

The TransNav management server connects to nodes over the service provider’s TCP/IP data communications network. The management system accesses a network through one or more nodes that are designated as management gateway nodes (MGN).

For in-band management, only one node is connected to the management server. Therefore, there is one MGN in a network that is managed in-band.

For out-of-band management, each node is connected to the management server either directly or through a router. Each node is considered a MGN.

This table lists the minimum requirements for a Sun Solaris system TransNav management server, including requirements allowing TN-Xpert to reside on the same workstation server.

### Table 2-1 Sun Solaris Requirements, TransNav Management Server

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Up to 100 nodes: 2 UltraSPARC IIIi CPU processors (1.5 GHz)</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 2 UltraSPARC IV CPU processors (1.6 GHz)</td>
</tr>
<tr>
<td></td>
<td>1 UltraSPARC T1 processors 6 core (1.0 GHz)</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>Up to 100 nodes: 4 GB, 2 MB cache</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 8 GB, 4 MB cache</td>
</tr>
<tr>
<td>Hard Drives</td>
<td>Up to 100 nodes: 73 GB of hard disk space (RAID controller optional; more disk space if a hot-spare is desired or if more storage is desired for log files)</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 146 GB of hard disk space (RAID controller optional; more disk space if a hot-spare is desired or if more storage is desired for log files)</td>
</tr>
<tr>
<td></td>
<td><strong>TransNav and TN-Xpert on same server:</strong></td>
</tr>
<tr>
<td></td>
<td>Up to 100 nodes: 100 GB of hard disk space</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 160 GB of hard disk space</td>
</tr>
<tr>
<td>CD-ROM Drive</td>
<td>Internal or External</td>
</tr>
<tr>
<td>Backup System</td>
<td>Internal is optional; SAN (Storage Area Network) is recommended</td>
</tr>
</tbody>
</table>
Windows Platform for TransNav Management Server

This table lists the minimum requirements for a Windows platform TransNav management server, including requirements allowing TN-Xpert to reside on the same server.

### Table 2-2 Windows Requirements, TransNav Management Server

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Up to 100 nodes: PowerEdge1850, 3.0 GHz</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: PowerEdge6850, 3.6 GHz</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>Up to 100 nodes: 4 GB, 2 MB cache</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 8 GB, 4 MB cache</td>
</tr>
<tr>
<td>Hard Drives</td>
<td>Up to 100 nodes: 73 GB of hard disk space</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 146 GB of hard disk space</td>
</tr>
<tr>
<td></td>
<td><strong>TransNav and TN-Xpert on same server:</strong></td>
</tr>
<tr>
<td></td>
<td>Up to 100 nodes: 100 GB of hard disk space</td>
</tr>
<tr>
<td></td>
<td>Up to 200 nodes: 160 GB of hard disk space</td>
</tr>
<tr>
<td>CD-ROM Drive</td>
<td>Internal or External</td>
</tr>
<tr>
<td>Monitor</td>
<td>Server only: High resolution 15-inch (1024 x 768)</td>
</tr>
<tr>
<td></td>
<td>Server and client: High resolution 21-inch (1280 x 1024)</td>
</tr>
<tr>
<td>Disk Backup System</td>
<td>Required if unable to back up TransNav database to server on the network.</td>
</tr>
<tr>
<td>Network</td>
<td>One or two 10/100BaseT Ethernet cards. One Ethernet Network Interface Card (NIC) connects to the Data Communications Network (DCN). The second optional Ethernet NIC connects to the Local Area Network (LAN) connecting the client workstations.</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td>Operating Environment</td>
<td>Sun Solaris 9 or 10</td>
</tr>
<tr>
<td></td>
<td>Solaris 9 recommended patch cluster: date stamp of July 7, 2004</td>
</tr>
<tr>
<td></td>
<td>Bash shell</td>
</tr>
<tr>
<td>PDF Viewer</td>
<td>To view product documentation:</td>
</tr>
<tr>
<td></td>
<td>Adobe® Acrobat® Reader® 8.0 or 9.0 for Windows and 7.0.9 or 8.1.3 for Solaris. Download the application for free from Adobe’s site at: <a href="http://www.adobe.com">www.adobe.com</a>.</td>
</tr>
</tbody>
</table>
You require a client workstation to access the TransNav management server from the graphical user interface (GUI). Force10 recommends installing the application directly on the client workstation for faster initialization, operation, and response time.

