Carrier VoIP

MSS15K, MG15K, and MDM Configuration Overview PT-AAL1/UA-AAL1/UA-IP/PT-AAL2

NN10114-511

Document status: Standard
Document version: 09.01
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

Contents

New in this release 7
Channel associated signaling (CAS) 7
PT-IP Nodal Provisioning Templates 8
Media Gateway 2pVSP4e function processor 8
Other changes 9

Overview of shelf-wide and CP configuration 11
Overview of Multiservice Switch 15000 software 12
Nodal Provisioning Template and node level configuration audits 14
Access control 14
ATM routing 15
IP networking (UA-IP)(PT-AAL2)(PT-IP) 16
Data collection system 17
LP feature configuration 17
Shelf/Module data 18
Network clock synchronization 19
OAM connectivity 19
Internode Emergency Stand Alone (ESA) for MG9000 27
Time of day 29

Overview of Multiservice Switch 15000 function processor configuration 31
Multiservice Switch 15000 function processor configuration (PT-AAL1 and UA-AAL1) 32
Multiservice Switch 15000/Media Gateway 15000 function processor configuration (UA-IP) 33
Multiservice Switch 15000/Media Gateway 15000 function processor configuration (PT-IP) 35
Task list for Multiservice Switch 15000 function processor configuration 35

Overview of Multiservice Switch 15000 interface configuration 37
Overview of interface configuration between network components (PT-AAL1/UA-AAL1) 38
VoA applications 38
Available component interfaces 38
Architecture example for Universal Access - AAL1 (UA-AAL1) 39

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Overview of interface configuration between network components (UA-IP) 43
VoIP applications 43
Available component interfaces 43
UA-IP architecture example 43
Overview of interface configuration between network components (PT-IP) 46
Link distribution (PT-AAL1 and UA-AAL1) 50
CS2000 link (PT-AAL1/UA-AAL1) 51
XA-Core link distribution (PT-AAL1/UA-AAL1) 51
SAM21 SC link distribution (UA-AAL1) 54
IW-SPM link distribution (PT-AAL1 and UA-AAL1) 55
DPT-SPM link distribution (PT-AAL1 and UA-AAL1) 56
MG4000 link distribution (PT-AAL1 and UA-AAL1) 56
MG9000 link distribution (UA-AAL1) 58
Internode Emergency Stand Alone for MG9000 60
Node-to-node ATM link distribution (PT-AAL1/UA-AAL1) 61
UAS link distribution (UA-AAL1) 62
DSL services link distribution (UA-AAL1) 63
Link distribution (UA-IP) 65
Multiservice Switch IP over ATM inter-shelf trunk interface (UA-IP) 66
MG9000 interface (UA-IP) 68
CS-LAN OC-12 interface (UA-IP) 71
CS-LAN GE interface (UA-IP) 71
Hairpin ATM/IP OC-3/OC-12 interfaces (UA-IP) 72
TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (UA-IP) 73
Media Gateway 15000 to MGC with H.248 (VSP3) interface (UA-IP) 73
Media Gateway 15000 to MGC with H.248 (VSP3-o) interface (UA-IP) 74
TDM trunk distribution (UA-IP) 74
TDM trunk preparation (LAPS STS) (UA-IP) 75
TDM ISUP trunk (VSP3-o) (UA-IP) 75
TDM ISUP trunk (VSP3) (UA-IP) 75
TDM PRI trunk profile (VSP3-o) (UA-IP) 76
TDM PRI trunk (VSP3-o) (UA-IP) 76
TDM PRI trunk profile (VSP3) (UA-IP) 76
TDM PRI trunk (VSP3) (UA-IP) 77
TDM PTS trunk profile (VSP3-o) (UA-IP) 77
TDM PTS trunk (VSP3-o) (UA-IP) 77
Link Distribution (PT-IP) 78
IP Core/CS-LAN interface (PT-IP) 78
TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (PT-IP) 79
Media Gateway 15000 to MGC with H.248 (VSP3-o/2pVSP4e) interface (PT-IP) 79
TDM trunk distribution (PT-IP) 80

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

TDM trunk preparation (LAPS STS) (PT-IP) 80

Overview of MDM server deployment and configuration 83

MDM server deployment scenarios 85

Servers required on the various workstations 85

MDP servers 109

Client-set servers 110

Overview of MDM server deployment 111

Deployment of servers using the dedicated network management approach 113

Deployment of MDM servers using the centralized network management approach 116

In-service migration of MDM servers to the centralized network management approach without using the higher-level management system as an aggregator 120

In-service migration of MDM servers to the centralized network management approach using the higher-level management system as an aggregator 122

Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client application 125

RADIUS configuration for centralized authentication 127

JAVA Web Start technology 128

MDM Admin Server redundancy 128

Workflow for centralized AAA on an MDM Admin Server in a VoA network with the Operator Client application 129

Auto-patching for MSS/MG15000 nodes from the MDM 133

Scheduling the MDMs 134

Controlling the auto-patch process 136

When the auto-patch script fails to download or apply a patch 137

MDM server configuration for Ethernet Routing Switch 8600 fault management (PT-AAL1 and UA-AAL1) 138

Downloading the ERS 8600 DCD cartridge from the ESD web site 139

Configuring MDM for ERS 8600 fault management 141

Verifying MDM configuration for ERS 8600 fault management 144

Overview of the EdgeLink 100 multiplexor to Multiservice Switch 15000 interface configuration 155

Use cases for Network incremental growth 159

Use cases for incremental growth of a Carrier VoIP network (PT-AAL1/UA-AAL1) 159

Addition of new FP pair (PT-AAL1/UA-AAL1) 160

Addition of new node-to-node ATM interface (PT-AAL1/UA-AAL1) 162

Addition of new MG4000 to Carrier VoIP network (PT-AAL1/UA-AAL1) 164

Addition of new MG9000 with OC-3 to Carrier VoIP network (UA-AAL1) 166

Addition of new MG9000 with DS1 IMA to Carrier VoIP network (UA-AAL1) 169

Addition of new MG9000 with DS3 ATM (UA-AAL1) 172

Addition of new IW-SPM (PT-AAL1/UA-AAL1) 174

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Addition of new DPT-SPM (PT-AAL1/UA-AAL1) 177
Use cases for incremental growth of a PT-AAL2 network 179
Use cases for incremental growth of a UA-IP network 184
Addition of new FP pair (UA-IP) 185
Addition of new MG9000 with OC-3 (UA-IP) 186
Addition of new MG9000 with STS-1/DS3 (UA-IP) 189
Addition of new MG9000 with DS1 IMA (UA-IP) 191
Addition of new Multiservice Switch inter-shelf IP interface to Carrier VoIP network (UA-IP) 194
Addition of new CS-LAN with GE (LAG and no LAG) (UA-IP) 197
Addition of new CS-LAN with OC-12 (UA-IP) 199
Addition of new VSP and TDM physical interface (UA-IP) 202
Addition of new TDM trunk interface (UA-IP) 205

SPFS configuration procedures 209
Updating the time of day for seasonal time changes task flow 270
Updating the time of day for seasonal time changes 271
Monitoring the script 275
NP Template taskflow 281
Accessing and using NP Templates 283
NP Template descriptions for PT-IP 288
SH-CPeD and SH-CPeE templates 288
VR template 289
FP card templates 290
Interface templates 293
Service templates 297
PRI Profile Template 304
PTS Profile Template 304
DS1/E1 ISUP trunk 305
28 DS1 ISUP trunk 306
63 ISUP E1 trunks 308
PRI trunks 309
PTS Trunks 311
Using the periodic routine exercise (REX) templates 313
REX scheduler 314

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

New in this release

This document provides a high-level overview of configuration for the following five solutions in the Carrier VoIP network:

- Packet Trunking - AAL1 (PT-AAL1)
- Universal Access - AAL1 (UA-AAL1)
- Universal Access - IP (UA-IP)
- Packet Trunking - AAL2 (PT-AAL2)
- Packet Trunking - IP (PT-IP)

This document gives an overview of the configuration for: Multiservice Switch 15000 and Media Gateway node including the Nortel Multiservice Data Manager. For an overview of the configuration of the Nortel Multiservice Data Manager software that manages these network elements, see *241-6001-801 Nortel Multiservice Data Manager Overview*.

This document includes the new features for release SN09U as follows:

- "Channel associated signaling (CAS)" (page 7)
- "PT-IP Nodal Provisioning Templates" (page 8)
- "Media Gateway 2pVSP4e function processor" (page 8)

Channel associated signaling (CAS)

Channel Associated Signaling (CAS), also known as Per-Trunk Signaling (PTS), allows CVoIP solutions to interface directly with a wide range of legacy switching systems which use CAS signaling. There are a large number of Per-Trunk Signaling systems that must access the Carrier VoIP network using legacy switching equipment. CAS allows the protocols required to access the Carrier VoIP network to continuously indicate their line state.

Channel associated signaling (CAS) Channel Associated Signaling (CAS), also known as Per-Trunk Signaling (PTS), allows CVoIP solutions to interface directly with a wide range of legacy switching systems which use CAS signaling. There are a large number of Per-Trunk Signaling

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

systems that must access the Carrier VoIP network using legacy switching equipment. CAS allows the protocols required to access the Carrier VoIP network to continuously indicate their line state. MG acts as a relay point for CAS signaling. Incoming CAS signals on the TDM interface are extracted from their CAS variant waveform according to the profile associated with each TDM endpoint and they are signalled to the Media Gateway Controller (MGC) using H.248. In the reverse direction, incoming CAS signals from MGC are applied to the designated TDM endpoints following the description indicated in the associated profile. The MGC controls a call upon received CAS signals and according to its switching capabilities as usual.

PT-IP Nodal Provisioning Templates

MDM Nodal Provisioning (NP) templates are available to configure MG15000s for the Packet Trunking IP (PT-IP) solution. The PT-IP solution uses the MG15000 as a media gateway for tandem trunking. The PT-IP NP Templates define one configuration for the MG15000 that is used when deployed in a Carrier VoIP PT-IP solution. See the following sections:

- "Overview of shelf-wide and CP configuration" (page 11)
- "Overview of Multiservice Switch 15000 function processor configuration" (page 31)
- "Overview of Multiservice Switch 15000 interface configuration" (page 37)
- Appendix "Using the MDM Nodal Provisioning Templates" (page 281)
- "Use cases for Network incremental growth" (page 159)

Media Gateway 2pVSP4e function processor

The voice services processor 4 with optical TDM interface (2pOC3ChSmIrVsp4e) functional processor (FP) offers double the capacity of the voice services processor 3 with optical TDM interface (VSP3-o), adds more packet FPGA capabilities, and is configurable for both wireline and wireless applications. The two on-board active optical TDM ports double the number of TDM connections (4032 TDM packet connections, up from 2016 provided by the VSP3-o), and therefore throughput, to deliver a higher DS0 density per shelf at a lowered cost per DS0. A variant of the VSP3-o, the 2pVsp4e is part of Nortel's Converged Media Solutions for Voice over IP (VoIP).

The following sections have been modified to incorporate this section:

- "Multiservice Switch 15000/Media Gateway 15000 function processor configuration (PT-IP)" (page 35)
- "VoIP applications" (page 47)
- "PT-IP architecture example" (page 48)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (PT-IP)" (page 79)
- "Media Gateway 15000 to MGC with H.248 (VSP3-o/2pVSP4e) interface (PT-IP)" (page 79)
- "TDM trunk preparation (LAPS STS) (PT-IP)" (page 80)
- "TDM ISUP trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PRI trunk profile (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PRI trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PTS trunk profile (VSP3-o/2pVSP4e) (PT-IP)" (page 82)
- "TDM PTS trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 82)
- "Adding new Function Processors to the MG15000" (page 179)
- "Adding a new FP pair to a node" (page 185)
- "Addition of new VSP and TDM physical interface (UA-IP)" (page 202)
- "Adding a new TDM trunk interface" (page 206)
- "Adding a new VSP or TDM physical interface" (page 203)
- "FP card templates" (page 290)
- "Service templates" (page 297)

Other changes

There were no other changes to this document that are not feature-related.

Copyright © 2006, Nortel Networks

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Overview of shelf-wide and CP configuration

This section is an overview of the shelf-wide and control processor (CP) configuration required by the Nortel Multiservice Switch 15000 software installed in your Carrier VoIP network. This section is intended for use with the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. The Configuration Attribute Summary contains tables of all the specific values to use when configuring Multiservice Switch 15000 nodes for the supported solutions.

The descriptions of Multiservice Switch 15000 software in this section contain cross-references to the corresponding sections in the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

> ***Note:*** Nortel recommends that all configuration changes contained in the Global Bulletin System (GBS) and the Method of Procedure (MOP) for the current release be reflected on the Multiservice Switch 15000 nodes before you perform the configurations described in this document.

All configuration tasks need to be performed using a copy of a completed Network Engineering Specification Book for your site. The Network Engineering Specification Books contain all the customer and site-specific information that the installer is likely to be prompted for when using the Nodal Provisioning templates or entering information marked as customer defined in the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Overview of Multiservice Switch 15000 software

Nortel Multiservice Switch 15000 software includes system functions for command processing, shelf management, file storage, data collection, and network management interfaces.

In a PT-AAL1 or UA-AAL1 solution, configure the shelf software applications of Multiservice Switch 15000 nodes using the PT-AAL1, or *WUA-AAL1 CPeD_Commissioning* template.

In a PT - AAL2 solution, configure the shelf software applications for the Control Processor CP3 (NTHW06) on MG15000 nodes with the PT-AAL2 SH-CPED template. The PT-AAL2 SH-CPED template defines shelf-wide parameters, including:

- CP-based configuration
- Network Synchronization with building-integrated timing supply (BITS)
- time of day synchronization
- the data collection system (DCS)
- the network management interface system (NMIS)
- asynchronous transfer mode (ATM) routing
- management virtual router (VR)
- VR/<CallP>

In a UA-IP solution, configure the shelf software applications as follows:

- for Multiservice Switch 15000 nodes use the UA-IP *SH-CPED* template to configure ATM routing
- for Media Gateway 15000-only node, use the UA-IP *SH-CPED-PVGnoARTG* template when ATM routing is not required
- for Media Gateway 15000-only nodes that are to be configured with the MG15000 periodic routine exercise (REX), use the *UA-IP SH-REX-Schedule* template as required for the solution to perform initial configuration of the REX application and feature

In a PT-IP solution, configure the shelf software applications as follows:

- for Media Gateway 15000 nodes use the *PT-IP SH-CPED* or the *PT-IP SH-CPEE* template to configure the base provisioning (The PT-IP SHCPEE template is for nodes in SDH networks.)
- for Media Gateway 15000-only nodes that are to be configured with the MG15000 periodic routine exercise (REX), use the *PT-IP SH-REX-Schedule* template as required for the solution to perform initial configuration of the REX application and feature. The REX template is the last template to be applied after you have configured the entire solution.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

A shelf commissioning template defines shelf-wide parameters for the following:

- CP-based configuration
- network synchronization with building-integrated timing supply (BITS)
- time of day synchronization
- the data collection system (DCS)
- the network management interface system (NMIS)
- asynchronous transfer mode (ATM) routing
- management virtual router (VR)
- voice services

This chapter provides more information about the functions of the base software applications and their configurations for the Multiservice Switch 15000.

Before you apply a shelf commissioning template, you must manually configure some applications. For information, see the following sections:

- "LP feature configuration" (page 17)
- "OAM connectivity" (page 19)

Next, apply one of the shelf commissioning templates as follows:

- *PT-AAL1 CPeD_Commissioning*
- *WUA-AAL1 CPeD_Commissioning*
- *UA-IP SH-CPED*
- *UA-IP SH-CPED-PVGnoARTG*
- *PT-AAL2 SH-CPED*
- *PT-IP SH-CPED* or *PT-IP SH-CPEE*

The shelf commissioning template configures the components described in the following sections:

- "ATM routing" (page 15) (not the *SH-CPED-PVGnoARTG* template)
- "IP networking (UA-IP)(PT-AAL2)(PT-IP)" (page 16)
- "Data collection system" (page 17)
- "Shelf/Module data" (page 18)
- "Network clock synchronization" (page 19)
- "Time of day" (page 29)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

You may need to perform additional configuration after applying a shelf commissioning template. For more information see your Network Engineering Specification Book. As well, the components for which you must perform additional configuration are described in the following sections:

- "Access control" (page 14)
- "ATM routing" (page 15)
- "IP networking (UA-IP)(PT-AAL2)(PT-IP)" (page 16)
- "OAM connectivity" (page 19)
- "Hitless activation of critical attributes" (page 22)

Nodal Provisioning Template and node level configuration audits

Multiservice Switch / Media Gateway configurations that were done using NP templates can be audited at a later date using the Nodal Provisioning Template audit tool. Also available is the Node level configuration audit which is an enhancement to the Nodal Provisioning template audit

The Nodal Provisioning Template audit tool allows the user to verify:

- whether the correct template was used for provisioning
- whether the values entered in the template were correct
- whether the template has been patched since it was originally applied
- whether the switch configuration has been manually changed since initial commissioning

If there is a mismatch between the template data and the on-switch data, the template can be reapplied to override the on-switch data, if desired. For more information on Nodal Provisioning see 241-6001-023 *Nortel Multiservice Data Manager Configuration Tools*.

For the Node level configuration audit the MSS/MG configuration data is compared against a template log and the discrepancies between the current configured view and the view represented by the template log are reported in the Node Level Audit report. An audit can be invoked from the Nodal Provisioning GUI for a MSS/MG provisioning view or be scheduled to run in a batch mode. See 241-6001-023 *Nortel Multiservice Data Manager Configuration Tools for more information*.

Access control

Network access control restricts user access to your network and keeps your data secure. Access control on Nortel Multiservice Switch 15000 nodes limits access to those users with the following:

- valid user IDs
- valid passwords

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- authorized remote IP access

Access control is set through the configuration of the *AccessControl* component and subcomponents. For the specific values to configure for the *AccessControl* components and subcomponents see: *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

For information on how to administer access control, see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

ATM routing

The ATM routing system is a connection-oriented system that provides dynamic runtime connection setup between Nortel Multiservice Switch 15000 nodes. The system allows them to interwork with other non-Multiservice Switch ATM equipment. Multiservice Switch ATM routing provides the addressing, signaling, and routing facilities to support permanent and switched virtual connections (PVCs and SVCs). These networking facilities allow you to set up ATM connections in real-time.

Hitless ATM routing for CP equipment protection is supported in the PT-AAL1, and UA-AAL1 solutions. This capability reduces interruptions to node call processing during

- a Hitless Software Migration (HSM)
- a CP equipment failure (including failure of the OAM Ethernet port or link)
- any maintenance actions resulting from a CP switchover

Hitless ATM routing for CP equipment protection, when provisioned, continuously synchronizes the standby CP routing database to the active CP routing database. The FPs also communicate with the active and standby CPs to ensure that both CPs get all the required port, address, and RCC information.

Configure the *AtmRouting (ARtg)* component to set ATM routing in a PT-AAL1, UA-AAL1, PT-AAL2, UA-IP, or PT-IP solution. For the specific values to configure this component, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For more information on Multiservice Switch ATM routing system see, *NN10600-700 Nortel Multiservice Switch 7400/15000/20000 ATM Technology Fundamentals* and *NN10600-702 Nortel Multiservice Switch 7400/15000/20000 ATM Routing and Signalling Fundamentals*.

IP networking (UA-IP)(PT-AAL2)(PT-IP)

Nortel Multiservice Switch 15000 Virtual Router (VR) system supports industry-standard IP networking for connectionless networking. Carrier VoIP networks support static routing as well as the dynamic routing protocol open shortest path first (OSPF). With OSPF, Multiservice Switch 15000 nodes learn dynamically, from neighboring routers, which routing paths through the network are available. This allows the node to adapt dynamically to faults elsewhere in the network and to calculate the most efficient path for all IP packets.

Carrier VoIP networks support Hitless OSPF for CP equipment protection. Hitless OSPF allows FP cards to continue forwarding, uninterrupted, over OSPF calculated routes during any of the following:

- Hitless Software Migration (HSM)
- CP equipment failure (including failure of the OAM Ethernet port or link)
- any maintenance actions resulting in a CP switchover

Hitless OSPF for CP equipment protection, when provisioned, continuously synchronizes the OSPF routing database of the standby CP with the routing database of the active CP.

Multiservice Switch 15000 nodes support Protected Default Routes on GE cards. You can specify two next hops, reachable through two different 4pGE FP cards, as the default route when you use Protect Default Routes. This allows the node to change packet forwarding from one next hop to the other in under a second if a 4pGE card, a link, or an adjacent router fails.

In UA-IP, PT-IP or PT-AAL2 solutions, provision IP networking under a Multiservice Switch 15000 Virtual Router component. For the specific values to provision for the Virtual Router component in UA-IP see:

- NN10225-512, *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2*
- NN10600-800, *Nortel Multiservice Switch 7400/15000/20000 IP Technology Fundamentals*
- NN10600-801, *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Data collection system

The data collected from each node by the data collection system (DCS) is information that is generated for troubleshooting, performance tuning, and billing. After the DCS collects alarms, logs, state change notifications (SCNs), and real-time statistics from nodes, it can either send the data to an external network management system for analysis or spool the data to the file system (for example, accounting data). In some cases, such as alarms data, the DCS will both spool and send data off-switch.

The DCS on Nortel Multiservice Switch 15000 nodes is controlled through the *Collector* component. For the specific values that need to be configured for the *Collector* component, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

For more information on the data collection system, see *NN10600-561 Nortel Multiservice Switch 7400/15000/20000 Data Management*.

LP feature configuration

The Software avList is intended to contain only those software applications that are supported. The software applications in the avList for the PT-AAL1/UA-AAL1 solutions include:

- base_XXX
- networking_XXX
- atmNetworking_XXX
- ip_XXX
- wanDte_XXX (for in-band OAM only)

The *wanDte* option depends on whether in-band OAM using AtmMpe is configured or not. If in-band OAM is configured, then *wanDte* needs to be configured as well.

Note 1: Do not include a fabric application version (AV) in the Software avList. The fabric AV is not required in the avList.

Note 2: Some Multiservice Switch (MSS) features and configurations may not be supported on Media Gateway 7480/15000/20000. Please contact your Nortel account representative to determine whether a specific base MSS feature is supported on your Media Gateway 7480/15000/20000 platform.

The software applications in the avList for the PT-AAL2 solution include:

- base_XX

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- networking_XX
- atmNetworking_XX
- ip_XX
- wanDte_XX
- pvg_XX
- patch_XX

The software applications in the avList for the UA-IP solution include:

- base_XXX
- networking_XXX
- atmNetworking_XXX
- ip_XXX
- wanDte_XXX
- ethernet_XXX
- pvg_XXX
- aal1Ces_XXX (Required only if VSP3 and 4pOC3TDM cards are to be configured)
- rex_XXX (if MG15000 periodic routine exercise (REX) is used)

The software applications in the avList for the PT-IP solution include:

- base_XXX
- networking_XXX
- atmNetworking_XXX
- ip_XXX
- wanDte_XXX
- ethernet_XXX
- pvg_XXX
- rex_XXX (if MG15000 periodic routine exercise (REX) is used)

Shelf/Module data

Usually, a Nortel Multiservice Switch 15000 shelf name should contain the Common Location Language Identifier (CLLI). CLLI is an industry-standard alphanumeric string to identify equipment location. The CLLI is, at most, 11 characters long. When the CLLI does not uniquely identify a single shelf instance, a twelfth character should be added to the CLLI from the valid character set to make the string unique.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Network clock synchronization

Network clock synchronization (NCS) ensures the accurate transmission and reproduction of synchronous data. NCS is used to synchronize the clocking of multiple ports and nodes by synchronizing to the signal originating from a single internal source or to a source external to the network.

For structured services, the transmit and receive interfaces must be timed from a single, common clock. With structured services, NCS forces the terminating equipment to transmit and receive at the same frequency.

Network clock synchronization is set through the configuration of the *NetworkSynchronization* component. For the specific values that need to be configured for the *NetworkSynchronization* components, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

> ***Note:*** NCS is responsible for clocking on synchronous data links but not with synchronizing the time of day. Network Time Synchronization (NTS) synchronizes the time of day on Nortel MDM workstations and Nortel Multiservice Switch 15000 nodes. For more information on NTS, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

OAM connectivity

This section discusses the OAM management topologies, for Nortel MDM and Nortel Multiservice Switch 15000 MSS/MG15000, in a PT-AAL1, UA-AAL1, UA-IP or PT-IP solution. There are two types of OAM management topologies: out-of-band OAM and in-band OAM.

An out-of-band topology is generally regarded as the typical management topology. Out-of-band management uses dedicated interfaces for management connectivity access via CP Ethernet links.

Out-of-band OAM connectivity

Connectivity can be established through a Communications Server LAN (CS LAN).

The CS LAN links are through the Ethernet ports on each Control Processor card in the Multiservice Switch 15000 shelf. The standard initial commissioning procedures configure out-of-band OAM connectivity, using Startup. Once connectivity is established to a MDM workstation, apply the nodal provisioning (NP) template PT-AAL1 *CPeD_Commissioning,*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

WUA-AAL1 CPeD_Commissioning, UA-IP SH-CPED, or UA-IP SH-CPED-PVGnoARTG, or PT-AAL2 SH-CPED. These templates modify the Ethernet port configuration according to the recommended parameters.

In-band OAM connectivity

An in-band management topology has Nortel Multiservice Switch 15000 nodes acting as gateways for remote nodes to send or receive OAM data.

For information on the supported in-band OAM topology and for definitions of terms, such as gateway node, used to describe in-band OAM configurations, see *NN10028-111 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

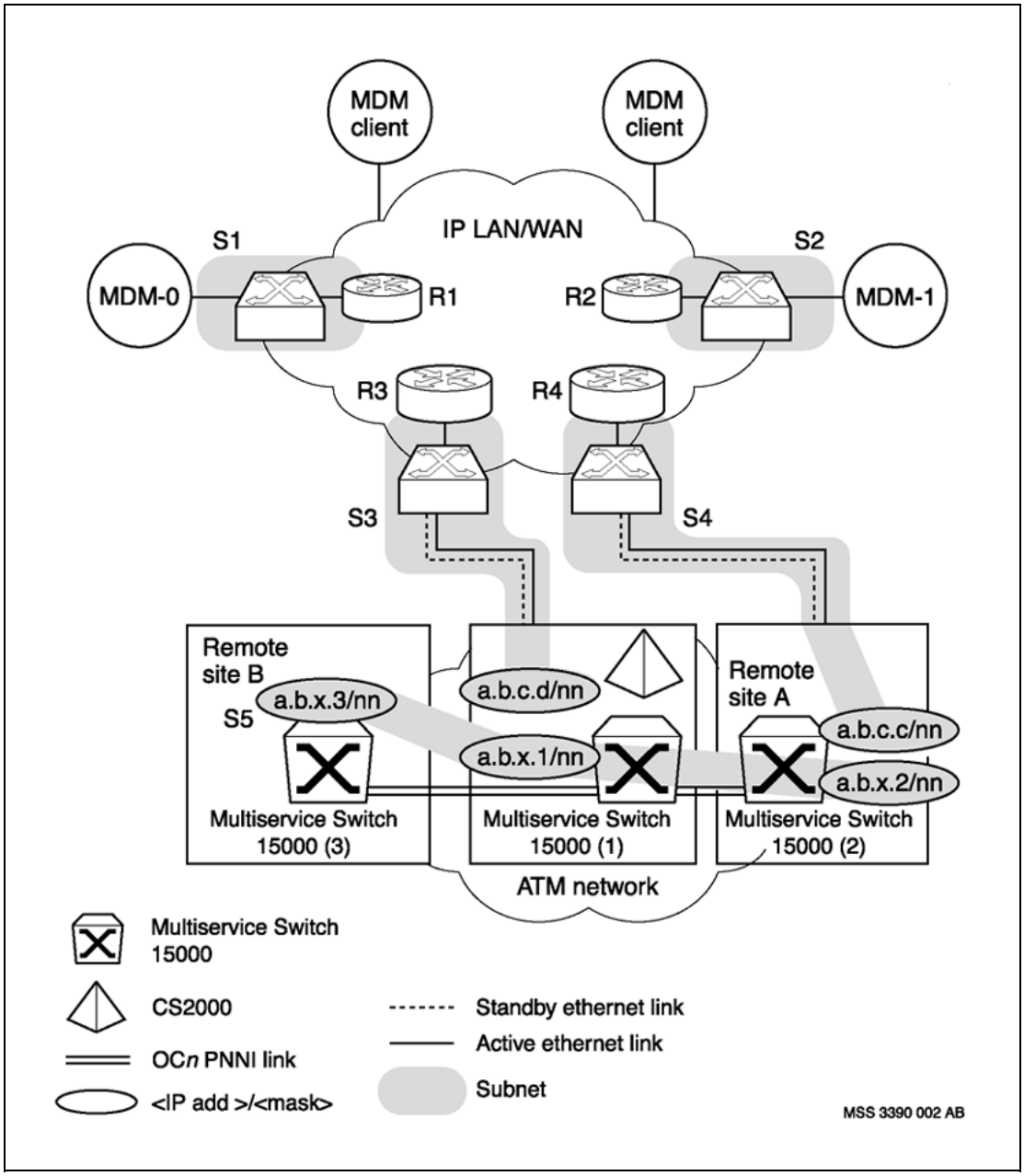
"A sample in-band OAM configuration" (page 21) illustrates a typical in-band OAM configuration. Multiservice Switch 15000 nodes are numbered 1, 2, and 3. Multiservice Switch 15000 node1 and 2 identify Gateway nodes. Multiservice Switch 15000 3 identifies a Remote node.

S1, S2, S3, S4 and S5 identify IP subnets. For each node there are two diverse static routes configured. For example, in the diagram, Multiservice Switch 15000 1, which is a Gateway node has the following diverse routes to MDM-0 and MDM-1: a.b.c.d/nn and a.b.c.c/nn. In the diagram, Multiservice Switch 15000 3, which is a Remote node, has the diverse routes to MDM-0 and MDM-1 through a.b.x.1./nn and a.b.x.2/nn.

In the diagram, node/routers are identified as R1 and R2.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

A sample in-band OAM configuration



The remote Multiservice Switch 15000 nodes are managed by way of in-band connectivity to each other and to the gateways.

Note: Where multiple gateways exist for redundancy, one gateway can appear as a remote to another.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

In-band connectivity uses ATMMPE (ATM Multi-Protocol Encapsulation) to encapsulate the OAM IP traffic over PNNI trunks. ATMMPE can be configured on the following cards, except where otherwise noted:

- 16pOC3SmIrAtm (PT-AAL1 and UA-AAL1 only)
- 4pOC3SmIrAtm
- 4pOC12SmIrAtm
- 12pDS3Atm (UA-AAL1 only)

Within the ATMMPE subnet, a Gateway node must have a direct ATMMPE ATM (PVC) link to every other node, including the other Gateway node.