### Table 2-2  Windows Requirements, TransNav Management Server (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Environment</td>
<td>Windows 2000 Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003. Microsoft client licenses are not required for clients to connect to TransNav software running on Microsoft Windows 2003 Server platform.</td>
</tr>
<tr>
<td></td>
<td>Windows Microsoft Vista (limited to TransNav Client running on Microsoft Vista)</td>
</tr>
<tr>
<td>PDF Viewer</td>
<td>To view product documentation: Adobe® Acrobat® Reader® 8.0 or 9.0 for Windows and 7.0.9 or 8.1.3 for Solaris. Download the application for free from Adobe's site at: <a href="http://www.adobe.com/">www.adobe.com/</a></td>
</tr>
<tr>
<td>FTP server application</td>
<td>To distribute TransNav software to network elements: Force10 recommends WAR FTP for Windows. Download the application for free from Adobe’s site at: <a href="http://www.warftp.org">www.warftp.org</a>.</td>
</tr>
<tr>
<td>Telnet server application</td>
<td>To access the TransNav management server remotely.</td>
</tr>
<tr>
<td>Compression software</td>
<td>Force10 recommends the popular compression application WinZip. See <a href="http://www.winzip.com/">www.winzip.com/</a></td>
</tr>
</tbody>
</table>

### Table 2-3  TransNav GUI Application Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Sun SPARC (Solaris version independent) workstation¹ or Windows PC capable of running Windows 2000 Professional, Windows XP Professional, Windows 2003 Server, or Windows Vista</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>Up to 100 nodes: 4 GB Up to 200 nodes: 8 GB</td>
</tr>
<tr>
<td>Hard Drive Space</td>
<td>73 GB or more recommended</td>
</tr>
<tr>
<td>Monitor</td>
<td>High resolution 21-inch (1280 x 1024) monitor or high resolution laptop</td>
</tr>
<tr>
<td>Network</td>
<td>One 10/100BaseT Ethernet Card</td>
</tr>
</tbody>
</table>
Table 2-3  TransNav GUI Application Requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td>Operating Environment</td>
<td>Any of the following operating environments:</td>
</tr>
<tr>
<td></td>
<td>Sun Solaris 9 or 10</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2000 Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows XP Professional Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Microsoft Vista (limited to TransNav Client running on Microsoft Vista)</td>
</tr>
<tr>
<td>PDF Viewer</td>
<td>To view product documentation:</td>
</tr>
<tr>
<td></td>
<td>Adobe® Acrobat® Reader® 7.0 or 8.0 for Windows and 7.0.8 for Solaris.</td>
</tr>
<tr>
<td></td>
<td>Download the application for free from Adobe’s site at: <a href="http://www.adobe.com/">www.adobe.com/</a></td>
</tr>
<tr>
<td>Compression software</td>
<td>Force10 recommends the popular compression application WinZip. See <a href="http://www.winzip.com/">www.winzip.com/</a></td>
</tr>
</tbody>
</table>

1 The GUI application has not been tested on the Sun i386 or Intel-based LINUX configurations.
The Node-level GUI is a subset of the TransNav server GUI. Access to the Node-level GUI requires a client workstation. Access to a TransNav management server is required only to download the Node-level GUI application to the client workstation or laptop. Information in the Node-level GUI is obtained directly from the Traverse platform. The Node-level GUI release must match the corresponding Traverse release to avoid unexpected behavior.

Table 2-4 Node-level GUI Application Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Windows PC or laptop capable of running Windows 2000 Professional,</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional, Windows 2003 Server, or Windows Vista</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>4 GB</td>
</tr>
<tr>
<td>Hard Drive Space</td>
<td>73 GB or more recommended</td>
</tr>
<tr>
<td>Monitor</td>
<td>High resolution 21-inch (1280 x 1024) monitor or high resolution laptop</td>
</tr>
<tr>
<td>Network</td>
<td>One 10/100BaseT Ethernet Card</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td>Operating Environment</td>
<td>Any of the following operating environments:</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2000 Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows XP Professional Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>Windows Microsoft Vista (limited to TransNav Client running on Microsoft</td>
</tr>
<tr>
<td></td>
<td>Vista)</td>
</tr>
</tbody>
</table>
Chapter 2
TransNav Management System Planning

Introduction
This chapter includes the following information on creating and managing a network using the TransNav management system:

- **Recommended Procedure to Create a Network**, page 2-9

The system can be set up to also contain the TN-Xpert management system, allowing you to access both the TransNav and TN-Xpert management systems, Traverse nodes, TE-100 nodes, and TE-206 nodes from a single server. Currently, the TE-206 nodes must be installed using the TN-Xpert management system and have an IP address assigned. They can then be discovered on the TransNav management system. For information on installing TN-Xpert, see the TransNav Xpert Installation Guide.

---

**Recommended Procedure to Create a Network**

Use these steps as a guideline to create a TransNav managed network.

**Table 2-5 Network Configuration Procedure and References**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 1    | Create a network plan. | Traverse Product Overview Guide  
TraverseEdge 50 User Guide  
TraverseEdge 100 User Guide  
TransAccess 200 Mux User Guide  
TransNav Management System Product Overview Guide  
TransNav Xpert Installation Guide  
TransNav Xpert Users Guide  
TraverseEdge 206 Users Guide |
<p>| 2    | Assign IP addresses to the management server(s) and network elements. | TransNav Management System Product Overview Guide, Section 2—“Management System Planning,” page 2-13 |
| 3    | Set a management server as the primary NTP server. | TransNav Management System Server Guide, Section 2—“Management Server Procedures,” Chapter 1—“Creating the Management Servers,” page 2-5 |
| 4    | Add routes for the node-ips to the management server. | This step depends on the server platform (Solaris or Windows) and local site practices. Contact your local site administrator. |
| 5    | Install the TransNav management system software. | TransNav Management System Server Guide, Section 1—“Installation and Description” |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Initialize, then start the server. Start the Primary server first, then initialize and start the Secondary servers.</td>
<td>TransNav Management System Server Guide, Section 2—Management Server Procedures, Chapter 3—“Server Administration Procedures,” page 2-27</td>
</tr>
</tbody>
</table>
Table 2-5 Network Configuration Procedure and References (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 11   | If necessary, configure equipment, cards, and interfaces. | Traverse Provisioning Guide, Section 2—Configuring TDM Equipment  
TraverseEdge 50 User Guide  
TraverseEdge 100 User Guide  
TransAccess 200 Mux User Guide  
TransNav Xpert Users Guide  
TraverseEdge 206 Users Guide |
| 12   | Create services or other applications. | Traverse Provisioning Guide  
TraverseEdge 50 User Guide  
TraverseEdge 100 User Guide  
TransAccess 200 Mux User Guide  
TransNav Xpert Users Guide  
TraverseEdge 206 Users Guide |
Chapter 3
IP Address Planning

Introduction
This chapter includes the following information on creating and managing a network using the TransNav management system:

- IP Addresses in a TransNav Network, page 2-13
- IP Addressing Guidelines, page 2-15
- Quality of Service, page 2-17
- Proxy ARP, page 2-18
- In-Band Management with Static Routes, page 2-19
- In-Band Management with Router and Static Routes, page 2-20
- In-Band Management of CPEs Over EOP Links, page 2-21
- Out-of-Band Management with Static Routes, page 2-23

IP Addresses in a TransNav Network
The network management model (in-band or out-of-band) determines the IP address requirements of the network. A TransNav-managed network requires a minimum of two separate IP network addresses as indicated below.