The customer-owned IP LAN/WAN must be configured with dynamic routing. Each MDM server must have a diverse path (when compared to the other server) through the IP LAN/WAN to the nodes. The routers connected to the Gateway node (identified in the diagram as R3 and R4) must each have a static route to the underlying ATMMPE subnet.

The dynamic routing protocol must be configured within the IP LAN/WAN such that it routes around any single failure of equipment or facilities within the domain.

Note: In-band connectivity is only supported over the ATM inter-shelf links. It is not supported over Gigabit Ethernet (GE) links.

Hitless activation of critical attributes

Hitless activation of critical attributes is supported in the UA-AAL1, PT-AAL1, PT-AAL2, UA-IP, and PT-IP solutions.

When HCA is enabled, a semantic check verifies if the conditions for a hitless activation have been met. If the conditions are not met, the semantic check fails. For activation of attributes supporting HCA, the operator must modify the set of changes so that the semantic checks pass. Then, assuming that operationally, the spared components are all available, activation of those attributes proceeds in a hitless fashion.

For those critical attribute changes which caused the HCA conditions to fail, those can be activated separately, with the associated outage, by disabling the HCA checks. Upon activation, the outage occurs and an alarm is generated, to warn the operator to re-enable the checks after the current activation sequence.

Operators must check the operational state of the nodes before using HCA activation. The following conditions must be met before the HCA activation will proceed:

- the MSS/MG type is 15000

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- the Prov ActivationMode component is provisioned and the Prov ActivationMode hitlessActivation attribute is set to enabled
- there is no mix of critical and non-critical attributes
- each of the critical attributes being changed supports HCA activation
- provisioning changes do not cause CP reset (changes only impact FPs)
- all the FPs on which the CAs are changed must be either 1:1 or 1+1 sparing and must support equipment protection
- no LPs are added or deleted
- no LP-card mapping changes
- no Shelf Card types are changed
- no Software LogicalProcessorType (LPT) changes

Any number of critical attributes can be changed within a single provisioning session as long as all the conditions are satisfied.

The HCA activation on nodes with equipment protection (EP) enabled, impacts the FPs where the CAs reside. It incrementally changes the CA provisioning on cards in 1:1 and 1+1 FP sparing configuration. Standby cards are reset first followed by a controlled switchover, after which the previously active cards are reset.

If you have provisioned and enabled Prov ActivationMode, (see the *NN10070-461 Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1* or *NN10419-461 Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks* for information on how to provision), and you want to make additional provisioning changes to CAs, you must disable HCA before making the provisioning changes.

> ***Note:*** If HCA activation is disabled, operators may make provisioning changes to critical attributes that may result in service outages when the critical attribute is activated.

See the procedures:

- "Enabling hitless activation mode" (page 24)
- "Making changes after HCA activation has been enabled" (page 24)

If a problem occurs during HCA, the activation pauses and displays a warning message. An operator can stop or continue the activation. See "Halting HCA activation" (page 26).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Enabling hitless activation mode

Prerequisites:

- HCA is provisioned

The following steps describes how to enable HCA activation. For instructions on how to make changes to CAs after HCA activation has been enabled, see "Making changes after HCA activation has been enabled" (page 24).

Enable the Hitless Activation Mode by performing the following steps.

Procedure steps

Step	Action
1	Log in with the appropriate permissions.
2	Enter provisioning mode so that you can issue the appropriate commands. `start prov`
3	Enable the ActivationMode component. `set Prov ActivationMode hitlessActivation enabled`
4	Perform a semantic check. `check prov`

5	Activate, confirm and commit the change.
	`activate prov`
	`confirm prov`
	`save prov`
	`commit prov`

—End—

Making changes after HCA activation has been enabled

Procedure steps

Step	Action
1	Log in with the appropriate permissions.
2	Enter provisioning mode so that you can issue the appropriate commands. `start prov`

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

3 Set the critical attributes.

set <critical attribute>

For example: apply a template.

4 Disable the ActivationMode component.

set Prov ActivationMode hitlessActivation disabled

5 Perform a semantic check.

check prov

The following shows sample output for this command.

```
ch pr
Lp/3
   Warning:
      Reason:  Lp/3 will be reset due to modifications
to the Lp/3 Eng Arc Ov component
Prov
   Warning:
    Activation will disrupt service for the following
component(s):
      Lp/3
ok              2005-06-16 10:48:50.10
```

6 Activate the change.

activate prov

```
act pr
    Prov Am; 2005-06-16 10:48:51.75
SET warning operator configurationError
70000043
    ADMIN: unlocked      OPER: enabled       USAGE: busy
    AVAIL:               PROC: initializing  CNTRL:
    ALARM:               STBY: notSet        UNKNW: false
    Id: 24        Rel: Lp/0
    Com: Prov Am hitlessActivation is disabled
    Int: 0/0/2/12008; casAlarm.cc; 1697; CG0108E

   You have 20 minutes in which to confirm activation.
```

7 Confirm the change.

confirm prov

Do not commit the change until you have ensured the operational condition has been cleared.

The following shows sample output for this command.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
conf pr
    Prov; 2005-06-16 10:48:59.16
CLR cleared operator operationalCondition                          70000007
    ADMIN: unlocked      OPER: enabled       USAGE: busy
    AVAIL:               PROC: initializing  CNTRL:
    ALARM:               STBY: notSet        UNKNW: false
    Id: 29        Rel: Lp/0
    Com: Activation confirmed. Rollback will not occur.
    Int: 0/1/2/11601; casAlarm.cc; 786; CG0108E
```

8 Enter the following command.

```
set Prov ActivationMode hitlessActivation enabled
```

9 Perform a semantic check.

```
check prov
```

The following shows sample output for this command.

```
Prov
   Upon activation a non-service disruptive activation will
occur.
ok              2005-06-16 10:49:08.40
```

10 Activate, confirm and commit the change.

```
activate prov
```

```
confirm prov
```

```
save prov
```

```
commit prov
```

—End—

Halting HCA activation

If a problem occurs on the standby FPs that are provisioned with the new critical attribute changes, an operator can stop the changes or continue the activation. If there is a problem, the activation pauses before proceeding with the next stage (controlled switchover). The following warning appears:

```
The Hitless Critical Activation is paused, pause reason:
<reason>
To resume, type Continue Prov.  To stop, type Stop Prov.
```

To start or stop the HCA activation, perform the following steps.

Procedure steps

Step	Action
1	Log in with the appropriate permissions.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2 Enter provisioning mode so that you can issue the appropriate commands.

```
start prov
```

3 Stop the activation.

```
stop prov
```

Note 1: Operators can stop HCA activation at any time if they are not expecting any impact to connections and they want to stop the HCA activation.

Note 2: If one or more connections cannot be created on the standby card (see following alarm) then it will take up to 10 minutes for the activation to pause.

```
Shelf Card/14 SpServ; 2005-05-25 11:50:18.68
MSG warning processing underlyingResourceUnavail 70120300
    ADMIN: unlocked      OPER: enabled USAGE: active
    AVAIL: degraded      PROC: CNTRL:
    ALARM:               STBY: hotStandby UNKNW: false
    Id: 74 Rel:
Com: AtmIf/1400 Uni; 2005-05-25 11:50:18.67
     SET minor processing underlyingResourceUnavail 70410600
     Id: 0E000001 Rel: LpP/14.15
     Int: 14/1/2/19401; jnPdus.cc; 435; CG0108E
     OrigCom: Cannot create one or more switched connections on standby.

Int: 0/1/2/2284; pcsSparedServ.cc; 499; CG0108E
```

—End—

Internode Emergency Stand Alone (ESA) for MG9000

InterNode ESA is supported in both the UA-AAL1 and UA-IP solutions and can support a maximum of 15 MG9000 nodes. MG9000 internode ESA uses the MSS15000's flat VR with static routing (RFC 1483 AtmMpe) to route ESA signaling between MG9000s in an ESA group. A new ATM connection is setup specifically to support ESA mode. In ESA mode each MG9000 has a separate IP address that is dedicated to the ESA function.

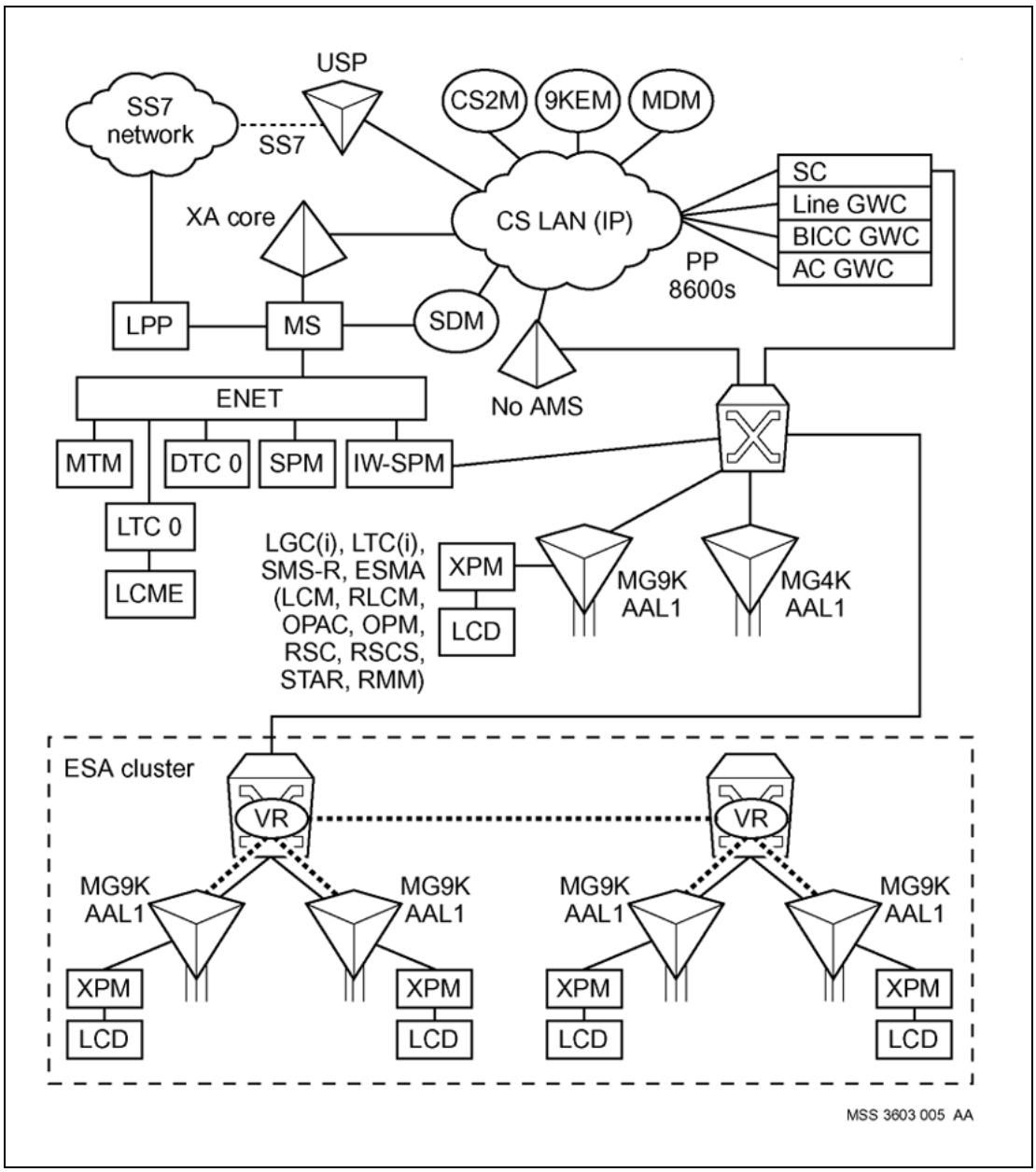
To support MG9000 internode ESA, you must provision the attributes described in the following tables of the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*:

- "LP feature configuration (PT-AAL1/UA-AAL1) with internode ESA"
- "Vr for bearer and control traffic with internode ESA"

Copyright © 2006, Nortel Networks Nortel Networks Confidential

"Typical deployment for Internode ESA" (page 28) shows a typical deployment scenario for this feature in a collapsed office (remote) that consists of a single Multiservice Switch 15000 which connects a group of MG9000 gateways to a set of PNNI links to the CS2000 site. If necessary, the collapsed office can use several Multiservice Switch 15000 switches.

Typical deployment for Internode ESA



See "Internode Emergency Stand Alone for MG9000" (page 60) for more information.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Time of day

The accurate tracking of time, both in the network and on each Nortel Multiservice Switch 15000 node, is essential for the proper functioning of performance data collection, accounting records, and other functions. There are three types of time to consider when configuring the time of day on Multiservice Switch 15000 nodes:

- Reference time is the date and time that is the official reference around the world. The universally accepted reference time is Coordinated Universal Time (UTC).
- Network time is the date and time to which all nodes in the network synchronize internally.
- Module time is the time on a particular node.

The time of day on a node is set through the *Time* component. For the specific values that need to be configured for the *Time* component, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Note: For a procedure for adjusting the time of day following the seasonal time change when switching between Standard and Daylight Saving Time, see Appendix "Time-of-day updates for seasonal time changes" (page 269).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Overview of Multiservice Switch 15000 function processor configuration

This chapter discusses function processors for the Nortel Multiservice Switch 15000 nodes for the following solutions:

- Packet Trunking - AAL1
- Universal Access - AAL1
- Universal Access - IP
- Packet Trunking - AAL2

Function processors (FPs) provide interface ports that connect network communication facilities to Multiservice Switch nodes. FPs support and execute real-time processes that enable service delivery.

There are several types of FPs and the software running on an FP determines the function of the FP.

Nortel recommends that you configure each FP with as diverse a mix of component interfaces as possible. Configure a mix of links to all the network components. In addition, distribute the links to each of the different components across as many FP card pairs as possible. A wide distribution of links prevents an FP failure from adversely affecting any component connections. For more information about how to configure links, see "Overview of Multiservice Switch 15000 interface configuration" (page 37).

For more information about link distribution and the ports to cable these links on, refer to your network plan.

This chapter includes the following topics:

- "Multiservice Switch 15000 function processor configuration (PT-AAL1 and UA-AAL1)" (page 32)
- "Media Gateway 15000 function processor configuration (PT-AAL2)" (page 33)
- "Multiservice Switch 15000/Media Gateway 15000 function processor configuration (UA-IP)" (page 33)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Multiservice Switch 15000/Media Gateway 15000 function processor configuration (PT-IP)" (page 35)
- "Task list for Multiservice Switch 15000 function processor configuration" (page 35)

Multiservice Switch 15000 function processor configuration (PT-AAL1 and UA-AAL1)

For both the Packet Trunking - AAL1 and Universal Access - AAL1 solution configurations, Nortel Multiservice Switch 15000 FPs are installed in 1+1 protected pairs. This means that you can install up to seven FP pairs on each shelf. A single Multiservice Switch 15000 shelf supports up to 112 1+1 APS protected OC-3 ATM ports, or an equivalent mix.

In the Universal Access - AAL1 solution, some FPs, such as the 12-port DS3 ATM FP, may provide multi-service data applications including DSL and are supported using single, unprotected FPs.

When installing FPs choose from the following:

- 4-port OC-3c card (single mode), to install any of the connections to the other components

  Note: Use this FP only if you require eight or fewer ports for access or trunking. If you need more than eight, use a 16-port OC-3 card

- 16-port OC-3 card, with LC connectors, to install any of the connections to the other components
- 4-port OC-12 card, to install interfaces between Multiservice Switch 15000 nodes or links to other ATM nodes

  Note: Only 4-port OC-12c/STM-4 FP, NTHW86 can be deployed.

- 12-port DS3 ATM card, supports DS3 Multiservice Switch ATM-to-Multiservice Switch ATM on 1:1 protected cards, or in unspared configurations for unprotected ATM services such as DSL, also supports a DS3 ATM interface to an MG9000
- 4-port DS3Ch Atm card, supports hot standby equipment protection and software migration for ATM services running over IMA in one-for-one equipment protected scenarios

To configure the FPs listed above, use the Nodal Provisioning tool and the following templates:

- *PT-AAL1/WUA-AAL1 FP-4pOC3SmIrAtm*
- *PT-AAL1/WUA-AAL1 FP-16pOC3SmIrAtm*
- *PT-AAL1/WUA-AAL1 FP-4pOC12SmIrAtm*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- *WUA-AAL1 FP-12pDS3Atm*
- *WUA-AAL1 FP-4pDS3ChAtm*

Media Gateway 15000 function processor configuration (PT-AAL2)

The following Media Gateway 15000 FPs are supported for the PT-AAL2 solution configuration:

- 4pOC12 SmIrAtm FP (NTHW86), installed as a pair of 1:1-protected 4pOC12ATM FPs
- 4pOC3SmIrAtm FP (NTHW15), unprotected 4pOC3ATM FP
- 2pOC3ChSmIrVsp3-o FP (NTHW77), installed as a pair of protected 2pOC3ChSmIrVsp3 (VSP3-o) FPs

To configure the FPs listed above, use the Nodal Provisioning tool and the following templates:

- PT-AAL2 FP-4pOC12SmIrAtm
- PT-AAL2 FP-4pOC3SmIrAtm_Unprotected
- PT-AAL2 FP-2pOC3ChSmIrVsp3-o

For information about using the Nodal Provisioning templates, refer to *241-6001-023 Nortel Multiservice Data Manager Configuration Management Tools*.

Multiservice Switch 15000/Media Gateway 15000 function processor configuration (UA-IP)

For the Universal Access - IP solution configuration, Nortel Multiservice Switch 15000 FPs are installed in 1+1 protected pairs.

A UA-IP solution supports the following FPs for Nortel Multiservice Switch 15000 nodes:

- a 4-port OC-12 FP card, for Multiservice Switch IP over ATM inter-shelf trunk interfaces, links to Communications Server LAN (CS LAN) or to other switches and routers
- a 4-port OC-3 FP card, for Multiservice Switch IP over ATM inter-shelf trunk interfaces, optical hairpins, and MG9000 interfaces
- a 12-port DS3 ATM FP card, used for Multiservice Switch 15000 nodes to MG9000 links, using DS3
- a 4-port DS3 Channelized ATM FP card, supports hot standby equipment protection and software migration for ATM services using the Multiservice Switch inverse multiplexing over ATM (IMA) feature, in one-for-one equipment protected scenarios. This is used for MG9000 links.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- a 4-port GE card, used for Gigabit Ethernet (GE) connection to a Communications Server LAN (CS LAN), or to other routers.
- a 4-port OC- 3 Channelized Single-mode (Sm) Intermediate reach (Ir) FP card (TDM), used for media gateway 15000 (MG15000) to time-division multiplexing (TDM) equipment links.
- a 2-port GE Multimode Short reach (Sr) VSP3 FP card, used to connect a Multiservice Switch 15000 node to a Media Gateway controller card using H.248. H.248 is the ITU-T gateway protocol.

  Note: A carrier-grade configuration does not use the GE ports. Therefore, no template is needed for these ports.

- a 2-port OC- 3 Channelized Single-mode (Sm) Intermediate reach (Ir) VSP3-o FP card, to connect a Multiservice Switch node to a Media Gateway controller card, using H.248. H.248 is the ITU-T gateway protocol.
- a 2-port OC- 3 Channelized Single-mode (Sm) Intermediate reach (Ir) VSP4e FP card, to connect a Multiservice Switch node to a Media Gateway controller card, using H.248. H.248 is the ITU-T gateway protocol.

To configure the FP cards listed above, use the Nodal Provisioning tool and the FP templates provided for a UA-IP solution. The pair of FPs must be in non-configured even/odd adjacent slots. After you apply the template, you can configure any of the interfaces on the FP card.

UA-IP supports the following FP templates for Multiservice Switch 15000 nodes:

- *UA-IP FP-4pOC12SmIrAtm*
- *UA-IP FP-4pOC3SmIrAtm*
- *UA-IP FP-12pDS3Atm*
- *UA-IP FP-4pDS3ChAtm*
- *UA-IP FP-4pGE*
- *UA-IP FP-4pOC3ChSmIr-TDM*
- *UA-IP FP-2pGeMmSrVsp3*
- *UA-IP FP-2pOC3ChSmIrVsp3-o*
- *UA-IP FP-2pOC3ChSmIrVsp4e*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Multiservice Switch 15000/Media Gateway 15000 function processor configuration (PT-IP)

For the Packet Trunking - IP solution configuration, Media Gateway 15000 FPs are installed in 1+1 protected pairs.

A PT-IP solution supports the following FPs for Media Gateway 15000 nodes:

- a 4-port GE card, used for Gigabit Ethernet (GE) connection to a Communications Server LAN (CS LAN), or to other routers for the packet side.
- a 2-port OC- 3 Channelized Single-mode (Sm) Intermediate reach (Ir) VSP3-o FP card, to connect a Multiservice Switch node to a Media Gateway controller card, using H.248. H.248 is the ITU-T gateway protocol.
- a 2-port OC- 3 Channelized Single-mode (Sm) Intermediate reach (Ir) VSP4e FP card, to connect a Multiservice Switch node to a Media Gateway controller card, using H.248. H.248 is the ITU-T gateway protocol.

To configure the FP cards listed above, use the Nodal Provisioning tool and the FP templates provided for a PT-IP solution. The pair of FPs must be in non-configured even/odd adjacent slots. After you apply the template, you can configure any of the interfaces on the FP card.

PT-IP supports the following FP templates for Media Gateway 15000 nodes:

- *PT-IP FP-4pGE*
- *PT-IP FP-2pOC3ChSmIrVsp3-o*
- *PT-IP FP-2pOC3ChSmIrVsp4e*

Task list for Multiservice Switch 15000 function processor configuration

To configure a function processor (FP) in Nortel Multiservice Switch 15000 nodes, configure the following:

- the physical ports on each FP pair.
- the ports on the FP pair to set the clocking source.
- any customer-defined configuration for each port, if necessary.
- the engineering and control parameters for each FP pair.
- the ATM resource control connection and buffer space for each FP pair.
- the frame (IP) resource control for each FP pair.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For more information on configuring FPs, see *NN10600-551 Nortel Multiservice Switch 7400/15000/20000 FP Configuration Reference*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Overview of Multiservice Switch 15000 interface configuration

This section provides an overview of Nortel Multiservice Switch 15000 interface configuration for the following solutions.

- Packet Trunking - AAL1
- Universal Access - AAL1
- Universal Access - IP
- Packet Trunking - AAL2
- Packet Trunking - IP

These interfaces are installed following initial installation of the node.

This section is meant to be used with the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. The *Attribute Summary* manual contains tables of all the specific values to use for configuring Multiservice Switch 15000 nodes.

All of the descriptions of configured interfaces in this section contain cross-references to the corresponding section in the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

This section contains the following topics:

- "Overview of interface configuration between network components (PT-AAL1/UA-AAL1)" (page 38)
- "Overview of interface configuration between network components (PT-AAL2)" (page 41)
- "Overview of interface configuration between network components (UA-IP)" (page 43)
- "Link distribution (PT-AAL1 and UA-AAL1)" (page 50)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Link Distribution (PT-AAL2)" (page 64)
- "Link distribution (UA-IP)" (page 65)
- "TDM trunk distribution (UA-IP)" (page 74)

Overview of interface configuration between network components (PT-AAL1/UA-AAL1)

This section gives an overview of interface configuration between Nortel Multiservice Switch 15000 nodes and other network components in a PT-AAL1 or UA-AAL1 solution.

VoA applications

Nortel Multiservice Switch 15000 nodes provide the core packet connectivity layer for Voice over ATM (VoA) applications. VoA includes the PT-AAL1 and UA-AAL1 solutions. In addition to the VoA application, the Core Packet Network provides connectivity for a variety of Next Generation Network services including voice, multi-media and data.

User administration for centralized authentication and authorization in a VoA network is also available with the deployment of MDM Admin Servers and the Operator Client application. See "Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client applicatio" (page 125) for more information.

The principal UA-AAL1 first office application is the Class 5 end office replacement program. This program is the first step towards evolving to a multiservice end-office built upon a distributed ATM network.

Available component interfaces

Nortel recommends that you configure each function processor (FP) with as diverse a mix of component interfaces as possible.

- For both PT-AAL1 and UA-AAL1 solutions, configure a mix of interfaces to the Communication Server 2000 (CS2000), Interworking Spectrum Peripheral Module (IW-SPM), and Multiservice Gateway 4000 (MG4000), as well as to other ATM network components, for example Multiservice Switch 15000 nodes.
- For a PT-AAL1 solution, also configure interfaces to the DPT-SPM component, if required.
- For a UA-AAL1 solution, also configure interfaces to the digital subscriber line (DSL), Media Gateway 9000 (MG9000), SAM21 SC, Universal Audio Server (UAS) components, and TDM core.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

In addition, distribute the interfaces to each of the different components across as many FP card pairs as possible. A wide distribution of these interfaces can reduce the impact of a catastrophic dual FP failure, and prevent it from adversely affecting any component connections. For more information on distributing interfaces and the ports on which to cable these interfaces, refer to your network plan.

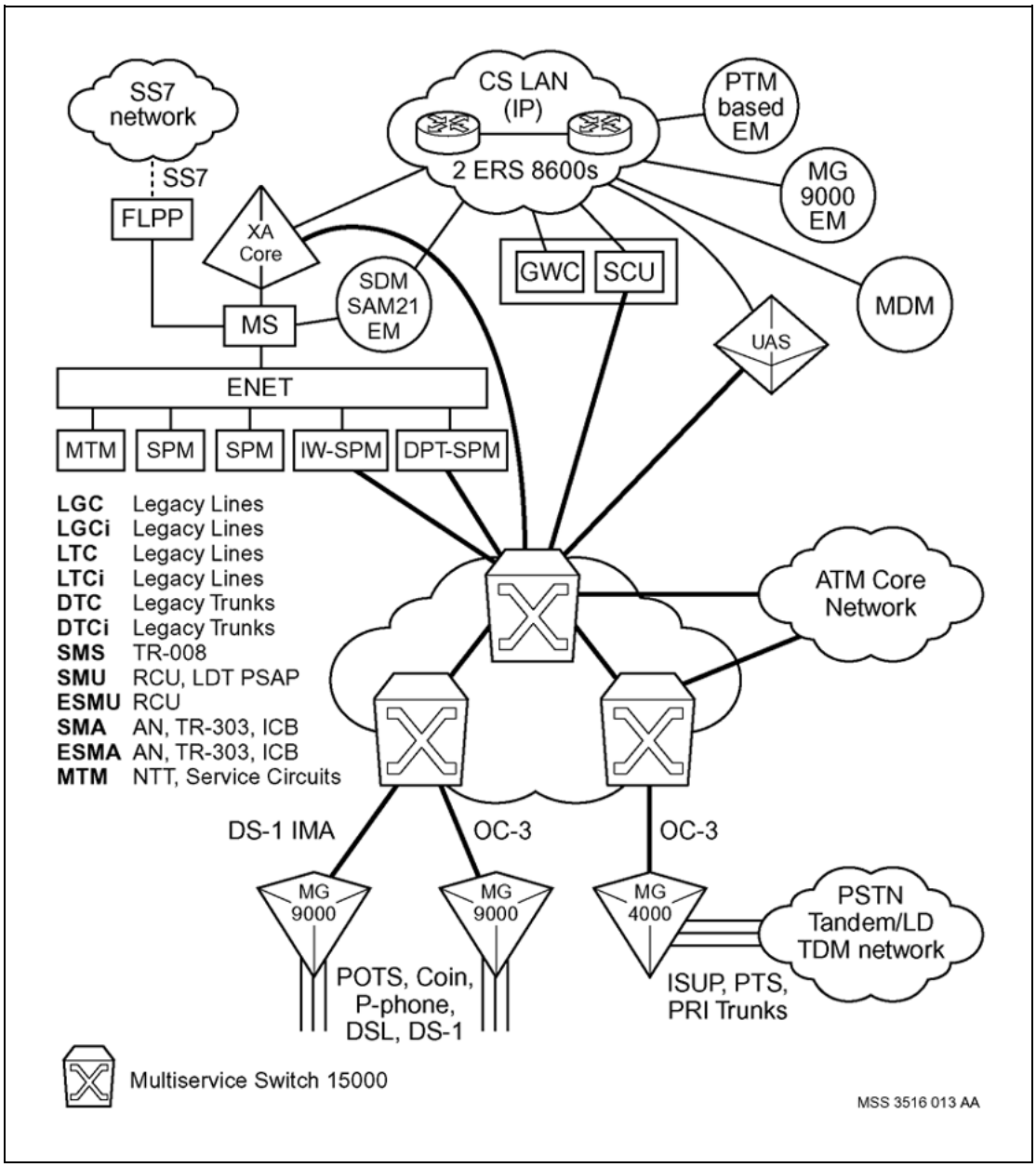
Architecture example for Universal Access - AAL1 (UA-AAL1)

The UA-AAL1 solution is a voice over ATM network solution that is equivalent to the DMS-100/500 switch. The solution provides End Office voice services using AAL1 for voice transmission. It is a hybrid solution that supports interworking with legacy ENET-based line and trunk services and peripherals. In addition to voice services, the UA-AAL1 solution provides DSL and DS-1 based private line services through the line gateway, using the ATM network for transport.

See "Class 5 end office (UA-AAL1 solution)" (page 40) for an example of the architecture for a UA-AAL1 solution.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

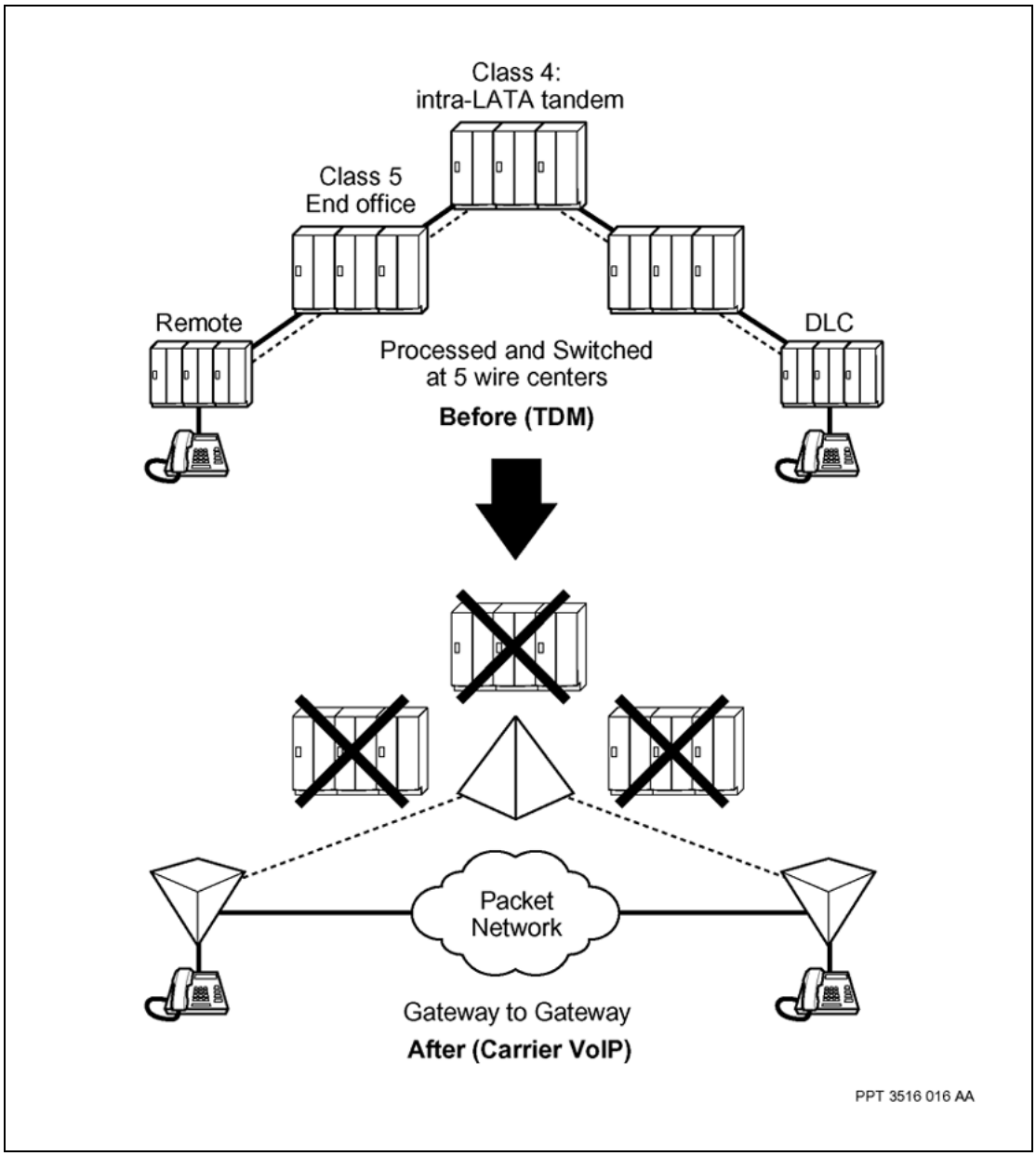
Class 5 end office (UA-AAL1 solution)



For an illustration of the evolution of a time division multiplexing (TDM) based network of class 5 and class 4 switches into a consolidated, distributed UA-AAL1 office, see "UA-AAL1 solution office architecture" (page 41).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

UA-AAL1 solution office architecture



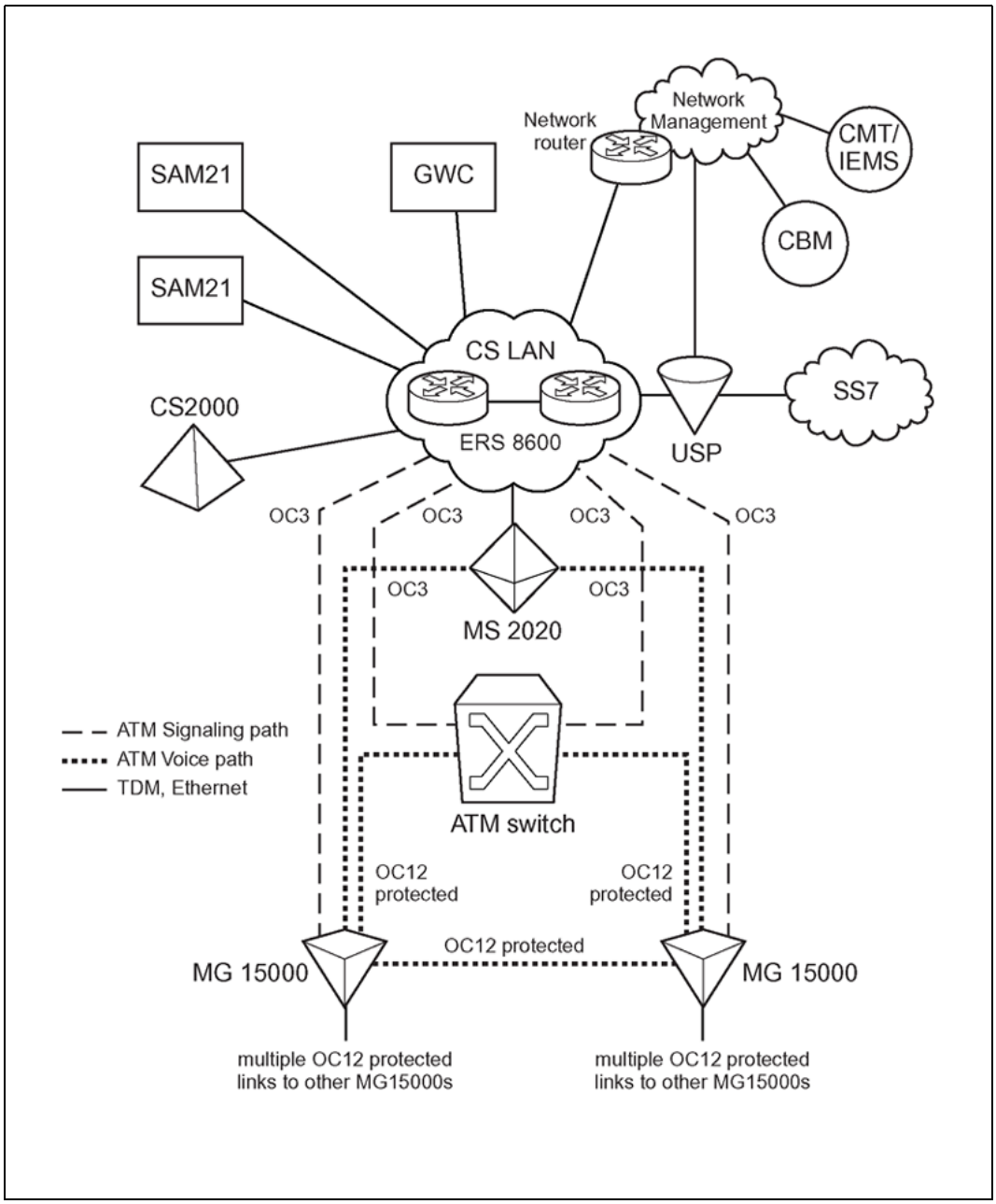
Overview of interface configuration between network components (PT-AAL2)

This section gives an overview of interface configuration between Media Gateway 15000 nodes and other network components in a PT-AAL2 solution. Media Gateway 15000 nodes are used as TDM-Packet network gateway switches. The Nortel International PT-AAL2 Wireless Solution provides a transit switching and call processing node in the network which

Copyright © 2006, Nortel Networks Nortel Networks Confidential

provides for the management of trunk connections to other offices, as well as, network-based services on those trunk connections. See "PT-AAL2 solution overview" (page 42).

PT-AAL2 solution overview



Standard configurations are defined for Multiservice Switch 15000 and Media Gateway 15000 equipment in the PT-AAL2 solution, and supported through nodal provisioning (NP) templates. NP templates simplify the initial commissioning in a PT-AAL2 solution and minimize

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

operator error in applying Multiservice Switch 15000 and Media Gateway 15000 equipment attributes. Refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* for more information.

Overview of interface configuration between network components (UA-IP)

This section gives an overview of interface configuration between Nortel Multiservice Switch 15000 nodes and other network components in a UA-IP solution.

VoIP applications

The UA-IP solution is a voice over IP (VoIP) network solution that is equivalent to the DMS-100/500 switch. It provides End-Office voice services using IP for voice transmission and signaling. It is both a greenfield and a hybrid solution. In the hybrid case, this solution supports interworking with legacy ENET-based line and trunk services and peripherals. In addition to voice services, the UA-IP solution provides DSL through the MG9000 line gateway.

Available component interfaces

For a UA-IP solution, configure interfaces to other Multiservice Switch nodes, to CS-LAN, and MG9000 components, as well as for optical hairpins.

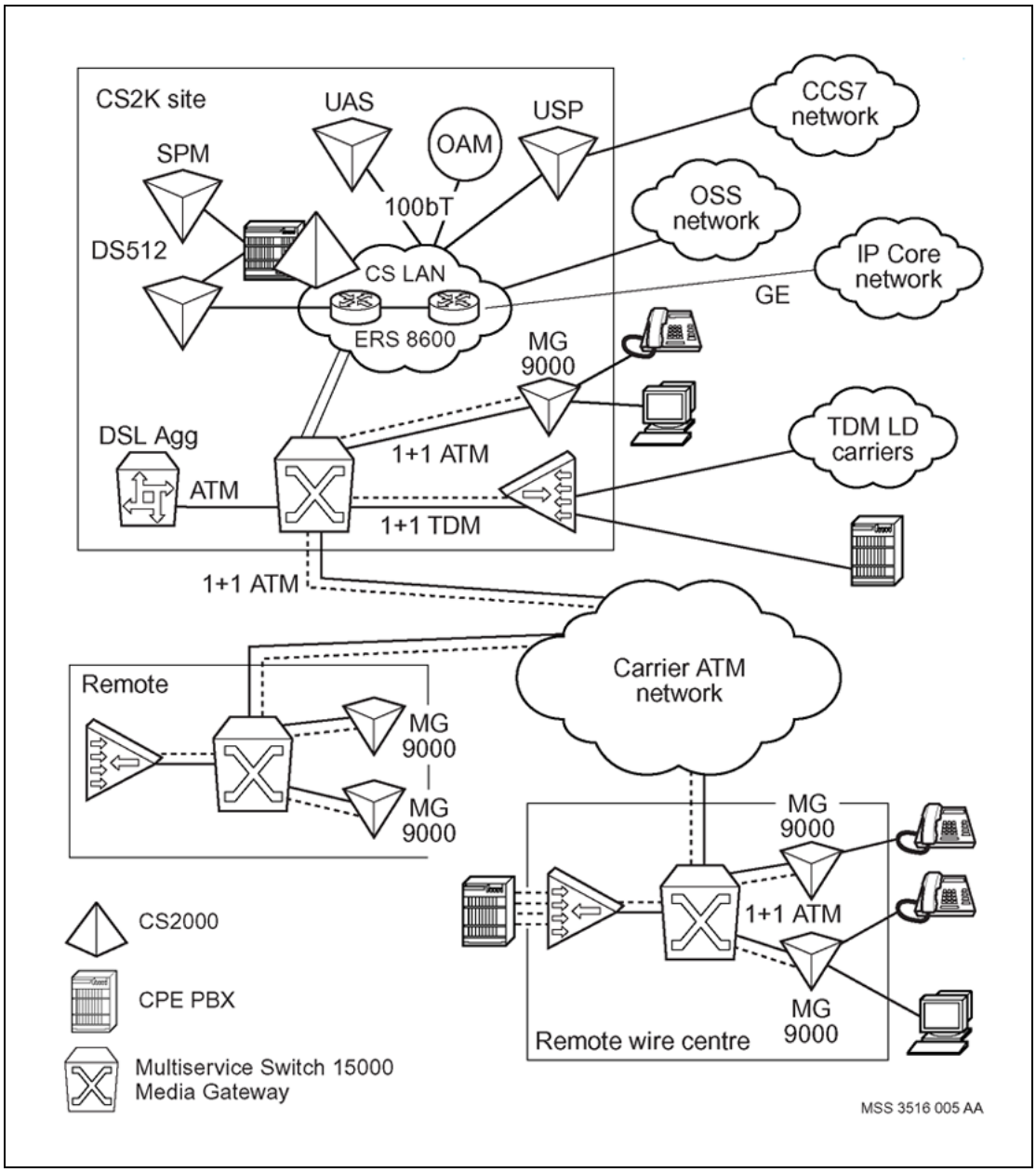
In addition, distribute the interfaces to each of the different components across as many FP card pairs as possible. A wide distribution of these interfaces can reduce the impact of a catastrophic dual FP failure, and prevent it from adversely affecting any component connections. For more information on distributing interfaces and the ports on which to cable these interfaces, refer to your network plan.

UA-IP architecture example

See "UA-IP architecture overview" (page 44) for an architecture overview of a UA-IP solution. In this model, a number of end-offices are replaced by remote Nortel Multiservice Switch 15000 nodes. These remote nodes aggregate IP traffic from a number of MG9000 line gateways and from primary rate interface (PRI) trunks from Media Gateway cards. Calls and signaling can go to other such offices that are also connected to either the IP Core network or the Carrier ATM Network

Copyright © 2006, Nortel Networks Nortel Networks Confidential

UA-IP architecture overview



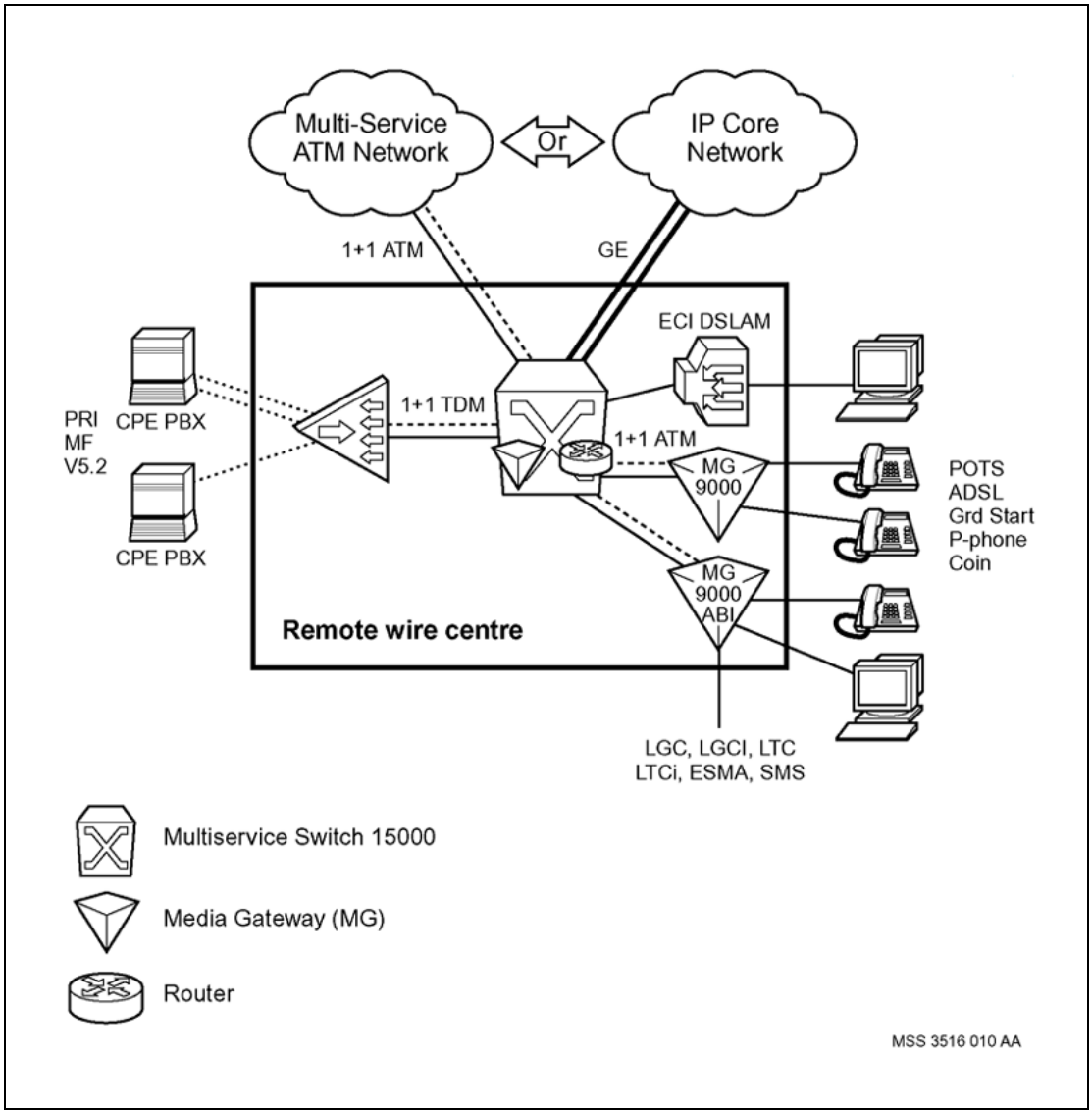
For an example of a configuration you can create using Multiservice Switch 15000 templates for Universal Access - IP, see "Remote wire centre (UA-IP)" (page 45) and "Example of remote wire centre and CS2000 site shelf configuration (UA-IP)" (page 46). This scenario is typical of a North American End-Office (EO) replacement configuration. Other configuration scenarios include:

- long-distance (LD) Tandem (in other words, a Class 4 office) replacement
- access Tandem replacement

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

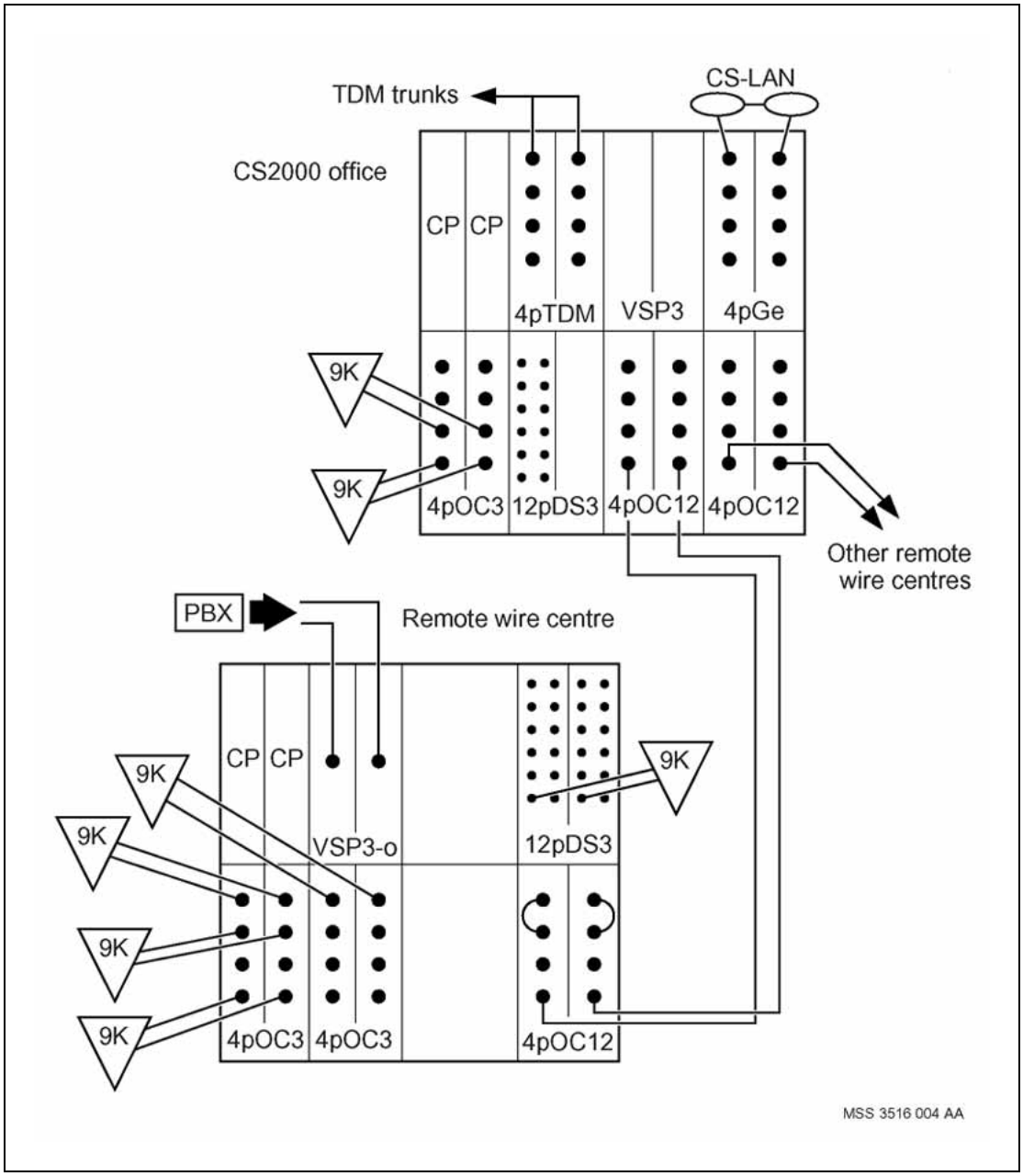
- Carrier-Hosted Services (CHS) with Multimedia Communications Server (MCS)

Remote wire centre (UA-IP)



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example of remote wire centre and CS2000 site shelf configuration (UA-IP)



Overview of interface configuration between network components (PT-IP)

This section gives an overview of interface configuration between Media Gateway 15000 nodes and other network components in a PT-IP solution. In the PT-IP solution, the MG15000 media gateway provides tandem trunking. There are Nodal Provisioning Templates (NP templates) available from the MDM for nodal provisioning that define one configuration for the MG15000 when deployed in a Carrier VoIP PT-IP solution.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

VoIP applications

The PT-IP solution is a voice over IP (VoIP) network solution that is a subset of the UA-IP solution. It provides End-Office voice services using IP for voice transmission and signaling. It is both a greenfield and a hybrid solution. In the hybrid case, this solution supports interworking with legacy ENETbased line and trunk services and peripherals. In a Packet Trunking Internet Protocol (PT-IP) solution, the Multiservice Data Manager (MDM) is the Element Management System (EMS) for the Media Gateway 15000 (MG15000) Network Element (NE). The templates are applicable for the following solutions:

- PMSC Wireless solution
- any vanilla-type use of MG15000 VoIP over GE in the PT-IP solution

As an IP “aggregation” router in the Carrier VoIP network the MG15000 is required to support the following services, according to the PT-IP Nodal Provisioning Templates PRD[1]:

- Cards: CP3, VSP3-o, 2pVSP4e, 4pGe, VSP4ea (phase 2), 2pVS (phase2)
- Carrier Grade - HSM, HEP, APS, and PDR hitless recovery from all single failures
- VIPR aggregation over GE, OC-3 ATM or OC-12 ATM
- Both local and remote subnet configurations (CD5694 [3])
- IP routing via PDR, static routes. Layer 2 and layer 3 local host only
- Trunks: ISUP, PRI and PTS (MF, etc....)
- G.711, G.726, G.729, EVRC, TrFO and RTO
- Out-of-band management using the CP OamEnet ports
- IP DiffServ - for traffic (datapath congestion) management
- Basic OAM security
- Enhanced H.248 signaling security
- REX
- HCA

Available component interfaces

For a PT-IP solution, configure the Media Gateway 15000 interfaces to Multiservice Switch nodes, to CS-LAN, and MGC components.

> ***Note:*** Distribute the interfaces to each of the different components across as many FP card pairs as possible. A wide distribution of these interfaces can reduce the impact of a catastrophic dual FP failure, and prevent it from adversely affecting any component connections. For

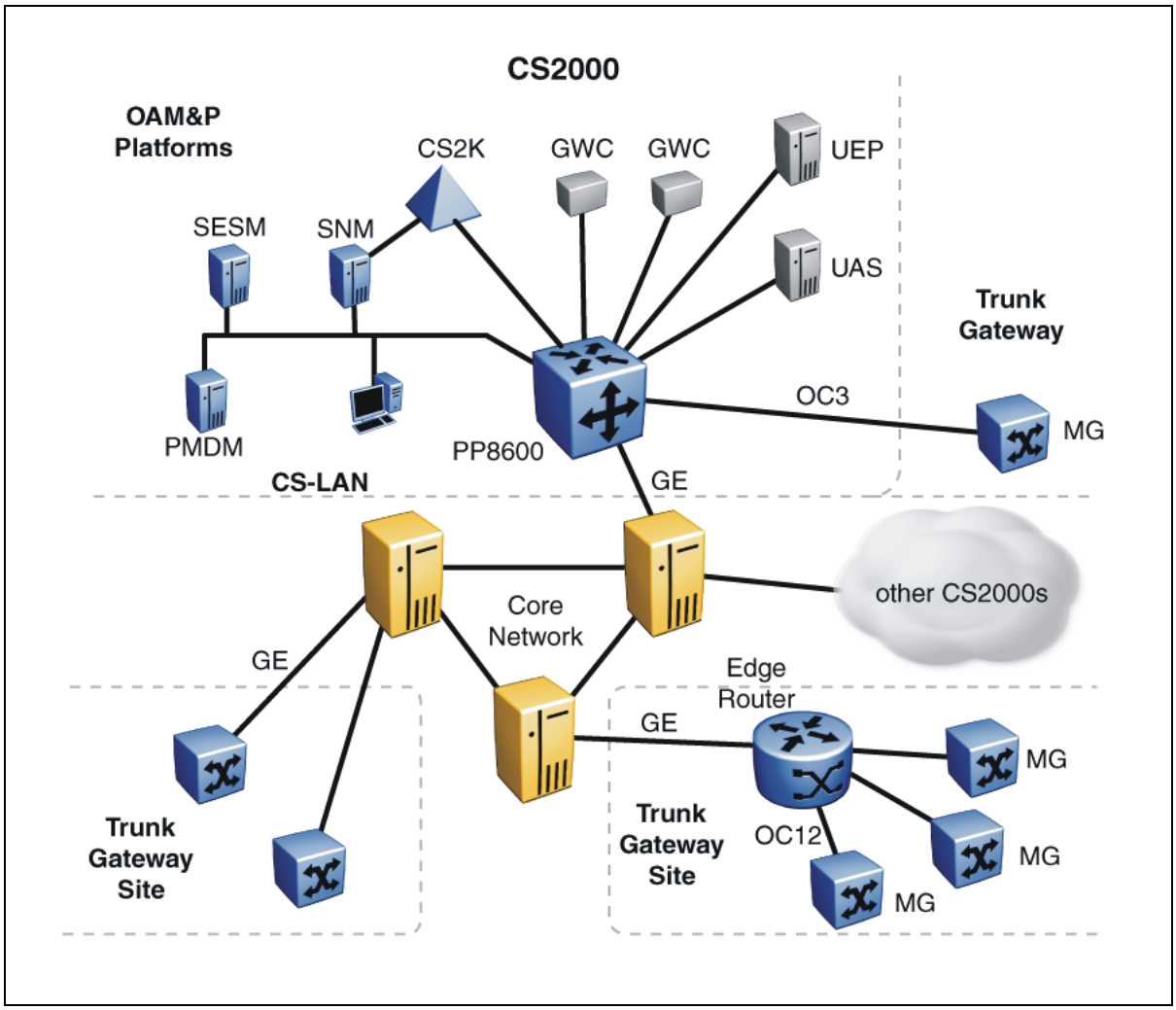
Copyright © 2006, Nortel Networks Nortel Networks Confidential

more information on distributing interfaces and the ports on which to cable these interfaces, refer to your network plan.

PT-IP architecture example

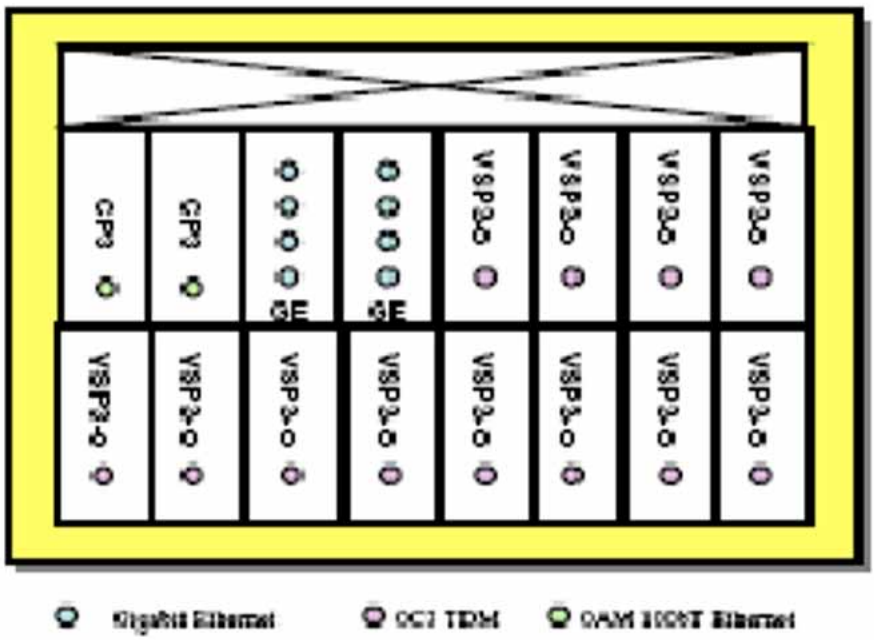
See "PT-IP architecture overview" (page 48) for an architecture overview of a PT-IP solution. In the PT-IP solution, the MG15000 media gateway provides tandem trunking. There are Nodal Provisioning Templates (NP templates) available from the MDM for nodal provisioning that define one configuration for the MG15000 when deployed in a Carrier VoIP PT-IP solution.

PT-IP architecture overview



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example of Maximum MG15000 GE configuration using VSP3-o FPs (PT-IP)



The following templates are provided for PT-IP configuration:

Nodal Provisioning Template summary

Template	Function
PT-IP SH-CPED	Defines shelf-wide parameters, including CP-based configuration, Network Sync (with BITS), TOD Sync, DCS, NMIS, VR/0 (management)
PT-IP SH-CPEE	International variant to support the E1 BITS interface and the CPeE card.
PT-IP FP-4pGe	Defines a pair of load-shared 4pGe FPs.
PT-IP FP- 2pOC3ChSmIrVsp 3-o	Defines a pair of 2pOC3ChSmIrVsp3-o (VSP3-o) FPs.
PT-IP FP- 2pOC3ChSmIrVsp 4e	Defines a pair of 2pOC3ChSmIrVsp4e (2pVSP4e) FPs.
PT-IP SH-VR	Creates a Vr/<n> for voice traffic and signaling, including the Vr Pp Ip LogicalIf (/28), Vr CustSpec and Vm components
PT-IP IF-IP-noLAG-4pGe	Defines a Gigi Ethernet interface to the IP Core or to a ERS8600 on a port on one 4pGe FP. The link is not aggregated (noLAG).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Template	Function
PT-IP IF-IP-LAG-4pGe	Defines a Gigi Ethernet interface to the IP Core or to a ERS8600 on one 4pGe FP. The link is aggregated (LAG).
PT-IP IF-MGC-H248-2pOC3ChSmIrVsp3-o	Defines the NSTA base structure, including the interface to the Media Gateway Controller using H.248 on 2pOC3ChSmIrVsp3-o (VSP3-o) FPs.
PT-IP IF-MGC-H248-2pOC3ChSmIrVsp4e	Defines the NSTA base structure, including the interface to the Media Gateway Controller using H.248 on 2pOC3ChSmIrVsp4e (2pVSP4e) FPs.
PT-IP IF-MGC-IpSec-2pOC3ChSmIrVsp3-o	Defines the IPSec secured signaling path between the Media gateway and the Media gateway controller.
PT-IP IF-OC3-TDM-2pOC3ChSmIrVsp3-o.st	Defines a LAPS-protected pair of OC3 ports on VSP3-o FPs.
PT-IP TT-Sts-TDM	Defines the Sts component under Laps, in preparation for assigning DS1 trunks.
PT-IP IF-STM1-TDM-2pOC3ChSmIrVsp3-o	Defines a LAPS-protected pair of STM1 ports on VSP3-o FP's, as well as provisions the VC4/0 component, in preparation for assigning E1 trunks.
PT-IP TT-PRI-Profile	Defines a profile for PRI that is common to all PRI TDM trunks on a VSP3-o
PT-IP TT-PTS-Profile	Defines a profile for PTS that is common to a set of PTS TDM trunks on a VSP3-o.
PT-IP TT-28DS1-ISUPTrunk	Creates an STS and defines the 28 DS1 ISUP trunks under a Laps and creates the linked Nsta Vgs Tprof Tag components. Many tandem solutions configure all trunks in the same manner.
PT-IP TT-ISUP-DS1-Trunks	Creates one DS1 ISUP trunk under an STS.
PT-IP TT-PRI-DS1-Trunks	Creates one DS1 PRI trunk under an STS.
PT-IP TT-PTS-DS1-Trunks	Creates one DS1 PTS trunk under an STS.
PT-IP TT-63E1-ISUP-Trunk	Creates the 63 E1 ISUP trunks under a VC4 and creates the linked Nsta Vgs Tprof Tag components.
PT-IP TT-ISUP-E1-Trunks	Creates one E1 ISUP trunk under a VC4.
PT-IP TT-PRI-E1-Trunks	Creates one E1 PRI trunk under a VC4.
PT-IP TT-PTS-E1-Trunks	Creates one E1 CAS/PTS trunk under a VC4.
SH-REX-Schedule	Adds support for REX, including scheduling.

Link distribution (PT-AAL1 and UA-AAL1)

This section describes link distribution between Nortel Multiservice Switch 15000 nodes and other network components, in a PT-AAL1 or UA-AAL1 solution. It includes the topics as follows:

- "CS2000 link (PT-AAL1/UA-AAL1)" (page 51)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "XA-Core link distribution (PT-AAL1/UA-AAL1)" (page 51)
- "SAM21 SC link distribution (UA-AAL1)" (page 54)
- "IW-SPM link distribution (PT-AAL1 and UA-AAL1)" (page 55)
- "DPT-SPM link distribution (PT-AAL1 and UA-AAL1)" (page 56)
- "MG4000 link distribution (PT-AAL1 and UA-AAL1)" (page 56)
- "MG9000 link distribution (UA-AAL1)" (page 58)
- "Internode Emergency Stand Alone for MG9000" (page 60)