**Note:** If your system includes TE-206 nodes, you must first commission the TransNav management system, then commission the TE-206 nodes using TN-Sight. You can then connect to the TE-206 nodes from the TransNav GUI using an IP address. For more information on managing TE-206 nodes from the TransNav GUI, see the TransNav Management System GUI Guide, Section 2—Administrative Tasks, Chapter 6—“Using TransNav GUI with TN-Sight”

- The IP address assigned to the Ethernet interface on the back of the shelf (bp-dcn-ip) determines the physical network.
- The IP address assigned to the node (node-ip) is used by the management server to manage the network.
Assign the relevant IP addresses through the CLI during node commissioning.

**Table 2-6 IP Address Node Connectivity Parameters**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required?</th>
<th>Description</th>
<th>Force10 Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-id</td>
<td>Required on every node.</td>
<td>A user-defined name of the node. Enter alphanumeric characters only. Do not use punctuation, spaces, or special characters.</td>
<td>Use the site name or location.</td>
</tr>
<tr>
<td>node-ip</td>
<td>Required on every node.</td>
<td>This parameter specifies the IP address of the node. This address is also known as the Router ID in a data network environment. In a non-proxy network, Force10 recommends that this address be the same as the bp-dcn-ip. If it is not equal to the bp-dcn-ip, it must be on a different IP network. Force10 recommends that the node-ips for all nodes in one network be on the same IP network.</td>
<td>10.100.100.x where x is between 1 and 254. Use a unique number for each network node.</td>
</tr>
<tr>
<td>bp-dcn-ip</td>
<td>Required on each node that is connected or routed to the management server or on any node with a subtended device.</td>
<td>This parameter specifies the IP address assigned to the Ethernet interface on the back of the node. In a non-proxy network, Force10 recommends that this address be the same as the node-ip. If it is not equal to the node-ip, it must be on a different IP network. Enter an IP address if this node is connected to the management server (either directly or through a router) or to a TransAccess product.</td>
<td>Use a different subnet for each site.</td>
</tr>
<tr>
<td>bp-dcn-mask</td>
<td>Required for each bp-dcn-ip.</td>
<td>Enter the appropriate address mask of the bp-dcn-ip address.</td>
<td>Depends on site practices.</td>
</tr>
<tr>
<td>bp-dcn-gw-ip</td>
<td>Required for each bp-dcn-ip.</td>
<td>If the node is connected directly to the management server, this address is the IP gateway of the management server. If there is a router between the management server and this node, this address is the IP address of the port on the router connected to the Ethernet interface on the back of the Traverse node.</td>
<td>Depends on site practices.</td>
</tr>
</tbody>
</table>
Table 2-6  IP Address Node Connectivity Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required?</th>
<th>Description</th>
<th>Force10 Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ems-ip</td>
<td>Required if there is a router between this node and the management server.</td>
<td>This address is the IP address of the TransNav management server. This IP address must be on a separate network from any node-ip and gcm-{a</td>
<td>b}-ip. For in-band management, this address must be on or routed to the same network as the bp-dcn-ip of the management gateway node (the node with the physical connection to the management server). For out-of-band management, this address must be connected or routed to all bp-dcn-ip addresses.</td>
</tr>
<tr>
<td>ems-gw-ip</td>
<td>Required for each ems-ip.</td>
<td>This address is the IP address of the port on the router connected to the Ethernet interface on the back of the Traverse shelf. This address is the same address as bp-dcn-gw-ip.</td>
<td>Depends on site practices.</td>
</tr>
<tr>
<td>ems-mask</td>
<td>Required for each ems-ip.</td>
<td>Required if there is a router between the node and the management server. This address is the address mask of the IP address on the management server (ems-ip).</td>
<td>Depends on site practices.</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>Required on the node acting as proxy server for the IP subnet.</td>
<td>Enable this parameter if this node is to be used as the proxy server for the IP subnet. The bp-dcn-ip and the node-ip of the proxy node must be the same IP address. Once you plan the network with one node as the proxy, you cannot arbitrarily re-assign another node to be the proxy ARP server.</td>
<td>Depends on network plan and site practices.</td>
</tr>
</tbody>
</table>

**IP Networks and Proxy ARP**

On the proxy node:

- The *Proxy ARP* parameter must be enabled on the management gateway node. In Map View, click a node, click the *Config* tab, and change the value in Proxy ARP to *enabled*.
- The bp-dcn-ip and the node-ip of the proxy node must be the same IP address.

In a proxy network, all of the node-ip addresses must be in the same subnetwork as the bp-dcn-ip of the proxy node.

Once you plan the network with one node as the proxy, you cannot arbitrarily re-assign another node to be the proxy ARP server.

**In-Band Management with Static Routes**

General guidelines to assign IP addresses in a TransNav network managed in-band with static routes are:

- Force10 recommends that all node-ip addresses are in a physically non-existent (virtual) IP network.
- For the node connected to the management server (either directly or through a router), all IP addresses provisioned on the node MUST be in separate networks.
• For all other nodes in the network, the node-id and the node-ip are the only required commissioning parameters.
• The management server must be able to communicate with all node-ip addresses.
  – Add routes to the management server using the node-ip, the address mask of the bp-dcn-ip, and bp-dcn-ip of the node that is connected to the management server.
  – The IP address of the management server must be on or routed to the same network as the bp-dcn-ip of the management gateway node.

Out-of-Band Management with Static Routes
General guidelines to assign IP addresses in a TransNav network managed out-of-band with static routes are:
• Force10 recommends that all node-ip addresses are in a physically non-existent (virtual) IP network.
• Each node is connected to the management server through an IP network. All IP addresses provisioned on one node are in separate networks.
• The management server must be able to communicate with all node-ip addresses.
  – Add routes using the node-ip, address mask of the bp-dcn-ip, and the IP address of the port on the router that is connected to the management server.
  – The IP address of the management server must be connected or routed to all bp-dcn-ip addresses.

Out-of-Band Management with no DCC Connectivity
If there is no DCC connectivity between individual nodes, each node must still communicate to the node-ip of the other nodes in the network. In this case, create routes at relevant IP routers for all node-ips in the network.

TraverseEdge 50 and TransAccess Mux
The node to which the TraverseEdge 50 or TransAccess Mux is connected must have the backplane IP address information provisioned:
• bp-dcn-ip: For in-band management, this address must be in a separate network than the bp-dcn-ip of the node that is connected to the management server.
• bp-dcn-gw-ip: This address is in the same subnetwork as the bp-dcn-ip of this node.
• bp-dcn-mask: The address mask of the bp-dcn-ip of this node.

The IP address of the TransAccess Mux will have the following characteristics:
• IP address: This IP address can be on the same subnetwork as the node bp-dcn-ip.
• Gateway: This IP address is the bp-dcn-ip of the node.
• Mask: This mask is the address mask of the bp-dcn-ip of the node.
• Trap-1: This address is the bp-dcn-ip of the node to which it is connected.
Quality of Service

The IP QoS (IP Quality of Service) routing protocol enables a Traverse node to broadcast its forwarding table over the backplane for the data control network (bp-dcn-ip), thus improving the quality of service over the backplane DCN ethernet interface. Setting up static routes on intermediate routers between the Traverse management gateway element and the TransNav management server is no longer necessary. Existing traffic engineering and security capabilities are not changed.

When IP QoS is enabled on the management gateway node during commissioning, source IP address packets are user-configured to block or allow traffic originated by certain IP hosts or networks using the access control list (ACL). Received packets are filtered, classified, metered, and put in queue for forwarding.