- "Node-to-node ATM link distribution (PT-AAL1/UA-AAL1)" (page 61)
- "UAS link distribution (UA-AAL1)" (page 62)
- "DSL services link distribution (UA-AAL1)" (page 63)

Note 1: On Multiservice Switch 15000 shelves, the ports on the cards are numbered from the bottom to the top.

Note 2: On Multiservice Switch 15000 shelves, the two control processors (CPs) are located in slots 0 and 1 and are correspondingly numbered 0 and 1.

CS2000 link (PT-AAL1/UA-AAL1)

The Communication Server 2000 (CS2000) is comprised of a number of platforms, including the XA-Core and one or more SAM21. It processes all call requests within the network and provides centralized call control between the media gateways (MG4000 and, in the case of the UA-AAL1 solution, MG9000), as well as between the TDM-based nodes and the ATM network.

CS2000 is connected to Nortel Multiservice Switch 15000 nodes by a minimum of four unprotected OC-3 links. Since the CS2000 has a load sharing protection mechanism, the OC-3 links are not 1+1 protected by Automatic Protection Switching (APS).

XA-Core link distribution (PT-AAL1/UA-AAL1)

A sub-platform of the CS2000, the XA-Core processes all call requests within the network. It provides centralized call control between the media gateways (MG4000 and, in the case of the UA-AAL1 solution, MG9000), as well as between the TDM-based nodes and the ATM network.

XA-Core connects to a Nortel Multiservice Switch 15000 shelf through two unprotected OC-3c links. The XA-Core provides the required link protection at the application layer.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Nortel recommends that the two links between the XA-Core and the Multiservice Switch network be connected to different Multiservice Switch 15000 nodes in order to create redundancy.

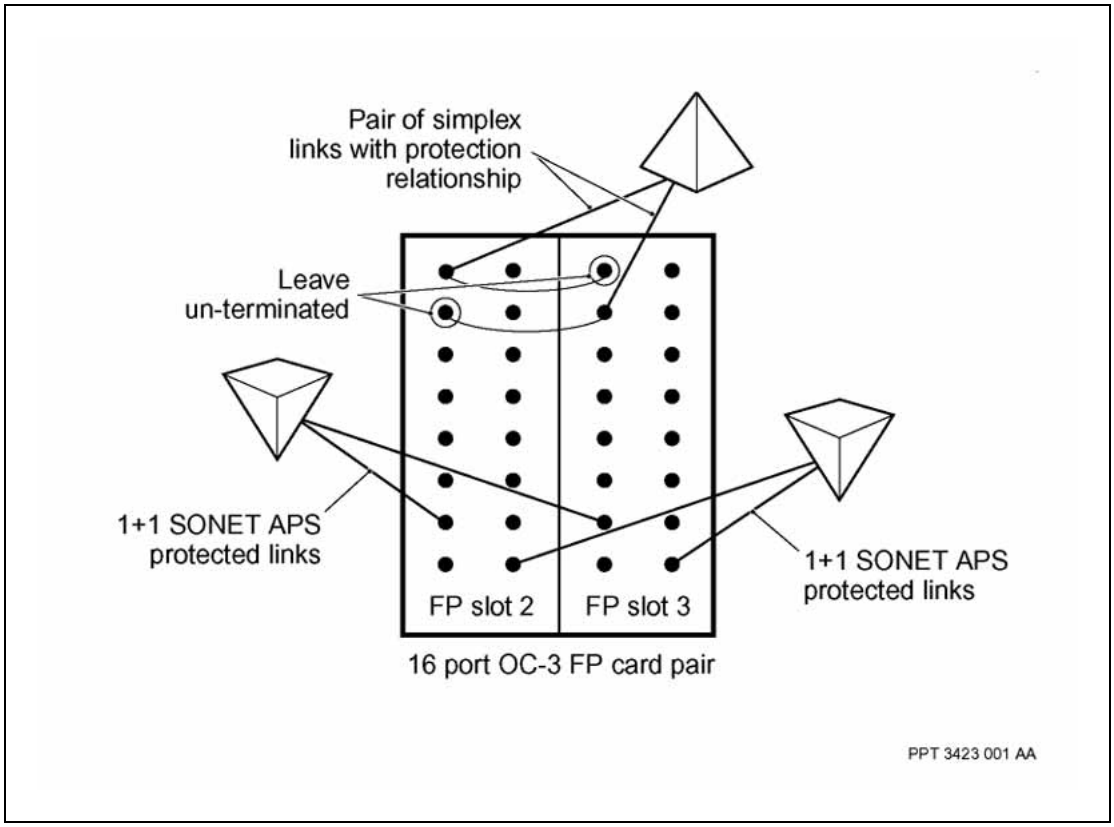
When both XA-Core links are connected to the same node, the XA-Core links can be configured to support hitless software migration (HSM) using the *WUA-AAL1 BridgedCS2k-ATM Interfaces-16pOC3* template.

OC-3 ATM link pairs must be connected to the Multiservice Switch 15000 node in a specific configuration to maintain service during a software upgrade (HSM). "OC-3 ATM link pairs" (page 53) illustrates the required configuration, and the following list identifies the specifics:

- OC-3 ATM links must be connected to 16pOC3SmIrATM FP cards. (Connection to 4pOC3SmIrATM FP card is not supported.)
- The two OC-3 from XA-Core links must not be connected to the same FP card. They must be connected to two adjacent cards that have a sparing relationship, for example, to the 16pOC3SmIrATM FP cards in slots 2 and 3; port 0 on card 2, port 1 on card 3.
- The corresponding SONET port on the mated FP card must be left not terminated. During HSM, mated FP cards upgrade one at a time, and the cell forwarding hardware behind the non terminated port is used to bring the link connected to the corresponding port on the mate card back into service during the migration.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

OC-3 ATM link pairs



To configure the XA-Core interface, use the Nodal Provisioning tool and the following templates:

- *PT-AAL1/WUA-AAL1 CS2000 Interface 4pOC3*
- *PT-AAL1/WUA-AAL1 CS2000 Interface 16pOC3*
- *WUA-AAL1 Bridged CS2K-ATM Interfaces-16pOC3*

To configure the XA-Core interface, configure the following:

- an appropriate FP pair, if not already done
- the engineering and control parameters for each FP pair, if necessary
- the interface for XA-Core or SAM21 SC
- any customer-defined customizing for ports on the FP pair, if necessary

For the specific values that need to be configured for XA-Core interface, see the table of values for XA-Core interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

SAM21 SC link distribution (UA-AAL1)

A sub-platform of the CS2000 in the Universal Access - AAL1 solution, the SAM21 is a 21 slot shelf that houses the Gateway Controllers (GWC) used for MG9000s. Each SAM21 shelf has two redundant Shelf Controllers (SC) each with a connection to the ATM network.

SAM21 SC links can be configured to support hitless software migration (HSM) using the *WUA-AAL1 BridgedSam21-ATM Interfaces-16pOC3* template.

OC-3 ATM link pairs must be connected in the Nortel Multiservice Switch 15000 node to maintain service during a software upgrade (HSM) of the node. The specific configuration is described in the list below. For a graphical representation, see "OC-3 ATM link pairs" (page 53).

- The OC-3 ATM links must be connected to 16pOC3SmIrATM FP cards. (Connection to 4pOC3SmIrATM FP card is not supported.)
- The two OC-3 from a SAM21 shelf links must not be connected to the same FP card. They must be connected to two adjacent cards that have a sparing relationship, for example, to the 16pOC3SmIrATM FP cards in slots 2 and 3; port 0 on card 2, port 1 on card 3.
- The corresponding SONET port on the mate FP card must left un-terminated. During HSM, mated FP cards upgrade one at a time, and the cell forwarding hardware behind this non terminated port is used to bring the link connected to the corresponding port on the mate card back in service during the migration.

To configure the SAM21 SC interface, use the Nodal Provisioning tool and the following templates:

- *WUA-AAL1 SAM 21 SC Interface-4pOC3*
- *WUA-AAL1 SAM 21 SC Interface-16pOC3*
- *WUA-AAL1 Bridged SAM21-ATM Interfaces-16pOC3*

To configure the SAM21 SC interface, configure the following:

- an appropriate FP pair
- the ATM interfaces
- the connection admission controls for each ATM interface
- the connection map for each ATM interface for a 16 port OC-3 FP
- the user network interface (UNI)
- traffic management parameters for each UNI

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values that need to be configured for the SAM21SC interface, see the table of values for the SAM21 SC interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

IW-SPM link distribution (PT-AAL1 and UA-AAL1)

The interworking SPM (IW-SPM) is a multi-applications high-speed platform used to provide bearer traffic interconnection between the time division multiplexing (TDM) core and the ATM fabric.

The IW-SPM acts as a bridge between the TDM core ENET using DS-512 connections and the ATM network using OC-3 links.

Each IW-SPM connects to the Nortel Multiservice Switch 15000 shelf over a protected OC-3 link. Each IW-SPM also communicates with the CS2000 over DS-512 links that run through the ENET.

To configure the IW-SPM interface, use the Nodal Provisioning tool and the following templates:

- *PT-AAL1/WUA-AAL1 IW-SPM Interfaces 4pOC3*
- *PT-AAL1/WUA-AAL1 IW-SPM Interfaces-16pOC3*

Note: You can configure these links with the values in the templates listed above or you can refer to the appropriate section of the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* for the values. Regardless of which method you use, have a Network Engineering Specification Book at hand as a reference when determining which values to enter into the templates.

To configure the IW-SPM interface, configure the following:

- an appropriate FP pair, if necessary
- the engineering and control parameters for each FP pair, if necessary
- the IW-SPM interface (which includes configuring any necessary customer-defined customizing for each port on the FP pair, line protection for the port, ATM interfaces, and user network interface)

For the specific values to configure for the IW-SPM interface, see the table of values for IW-SPM in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

DPT-SPM link distribution (PT-AAL1 and UA-AAL1)

The dynamic packet trunking SPM (DPT-SPM) is a class designation of the IW-SPM and is similar in all respects, including configuration.

To configure the DPT-SPM interface, use the Nodal Provisioning tool and the following templates:

- *PT-AAL1/WUA-AAL1 DPT-SPM Interfaces-4pOC3*
- *PT-AAL1/WUA-AAL1 DPT-SPM Interfaces-16pOC3*

Note: You can configure these links with the values in the templates listed above or you can refer to the appropriate section of the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* for the values. Regardless of which method you use, have a Network Engineering Specification Book at hand as a reference when determining the values to enter into the templates.

For the specific values that need to be configured for the DPT-SPM interface, see the table of values for DPT-SPM interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG4000 link distribution (PT-AAL1 and UA-AAL1)

The Multi-service Gateway 4000 (MG4000) is the trunk gateway between the TDM-based network and the ATM network.

The MG4000 collects TDM traffic and carries it into the ATM network through TDM-based OC-3 connections to the OC-3c interfaces in the ATM network. Two permanent virtual circuit (PVC) connections are configured between the CS2000 and the MG4000.

The MG4000s connect to the Nortel Multiservice Switch 15000 shelf over protected OC-3 links. To configure these links, first configure the ATM interfaces, and then configure two PVC connections between each MG4000 and the communication server (CS2000).

When configuring the PVCs, keep the following items in mind:

- The CS2000 has four unprotected OC-3 links into Multiservice Switch 15000 shelves. When creating the two PVC connections from one MG4000 to a CS2000, configure both of these PVC connections to go to the same pair of unprotected links, one to each of the two ports in the same FP pair. Each of the two PVC connections from one MG4000 cannot go to a different FP pair.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- Half of the PVC connections from the MG4000s must go to one of the pairs of protection group CS2000 links, while the other half must go to the other pair of protection group CS2000 links.
- The two PVC connections from each MG4000 should take the shortest route possible between the MG4000s and the CS2000. However, the two routes should also be as diverse as possible within your network topology. Each of the PVC connections should connect across different shelves, FP pairs, or physical links to decrease the common points of failure on each PVC.
- If the PVC needs to go across a link between Multiservice Switch 15000 shelves, select the link with the least number of PVC connections already running across it. Choose this link to ensure that the inter-shelf links load-share the PVC control connections.
- Define the PVC relay points as follows:
  - The relay points at the CS2000's ATM interface must be identified by the same VPI.VCI used for the CS2000's link.
  - The relay points at the MG4000's ATM interface must be identified by the same VPI.VCI used for the MG4000's link.
  - The relay points at either end of an inter-shelf link over which the PVC crosses must both be identified by the same VPI.VCI (Nortel recommends giving PVC1 a value or name equal to the SPM number plus 100 and PVC2 a value or name equal to the SPM number plus 300).
  - The other relay points on the PVC are selected using unused VPI.VCIs. You could chose to start at the top of the VCI range and progress downwards.

  To configure the MG4000 interface, use the Nodal Provisioning tool and the following templates:
  - *PT-AAL1/WUA-AAL1 MG4000 ATM Interfaces 4pOC3*
  - *PT-AAL1/WUA-AAL1 MG4000 ATM Interfaces 16pOC3*

To configure the MG4000 interface, configure the following:

- the FP and engineer the parameters, if not already done
- a Multiservice Switch OC-3 interface for the MG4000
- the MG4000 interface for each FP type

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values that need to be configured for the MG4000 interface, see the table of values for MG4000 ATM interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG9000 link distribution (UA-AAL1)

The Multi-service Gateway 9000 (MG9000) is a multi-service platform that is used with the Universal Access - AAL1 solution. It supports switched lines (for example, POTS), DS1 private line, and DSL services.

The MG9000 physically connects to the ATM network with OC-3, DS3 or DS1 IMA links. The MG9000 is connected logically to the Services Application Module 21 (SAM21) shelf controllers (SC) using four switched virtual circuits (SVC).

For the specific values to configure for the MG9000 interface, see the tables of values for MG9000 ATM interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG9000 OC-3 link distribution (UA-AAL1)

The MG9000 can connect to a Nortel Multiservice Switch 15000 node using a 1+1 LAPS-protected OC-3 interface. To configure the MG9000 OC-3 interfaces, use the Nodal Provisioning (NP) tool, and the templates as follows:

- *WUA-AAL1 MG9000 ATM Interfaces-4pOC3*
- *WUA-AAL1 MG9000 ATM Interfaces-16pOC3*

MG9000 DS1 IMA link distribution (UA-AAL1)

The MG9000 can connect to a Nortel Multiservice Switch 15000 node using a DS1 IMA interface. This interface consists of between 2 and 8 DS1s on a DS3 port of a 1:1 equipment-protected 4-port DS3 (channelized to DS1 for IMA) ATM FP.

To configure the MG9000 DS1 IMA interfaces, use the Nodal Provisioning tool, and the following templates:

- *WUA-AAL1 DS3 port-4pDS3ChAtm*
- *WUA-AAL1 MG9000 2xDS1-IMA ATM Interface-4pDS3ChAtm*
- *WUA-AAL1 1xDS1-IMA Link - 4pDS3ChAtm*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

MG9000 DS3 link distribution (UA-AAL1)

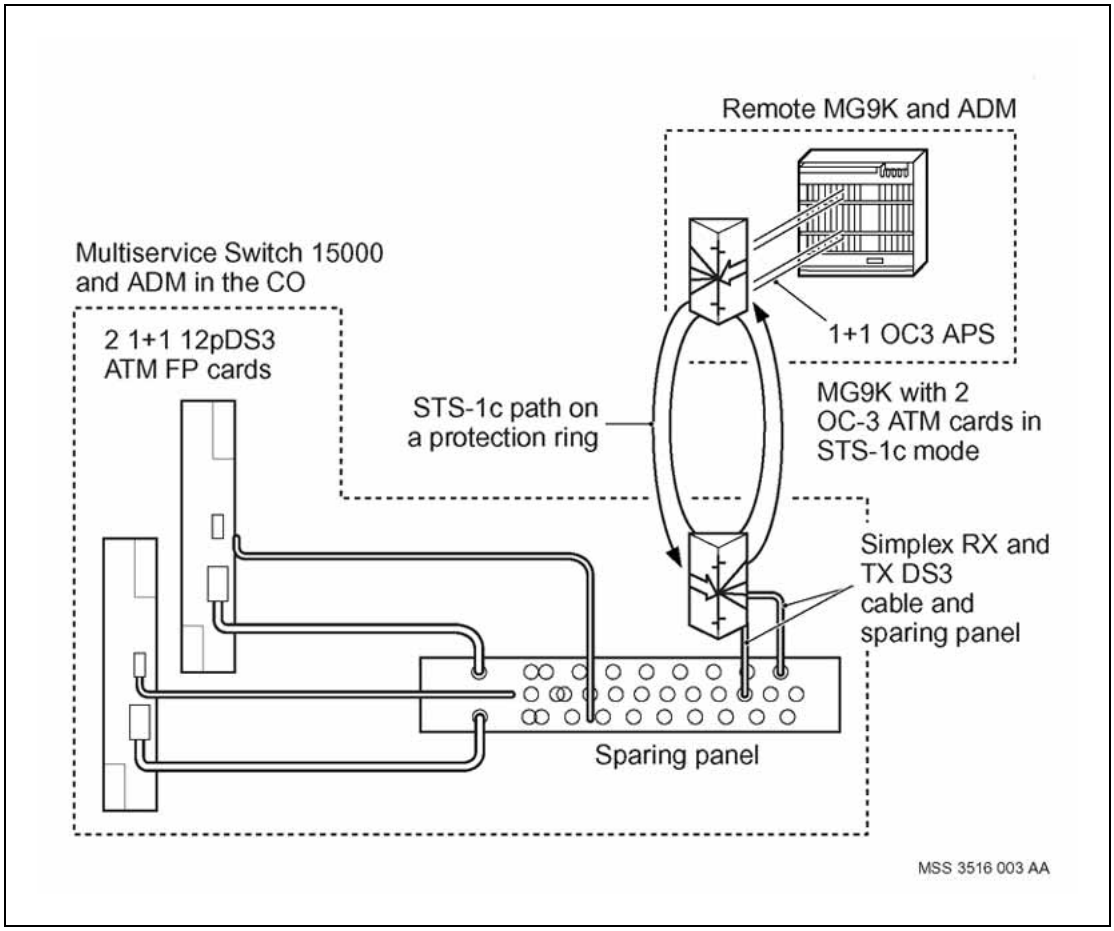
The MG9000 can connect to a Nortel Multiservice Switch 15000 node using a DS3 interface, on a 1:1 equipment-protected 12-port DS3 ATM FP. To configure the MG9000 DS3 interfaces, use the Nodal Provisioning tool, and the *WUA-AAL1 MG9000 ATM Interface-12pDS3* template.

For an illustration of the MG9000 DS3 link, see "MG9000 DS3 to Multiservice Switch 15000 DS3 with optical transport" (page 59).

The MG9000 DS3 interface is a less costly connection than, for example, an OC-3, to an ATM backbone. However, it still meets bandwidth requirements. Additional cost savings are available when a fiber data path between the Multiservice Switch 15000 node and MG9000 is not available for connection.

Note: Even though the MG9000 DS3 interface uses a 12-port FP, it only supports the use of ports 0 through 3. Connect the 4-port DS3 sparing panel to the p0 connector on the FP faceplate for the DS3 ports. Connect it to the P3 connector on the FP faceplate for sparing panel control.

MG9000 DS3 to Multiservice Switch 15000 DS3 with optical transport



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Internode Emergency Stand Alone for MG9000

To use internode emergency stand alone (ESA) in your UA-AAL1 MG9000 network, you must perform some shelf configuration on the Software (Sw) and Virtual Router (vr) components manually after the nodal provisioning template has been applied.

For detailed component configuration, refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

A list of possible deployment scenarios for internode ESA are as follows:

- MG9000 connected to 4pOC3 FP card with ipRoutes > 0
- MG9000 connected to 16pOC3 FP card with ipRoutes > 0

  Note: The AtmIf Vcc Nep, AtmMpe Ac and VirtualRouter ProtocolPort components must be manually configured for MG9000 according to the configuration attributes listed in the following tables of *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*:

  — "OC-3 configuration for internode ESA"

  — "DS-3/STS-1 interface configuration to support MG9000 internode ESA"

  — "DS-1 IMA interface configuration to support MG9000 internode ESA"

- MG9000 connected to 16pOC3 FP card with ipRoute = 0; only supports a hairpin configuration
- MG9000 STS-1 connected to 12pDS3 FP cards (which do not support IP)
- MG9000 IMA connected to 4pDS3 FP cards (which do not support IP)

  — For MG9000 on these cards, an IP hairpin is required.

  — PVC is needed between the MG9000 to the hairpin port.

Hairpins can be provisioned on:

- A new pair of 4pOC3 cards.
- Spare pair of 1+1 OC12 or OC3 ports on either 4pOC12 (PQC12) or 4pOC3 (assume ipRoutes > 0)
- Pair 16pOC3 with ipRoutes>0

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Use the UA-IP Hairpin NP templates to configure the hairpin interfaces.

For more information about Inter-node ESA attributes, refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Node-to-node ATM link distribution (PT-AAL1/UA-AAL1)

Nortel Multiservice Switch 15000 nodes support a node-to-node ATM interface, in a Universal Access - AAL1 solution. Configure these links as protected OC links on either OC-3 or OC-12 cards. When you configure this service, the ATM Interface (AtmIf) component and its subcomponents, ConnectionAdministrator (CA) and Private Network-to-Network Interface (PNNI) are always created as well.

To configure the Multiservice Switch for ATM Interface with PNNI, use the Nodal Provisioning tool and the following templates:

- PT-AAL1/WUA-AAL1 ATM PNNI Interfaces-4pOC3
- PT-AAL1/WUA-AAL1 ATM PNNI Interfaces-16pOC3
- PT-AAL1/WUA-AAL1 ATM PNNI Interfaces-4pOC12
- WUA-AAL1 ATM PNNI Interfaces-12pDS3

To configure the Multiservice Switch for ATM Interface with PNNI in the Packet Trunking - AAL1 solution, configure the following:

- an appropriate FP pair, if necessary
- the ATM PNNI interface for the appropriate FP type
- any customer-defined customizing for each port on the FP pair, if necessary
- line protection for the FP pair
- the ATM interfaces
- the PNNI interface

To configure the Multiservice Switch 15000 node for ATM Interface with PNNI in the Universal Access - AAL1 solution, configure the following:

- an appropriate FP pair
- line protection for the port
- the ATM interfaces
- the connection admission controls for each ATM interface

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For a 16 port OC-3 or 4 port OC-12 FP, configure the PNNI interface for the connection map for each ATM interface.

If MG9000 interNode ESA support is required over the PNNI link, the AtmIfVcc Nep, AtmMpe Ac, and VirtualRouter ProtocolPort components need to be configured as described in the table "MSS15000 to MSS15000 configuration to support MG9000 internode ESA" in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

For the specific values that need to be configured for Multiservice Switch ATM trunks, see the table of values for ATM trunk configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

UAS link distribution (UA-AAL1)

In the Universal Access - AAL1 solution, the universal audio server (UAS) is a SAM16 shelf-based peripheral that provides services such as the following:

- conferencing
- voice mail
- announcements

Currently, the UAS is limited to providing the multi-casting capabilities necessary for local Communication Assistance for Law Enforcement Act (CALEA).

The UAS is connected to the ATM network by a OC-3 link. Call control is provided by the GWC. The CS LAN the signalling between the UAS and the GWC.

To configure the UAS interface, use the Nodal Provisioning tool and the following templates:

- *WUA-AAL1 UAS ATM Interface-4pOC3*
- *WUA-AAL1 UAS ATM Interface-16pOC3*

To configure the UAS interface, configure the following:

- an appropriate FP pair
- the ATM interfaces
- the connection admission controls for each ATM interface
- the connection map for each ATM interface for a 16 port OC-3 FP

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- the user network interface (UNI)
- traffic management parameters for each UNI

For the specific values that need to be configured for the UAS interface, see the table of values for UAS ATM UNI link configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

DSL services link distribution (UA-AAL1)

In a Universal Access - AAL1 solution, you can configure Nortel Multiservice Switch 15000 nodes to support digital subscriber line (DSL) service. Each MG9000 supports DSL subscriber line access. The MG9000 then transfers the DSL connections across a Multiservice Switch ATM network using only the following virtual connections:

- permanent virtual connection (PVC)
- permanent virtual path (PVP)
- soft permanent virtual connection (SPVC)
- soft permanent virtual path (SPVP)

These DSL connections terminate at an Internet Service Provider (ISP).

There are some restrictions on the DSL service in the UA-AAL1 network. These restrictions are designed to ensure the quality and reliability of Public Switched Telephone Network (PSTN) voice traffic. The following restrictions apply to this interface:

- no signaling, routing or ILMI control channels are supported
- must be provisioned as an I.610 OAM segment boundary to prevent OAM segment cells from entering the Multiservice Switch network from the ISP network
- no connections between the ISP network and an FP that supports any device
- DSL ISP UNI interfaces require at least one ATM End System Address (AESA) to be provisioned when SPVCs and SPVPs are used to connect with the MG9000s

Connections between the Carrier VoIP network and ISP networks are left unprotected, therefore, an unprotected FP is used for all these connections or any similar connections to data-only networks.

In order to configure DSL connections across the Multiservice Switch ATM network, use Nortel Multiservice Data Manager ATM Service Provisioning tool to provision the connections. For more information on this tool, see

Copyright © 2006, Nortel Networks Nortel Networks Confidential

241-6001-600 Nortel Multiservice Data Manager Service Provisioning for ATM User Guide. In conjunction with this tool, MDM has a circuit management database and circuit viewer application that allows you to track all virtual circuits (VCs) and virtual paths (VPs) that have been created in the network.

Configure the UNI connection using the command line interface (CLI) with the *NN10400-006 Nortel Multiservice Data Manager Network Configuration* and the *241-6001-023 Nortel Multiservice Data Manager Configuration Tools*. How you configure the UNI is dependent on the type of DSL aggregator being used.

To configure a subscriber's DSL service, perform the following tasks:

- Provision the Vcc endpoints into the MG9000 and the ISP DSL aggregator.
- Use the ATM Service Provisioning tool to provision the PVC or SPVC in the Multiservice Switch network from the MG9000 to the ISP.
- Alternatively, the Vcc can be carried by an existing PVP or SPVP between the MG9000 and the ISP, or a new PVP or SPVP can be added to carry the subscriber's DSL traffic.

For more information on ATM configuration, see *NN10600-710 Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*.

Link Distribution (PT-AAL2)

In a Carrier VoIP PT-AAL2 solution, signaling between MGC and MG15000 is done over IPoATM. Templates are available for interface configuration between Media Gateway 15000 nodes and other network components in a PT-AAL2 solution. See "Summary of NP templates for PT-AAL2" (page 64) for a summary of the templates required for MG15000 PT-AAL2 provisioning.

For network growth scenarios that have you adding FPs to your MG15000s in the PT-AAL2 solution after initial configuration, refer to "Use cases for incremental growth of a PT-AAL2 network" (page 179).

Summary of NP templates for PT-AAL2

Template	Definition
PT-AAL2 SH-CPED	Defines shelf-wide parameters, including CP-based configuration, Network Sync (with BITS), TOD Sync, DCS, NMIS, ATM Routing, VR/mgmt (management), VR/<CallP>
PT-AAL2 FP-4pOC12SmIrAtm	Defines a pair of 4pOC12ATM FP's.
PT-AAL2 FP-4pOC3SmIrAtm_Unprotected	Defines an unprotected 4pOC3ATM FP's.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Template	Definition
PT-AAL2 FP-2pOC3ChSmIrVsp3-o	Defines a pair of 2pOC3ChSmIrVsp3 (VSP3-o) FP's. This template is used in the UA-IP and PT-IP solution set, as well.
PT-AAL2 IF-MGX-4pOC12SmIrAtm	Defines an interface to a 3rd party ATM switch on a 1+1 protected port of the 4pOC12 FP.
PT-AAL2 IF-AS-4pOC3SmIrAtm	Defines an interface to the Audio Server on an unprotected port of the 4pOC3 FP (eg:UAS, MS20X, or AMS). Provisions an unprotected SONET port with an ATMIF on a 4pOC3SmIrAtm FP for a UNI interface to an audio server network element.
PT-AAL2 IF-PNNI-4pOC12SMIrAtm	Defines an ATM PNNI interface on a 1+1-protected port of the 4pOC12 FP. Provisions a LAPS-protected pair of SONET ports with an ATMIF on 4pOC12SmIrAtm FP's for a PNNI interface to another MG15000.
PT-AAL2 IF-TDM-2pOC3ChSmIrVsp3-o	Defines a LAPs-protected SONET pair of TDM ports on 2pOC3ChSmIrVsp3-o FPs.
PT-AAL2 IF-MGC-H248-2pOC3ChSmIrVsp3-o	Defines the NSTA base structure, including the interface to the Media Gateway Controller using H.248 on 2pOC3ChSmIrVsp3 (VSP3-o) FP's.
PT-AAL2 TT-28ISUPTrunks-2pOC3ChSmIrVsp3-o	Defines an Sts component under LAPS on 2pOC3ChSmIrVsp3 (VSP3-o) FP's and 28 ISUP TDM trunks terminating on a VSP3-o.

For the specific values to configure PT-AAL2 interfaces, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Link distribution (UA-IP)

This section describes link distribution between Nortel Multiservice Switch 15000 nodes and other network components, in a UA-IP solution. It includes the topics as follows:

- "Multiservice Switch IP over ATM inter-shelf trunk interface (UA-IP)" (page 66)
- "MG9000 OC-3 interface (UA-IP)" (page 69)

Copyright © 2006, Nortel Networks

- "MG9000 DS1 IMA interface (UA-IP)" (page 69)
- "MG9000 STS-1/DS3 interface (UA-IP)" (page 70)
- "CS-LAN OC-12 interface (UA-IP)" (page 71)
- "CS-LAN GE interface (UA-IP)" (page 71)
- "Hairpin ATM/IP OC-3/OC-12 interfaces (UA-IP)" (page 72)
- "TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (UA-IP)" (page 73)
- "Media Gateway 15000 to MGC with H.248 (VSP3) interface (UA-IP)" (page 73)
- "Media Gateway 15000 to MGC with H.248 (VSP3-o) interface (UA-IP)" (page 74)

Note 1: On a Multiservice Switch 15000 shelf, the ports on the cards are numbered starting at the bottom and working up.

Note 2: On a Multiservice Switch 15000 shelf, the two control processors (CPs) are located in slots 0 and 1 and are correspondingly numbered 0 and 1.

Note 3: The names of the templates you use to create the interfaces in a UA-IP solution include the prefix IF. This denotes a template that sets up parameters for an interface which usually (but not always) corresponds to physical facilities. This can be a single port, a pair of protected ports, a logical interface such as an ATM interface to another network element (NE, for example MG9000), or an IP interface (for example to a media gateway controller or MGC), and so on.

Note 4: There is no change to the MSS15000 configuration to support internode ESA in the UA-IP solution.

Multiservice Switch IP over ATM inter-shelf trunk interface (UA-IP)

In a UA-IP solution, you can link a remote Nortel Multiservice Switch 15000 node with IP over ATM to another Multiservice Switch 15000 node at a CS2000 site, in a UA-IP solution. This requires a Multiservice Switch IP over ATM inter-shelf trunk interface. The Multiservice Switch 15000 node is used as a packet core network element. Multiservice Switch 15000 nodes can connect either directly through fiber, or through a synchronous optical network (SONET).

Generally, in a UA-IP solution, one primary Multiservice Switch 15000 node is situated in the office with the CS-LAN. It is connected to the CS-LAN via Gigabit Ethernet (GE), or OC-12. Other Multiservice Switch 15000 nodes are at the same site, but are not necessarily connected to the CS-LAN for IP control/bearer traffic. The remaining Multiservice Switch 15000 nodes are situated in Remote Wire Centres (RWCs).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

The primary Multiservice Switch 15000 node connected to the CS-LAN likely has an inter-shelf IP interface to each of the other nodes. The other nodes are not necessarily directly linked to another RWC. In most cases, an IP over ATM connection is used for bearer path IP between each RWC and every other RWC.

To configure Multiservice Switch IP over ATM inter-shelf trunk interface, use the Nodal Provisioning tool and either of the following templates:

- *UA-IP IF-MSS-IPoATM-4pOC3SmIrAtm*
- *UA-IP IF-MSS-IPoATM-4pOC12SmIrAtm*

For Multiservice Switch IP over ATM inter-shelf trunk interface in a Universal Access - IP solution, configure the following and then activate the changes:

- an appropriate FP pair
- line protection for the port
- the ATM interfaces
- apply the *UA-IP AC-RWC-Bearer* template for each RWC-to-RWC bearer path connection (See "RWC bearer VCC distribution (UA-IP)" (page 68) for more information.)
- the connection admission controls for each ATM interface
- the ATM private network-to-network interface (PNNI)
- the connection maps for each ATM interface
- manually create IP routing (for example static route) entries

Apply either of the *UA-IP IF-MSS-IPoATM-4pOC3SmIrAtm* or *UA-IP IF-MSS-IPoATM-4pOC3SmIrAtm* templates to the remote end of the link. Then apply the template to the CS2000 end of the link.

Apply the *UA-IP AC-RWC-Bearer* template to each remote Multiservice Switch 15000 node, on the new node n-1 times and one on each remote node. Also, configure the nailed-up relay points (NRPs) on the CS2000 site node.

For the specific values to configure for Multiservice Switch IP over ATM inter-shelf trunk interface, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

RWC bearer VCC distribution (UA-IP)

This section describes ATM connection distribution on Nortel Multiservice Switch 15000 nodes in a UA-IP solution. Apply this provisioning at initial commissioning of the node, or on existing node-to-node interfaces for capacity growth.

In a UA-IP solution, you can provision an asynchronous transfer mode (ATM) virtual channel connection (VCC) for IP connectivity between remote wire centres (RWCs).

To provision Multiservice Switch 15000 nodes for the RWC bearer VCC, use the Nodal Provisioning tool, and either of the following templates:

- *UA-IP AC-RWC-Bearer-4pOC12SmIrAtm*
- *UA-IP AC-RWC-Bearer-4pOC3SmIrAtm*

These templates define an ATM connection for bearer path traffic from a node at a Remote Wire Centre going to a node at another Remote Wire Centre. The ATM connection is over either an existing OC-12 IPoATM trunk or an existing OC-3 IPoATM trunk.

To configure the RWC bearer VCC on a Multiservice Switch 15000 node in a UA-IP solution, configure the following:

- an appropriate FP pair, if necessary
- Multiservice Switch IP over ATM inter-shelf trunk interface on 4pOC12SmIrAtm or 4pOC3SmIrAtm FP cards
- the LAPS STS on the above FP cards

For the specific values to configure an ATM connection - RWC bearer VCC, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG9000 interface (UA-IP)

The Multi-service Gateway 9000 (MG9000) is a multi-service platform that is used with the UA-IP solution.

The MG9000 physically connects to the network with OC-3, DS1 IMA, or STS-1 DS3 links.

For the specific values to configure for the MG9000 link distribution, see the tables of values for MG9000 interface configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

MG9000 OC-3 interface (UA-IP)

The MG9000 can connect to Nortel Multiservice Switch 15000 nodes using an optical link (1 + 1 OC-3).

The MG9000 carries IP traffic to the virtual router (VR) over 2 or 3 virtual channel connections (VCCs) as follows:

- MG9000 carries IP traffic over an rt-VBR Vcc that carries all voice traffic plus the H.248 control traffic. This Vcc requires a /27 subnet, because it has up to 16 IP devices connected to it, plus the Multiservice Switch 15000 node's protocol port address.
- MG9000 carries IP traffic over an nrt-VBR Vcc that carries the operations, administration, and maintenance (OAM) traffic for the MG9000. This Vcc requires a /29 subnet for three IP addresses: two IP addresses on the MG9000, plus the Multiservice Switch 15000 node's protocol port addresses.
- MG9000 carries IP traffic over an optional rt-VBR that carries other signalling (PPVM) and control traffic for MG9000 ABI cards.

To configure the MG9000 OC-3 interface, use the Nodal Provisioning tool and the *UA-IP IF-MG9000-4pOC3SmIrAtm* template

> ***Note:*** In a UA-IP solution, the NP templates for the MG9000 interfaces do not configure an ABI connection, just the basic CC (bearer and H.248) and OAM Vccs. For these Vccs, the maximum traffic contract is the default. For example, by default, it assumes that 2 shelves are configured on the MG9000 OC-3 port. It is up to the installer to change this if necessary, using the values in the Network Engineering Specification Book.

For the specific values to configure for an MG9000 OC-3 link, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG9000 DS1 IMA interface (UA-IP)

The MG9000 can connect to Nortel Multiservice Switch 15000 nodes using a DS1 IMA interface. This interface is an ATM interface that uses a DS1 line standard format, and inverse multiplexing for ATM (IMA).

The difference between the MG9000 DS1 IMA interfaces in a UA-IP versus a UA-AAL1 solution is that the NP template for UA-IP does not configure an ATMIf Uni Sig Vcd subcomponent. Also for UA-IP, the AtmIf component attributes have different values.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

To configure the MG9000 DS1 IMA link, use the Nodal Provisioning tool and the following templates:

- *UA-IP IF-DS3port- 4pDS3ChAtm*
- *UA-IP IF-MG9000-8xDS1-4pDS3ChAtm*

The *UA-IP IF-DS3port- 4pDS3ChAtm* template creates a DS3 port on 4pDS3ChAtm FPs. This template is preparation for adding IMA-linked interfaces.

The *UA-IP IF-MG9000-8xDS1-4pDS3ChAtm* template creates an interface to an MG9000 on 4pDS3ChAtm FP cards. It provisions an IMA group of 8 DS1s with an ATMIF on the FP cards. If you require less than 8 DS1s, manually delete the extra ones.

> ***Note:*** The MG9000 DS1 IMA interface requires an optical hairpin. You must configure the hairpin components first, before configuring the MG9000 DS1 IMA link. For more information, see "Hairpin ATM/IP OC-3/OC-12 interfaces (UA-IP)" (page 72).

For the specific values to use for the MG9000 DS1 IMA interface configuration, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MG9000 STS-1/DS3 interface (UA-IP)

The MG9000 can connect to Nortel Multiservice Switch 15000 nodes using a Synchronous Transport Signal level (STS-1) interface. This interface terminates on the node as a DS3 line standard format. The DS3 format is used to carry information over a T3 trunk.

To configure an MG9000 STS1/DS3 interface on Multiservice Switch 15000 nodes use the Nodal Provisioning tool and the *UA-IP IF-MG9000-12pDS3Atm* template.

The UA-IP version of the NP template, unlike the UA-AAL1 version, does not require an ATMIf Uni Sig Vcd subcomponent. Also, the values for AtmIf component attributes in the UA-IP solution are different.

> ***Note:*** The MG9000 STS-1 DS-3 interface requires the use of an optical hairpin. For more information, see "Hairpin ATM/IP OC-3/OC-12 interfaces (UA-IP)" (page 72).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values to configure for the STS1/DS3 interface, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

CS-LAN OC-12 interface (UA-IP)

In a UA-IP solution, you can add CS-LAN interfaces to Nortel Multiservice Switch 15000 nodes. This provides IP connectivity from the node to the CS-LAN. A CS-LAN consists of a pair of ERS 8600s.

One of the supported interfaces to the CS-LAN is via OC-12 links, unprotected, from each of two Multiservice Switch 15000 nodes. The two nodes are connected with a 1+1 protected inter-shelf link.

> ***Note:*** For a new customer deployment, Nortel recommends that you use a GE interface, not an OC-12 interface, to a CS-LAN.

The Multiservice Switch 15000 node connects to the CS-LAN via a synchronous optical network (SONET) port on a 4pOC12SmIrAtm FP card. The two ERS 8600s must be connected to two different Multiservice Switch 15000 nodes, via OC-12.

To configure the Multiservice Switch 15000 node for CS-LAN OC-12, use the Nodal Provisioning tool, and the *UA-IP IF-CSLAN-4pOC12SmIrAtm* template.

For the specific values to configure for a CS-LAN OC-12 link, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

CS-LAN GE interface (UA-IP)

In a UA-IP solution, you can connect Nortel Multiservice Switch 15000 nodes to a Communications Server LAN (CS-LAN), via a Gigabit Ethernet (GE) link. A CS-LAN consists of a pair of ERS 8600s.

This interface provides IP connectivity from a Multiservice Switch 15000 node to a CS-LAN. The interface is via GE links on a single Multiservice Switch 15000 node with protected routes.

> ***Note:*** For a new customer deployment, Nortel recommends that you use a GE interface, not an OC-12 interface, to a CS-LAN.

To configure the Multiservice Switch 15000 node for CS-LAN GE, use the Nodal Provisioning tool, and the following templates:

- *UA-IP IF-CSLAN-noLAG-4pGE*
- *UA-IP IF-CSLAN-LAG-4pGE*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values to configure for a CS-LAN GE link, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

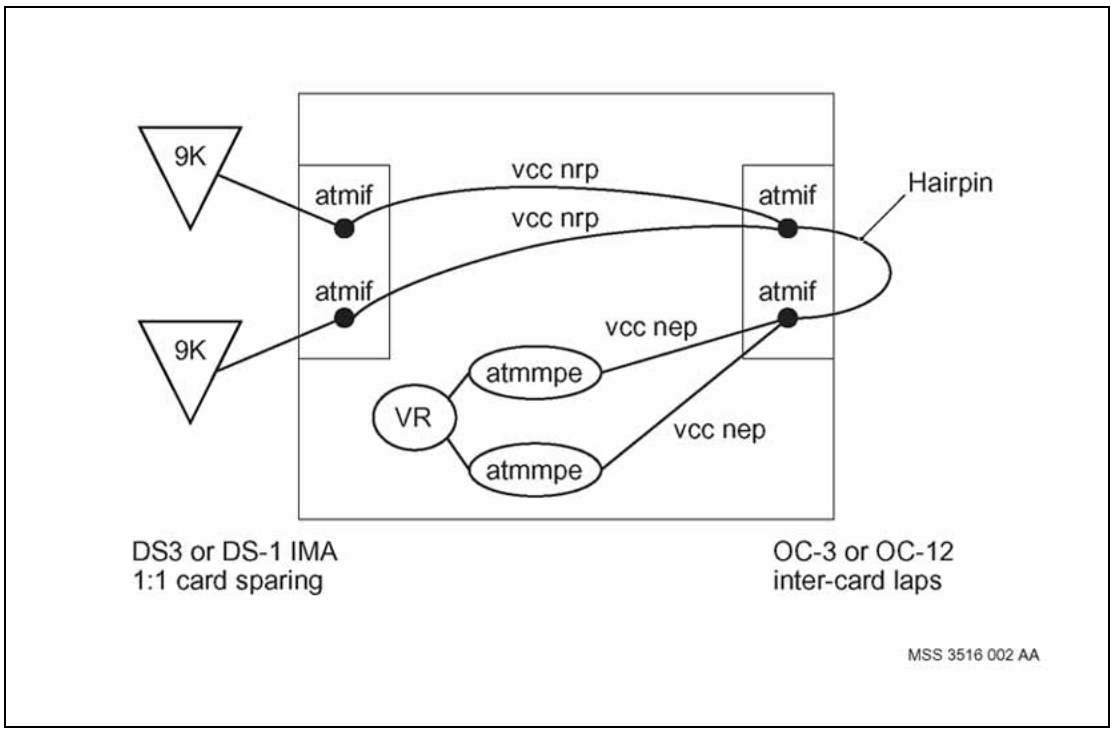
Hairpin ATM/IP OC-3/OC-12 interfaces (UA-IP)

In a Universal Access - IP solution, you must define an optical hairpin for a Nortel Multiservice Switch 15000 link to an MG9000 that uses either DS3 or inverse multiplexing for ATM (DS1-IMA). Deploy the optical hairpin in a Multiservice Switch 15000 node on a 4-port OC-3 or OC-12 ATM FP card.

An MG9000 STS-1/DS3 link uses a 12pDS3ATM FP card. An MG9000 DS1 IMA link uses a 4pDS3ChAtm (DS1 IMA) FP card. Neither of these FP cards supports carrier grade IP, therefore, these FPs can only terminate the ATM layer. For IP forwarding, you must use an optical hairpin.

For an illustration of a hairpin IP connection see "Optical hairpin IP connection" (page 72).

Optical hairpin IP connection



For an illustration of a hairpin IP connection used in a remote wire centre configuration, see "Example of remote wire centre and CS2000 site shelf configuration (UA-IP)" (page 46).

Deploy the optical hairpin on a pair of FP cards available expressly for this purpose, or else on a pair of optical cards with spare capacity.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

To configure a Hairpin ATM/IP interface, use the Nodal Provisioning tool, and either of the following templates:

- *UA-IP IF-Hairpin-4pOC12SmIrAtm*
- *UA-IP IF-Hairpin-4pOC3SmIrAtm*

For the specific values to configure for a Multiservice Switch 15000 hairpin ATM/IP interface, see the section on Hairpin ATM/IP link configuration in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (UA-IP)

In a UA-IP solution, you can connect the Media Gateway 15000 of a Nortel Multiservice Switch 15000 node to TDM equipment, with a pair of OC-3 TDM links.

To configure the OC-3 TDM, use the Nodal Provisioning tool, and either of the following templates:

- *UA-IP IF-TDM-4pOC3ChSmIr*
- *UA-IP IF-TDM-2pOC3ChSmIrVsp3-o*

For the specific values to configure for an OC-3 TDM link, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Media Gateway 15000 to MGC with H.248 (VSP3) interface (UA-IP)

In a UA-IP solution, you can connect Nortel Multiservice Switch 15000 nodes to a Media Gateway Controller (MGC) with H.248 via a pair of VSP3 FP cards. H.248 is the ITU-T gateway control protocol, one of the control interfaces used between the MGC and the Media Gateway.

To configure the interface of the Media Gateway card of a Multiservice Switch 15000 node to MGC with H.248, use the Nodal Provisioning tool, and the *UA-IP IF-MGC-H248-2pGeMmSrVsp3* template.

For the specific values to configure for this link to MGC with H.248, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Media Gateway 15000 to MGC with H.248 (VSP3-o) interface (UA-IP)

In a UA-IP solution, you can connect the Media Gateway card of a Nortel Multiservice Switch 15000 node to a Media Gateway Controller (MGC) with H.248 via a pair of either 2-port VSP3-o or 2pVSP4e FP cards. H.248 is the ITU-T gateway control protocol which is one of the control interfaces used between the MGC and the Media Gateway.

To configure the interface of the Media Gateway card of a Multiservice Switch 15000 node for MGC with H.248 using the 2-port VSP3-o FP card, use the Nodal Provisioning tool, and the *UA-IP IF-MGC-H248-2pOC3ChSmIrVsp3-o* template.

Media Gateway 15000 to MGC with H.248 (VSP3-o) interface (UA-IP) with IPSec

If you have elected to implement IPSec security, configuration of the interface to the MGC for call control connections between a switched MG node and an MGC in a Voice over IP (VoIP) solution is done using the Nodal Provisioning tool and the *IF-MGC-IPSEC-2pOC3ChSmIrVsp3-o* template. This template provisions the Ctrl/mg SecurityPolicyDatabase (spd) component structure that is required to add IPSec protection for the control connection to MGC on 2pOC3ChSmIrVsp3 FP's. The spd component is a sub-component of the Nsta and ctrl/mg component.

You must also use the template IF-MGC-IPSEC-ping-2pOC3ChSmIrVsp3-o to configure the policy components for the Ctrl/mg component which will allow ICMP pings to be sent and received on 2pOC3ChSmIrVsp3 FP's.

> ***Note:*** You must provision the *IF-TDM-2pOC3ChSmIrVsp3-o* template and the Nsta hierarchy before provisioning with the IPSec templates.

Refer to the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* for more information about an MGC with an H.248 link and IPSec.

TDM trunk distribution (UA-IP)

This section describes TDM trunk distribution on a Nortel Multiservice Switch 15000 Media Gateway node, in a UA-IP solution. It includes the following topics:

- "TDM trunk preparation (LAPS STS) (UA-IP)" (page 75)
- "TDM ISUP trunk (VSP3-o) (UA-IP)" (page 75)
- "TDM ISUP trunk (VSP3) (UA-IP)" (page 75)
- "TDM PRI trunk (VSP3) (UA-IP)" (page 77)
- "TDM PRI trunk profile (VSP3-o) (UA-IP)" (page 76)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "TDM PRI trunk (VSP3-o) (UA-IP)" (page 76)
- "TDM PRI trunk profile (VSP3) (UA-IP)" (page 76)
- "TDM PTS trunk profile (VSP3-o) (UA-IP)" (page 77)
- "TDM PTS trunk (VSP3-o) (UA-IP)" (page 77)

TDM trunk preparation (LAPS STS) (UA-IP)

In a UA-IP solution, you can provision TDM trunks on VSP cards on a Media Gateway. First, you must set up the STS components for the TDM trunks. The TDM trunks must be on either 4pOC3ChSmIr (TDM) or 2pOC3ChSmIrVsp3 (VSP3-o) FP cards.

Apply this provisioning at initial commissioning of Nortel Multiservice Switch 15000 nodes or on TDM slots, that are not in use, for later capacity growth.

To prepare the node for the TDM trunks on a TDM card, use the Nodal Provisioning tool and the *UA-IP TT-LapsSts-TDM* template:

For the specific values to configure for TDM trunk preparation, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM ISUP trunk (VSP3-o) (UA-IP)

In a UA-IP solution, you can provision TDM ISUP trunks on the VSP3-o cards of Media Gateway.

Use the Nodal Provisioning tool and the *UA-IP TT-ISUPTrunk-2pOC3ChSmIrVsp3-o* template to configure the node with the TDM ISUP trunks on a VSP3-o card.

For the specific values to configure for a TDM ISUP trunk, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM ISUP trunk (VSP3) (UA-IP)

In a UA-IP solution, you can provision an ISUP trunk on the VSP3 cards of Media Gateway.

Note: On a VSP3 card, the ISUP and PRI trunk settings are common.

To provision Nortel Multiservice Switch 15000 nodes for a TDM ISUP (VSP3) trunk, use the Nodal Provisioning tool, and the *UA-IP TT-ISUPTrunk-2pGeMmSrVsp3* template.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values to configure for a TDM ISUP trunk (VSP3), see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PRI trunk profile (VSP3-o) (UA-IP)

In a UA-IP solution, you can provision a TDM primary rate interface (PRI) trunk profile on the VSP3-o cards of Media Gateway. The PRI trunk profile is common to all PRI trunks on a VSP3-o FP card.

To provision Multiservice Switch 15000 nodes for the TDM PRI trunk profile, use the Nodal Provisioning tool, and the *UA-IP TT-PRIProfile -2pOC3ChSmIrVsp3-o* template.

For the specific values to configure for a TDM PRI trunk profile, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PRI trunk (VSP3-o) (UA-IP)

In a UA-IP solution, you can provision a TDM primary rate interface (PRI) trunk on the VSP3-o cards of Media Gateway.

To provision Multiservice Switch 15000 nodes for the TDM PRI trunk on VSP3-o, use the Nodal Provisioning tool, and the *UA-IP TT-PRITrunk -2pOC3ChSmIrVsp3-o* template.

For the specific values to configure for a TDM PRI trunk, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PRI trunk profile (VSP3) (UA-IP)

In a UA-IP solution, you can provision a TDM primary rate interface (PRI) trunk profile on the VSP3 cards of a Media Gateway.

To provision Multiservice Switch 15000 nodes for the TDM PRI (VSP3) trunk profile, use the Nodal Provisioning tool, and the *UA-IP TT-PRIProfile-2pGeMmSrVsp3* template.

For the specific values to configure for a TDM PRI trunk profile (VSP3), see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

TDM PRI trunk (VSP3) (UA-IP)

In a UA-IP solution, you can provision a PRI trunk on the VSP3 cards of Media Gateway.

> ***Note:*** On a VSP3 card, the ISUP and PRI trunk settings are common, or in other words, used for both.

To provision Nortel Multiservice Switch 15000 nodes for a TDM PRI (VSP3) trunk, use the Nodal Provisioning tool, and the *UA-IP TT-PRITrunk-2pGeMmSrVsp3* template.

For the specific values to configure for a TDM PRI trunk (VSP3), see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PTS trunk profile (VSP3-o) (UA-IP)

In a UA-IP solution, you can provision a Per-Trunk Signaling (PTS) trunk profile on the VSP3-o cards of Media Gateway. A PTS trunk profile is common to all PTS trunks using a specific profile on a VSP3-o FP card.

To provision Multiservice Switch 15000 nodes for the TDM PTS trunk profile (VSP3-o), use the Nodal Provisioning tool, and the *UA-IP TT-PTSProfile-2pOC3ChSmIrVsp-o* template.

For the specific values to configure for a TDM PTS trunk profile (VSP3-o), see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PTS trunk (VSP3-o) (UA-IP)

In a UA-IP solution, you can provision a Per-Trunk Signaling (PTS) trunk on the VSP3-o cards of Media Gateway.

To provision Multiservice Switch 15000 nodes for the TDM PTS trunk (VSP3-o), use the Nodal Provisioning tool, and the *UA-IP TT-PTSTrunk-2pOC3ChSmIrVsp3-o* template.

For the specific values to configure for a TDM PTS trunk (VSP3-o), see *Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2/PTIP*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Link Distribution (PT-IP)

The MDM manages the MG15000s over IP and is usually connected to the CS-LAN or some other management network that is connected to the CSLAN. The MG15000 cannot be managed through GE links, therefore, the CP Ethernet ports are connected to the CS-LAN (ERS8600s). In-band managed MG15000s are not used in the PT-IP solution.

This section describes link distribution between Media Gateway 15000 nodes and other network components, in a PT-IP solution. It includes the topics as follows:

- "IP Core/CS-LAN interface (PT-IP)" (page 78)
- "Media Gateway 15000 to MGC with H.248 (VSP3-o/2pVSP4e) interface (PT-IP)" (page 79)
- "TDM trunk distribution (PT-IP)" (page 80)

IP Core/CS-LAN interface (PT-IP)

In a PT-IP solution, you can connect Media Gateway 15000 nodes to a Communications Server LAN (CS-LAN), via a Gigabit Ethernet (GE) link. A CS-LAN consists of a pair of ERS 8600s.

IP Core/CS-LAN: The MG15000 connects to either the IP Core network (directly to two different edge routers) or a pair of ERS8600s. A pair of GE links are used for each VR, linked through the LAN. These links carry the bearer, control, and signaling traffic from the MG15000 to the destination MG15000 (or other standards compliant gateway) or CS-LAN (for signaling and control). Each link requires two IP addresses, one for the Vr Pp end and another for the router; hence a minimum of /30 netmask is required for each link. While the amount of traffic over the IP trunk links will vary, depending on the customer's deployment, the VRs are always engineered to be nonblocking in order to avoid any congestion scenarios.

This interface provides IP connectivity from a Media Gateway 15000 node to a CS-LAN. The interface is via GE links on a single Media Gateway 15000 node with protected routes.

To configure the Media Gateway 15000 node for CS-LAN GE, use the Nodal Provisioning tool, and the following templates:

- *PT-IP IF-IP-noLAG-4pGE*
- *PT-IP IF-IP-LAG-4pGE*

For GE links, the maximum 1+1 carrier grade configuration is 12096 trunks with six pairs of VSP3-o and one pair of 4pGe cards (two links each deployed). There are two aspects of the packetized voice traffic that must be engineered for:

- bandwidth: GE links can carry a finite number of bits per second, which translates into a finite number of voice calls, which use a constant

Copyright © 2006, Nortel Networks Nortel Networks Confidential

number of bits per second per call. Also, when the IP frames are transmitted across the cell-based fabric, each calls uses up a fix number of cells per second on the 4pGE cards fabric links.

- packet processing: the network processor on the 4pGE card can only forward a fixed number of voice packets per second.

For the specific values to configure for a CS-LAN GE link, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*

TDM OC-3 interfaces on the Multiservice Switch 15000 Media Gateway 15000 (PT-IP)

In a PT-IP solution, you can connect the Media Gateway 15000 node to TDM equipment, with a pair of OC-3 TDM links.

To configure the OC-3 TDM, use the Nodal Provisioning tool, and the one of the following templates:

- *PT-IP IF-OC3-TDM-2pOC3ChSmIrVsp3-o*
- *PT-IP IF-OC3-TDM-2pOC3ChSmIrVsp4e*

For the specific values to configure for an OC-3 TDM link, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* .

Media Gateway 15000 to MGC with H.248 (VSP3-o/2pVSP4e) interface (PT-IP)

In a PT-IP solution, you can connect the Media Gateway card of a Media Gateway 15000 node to a Media Gateway Controller (MGC) with H.248 via a pair of 2-port VSP3-o FP cards. H.248 is the ITU-T gateway control protocol which is one of the control interfaces used between the MGC and the Media Gateway.

To configure the interface of the Media Gateway 15000 node for MGC with H.248 using the 2-port VSP3-o FP cards, use the Nodal Provisioning tool, and the *IF-MGC-IPSec-2pOC3ChSmIrVsp3-o* template.

To configure the interface of the Media Gateway 15000 node for MGC with H.248 using the 2pVSP4e FP cards, use the Nodal Provisioning tool, and the *IF-MGC-IPSec-2pOC3ChSmIrVsp4e* template.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Media Gateway 15000 to MGC with H.248 (VSP3-o) interface (PT-IP) with IPSec

If you have elected to implement IPSec security, configuration of the interface to the MGC for call control connections between a switched MG node and an MGC in a Voice over IP (VoIP) solution is done using the Nodal Provisioning tool and the IF-MGC-IPSEC-2pOC3ChSmIrVsp3-o template. This template provisions the Ctrl/mg SecurityPolicyDatabase (spd) component structure that is required to add IPSec protection for the control connection to MGC on 2pOC3ChSmIrVsp3 FP's. The spd component is a sub-component of the Nsta and Ctrl/MG component.

> ***Note:*** You must provision the IF-TDM-2pOC3ChSmIrVsp3-o and the IF-MGC-H248-2pOC3ChSmIrVsp3-o templates before provisioning with the IPSec template.

Refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* and *NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management* for more information about an MGC with an H.248 link and IPSec.

TDM trunk distribution (PT-IP)

This section describes TDM trunk distribution on a Nortel Multiservice Switch 15000 Media Gateway node, in a PT-IP solution. It includes the following topics:

- "TDM trunk preparation (LAPS STS) (PT-IP)" (page 80)
- "TDM ISUP trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PRI trunk profile (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PRI trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 81)
- "TDM PTS trunk profile (VSP3-o/2pVSP4e) (PT-IP)" (page 82)
- "TDM PTS trunk (VSP3-o/2pVSP4e) (PT-IP)" (page 82)

TDM trunk preparation (LAPS STS) (PT-IP)

In a PT-IP solution, provision TDM trunks on VSP cards on a Media Gateway. First, you must set up the STS components for the TDM trunks. The TDM trunks must be on either the 2pOC3ChSmIrVsp3-o (VSP3-o) or 2pOC3ChSmIrVsp4e (2pVSP4e) FP cards.

To prepare the node for the TDM trunks on a TDM card, use the Nodal Provisioning tool and the *PT-IP TT-Sts-TDM-VSP* template or for the E1 solution use the *PT-IP IF-STM1-TDM-2pOC3ChSmIrVsp* template

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For the specific values to configure for TDM trunk preparation, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* .

TDM ISUP trunk (VSP3-o/2pVSP4e) (PT-IP)

In a PT-IP solution, you can provision TDM ISUP trunks on the VSP3-o or 2pVSP4e cards of Media Gateway. ISUP trunks can be configured one at a time, 28 at a time for North American DS1s, or 63 at a time for International E1s.

Use the Nodal Provisioning tool and the following templates to configure the node with the TDM ISUP trunks on a VSP3-o or 2pVSP4e FP cards.

- *PT-IP TT-ISUP-DS1-Trunk*
- *PT-IP TT-ISUP-E1-Trunk*
- *PT-IP TT-ISUP-28DS1-Trunk*
- *PT-IP TT-ISUP-63E1-Trunk*

For the specific values to configure for a TDM ISUP trunk, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PRI trunk profile (VSP3-o/2pVSP4e) (PT-IP)

In a PT-IP solution, you can provision a TDM primary rate interface (PRI) trunk profile on the VSP3-o or 2pVSP4e FP cards of Media Gateway. The PRI trunk profile is common to all PRI trunks on the VSP3-o/2pVSP4e FP cards.

To provision Multiservice Switch 15000 nodes for the TDM PRI trunk profile, use the Nodal Provisioning tool, and the PT-IP TT-PRI-Profile template.

For the specific values to configure for a TDM PRI trunk profile, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* .

TDM PRI trunk (VSP3-o/2pVSP4e) (PT-IP)

In a PT-IP solution, you can provision a PRI trunk on the VSP3-o/2pVSP4e cards of Media Gateway.

To provision Media Gateway 15000 nodes for a TDM PRI (VSP3-o) trunk, use the Nodal Provisioning tool, and the PT-IP *TT-PRI-DS1-Trunk-VSP* or *PT-IP TT-PRI-E1-Trunk-VSP* template, respective of the configuration.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

For the specific values to configure for a TDM PRI trunk (VSP3), see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* .

TDM PTS trunk profile (VSP3-o/2pVSP4e) (PT-IP)