The ACL searches received IP address packets for the longest prefix match of the source IP address. When the address is found, it is dropped or forwarded according to the ACL settings (permit or deny). If no instruction is present in the ACL, the packet is forwarded.

Outgoing IP address packets are prioritized as either High Priority or Best Effort and put in queues for forwarding. The queue size for outgoing address packets is set by the percent of available bandwidth.

Figure 2-2  IP Quality of Service

See the TransNav Management System GUI Guide, Chapter 1—“Creating and Deleting Equipment Using Preprovisioning,” Node Parameters, page 3-3 for detailed information about setting up IP Quality of Service in a TransNav-managed network.
Proxy ARP

Proxy address resolution protocol (ARP) is the technique in which one host, usually a router, answers ARP requests intended for another machine. By faking its identity, the router accepts responsibility for routing packets to the real destination. Using proxy ARP in a network helps machines on one subnet reach remote subnets without configuring routing or a default gateway. Proxy ARP is defined in RFC 1027.

In this example network, the EMS server communicates through an IP network to Node 1. Node 1 (the proxy node) learns all the IP addresses of the nodes in the subtending network and takes responsibility to route packets to and from the correct destinations.

The EMS server keeps the IP-to-network-address mapping found in the reply in a local cache and uses it for later communication with the nodes. The proxy node can proxy addresses for any Traverse node, TraverseEdge node, or TransAccess Mux equipment connected to it.

In a proxy network, all of the node-ip addresses must be in the same subnetwork as the bp-dcn-ip of the proxy node. On the proxy node, the Proxy ARP parameter is enabled and the bp-dcn-ip and the node-ip must be the same IP address. Once you plan the network with one node as the proxy, you cannot arbitrarily re-assign another node to be the proxy ARP server.
In-band management with static routes means the management server is directly connected by static route to one node (called the management gateway node), and the data communications channel (DCC) carries the control and management data.

In this simple example, the TransNav management server (EMS server) is connected to a management gateway node (Node 1) using the Ethernet interface on the back of the shelf. The server communicates to the other nodes in-band using the DCC.

In this example, to get the management server to communicate to all nodes, add routes on the server to the node-ip of each node. The server communicates with the nodes using the bp-dcn-ip of the management gateway node (Node 1). Note that all IP addresses on Node 1 (node-ip and bp-dcn-ip) are in separate networks.

Node 2 has a subtending TransAccess Mux (either a TA155 or a TA200) connected by Ethernet. The bp-dcn-ip address is necessary to connect the TransAccess system. The bp-dcn-ip of this node must be in a separate network from the bp-dcn-ip on Node 1.

At Node 3, the node-id and the node-ip are the only required commissioning parameters. However, Node 3 also has a subtending TraverseEdge 100 network managed in-band through the management gateway node. The IP address requirements are the same as for the Traverse platform.

See the topic [IP Addresses in a TransNav Network](#), page 2-13 for detailed information about assigning IP addresses in a TransNav-managed network.
In this example, the management server is connected by static route to a router that, in turn, is connected to the management gateway node (Node 1). The server communicates to the other nodes in-band using the DCC.

In this example, to get the management server to communicate to each node, add routes on the server to the node-ip of each node. The gateway through which the management server communicates with the nodes is the IP address of the port on the router connected to the server.

At the router, add the routes for each node-ip using the gateway bp-dcn-ip of the management gateway node (Node 1).

See the topic IP Addresses in a TransNav Network, page 2-13 for detailed information about assigning IP addresses in a TransNav-managed network.
In this example, the management server is connected by static route to a router that, in turn, is connected to the management gateway node (Node 1). The server communicates to the other nodes in-band using the DCC, including the node that has CPE devices attached (Node 3). The IP packets from CPE devices are forwarded through the node over electrical cards to EOP links on the EoPDH cards, and then through the Ethernet Control Channel interface (ECCI) for forwarding over the system by Traverse Ethernet services.

In the above example, add routes on the management server to communicate to the node-ip of the nodes that have CPEs attached. This allows IP packets from the CPEs to be transmitted over the Traverse system. The server communicates with all the nodes over a static route using the bp-dcn-ip of the management gateway node (Node 1).

At Node 3, the node-id and node-ip are required commissioning parameters, as are the CPE-ip’s of each CPE device. A default ECC interface gateway IP address (ecci-gw-ip) must also be configured on each CPE device to allow all IP packets to be sent through the electrical card to the ECC interface on the node. Node 3 must have an EoPDH card with an EOP port set up. Each EOP port is a member port on the ECC interface. The VLAN tag of each ECCI member port corresponds to the management VLAN of the attached CPE device, thus providing the interface between the CPEs and the management system using an ECC interface.
The EoPDH cards are connected by EOP links through the electrical cards to the CPEs as shown below.

![Connecting CPEs through EOP Links](image)

**Figure 2-7  Connecting CPEs through EOP Links**

See the topic [IP Addresses in a TransNav Network](#), page 2-13 for detailed information about assigning IP addresses in a TransNav-managed network.
Out-of-band management with static routes means that the management server is directly connected by static route to each node by the Ethernet interface on the back of each shelf. In this example, the management server communicates to each node directly or through a router.

Add a route to the management server using the bp-dcn-ip of Node 1. Add separate routes to the node-ip of Node 2 and Node 3 using the IP address of the port on the router connected to the server (Port IP A) as the gateway address.

At each router in the network, an administrator must add a route to the node-ip of the nodes.

At Node 2, the bp-dcn-ip can be in the same network as the TransAccess Mux connected to it.

See the topic IP Addresses in a TransNav Network, page 2-13 for detailed information about assigning IP addresses in a TransNav-managed network.
Chapter 4
Network Time Protocol (NTP) Sources

Introduction
This chapter includes the following information on managing a Traverse network:

• NTP Sources in a Traverse Network, page 2-25
• NTP Sources on a Ring Topology, page 2-26
• NTP Sources on a Linear Chain Topology, page 2-26

NTP Sources in a Traverse Network
Network Time Protocol provides an accurate Time of Day stamp for performance monitoring and alarm and event logs. Force10 recommends using the TransNav management system server as the primary NTP source if you do not already have a NTP source defined. If no primary NTP source is configured, the TransNav system defaults to the TransNav server as the primary NTP source. A secondary NTP IP server address is optional.

Depending on the topology, configure a primary NTP source and a secondary NTP source for each node in a network.
• For ring topologies, see NTP Sources on a Ring Topology, page 2-26.
• For linear chain topologies, see NTP Sources on a Linear Chain Topology, page 2-26.

Daylight Saving Time
As part of a United States federal energy conservation effort, Daylight Saving Time (DST) starts three weeks earlier and ends one week later than in years prior to 2007. Certain telecommunications products contain the ability to synchronize to a network clock or automatically change their time stamp to reflect time changes. Each device may handle the recent change in DST differently.

All dates displayed in the TransNav management system CLI for alarms, upgrade times, events, and performance monitoring (PM) will include the new DST as part of Release TN3.1.x. The TraverseEdge 100 system CLI will include the new DST as part of Release TE3.2.
**NTP Sources on a Ring Topology**

Force10 recommends using the adjacent nodes as the primary and secondary NTP sources in a ring configuration. Use the Management Gateway Node (MGN) or the node closest to the MGN as the primary source and the other adjacent node as the secondary source. The following example shows NTP sources in a ring topology.

![NTP Sources on a Ring Topology](image)

**Figure 2-9  NTP Sources on a Ring Topology**

In the above example, the MGN selects the management server as the primary NTP server and does not select a secondary server. At Node 2, you would configure the primary server as Node 1 (the MGN), and the secondary server as Node 3.

**NTP Sources on a Linear Chain Topology**

On a linear chain topology, Force10 recommends using the upstream node as the primary NTP source and the management server as the secondary NTP source.