In a PT-IP solution, you can provision a Per-Trunk Signaling (PTS) trunk profile on the VSP3-o/2pVSP4e cards of Media Gateway. A PTS trunk profile is common to all PTS trunks using a specific profile on the VSP3-o/2pVSP4e FP cards.

To provision Multiservice Switch 15000 nodes for the TDM PTS trunk profile, use the Nodal Provisioning tool, and the *PT-IP TT-PTSProfile* template.

For the specific values to configure for a TDM PTS trunk profile, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

TDM PTS trunk (VSP3-o/2pVSP4e) (PT-IP)

In a PT-IP solution, you can provision a Per-Trunk Signaling (PTS/Cas) trunk on the VSP3-o/2pVSP4e cards of Media Gateway.

To provision Multiservice Switch 15000 nodes for the TDM PTS trunk, use the Nodal Provisioning tool, and the *PT-IP TT-PTS-DS1* or the *PT-IP TT-PTS-E1 Trunk* template.

For the specific values to configure for a TDM PTS trunk, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Overview of MDM server deployment and configuration

Nortel Multiservice Data Manager (MDM) is one of the network element management tools used in Carrier VoIP networks. It performs:

- fault management
- configuration management
- performance management
- security management

It does this for the ATM network and the IP network in the following solutions:

- Packet Trunking - AAL1 (PT-AAL1)
- Universal Access - AAL1 (UA-AAL1)
- Universal Access - IP (UA-IP)
- Packet Trunking - AAL2 (PT-AAL2)
- Packet Trunking - IP (PT-IP)

In addition, MDM provides data feed of fault and performance information to a higher-level management system for additional processing. MDM software is installed on servers that are connected through IP connectivity to Multiservice Switch 15000 nodes.

MDM servers are deployed using Sun Netra 240 hardware platforms with Server Platform Foundation Software (SPFS). Some MDM server configurations (client-set servers, Admin Servers and consolidated management servers) can also be deployed using the legacy Sun Fire V480 hardware platform.

The MDM can also be configured to host server configurations that provide centralized authentication and authorization for deployments of the Operator Client application in a VoA network. See "Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client applicatio" (page 125).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

In a secured VoIP network, centralized AAA is configured on the Integrated EMS. Some configuration is required on the MDM to allow Operator Client sessions and MDM Toolset sessions to access the Integrated EMS for authentication and authorization. See *NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* for more information.

The MDM can also be configured to provide consolidated network management for both VoA and VoIP networks using centralized or dedicated network management deployments. A hierarchical topology of MDM consolidated management (CM) servers partitions the network according to geographic, traffic, or other network management needs. The consolidated management servers aggregate fault management data from the MSS/MG15000 switches in the network partition into regional and entire network views, and provide configuration management of the associated MSS/MG15000 nodes. For more information on consolidated management (CM) server deployment, see "Deployment of MDM servers for the consolidated network management approach" (page 131)

Where MDM connections to other MDM server or to a higher-level management system are not secured using IPSec or SSH, SunScreen firewall software can be deployed on the MDM server to provide congestion controls to counter denial of service attacks. For more information, see SunScreen software deployment and configuration.

The term higher-level management system, as used in this document, refers to the application that provides additional processing of fault and performance information. In a voice over IP (VoIP), or UA-IP or PT-IP, solution, this is the Integrated Element Management System (IEMS). In a voice over ATM (VoA), or PT-AAL1 or UA-AAL1, solution, this is the SuperNode Data Manager (SDM). The higher-level management system can also be a customer operational support system (OSS), the nature of which depends on the particular customer environment.

For more information about integrated EMS, see the integrated EMS documentation suite for this release.

For more information about SDM, see the SDM documentation suite for this release.

For more information about performance data flow to a higher-level management system, see *NN10158-711 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Performance PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

The following sections contain information about MDM server deployment and configuration:

- "MDM server deployment scenarios" (page 85)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "Overview of MDM server deployment" (page 111)
- "Deployment of servers using the dedicated network management approach" (page 113)
- "Deployment of MDM servers using the centralized network management approach" (page 116)
- "Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client applicatio" (page 125)
- "Deployment of MDM servers for the consolidated network management approach" (page 131)
- "Auto-patching for MSS/MG15000 nodes from the MDM" (page 133)
- "MDM server configuration for Ethernet Routing Switch 8600 fault management (PT-AAL1 and UA-AAL1)" (page 138)
- "Deploying MDM servers with Server Platform Foundation Software (SPFS)" (page 146)

MDM server deployment scenarios

The tables in this section list Nortel Multiservice Data Manager server deployment scenarios for the management of Nortel Multiservice Switch nodes. These tables also list MDM software applications that need to be running on the servers for each of these scenarios.

For more information on the MDM server deployment scenarios, see *241-6001-310 Nortel Multiservice Data Manager Server Reference*.

The following sections contain tables with MDM server and software application information:

- "Servers required on the various workstations" (page 85)
- "Client-set servers" (page 110)
- "MDP servers" (page 109)
- "Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client applicatio" (page 125)

Servers required on the various workstations

"Required servers on all workstations" (page 87) list the various servers and software applications for each of the following MDM deployments.

- MDM standalone server

  MDM workstation that is configured to support the main server processes to perform surveillance, network data gathering (fault, security, and/or performance), configuration, and distribution of network data to higher level management system in the network. This MDM

Copyright © 2006, Nortel Networks Nortel Networks Confidential

deployment provides X11 access from remote and local operator desktops to the MDM Toolset user environment.

- MDM server-set

  MDM workstations configured in sets that collectively run the complete set of fault, configuration, and performance management for the network. The MDM server-set supports the main server processes for performing surveillance, network data gathering (fault, security, and/or performance), and distribution of network data to higher level management systems. Server-sets can be configured to host specific types of server processes according to network needs. The MDM client-sets that connect, through X11, to theMDM server-sets run on different workstations and provide the necessary hardware, GUI, and CLI tools for operator access.

- MDM client-set

  MDM workstations that run a small set of MDM processes for X11 desktop applications to connect to the MDM server-set. The MDM client-set uses the MDM Service Selection feature. For a large network, you may elect to run client-set and server-set configurations to reduce the traffic load, caused by operator interaction with the system, on the server-sets. The client-set/server-set deployment off loads the GUIs, locally, to your operator base on the MDM desktop application from the MDM server-set. To use Service Selection feature, refer to Service Selection sections in NN10400-300,*NN10400-300 Nortel Multiservice Data Manager Administration Tools*.

- MDM Admin Server

  MDM workstation that includes the Security Server and JAVA Web Start packages to provide centralized AAA with Operator Client desktop access in a VoA solution. The MDM Admin Server is deployed with the MDM server-set. For more information, see "Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client applicatio" (page 125).

- MDM Server

  MDM workstation that includes server-set functionality, and supports connection to the IEMS server for centralized AAA. The MDM Server supports the MDM Toolset environment and hosts the JAVA Web Start (JWS) software for Operator Client access.

- MDM consolidated management (CM) server

  MDM servers that aggregate fault management data from lower level MDM servers in a consolidated management hierarchy topology, and provide configuration management access to the MDM servers managing the MSS/MG15000 switches in the hierarchy. A CM server

Copyright © 2006, Nortel Networks Nortel Networks Confidential

supports the MDM Toolset environment and hosts the JAVA Web Start (JWS) software for Operator Client access.

For more information about MDM deployments, refer to *NN10028-111 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

For more information about the software applications appearing in the following table, refer to *241-6001-310 Nortel Multiservice Data Manager Server Reference*. Other documents with information about specific software applications are noted in the table where applicable.

For more information about attributes and configured values, refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Required servers on all workstations

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Fault Management						
Data Management Agent (dma)	Yes	Yes	Yes	Yes	Yes	dma is used for global alarm clear.
FMDR	Yes	Yes	Yes	Yes	No	FMDR provides surveillance connections between MDM and Multiservice Switch 15000 nodes.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
GMDR	Yes	Yes	Yes	Yes	Yes	GMDR is part of the fault surveillance stack that merges all the data flow from OAMCs and FMDRs, on both the local and redundant workstation.
IP Discovery Server (ipdsvr)	Yes	Yes	Yes	No	No	If IP Discovery is used for ERS 8600 enrolment, ipdsvr is required.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Network Data Access Mediator (NDAM)	Yes	Yes	Yes	Yes	Yes	NDAM provides fault management data to high-level applications, IEMS and SDM.
Network Model co-ordinator	Yes	Yes	Yes	Yes	Yes	Network Model software applications are part of the Network Model support system. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

Copyright © 2006, Nortel Networks

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Network Model edit server (EDSERVER)	Yes	Yes	Yes	Yes	Yes	EDSERVER lets you edit network models using the Network Viewer tool. To use Network Viewer in edit mode, both the EDSERVER and NMSERVER must be running. Security must also be configured, and there are multiple levels of security possibilities.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Network Model server	Yes	Yes	Yes	Yes	Yes	The server responsible for handling API requests from the Network Model Provider utility. It provides information from the Network Model utility to the fault tools. and gives access to information about the active surveillance network model. NMSERVER communicates with Network Model Provi

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						der through the IPI interface, which is an IPC version of API protocol
Network Model Surveillance updater (SURNUP)	Yes	Yes	Yes	Yes	Yes	SURNUP server is the MDM server responsible for keeping the active network model up-to-date with current component state information. It receives component state information from a GMDR server that maps states,

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						component status, and alarms from the network into a raw component state.
psvagent	Yes	Yes	Yes	Yes	No	For the MSS Shelf View tool to work, the psv agent (with no parameter) is required. PSVAGENT gathers information about devices and passes it to the Shelf View application.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
RTAC	Yes	Yes	Yes	Yes	Yes	RTAC collects all the alarms received by MDM servers that originate on Multiservice Switch nodes, and stores them in a file. The operator can access this file to perform historical searches.
SMDR	Yes	Yes	Yes	Yes	No	If MDM manages the Ethernet Routing Switch 8600, SMDR provides surveillance connections between MDM

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						servers and ERS 8600 nodes.
TSVR	Yes	Yes	Yes	No	No	If MDM manages the Ethernet Routing Switch 8600, TSVR receives traps from ERS 8600 nodes.
System/base						
Communication Manager (FTDM)	Yes	Yes	Yes	Yes	Yes	Communication Manager manages all the Multiservice Switch connections.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Context server	Yes	Yes	Yes	Yes	Yes	Context server allows the sharing of information between applications to reduce keystrokes.
Host Group Directory Server (HGDS)	Yes	Yes	Yes	Yes	No	HGDS defines groupings of Multiservice Switch nodes into offices. This application is used by FMDR, PMSP, and the Command Console.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
MNSD agent	Yes	Yes	Yes	Yes	Yes	MNSD agent exchanges service names between applications so that socket numbers do not need to be configured elsewhere.
MNSD level 2	No	Yes	Yes	Yes	Yes	MNSD level 2 provides the respective port of the MDM server process in the selected host to the remote client applications. This allows an application to connect to the server pro

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						cess autom atically.
NTP	Yes	Yes	Yes	No	Yes	NTP synch ronize s the MDM time with a central time server and suppor ts MSS nodes that request time synch roniz ation. The MDM NTP server is req uired only whe n the MDM is not ins talled on the SPFS works tation (SPFS provid es its own NTP)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
OAMC (Log Collector)	Yes	Yes	Yes	Yes	Yes	OAMC injects alarms into the work station for servers when SVM has a server failure. The OAM log collector collects security audit logs (SAL's) from the local platform and displays them on the System Log Display tool for use in debugging MDM applications. For OAMC to function correctly, it must

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						connect to GMDR.
SALCserver	Yes	Yes	Yes	Yes	No	The SALC server can be paired with an FMDR and does not need to connect to GMDR.
Workstation surveillance	Yes	Yes	Yes	Yes	Yes	Workstation surveillance monitors disk, CPU, memory utilization and Ethernet utilization on the local system and monitors connectivity to other MDM systems.
Configuration Management						

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Backup controller	Yes	Yes	Yes	Yes	No	The Backup Controller and PP Backup Provider must be started as a pair. The Backup Controller receives requests from the MSS/MG15000s and SNMP Backup tools (GUI and CLI) and connects to the PP Backup Provider.
Data Synchronization Server	Yes	Yes	Yes	Yes	No	
MSS Command Access Server (PPAccessServer)	Yes	Yes	Yes	Yes	Yes	

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
MSS Config Model Server (pcms)	Yes	Yes	Yes	Yes	No	Config Model server controls shared memory for Multiservice Switch nodal provisioning applications.
NP configuration manager	Yes	Yes	Yes	Yes	No	NP Config server and NP Config Manager support the Multiservice Switch nodal provisioning applications.
NP configuration server	Yes	Yes	Yes	Yes	No	
PP Backup provider	Yes	Yes	Yes	Yes	No	See Backup Controller.
PP Restore provider	Yes	Yes	Yes	Yes	No	See Restore Controller.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Pserver	Yes	Yes	No	Yes	No	Pserver connects an MDM API (Network Model, Alarms and Status) to a specific IP socket on the MDM workstation. For more information, see *241-6001-201 Nortel Multiservice Data Manager Network Model API Reference*. This application communicates alarms to the higher-level manag

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						ement system .
Restore controller	Yes	Yes	Yes	Yes	No	The Restore Controller and PP Restore Provider must be started as a pair. The Restore Controller receives requests from the MSS/MG15000s and SNMP Backup tools (GUI and CLI) and connects to the PP Restore Provider.
Performance Management						

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
Data Viewer Agent (PMAGENT)	Yes	Yes	Yes	Yes	Yes	Data Viewer tool lets you collect and display real-time performance information for the MSS, Multiservice Provider Edge (MPE), and SNMP devices in the network.
PMSP Server	Yes	Yes	No	Yes	No	PMSP server is used in Carrier VoIP networks to collect and convert PM statistics from MSS processors, cards, IP interfaces, VSP

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						processors, and ATM interfaces.
Security and Centralized AAA						
GMDRAGENT	Yes	Yes	Yes	Yes	Yes	If you have elected to use Operator Client in your network, this agent is required on the MDM for fault and operator console.
Network Model Agent (NMAGENT)	No	No	Yes	Yes	Yes	If you have elected to use Operator Client in your network, this agent is required on the MDM for fault and

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						operator console.
RADIUS Interface (RADIUS Proxy)	No	No	Yes	No	No	Used for authentication of the MSS/MG15000.
RTACAGENT	No	No	Yes	Yes	Yes	If you have elected to use Operator Client in your network, this agent is required on the MDM for fault and operator console.
secureFTPD	Yes	Yes	Yes	Yes	Yes	The secure FTP daemon between MDM servers and Multiservice Switch nodes

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						that encrypts the FTP transmissions.
Sun One IS	No	No	Yes	No	No	Used to direct authentication and authorization requests in networks that use the Operator Client application and Central AAA.
Sun One IS	No	No	Yes	No	No	The central database where each userID and its associated password are stored and maintained when

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Names in MDM Server Administration tool	Standalone server	Server-set or PM server	MDM Admin Server (VoA)	MDM Server (VoIP)	CM server	Notes
						Central AAA is used.
JWS	No	No	Yes	Yes	Yes	JWS server only if OC is installed.

MDP servers

To manage the Management Data Provider (MDP) servers, use the Server Administration tool. See the table "MDP servers" (page 109) for information about the Server Administration tool options.

For more information about using the Server Administration tool to manage MDP servers, see *241-6001-309 Nortel Multiservice Data Manager Management Data Provider*. Also, in the table "MDP servers" (page 109), see the Comments column for names of other useful reference documents, where available.

For more information, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

MDP servers

Server Administration tool option	Standalone server	Server-set or PM server	MDM Admin Server	Comment
MDP Data Model Manager (mdpdmm)	Yes	Yes	Yes	This server manages the MDP Data Model Manager.
MDP Disk Manager (mdpdiskmgr)	Yes	Yes	Yes	This server manages the disk utilization of MDP files on MDM servers.
MDP File Mover Manager (mdpfmmgr)	Optional	Optional	Optional	This server manages the MDP File Mover.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Server Administration tool option	Standalone server	Server-set or PM server	MDM Admin Server	Comment
MDP MSS File Manager (mdpppmgr)	Yes	Yes	Yes	This server manages the node file manager used by MDP.
MDP MSS Prober Manager (mdpfpmgr)	Yes	Yes	Yes	This server manages the collection of spooled node data.
MDP Statistics Retrieval System (MDPSRS)	Yes	Yes	Yes	MDPSRS polls nodes for non-spooled real-time statistical information. Statistic records are converted to bulk data format (BDF) and transferred to a performance or billing host for down-stream processing.

Client-set servers

This MDM server is used to reduce the load caused by operator use on the MDM server-set workstations. Any workstation with MDM software can run an MDM client-set and connect to the MDM server-set using the MDM Service Selection feature. The table below lists the MDM configuration required on a MDM client-set.

For more information about the software applications appearing in the following table, refer to *241-6001-310 Nortel Multiservice Data Manager Server Reference*. For more information about attributes and configured values, refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Configuration servers

Software application	Comments
Context server	This server allows the sharing of information between applications to reduce keystrokes
GMDR	MDM server-set GMDR connects as lower-level GMDR to this client-set GMDR. You can select to connect to all or some of the GMDR in a server-set depending on your choice to view the entire network or part of it.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Software application	Comments
Log Collector (OAMC)	Log Collector (OAMC) injects alarms into the workstation for servers when SVM has a server failure. The OAM log collector collects security audit logs (SAL's) from the local platform and displays them on the System Log Display tool for use in debugging MDM applications. For OAMC to function correctly, it must connect to GMDR.
MNSD level 2	MNSD level 2 communicates with the remote MDM hosts to track the service name and socket number of their MDM server processes. It feeds the information to MNSD agent and allows an application to connect to the server remotely and automatically. Do not include MDM client-set host in the command parameter.
MNSD agent	MNSD agent exchanges service names between applications so that socket numbers do not need to be configured elsewhere.
Workstation surveillance	Workstation surveillance monitors disk, CPU, memory utilization and Ethernet utilization on the local system and monitors connectivity to other MDM systems.

Overview of MDM server deployment

Nortel Multiservice Data Manager (MDM) servers are deployed using either the dedicated or centralized network management approach during the initial installation. In the dedicated network management approach, each office requires a pair of MDM servers while in the centralized network management approach, a single pair of MDM servers can manage the MSS15000/MG15000 nodes in several offices.

MDM servers can be migrated from the dedicated to the centralized network management approach while in-service if you want only one pair of MDM servers to manage the MSS15000/MG15000 nodes in several offices.

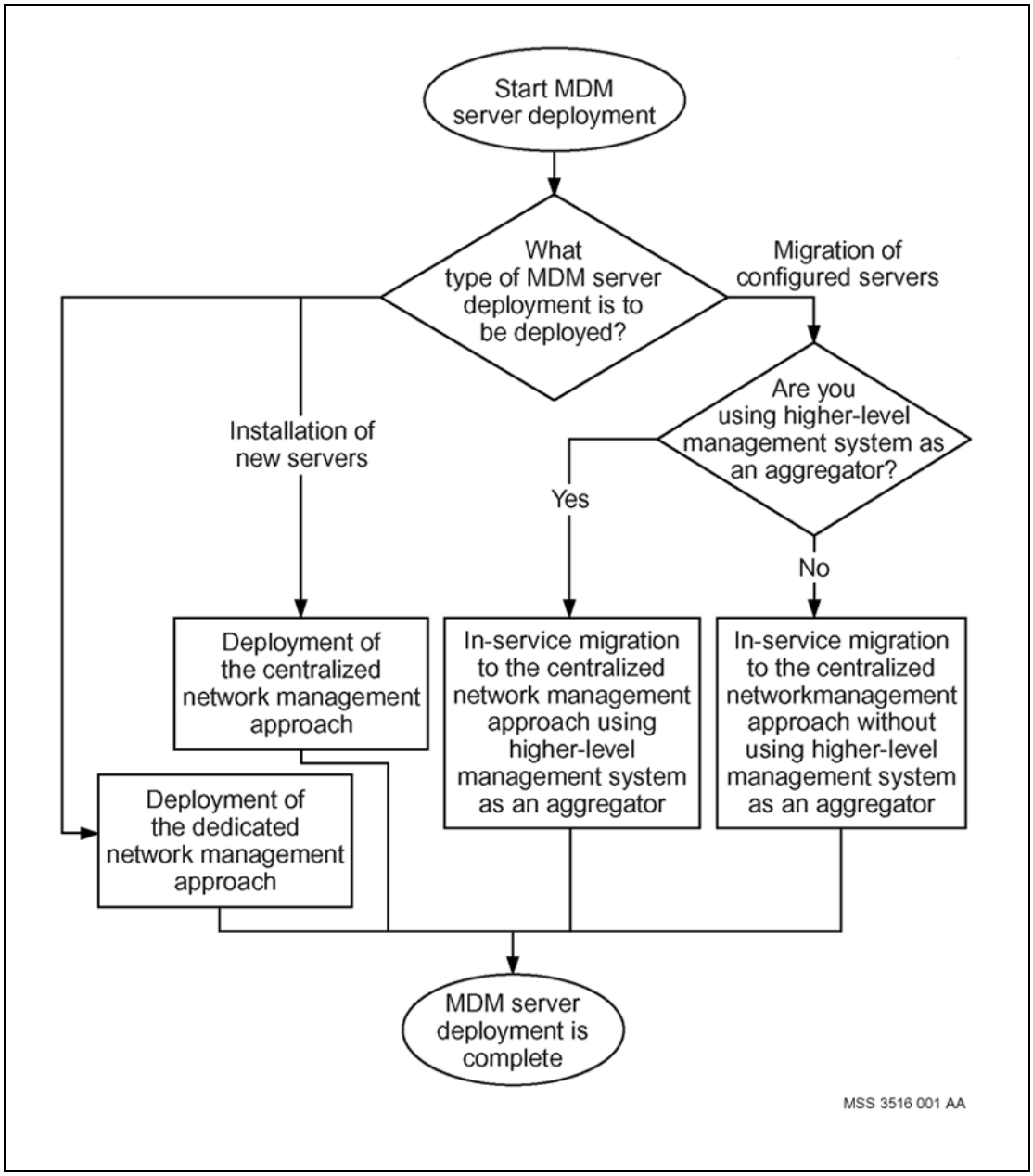
In-service migrations of MDM servers from the dedicated to centralized network management approach follow one of two methods. The choice of method to follow depends on whether you want to use the higher-level management system as an aggregator. See "Deployment of servers" (page 111).

Deployment of servers

This section shows you the sequence of tasks involved in deploying Nortel MDM servers in either the dedicated or centralized network management approach during an initial installation or as part of an in-service migration. To link to any procedure, go to "Methods for deploying servers" (page 112).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Deployment of servers



Prerequisites for deploying servers using the dedicated network management approach

See the requisite information in the Installation Method document that describes Nortel MDM software loading and configuration.

Methods for deploying servers

- "Deployment of servers using the dedicated network management approach" (page 113)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Deployment of MDM servers using the centralized network management approach" (page 116)
- "In-service migration of MDM servers to the centralized network management approach without using the" (page 120)
- "In-service migration of MDM servers to the centralized network management approach using the higher-" (page 122)

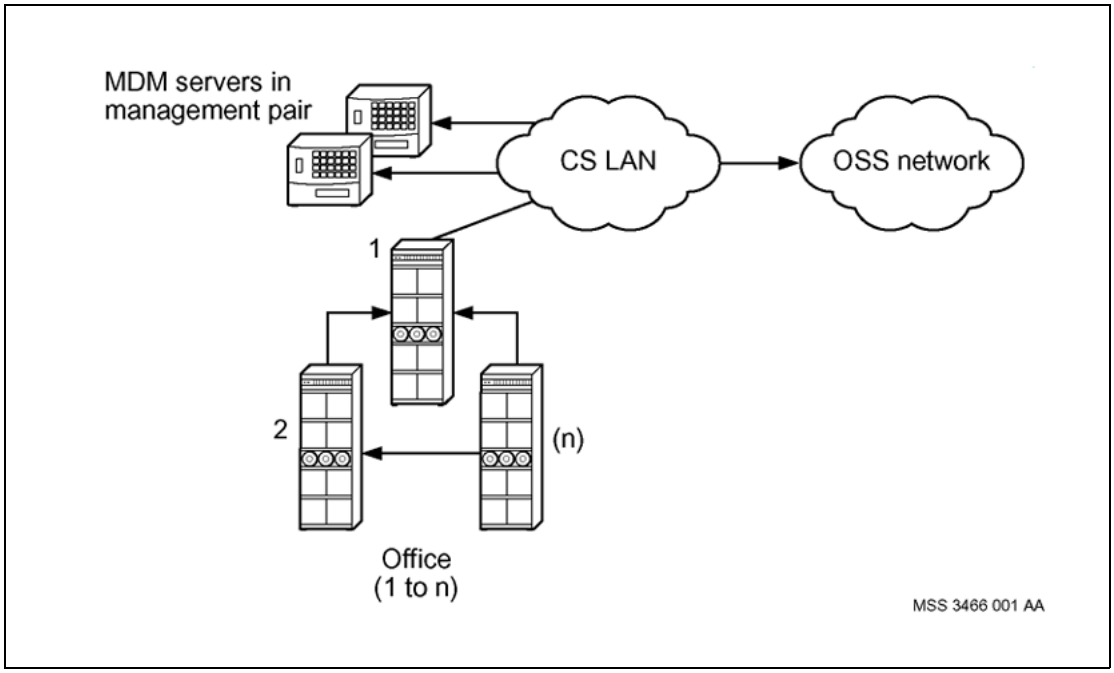
Deployment of servers using the dedicated network management approach

In the dedicated network management approach, each office requires a pair of Nortel Multiservice Data Manager servers to manage the MSS15000/MG15000 nodes in that office. See the "Servers deployed using the dedicated network management approach" (page 113).

- "Prerequisites for deploying servers using the dedicated network management approach" (page 112)
- "Deploying servers using the dedicated network management approach task" (page 114)

Note: The deployment of MDM servers is performed by representatives from Nortel GNPS as part of the initial installation.

Servers deployed using the dedicated network management approach



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Prerequisites for deploying servers using the dedicated network management approach

See the requisite information in the Installation Method document that describes Nortel Multiservice Data Manager software loading and configuration.

Deploying servers using the dedicated network management approach task

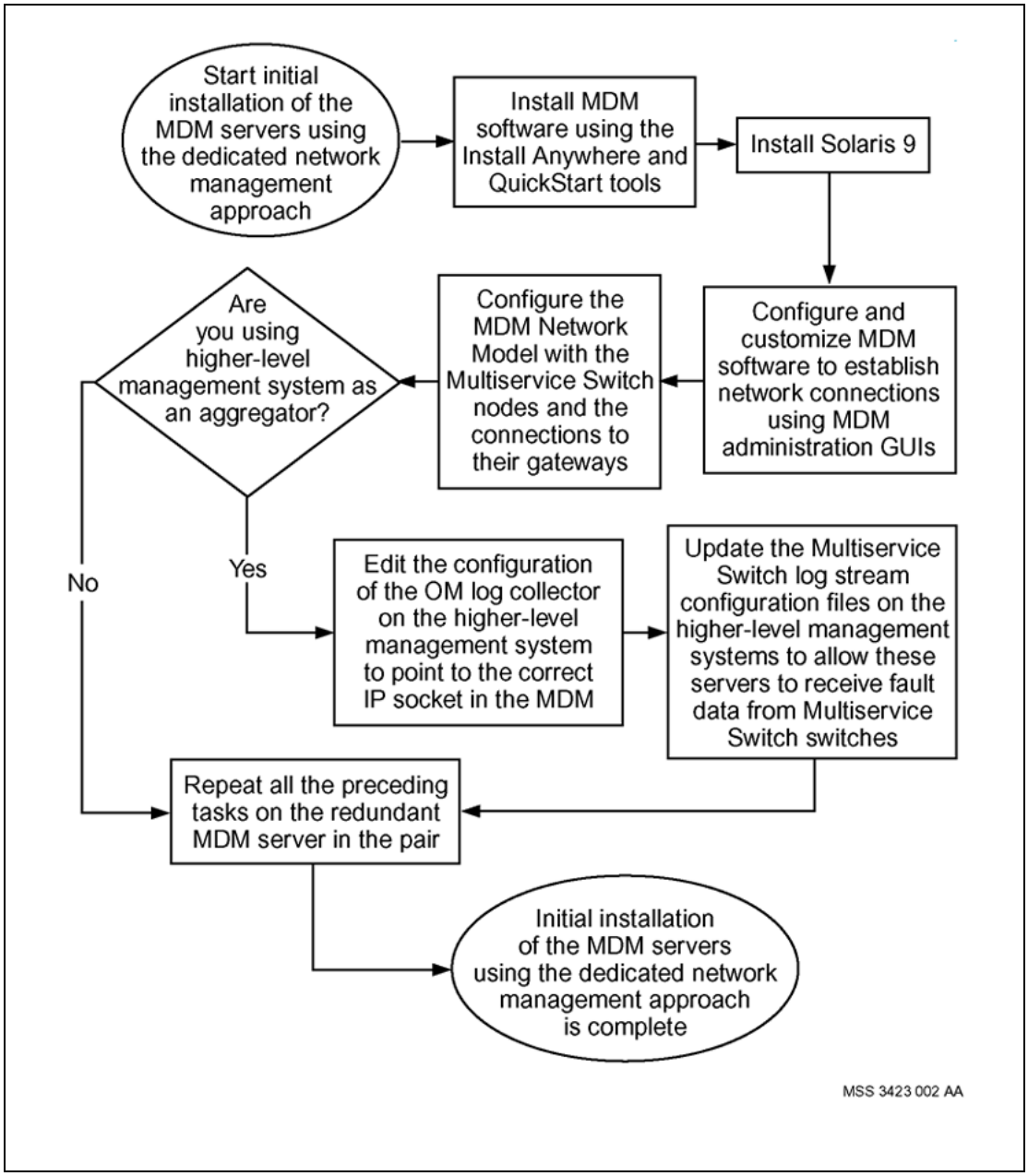
The "Deployment of servers using the dedicated network management approach task flow" (page 115) shows you the sequence of tasks performed to deploy Nortel MDM servers using the dedicated network management approach for the following solutions:

- Packet Trunking - AAL1
- Universal Access - AAL1
- Packet Trunking - AAL2
- Universal Access - IP

For additional information on the tasks, go to "Task flow references" (page 115).

Copyright © 2006, Nortel Networks

Deployment of servers using the dedicated network management approach task flow



Prerequisites to deploying servers using the centralized network management approach

See the requisite information in the Installation Method document that describes MDM software loading and configuration.

Task flow references

- Loading MDM software. See *241-6001-100 Nortel Multiservice Data Manager Software Installation and Initial Configuration*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- Installing Solaris. See *NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.
- Configuring server software with the QuickStart tool. See *241-6001-100 Nortel Multiservice Data Manager Software Installation and Initial Configuration*. Configuring servers for Nortel Multiservice Switch nodes. See *241-6001-303 Nortel Multiservice Data Manager Administration*. Configuration. See *241-6001-309 Nortel Multiservice Data Manager Management Data Provider*.
- Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
- Installing and configuring the log delivery application. For voice over ATM (VoA) (UA-AAL1 and PT-AAL1), see Configuration Management in the SDM documentation suite for this release. Log delivery application overview. See Product Overview in the SDM documentation suite for this release. For voice over IP (VoIP) (UA-IP and PT-IP), see the integrated EMS documentation suite.

Deployment of MDM servers using the centralized network management approach

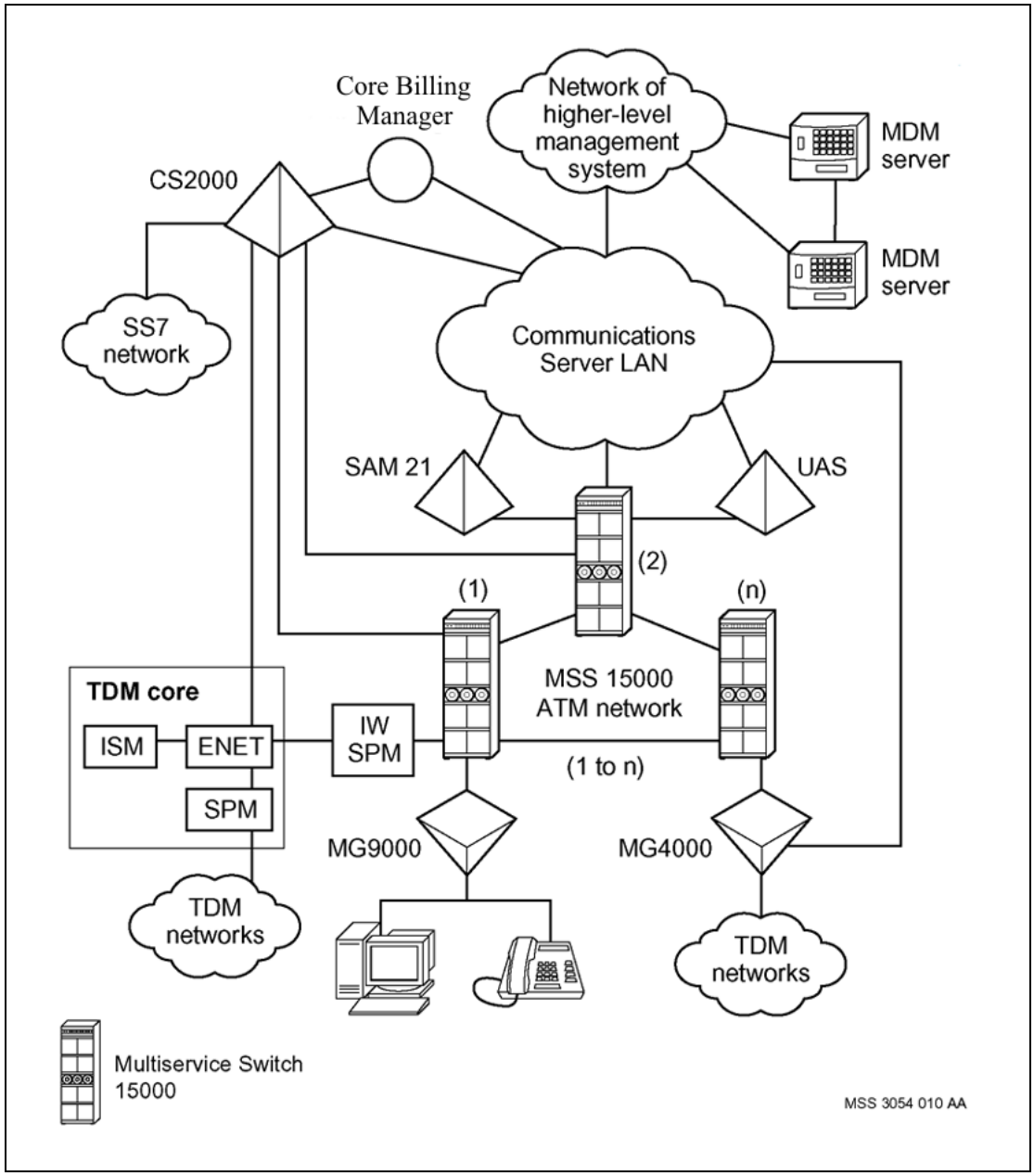