In the following example, Node 1 (the MGN) selects the management server as the primary NTP server and does not select a secondary server. At Node 2, you would configure Node 1 as the primary NTP server and the management server as the secondary source.

![NTP Sources on a Linear Chain Topology](image)

**Figure 2-10  NTP Sources on a Linear Chain Topology**
INDEX

A
Access
groups
see Role-based Access Control
Accounting data
basis, 1-10
Administration
data collection, 1-11
nodes, 1-10
reports, 1-11
Alarms
GUI windows, 1-7
node group, 1-7, 1-16
Auto-discovery
intelligent control plane, 1-8

C
CLI
commands
description, 1-18
Configuration
management
equipment, 1-8
multiple servers, 1-9
preprovisioning, 1-9
service provisioning, 1-9
Control
RBAC, see Role-based Access Control
Control module
remote restore, 1-11

D
Dataset snapshots, 1-12
Daylight Saving Time
support, 2-25
Domain
security
see Role-based Access Control

E
Event
management, 1-7

F
Fault
management, 1-7

G
Graphical user interface
fault and event management, 1-7
hardware requirements, 2-5
node-level GUI, 2-7
menu bar, 1-16
performance management, 1-10
shelf view, 1-17
software requirements, 2-5
node-level GUI, 2-7
types, 1-15
views
map view, 1-15
navigation tree, 1-16
network map, 1-15
GUI, see Graphical user interface

H
Hardware
requirements
GUI application, 2-5, 2-7
Sun Solaris server, 2-3
Windows, 2-4

I
Intelligent control plane
auto-discovery, 1-8
connectivity
node, 1-4
service, 1-11
preprovisioning, 1-9
Interoperability
third party management systems
SNMP traps, 1-4
TL1 interface, 1-4
IP address
requirements, 2-13

M
Management
plane
equipment configuration, 1-8
server
primary, 1-3, 2-2
secondary, 1-3, 2-2
system
dataset snapshots, 1-12
fault management, 1-7
Index

reports, 1-11
security, Role-based Access Control, 1-10
software components, 1-1

Management system
hardware requirements
  GUI application, 2-5
  node-level GUI application, 2-7
  Sun Solaris server, 2-3
  Windows, 2-4
server software requirements
  GUI application, 2-5
  Sun Solaris, 2-3
  Windows, 2-4
software requirements
  node-level GUI application, 2-7

Map view
  group map, 1-15
  network map, 1-15
MaxNoOfUserSessions, see Server, parameter

N
Navigation tree
  GUI, 1-16
Network planning
  creation process, 2-9
  IP addresses, 2-13, 2-15
  NTP sources, 2-25
Node
  security
    see Role-based Access Control
Node-level GUI
  application requirements, 2-7

O
Operating system
  requirements
    node-level GUI, 2-7
    Sun Solaris server, 2-3
    Windows server, 2-4

P
Primary server, see Servers
Proxy ARP, 2-18

R
Report
  types, 1-11
Reports
  dataset snapshots, 1-12
Role-based Access Control
  access groups, 1-10
  functional groups, 1-3, 1-10
  security
    domain, 1-10
    node, 1-10
    server, 1-10

S
Scalability, see System
Secondary server, see Servers
Security management, see Role-based Access Control
Servers
  function
    primary, 1-9
    secondary, 1-9
  import
    time, 1-9
  multiple, 1-9
  parameter
    MaxNoOfUserSessions, 1-4
    primary
Shelf
  view
    GUI, 1-17
Software
  requirements
    GUI application, 2-5, 2-7
    Sun Solaris server, 2-3
    Windows, 2-4
System
  interoperability, 1-4
  requirements, see Management system
  scalability, 1-5
  simultaneous users, 1-4

T
TL1
  interface
    description, 1-18

U
Users
  simultaneous, 1-4
  MaxNoOfUserSessions, 1-4