In the centralized network management approach for deploying Nortel MDM servers a single pair of servers can manage the Nortel Multiservice Switch nodes in several offices. The reduction of the number of pairs of servers needed to manage the offices in a network results in a cost reduction for the customer.

See the "Deployment of servers using the centralized network management approach task flow" (page 119). This figure displays the centralized OAM for a network consisting of one office. A second office could be connected to the pair of servers pictured in the figure.

- "Prerequisites to deploying servers using the centralized network management approach" (page 115)
- "Task flow references" (page 119)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Servers deployed using the centralized network management approach



Prerequisites to deploying servers using the centralized network management approach

See the requisite information in the Installation Method document that describes MDM software loading and configuration.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

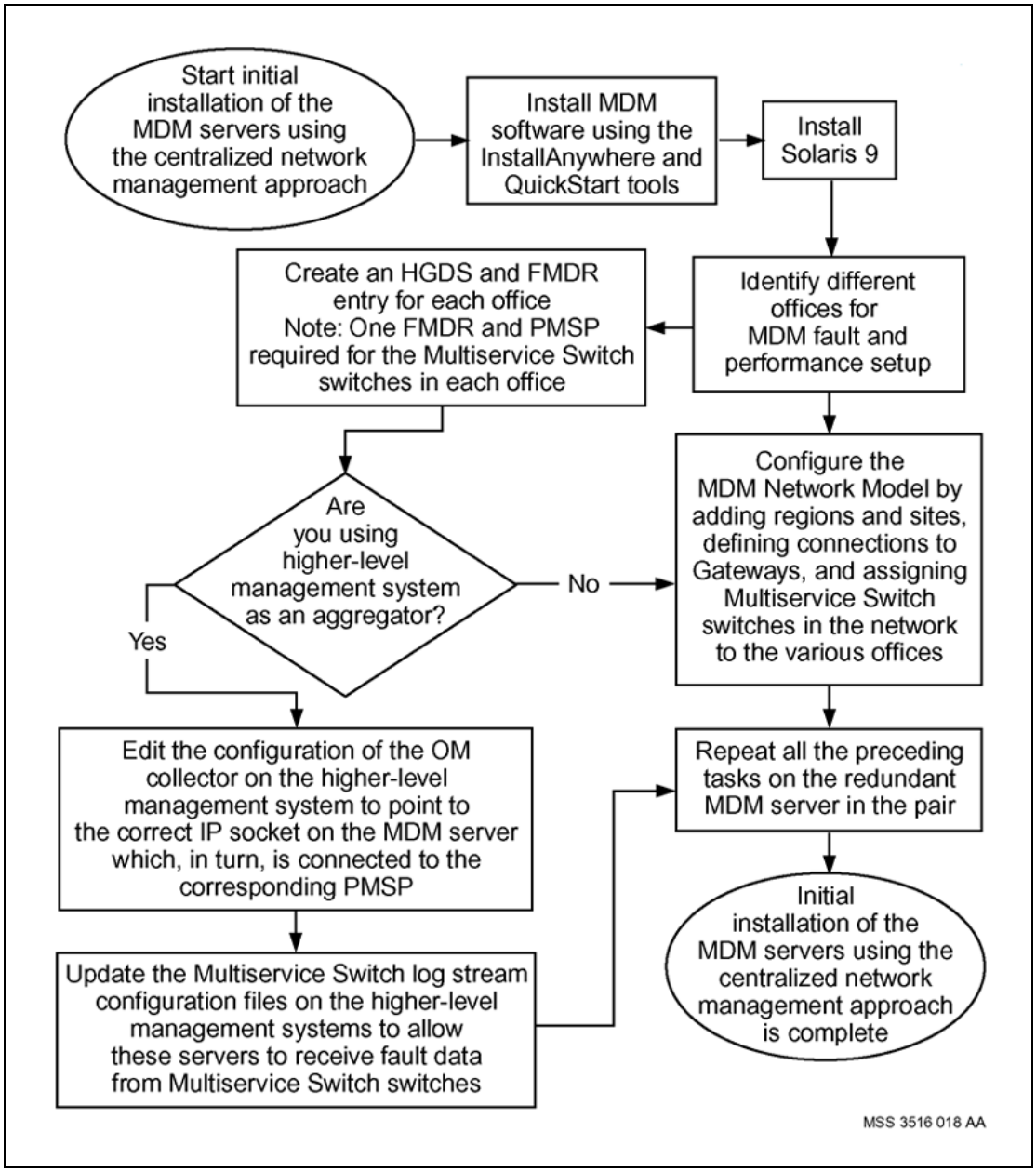
Deploying servers using the centralized network management approach task

The "Deployment of servers using the centralized network management approach task flow" (page 119) shows you the sequence of tasks performed to deploy Nortel MDM servers using the centralized network management approach for the Packet Trunking - AAL1, Universal Access - AAL1, or Universal Access - IP solutions. For additional information on the tasks, go to "Task flow references" (page 119).

Note: The centralized network management approach for deploying MDM servers can be used with the Packet Trunking - AAL1 solution which employs higher-level management system aggregation. This approach can also be used with the Universal Access - AAL1, and Universal Access - IP solutions, in which the server is directly connected to the OSS network.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Deployment of servers using the centralized network management approach task flow



Task flow references

- Loading MDM software. See *241-6001-100 Nortel Multiservice Data Manager Software Installation and Initial Configuration*.
- Installing Solaris. See *NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.
- Configuring MDM software with the QuickStart tool. See *241-6001-100 Nortel Multiservice Data Manager Software Installation and Initial*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuration. Configuring servers for Nortel Multiservice Switch nodes and FMDR server redundancy for surveillance access. See *241-6001-303 Nortel Multiservice Data Manager Administration*. Configuration. See *241-6001-309 Nortel Multiservice Data Manager Management Data Provider*.

- Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
- Edit the configuration of the OM log collector. See the SDM documentation.
- Installing and configuring the log delivery application. See Configuration Management in the SDM documentation suite for this release. Log delivery application overview. See Product Overview in the SDM documentation suite for this release. For voice over IP (VoIP) (UA-IP and PT-IP), see the integrated EMS documentation suite.
- Select if MDM alarms are sent to every SDM server in the network or only one. See the SDM documentation.

In-service migration of MDM servers to the centralized network management approach without using the higher-level management system as an aggregator

Migrate Nortel Multiservice Data Manager servers in your network from the dedicated to the centralized network management approach while in-service if you want one pair of servers to manage the Nortel Multiservice Switch nodes in several offices. Follow this method if your network does not use the higher-level management system as an aggregator.

Note: An in-service migration of MDM servers to the centralized network management approach is not a hitless software migration. While the migration has no effect on network service and causes no service outage, it may result in the interruption of the operator's view of the Multiservice Switch network.

- "Prerequisites for an in-service migration to the centralized network management approach without usi" (page 120)
- "In-service migration to the centralized server network management approach without using the higher-" (page 121)

Prerequisites for an in-service migration to the centralized network management approach without using the higher-level management system as an aggregator

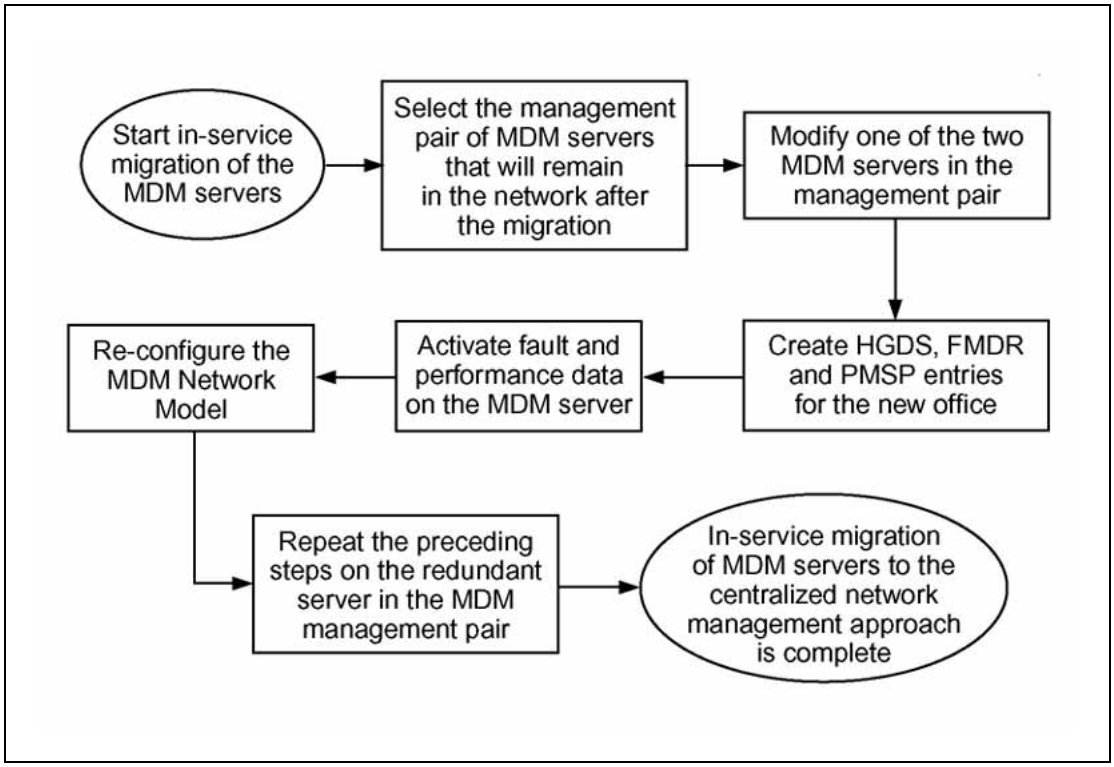
See the prerequisite information in *NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

In-service migration to the centralized server network management approach without using the higher-level management system as an aggregator task flow

The "In-service migration to the centralized network management approach without using the higher-level m" (page 121) shows you the sequence of tasks needed to perform an in-service migration of Nortel MDM servers from the dedicated to the centralized network management approach in a network without using the higher-level management system as an aggregator. For additional information on the tasks, go to "Task flow references" (page 121).

In-service migration to the centralized network management approach without using the higher-level management system as an aggregator task flow



The pair of servers not selected to remain in the network following the in-service migration are now available for redeployment.

Task flow references

- Deploying Regionalized Models and Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
- Performance Measurement Stream Processor (PMSP) and FMIP Management Data Router. *241-6001-310 Nortel Multiservice Data Manager Server Reference*. Configuring MDM servers for Nortel Multiservice Switch nodes and FMDR redundancy for surveillance

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

access. See *241-6001-303 Nortel Multiservice Data Manager Administration*.

- Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

In-service migration of MDM servers to the centralized network management approach using the higher-level management system as an aggregator

Migrate Nortel MDM servers in your network from the dedicated to the centralized network management approach if you want one pair of servers to manage the Nortel Multiservice Switch nodes in several offices. Follow this method if your network uses the higher-level management system as an aggregator.

Note: An in-service migration of MDM servers to the centralized network management approach is not a hitless software migration. While the migration has no effect on network service and causes no service outage, it can interrupt the operator's view of the Multiservice Switch network.

- See "Prerequisites for an in-service migration to the centralized network management approach using the h" (page 122)
- See "In-service migration to the centralized server network management approach using the higher-level ma" (page 122)

Prerequisites for an in-service migration to the centralized network management approach using the higher-level management system as an aggregator

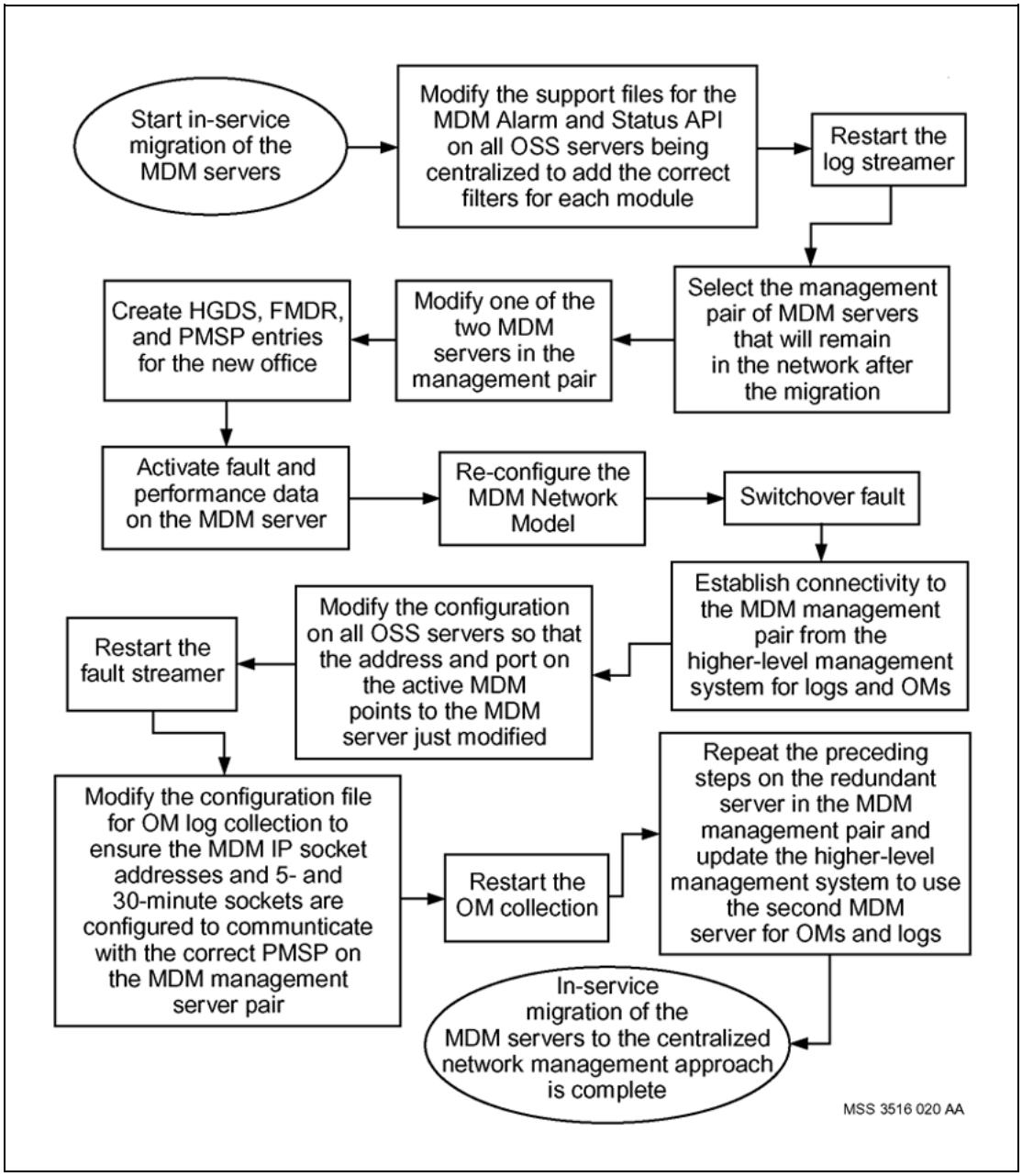
See the prerequisite information in *NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.

In-service migration to the centralized server network management approach using the higher-level management system as an aggregator task flow

The "In-service migration to the centralized network management approach using the higher-level managemen" (page 123) shows you the sequence of tasks needed to perform an in-service migration of Nortel MDM servers from the dedicated to the centralized network management approach in a network using the higher-level management system as an aggregator. For additional information on the tasks, go to "Task flow references" (page 121).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

In-service migration to the centralized network management approach using the higher-level management system as an aggregator task flow



The pair of servers not selected to remain in the network following the in-service migration are now available for redeployment.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task flow references

For the documentation references for the tasks as follows, see the table "Reference documentation for task flow" (page 124).

- See the SDM documentation. [If you are using SDM as an aggregator, modify the *RegMsg.API, CreateMsg.API, GetMsg.API* log streamer files on both SDM servers to have the correct filters for the modules that are specific to them.]
- Install and configure higher-level management system application.
- Deploying Regionalized Models and Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
- Activate higher-level management system application.
- See the SDM documentation. [Establish the connection to the management MDM server pair from the SDM server.
  - If you are using SDM as an aggregator, modify the log streamer *plslog.cfg* file so that the address and port on the currently in use MDM server point to the primary MDM server of the management pair that will remain in the network following the migration.
  - Restart the fault streamer as specified in the SDM documentation.]
- Performance Measurement Stream Processor (PMSP) and FMIP Management Data Router. See *241-6001-310 Nortel Multiservice Data Manager Server Reference*. Configuring MDM servers for Multiservice Switch nodes and FMDR redundancy for surveillance access. See *241-6001-303 Nortel Multiservice Data Manager Administration*.
- Using Network Viewer to build a Network Model. See *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

Reference documentation for task flow

Task	SDMCBM reference (VoA)	integrated EMS reference (VoIP)
Install and configure the log delivery application	See Configuration Management in the SDM documentation suite for this Carrier VoIP release.	See the integrated EMS documentation suite for this release.
Log delivery application overview	See Product Overview in the SDM documentation suite for this Carrier VoIP release.	See the integrated EMS documentation suite for this release.
Activate log delivery application	See Upgrades in the SDM documentation suite for this Carrier VoIP release.	See the integrated EMS documentation suite for this release.

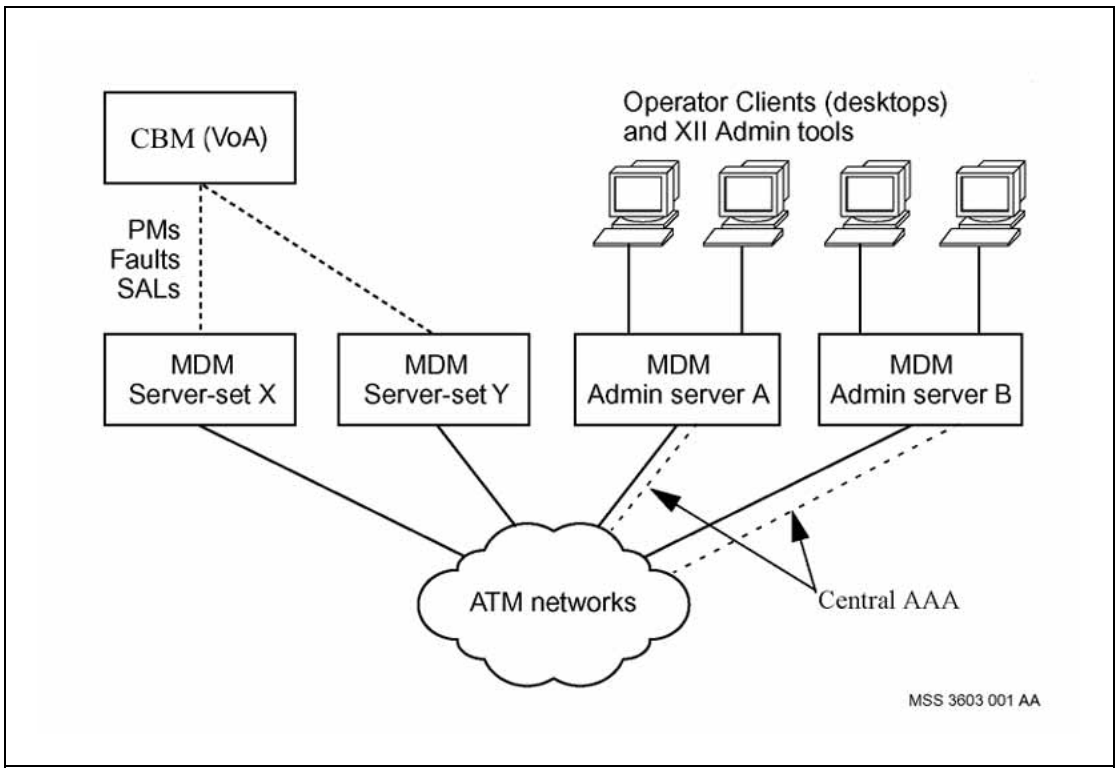
Copyright © 2006, Nortel Networks Nortel Networks Confidential

Deploying MDM Admin Servers for centralized AAA in a VoA network with the Operator Client application

If you deploy Operator Client in your VoA network, client-sets can be re-deployed as MDM Admin Servers. MDM Admin Servers support user administration and mediate access to the administrative X11 based tools of the MDM Toolset. The MDM Admin Servers host the full set of MDM servers found on the MDM server-set as well as those servers that make up the user administration server for the Operator Client application and centralized AAA. The MDM Admin Server hosts all the servers required to provide centralized AAA and it provides base network information for the GUI tools on the Operator Client desktops. The servers that enable centralized AAA and Operator Client functionality are installed with the traditional MDM servers.

See the "Typical deployment of MDM Admin Servers with the Operator Client application in a VoA network" (page 125) for a high-level view of MDM Admin Server deployment in a VoA network.

Typical deployment of MDM Admin Servers with the Operator Client application in a VoA network



The MDM Admin Servers host the following new servers that support user administration for centralized AAA in an Operator Client environment:

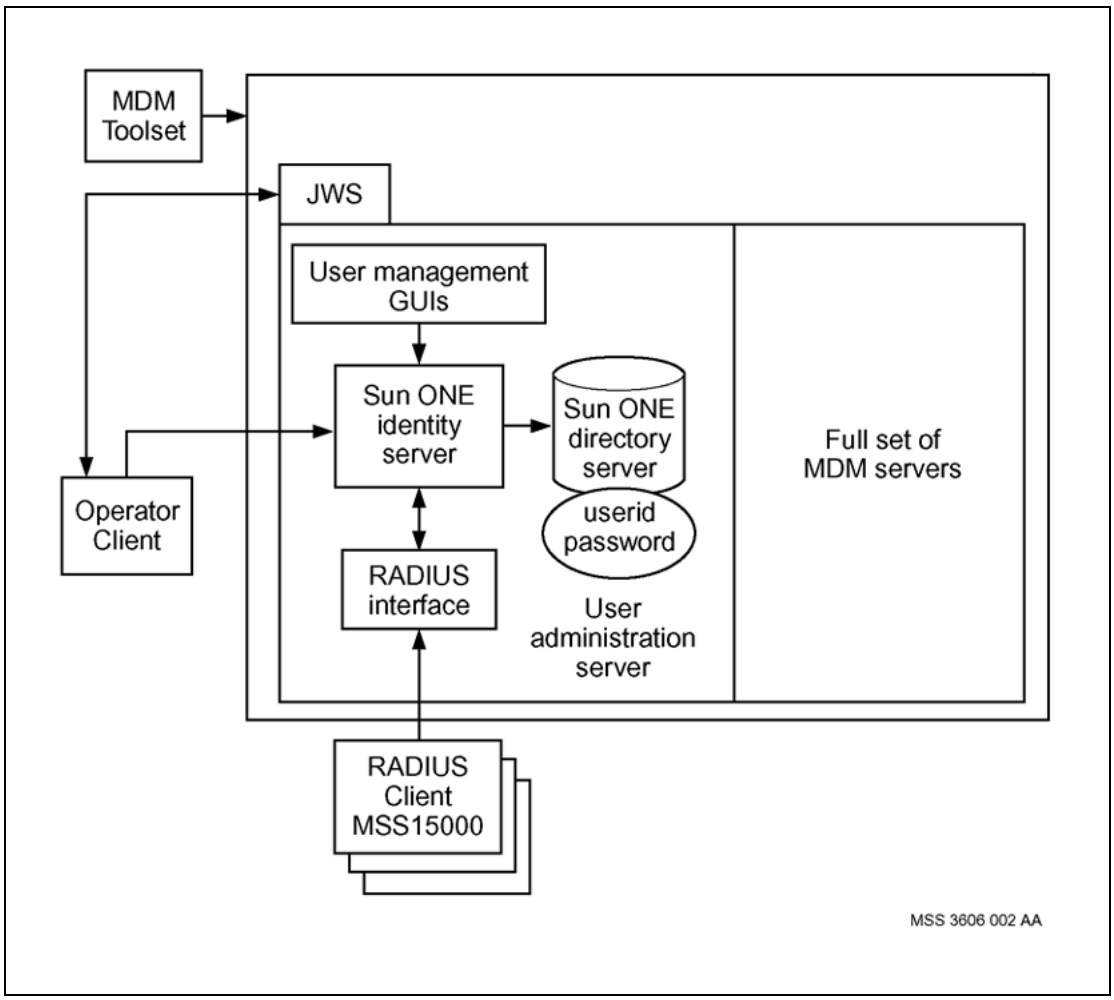
- Sun ONE Identity Server (IS) - used for authentication and authorization of users on Operator Client desktops

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- Sun ONE Directory Server (DS) - central database where each userID and its associated password are stored and maintained
- RADIUS proxy- Nortel NEs are authenticated through the MDM RADIUS interface

The following diagram shows how user access is managed through the Sun ONE Identity Server (IS) for centralized authentication and authorization in an Operator Client environment. The full set of MDM servers available on the MDM Admin Server is equivalent to a standalone or server-set MDM without the PMSP server and pserver. See "MDM Admin Server for centralized user administration of the Operator Client application in a VoA net" (page 126).

MDM Admin Server for centralized user administration of the Operator Client application in a VoA network



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

To re-deploy the MDM client-sets as MDM Admin Servers that enable Operator Client, you require the software package *MDM Operator Client and User Administration*. When this package is launched, Security server and Java Web Start server are pre-selected in the installation panel, by default. However, it is recommended that when you install this package for a VoA solution, ensure that the Security server and Java Web Start server options are selected in the installation panel. Refer to "Installing MDM software" in *NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*.

RADIUS configuration for centralized authentication

The RADIUS interface can be used to provide centralized authentication for the MSS/MG15000 instead of the local authentication available on-switch. That is, the MSS/MG15000 node can be configured to authenticate with the RADIUS interface on the MDM Admin Server. The RADIUS interface on the MDM Admin Server, redirects RADIUS authentication requests to the Sun ONE IS server.

Task flow references for RADIUS configuration

The configuration of RADIUS to support centralized authentication for MSS/MG15000 includes the following:

- configuration of RADIUS interface on the MDM (RADIUS interface)
- configuration of the RADIUS secret
- configuration of RADIUS on MSS/MG15000 (RADIUS client, which authenticates using the MDM RADIUS interface)

Configuration of the RADIUS interface on the MDM

Configure the RADIUS interface on the MDM according to the procedures in the RADIUS interface configuration chapter of *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*.

Configuration of the RADIUS shared secret

The RADIUS shared secret must have the same value and must be configured on both the MDM and the MSS/MG15000 nodes. The same secret must be used for both the RADIUS proxy (the MDM RADIUS interface) and the RADIUS client (the Multiservice Switch). It is recommended that you perform the "Configuring Multiservice Switch nodes for RADIUS" procedure at the same time so that you can enter the shared secret in both locations and avoid errors. Refer to "Configuring shared secrets" in the "RADIUS Interface configuration" chapter of *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Configuration of the RADIUS client on the MSS/MG15000 node

Configure the RADIUS clients on each of the MSS/MG15000 nodes to pass authentication requests through the RADIUS interface to the Sun ONE IS server. Ensure that you have added OAMradius in the featurelist of the Cp (that is, `set sw lpt/cp fl oamradius`).

CAUTION
Risk of surveillance data loss
Do not remove local user IDs from the MSS that are used by the MDP, FMDR, and PMSP surveillance servers. If you remove these user IDs and the central AAA server goes down, surveillance data may be lost. Ensure you retain the local user IDs for MDP, FMDR, and PMSP in addition to a debug level user ID.

It is necessary to remove local users from the MSS/MG15000 nodes if they are to be centrally authenticated using the MDM Admin Server. However, it is recommended that you maintain user IDs for the MDP, PMSP, and GMDR surveillance servers, as well as, at least one user with an impact of Debug on the MSS/MG15000 nodes.

Refer to "Configuring Multiservice Switch nodes for RADIUS" in the Centralized authentication configuration chapter of *NN10600-601 Nortel Multiservice Switch 7400/15000/20000 Security Management*.

JAVA Web Start technology

Java Web Start (JWS) technology is used to automatically download the applications available through Operator Client directly to the operator's desktop or PC. The JWS automatic download of applications decreases the load on the servers that is derived from operator use which helps preserve server reliability. When the JWS files have been downloaded, and if the files on your desktop are current, you will get the Operator Client window and a login screen. Enter your user ID and password and they will be authenticated at the MDM Admin Server. After authentication, the applications that the user is entitled to use are enabled.

MDM Admin Server redundancy

To ensure reliability and redundancy of user parameters and access, the MDM Admin servers should be configured in a redundant manner. One MDM Admin server is configured as the primary server and the other as the secondary or redundant server. Refer to the section "Setting up redundant Directory Servers" in the Configuring the User Administration system chapter in *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*.

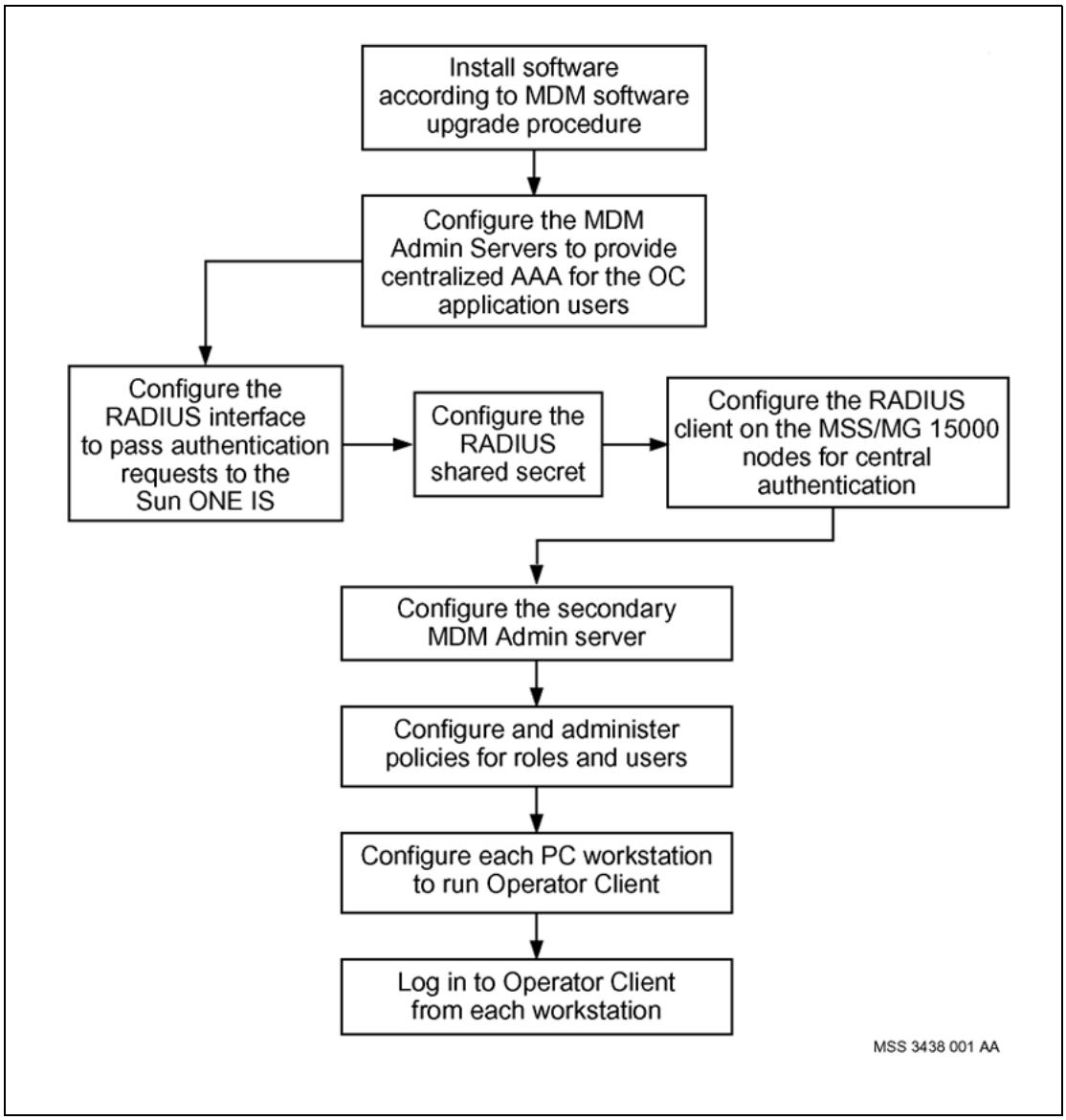
Copyright © 2006, Nortel Networks Nortel Networks Confidential

Workflow for centralized AAA on an MDM Admin Server in a VoA network with the Operator Client application

Operator Client requires installation and server configuration to enable user administration and centralized AAA. See the "Workflow to use the MDM Admin Server for centralized AAA" (page 130). See also, For information about for more information about MDM Admin Server configuration for centralized AAA in a VoA network reference.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Workflow to use the MDM Admin Server for centralized AAA



MDM Admin Server configuration for centralized AAA in a VoA network references

For information about	Refer to
Upgrading the MDM server to be an MDM Admin Server for User Administration of Operator Client desktops	*NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*, see the procedure Installing MDM software.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

For information about	Refer to
Operator Client architecture	*241-6001-101 Nortel Multiservice Data Manager Engineering Overview*
Operator Client Port configuration	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* *NN10400-607 Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*
Configuring User authentication RADIUS centralized authentication	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration* *NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals* *NN10600-601 Nortel Multiservice Switch 7400/15000/20000 Security Management*
User administration	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration* *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP* *NN10028-111 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Deployment of MDM servers for the consolidated network management approach

In the consolidated network management approach for deploying Nortel Multiservice Data Manager servers, a hierarchical topology of consolidated management (CM) servers is used to partition the network according to geographical, traffic flow or other network management needs. A CM server can be deployed using either the Sun Fire V480 hardware platform or the Sun Netra 240 platform with SPFS.

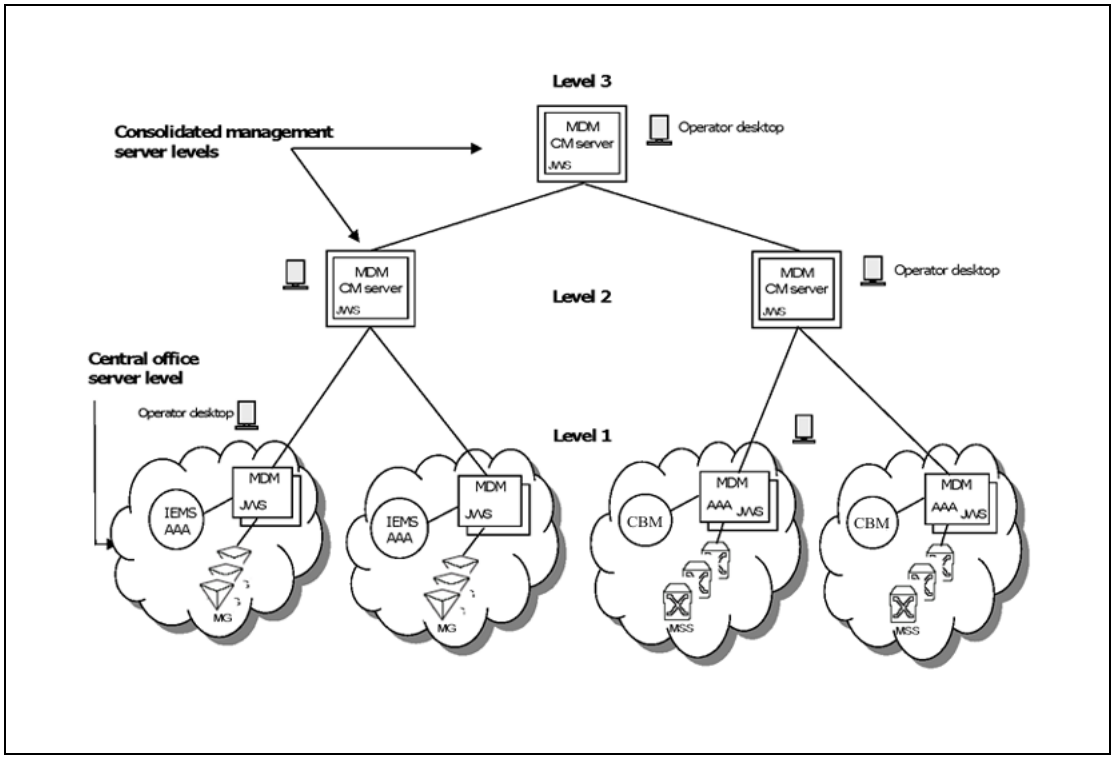
The hierarchical topology can have as many layers as are required to partition the network into the required regional views. The lowest level of the topology consists of the MDM servers connected to the MSS/MG switches. These lowers level MDM servers are located in the central office (dedicated deployment) or in the NOC (centralized deployment). The intermediate

Copyright © 2006, Nortel Networks Nortel Networks Confidential

levels of the topology consist of CM servers that consolidate management information into regional views of the network. The CM server at the highest level of the topology provides the management view of the entire network.

Level 1 MDM servers are central office servers that directly manage the MSS/MG15000 switches. Levels 2 and 3 represents MDM consolidated management servers. The number of levels in the hierarchical topology depends on the needs of the network. Consolidated management servers may be deployed singly, or in redundant pairs for greater reliability.

Sample Multiservice Data Manager consolidated management server configuration



Each CM server maintains a network model for the lower level CM servers and MSS/MG15000 switches connected to it in the hierarchy. This allows the operator on the CM server to monitor the entire network below it in the partition.

Each CM server aggregates fault data from the MSS/MG15000 switches through the intermediate levels of CM servers.

To perform configuration management for the MSS/MG15000 switches, the operator uses the service selection feature to access the MDM server managing the nodes to be changed. The System Wide Service Selection feature is used to define the MDM server in the office most commonly accessed by the operator for MSS/MG15000 configuration changes. The

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

System Wide Service Selection feature must be configured for both MDM Toolset access and Operator Client access. An operator can use the User Specific Service Selection feature to connect to an MDM server in an alternate office when changes to other MSS/MG15000 switches are required.

To support configuration management using the service selection feature, the /etc/hosts file on the CM server must be configured to allow access to the MDM servers that manage the MSS/MG15000 switches in the partition. The /etc/hosts file on the MDM servers managing the MSS/MG15000 switches should not contain addresses of the CM servers. The userids and passwords for the CM operators must be replicated on all the central AAA servers providing authentication and authorization services for the MSS/MG15000 switches.

For more information on the MDM service selection feature, see *NN10400-300 Nortel Multiservice Data Manager Administration Tools*.

For more information on using the MDM service selection features from CM servers, see *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

An operator logged in to a CM server has access to the network model covering the MDM servers and MSS/MG15000 switches in the lower levels in the network partition managed by the CM server. A CM server aggregates fault data from the MSS/MG15000 switches through the intermediate levels of CM servers.

Security audit logs are not aggregrated by CM servers. Security audit logs collected by the MDM server managing the MSS/MG switches continue to be directed to the higher level management system. Security audit logs generated by the CM server are stored locally on the server.

Operators using a CM server have access to network management information and configuration functions for only those network elements that are at a lower level in the hierarchy. MDM Toolset users are authenticated locally by the CM server. Some additional configuration is require to configure Operator Client users on the appropriate central AAA servers.

Auto-patching for MSS/MG15000 nodes from the MDM

Auto-Patch is a scheduled process that automatically downloads and applies released MSS/MG15000 non-disruptive patches to your switches with a single script that is activated and run from a Nortel Multiservice Data

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Manager. Activation of the auto-patch process includes configuring the cron utility to schedule the download and application of non-disruptive patches to the nodes you have identified in the script.

You must download the Patch Av from the Nortel patch distribution site to the MDM that is configured to be the SDS. At the scheduled time, the script is activated, and the MDM issues on-switch commands that trigger the following sequence of activities:

1. Verification to see if the SDS has a later version of the Patch Av than those in the active node.
2. Download of the Patch Av when the -download option is specified in the script.
3. Calculation of the necessary Sw patchlist by comparison with the active node configuration which is followed by application of only the required patches and commitment of the view when the -apply option is specified in the script.

You will configure your MDMs to run the auto-patch process as a redundant pair and configure the *ppautopatch* script to run on a regular basis. You configure the frequency and timing of the downloads and applications from the cron utility or any similar scheduling method that you use in your network. See "Scheduling the MDMs" (page 134).

When necessary, as in the case of performing an HSM or time-of-day (tod) change, you can inhibit the script from running. For the procedure that prevents the auto-patch script from running, see "Controlling the auto-patch process" (page 136).

Scheduling the MDMs

You can schedule and configure auto-patching from the crontab on any Multiservice Data Manager (MDM). To set up the cron entries on the MDM that is the SDS, use the <Patch distribution completion> information as the start time for the "ppautopatch" script. That is, the day-of-week and/or time-of-day that your patch distribution has completed putting new patch updates (if any) onto the SDS sites. (This would be T_0.)

On the mate MDM, calculate the start time by adding <max duration> to <Patch distribution completion> information
(<max duration> + <Patch distribution completion> = T_1).

It is assumed that <Patch distribution completion> coincides with regular maintenance windows during which patch download and application are acceptable. If this is not the case, adjust the script start times accordingly.

Note: The script can be run concurrently on different groups of nodes.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

As an example, you can configure and schedule redundant MDM hosts to perform in the following manner:

- At time T_0, the MDM configured to be the SDS can be scheduled to download all the patches available on the SDS to the nodes and apply those patches that are eligible for auto-patching to the MSS/ MG15000's it manages. Maximum time allotment of 1 hour.
- At time T_1, which equals T_0 + 1 hour, the mate MDM can be scheduled to download all the patches to the nodes and apply those patches that are eligible for auto-patching to the MSS/ MG15000's it manages. For any patches that were successfully processed by the first MDM, the auto-patching script from the mate MDM will skip the download and apply tasks after checking the active node conditions. The maximum time allotments for both the MDMs must match.

There is no specific order required as to how the command attributes are entered; however, the order shown below is recommended because sometimes, the **`ps -ef`** command truncates the returned parameters. If you use the recommended order, the "-nodes" parameter value will be sure to appear. The recommended script command line options are as follows:

```
/opt/MagellanNMS/bin/ppautopatch
-nodes <Group name>

-nuser <Node userid> <Node password>

-download
-host <SDS address>

-huser <SDS host userid> <SDS password>

-apply
-max_duration { <n> h | m}
```

Note 1: When the ppautopatch command is scheduled and configured from the crontab, you must specify the entire executable path to the ppautopatch script, as follows:
`/opt/MagellanNMS/bin/ppautopatch`

Note 2: It is recommended that any passwords provided on the command line are in an encrypted password file.

Refer to *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2* for the complete set of command line attributes.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Controlling the auto-patch process

It is recommended that you prevent the auto-patching script from running on both MDMs before you perform an HSM and on the days that you have time-of-day (tod) changes scheduled.

Before doing an HSM or before tod changes are scheduled to be made, ensure that no auto-patch script ("ppautopatch") is running and that it does not run during the HSM or tod change. Issue the following commands on both MDM servers where a "ppautopatch" script could be configured to run for the node being upgraded:

1. Issue:

   touch /opt/MagellanNMS/cfg/private/noppautopatchrun

2. Issue:

   ps -ef | grep ppautopatch

If the second command returns only one response, such as the following, it is ok to go ahead with the HSM:

```
ps -ef | grep ppautopatch
root 6453 29431 0 09:10:53 pts/11 0:00 grep ppautopatch
```

If the second command returns one or more additional responses, such as the following, then the script "ppautopatch" is running.

```
ps -ef | grep ppautopatch
root 2112 282 0 Dec 03 ? 13:50 ppautopatch -nodes OFFICE1
-nuser config config /opt/MagellanNMS/cfg/private/config.pwd
-download -host 47.1.2.3 -huser pp15ksw
/opt/MagellanNMS/cfg/private/host.pwd -apply
-max_duration 1 h
root 6453 29431 0 09:10:53 pts/11 0:00 grep ppautopatch
```

Note 1: The script does not typically take a long time to run so, generally, it is recommended to wait until all "ppautopatch" scripts are finished and then start the HSM.

Note 2: On an MDM that manages nodes in more than one Carrier VoIP office, a running script may not necessarily include the node to be upgraded (refer to the -nodes parameter value for the "ppautopatch" script). If you are sure that none of the running scripts pertain to the node being upgraded, you can proceed with the HSM.

Note 3: The "noppautopatchrun" file should be deleted on both MDM servers after the HSM is completed. If performing HSM on a series of nodes from the same MDM, it is recommended not to remove the file until after all the HSMs have been performed.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

When the auto-patch script fails to download or apply a patch

The script downloads and applies any non-disruptive patch that has a Released GEN status. When issues that prevent the potential download and/or application of an eligible patch to an MSS/MG15000 node are encountered, the script generates alarms. These SET alarms provide notification that the auto-patch attempt did not complete as expected. The alarm details and ppautopatch log file provide details about successes and failures each time the script runs. Generally, an alarm raised (SET) against a component on one MDM must be cleared (CLR) by the same MDM.

Alarms with error paths that are specific to an MSS/MG15000 node that the MDM is trying to reach are handled differently from alarms raised against an MDM component by a specific MDM. If the script runs on the first MDM and fails because it is not able to access a specific node, a SET alarm is issued. The SET alarm is cleared when the mate MDM runs the script successfully at its scheduled time.

The successful execution of a script that runs on one platform (the mate MDM) can clear the SET alarm that was issued by the script running on the other platform (the first MDM). That is, when the mate MDM runs the script and successfully processes the MSS/MG15000 node at the later time, a CLR alarm is issued that clears the original SET that was generated on the first MDM.

> ***Note:*** Remember that the script runs on both MDM's in a server pair, offset from each other in time, and the standard configuration has the MDM surveillance server processes cross-connected to feed alarms between a mated pair of server platforms.

If both the SDS MDM and the mate MDM have run the script on what appears to be an eligible patch and the patch is not auto-applied by the script, there may be a problem with the patch itself. Contact Nortel GNTS and provide them with information about the patch, such as the date it was downloaded from Nortel, patch name, and type.

For more information about auto-patching, see the following table:

For more information about	refer to
The auto-patch process including process control, disk management, and error logs	"Configuring the auto-patch process" in *NN10400-300 Nortel Multiservice Data Manager Administration Tools*
Auto-patch log cleanup	*NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For more information about	refer to
Attributes available for the auto-patch feature	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*
Alarms that occur during the auto-patch process	*NN10092-911 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Overview PT-AAL1/UA-AAL1/UA-IP/PT-IP*

MDM server configuration for Ethernet Routing Switch 8600 fault management (PT-AAL1 and UA-AAL1)

This section describes fault management when using the higher-level management system in a voice over ATM (VoA) solution only. VoA refers to Packet Trunking - AAL1 (PT-AAL1) or Universal Access - AAL1 (UA-AAL1) only.

In voice over IP solution (VoIP), the Integrated Element Management System (Integrated EMS) handles Ethernet Routing Switch 8600 (ERS 8600) faults directly, without involving MDM servers. It does not handle Nortel Multiservice Switch 15000 or Media Gateway faults directly. For those faults, Integrated EMS uses the MDM. For more information about fault management for VoIP, refer to the Integrated EMS documentation suite for this release.

Customers with MDM servers in a network have the option of configuring the servers to receive SNMPv2c traps from a set of ERS 8600 nodes that are performing as the CS LAN in a office. These traps are merged into the same stream of alarms, originating from Multiservice Switch 15000 nodes and MDM servers, that is being forwarded to the higher-level management system where they are converted into the SCC2 format.

Note: Fault collection is the only aspect of ERS 8600 network management that is integrated into MDM in the solution. All other aspects of ERS 8600 network management continue to be supported as before. For the details on OAM tasks and access for managing Multiservice Switch nodes, see *NN10028-111 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

- "Downloading the ERS 8600 DCD cartridge from the ESD web site" (page 139)
- "Configuring MDM for ERS 8600 fault management" (page 141)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "Verifying MDM configuration for ERS 8600 fault management" (page 144)

Downloading the ERS 8600 DCD cartridge from the ESD web site

After verifying that the MDM server has sufficient disk space, you can begin to download the ERS 8600 cartridge and accompanying documentation from Nortel ESD web site. When you download the software, a copy of the software is placed in the directory you specify.

- "Prerequisites" (page 139)
- "Procedure steps" (page 139)
- "Variable values" (page 141)

Prerequisites

- Ensure that there is enough disk space on the MDM server.
- You need to have root access to login to the MDM servers.
- You need a Nortel Web access account with a user ID and password to enter into the appropriate fields when prompted to log in. Contact your Nortel customer representative for more information on accessing the web site.
- Refer to the software downloads area of the Nortel web site () to determine the software load that you must install to manage ERS 8600 nodes.
- The software you need to download may be composed of more than one file. Ensure that you download all software files that belong to the release you require.

Procedure steps

Step	Action
1	Login to the MDM server as the root user.
2	Open an xterm session.
3	Start Netscape and go to .
4	In the Technical Support section of the window, click *Software Downloads*. The Technical Support window opens.
5	In the *Select from* section of the Technical Support window, select *Product Families* and *Preside* from the items contained in the list boxes.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

The ... *choose a product* ... list box fills with item names.

6 In the ... *choose a product* ... section, select *Multiservice Data Manager Device Integration Cartridges* from the items contained in the list box.

The ... *and get the content* list box fills with item names.

7 In the ... *and get the content* section, select *Software* from the items contained in the list box and click *Go*.

The Multiservice Data Manager Device Integration Cartridges window opens.

8 In the Multiservice Data Manager Device Integration Cartridges window, click on *MDM ERS 8600 Cartridge V3.4.0*.

Note 1: If version 3.4.0 of the software does not appear in the window, contact your Nortel account prime.

Note 2: The software you want to download may be composed of more than one file. Ensure that you download all software files that belong to the release you require.

The Software: Software Detail Information window opens.

9 Click on the load name listed beside the File Download heading.

A File Download dialog opens.

10 In the File Download dialog, select the Save this file to disk option.

A Save As dialog opens.

11 Specify a folder in the home directory of the userID of the MDM user to indicate where you want the software placed. This is typically:

```
/tmp/pp8600DCDSW
```

12 Click *Save*.

13 Repeat step 5 to step 12 except download *241-6003-100 Preside Generic Device Integration Installation Guide* by selecting *Documentation* rather than *Software* in step 7 and specify the **`/tmp/pp8600DCDdoc`** rather than **`/tmp/pp8600DCDSW`** folder in step 11.

14 On the MDM server, use the xterm window to change directories to the directory containing the software. (This is the same directory you specified in step 11.):

```
cd /tmp/pp8600DCDSW
```

15 Untar the software:

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
tar -xvf <load_name> .tar
```

16 Repeat step 1 through step 15 on the other MDM server to download the software.

—End—

Variable values

Variable	Value
`<load_name>`	The name of the software load file that you want to download.

Configuring MDM for ERS 8600 fault management

After downloading and untarring the software for the node's DCD cartridge, configure Nortel MDM servers to receive SNMPv2c traps from ERS 8600 nodes.

- "Prerequisites" (page 141)
- "Procedure steps" (page 142)
- "Variable values" (page 144)

Prerequisites

- Install the ERS 8600 DCD cartridge on the MDM servers. For details, see "Downloading the ERS 8600 DCD cartridge from the ESD web site" (page 139).
- The DCD cartridge needs to support the version of the software that is running on the ERS 8600 nodes.
- Prior to configuring MDM servers, use the Release Update GUI to delete the release version number (SNxx). To delete it, leave the Carrier VoIP Release blank. The GUI modifies the */opt/MagellanNMS/system/info/release.name* file. If you do not delete the release information, the *packageadd* process fails and an error message is produced.
- You need to have root access to login to MDM servers.
- You need a list of the nodes that you are going to manage with MDM servers. Include the device name and IP address for each node on that list as well.
- You need to know the SNMP community string for each node that you are going to manage with MDM.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- You need to know the host name or IP address of the MDM servers when establishing cross-connectivity between the servers.

Procedure steps

Step	Action
1	Login to the server as the root user.
2	Open an xterm session.
3	In the xterm window, change directory to the newly untarred directory containing the software file you downloaded in step 14 of "Downloading the ERS 8600 DCD cartridge from the ESD web site" (page 139). Generally, the newly untarred file is in the **`./Passport8600`** directory.
4	Add the DCD cartridge to the SVMList by executing the following command: **`pkgadd -d . <filename>`**
5	Add the SMDR and TVSR fault servers to the Server Administration configuration using the GUI of the Server Administration tool. For details on using the Server Administration tool, see *241-6001-303 Nortel Multiservice Data Manager Administration*.
6	Add the SMDR fault server to your General Management Data Router server configuration using the GUI of the GMDR Administration tool. For details on using the GMDR Administration tool, see *241-6001-303 Nortel Multiservice Data Manager Administration*.
7	Add the following line to the **`/opt/MagellanNMS/cfg/smdr.svr`** file: **`: <host> :idi_PP8600dcd:0:0:`**
8	Re-enter the Carrier VoIP release version number in the */opt/MagellanNMS/system/info/release.name* file. Use the Carrier VoIP MDM Software Migration GUI to set Carrier VoIP Release. Use the format: SNxx.y. For example, SN06.2 or SN07. The release number is the same one that you deleted prior to beginning this procedure.
9	Repeat step 1 to step 8 on the other MDM server.
10	Establish server cross-connectivity between the two servers using the GUI of the GMDR Administration tool.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For details, see the procedure for configuring GMDR to access surveillance data servers in *241-6001-303 Nortel Multiservice Data Manager Administration*.

> ***Note:*** When you enter the server name of the other server in the Server Name field of the GMDR Add Server dialog, use the SMDR suffix.

11 Repeat step 10 on the other server.

12 From the Fault menu in the main MDM dialog, select *IP Discovery* in order to use the IP discovery application to find the nodes.

The IP Device Discovery dialog opens.

For details on using the IP Discovery application, see *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*.

13 In the IP Device Discovery window, select the *Network Settings* tab and specify the IP address, community string, port, device type, and SNMP version information in the provided fields.

14 From the Device menu in the IP Device Discovery dialog, select the *Discover* ... option.

The Discovery dialog opens.

15 Enter the IP address of the node you wish to find in the IP Address field.

16 Select both the Register to Receive Traps check box and ERS 8600 option from the Discover As drop-down menu in the Options area of the Discovery window.

> ***Note:*** You may need to expand the Options area of the Discovery window in order to see the Register to Receive Traps check box and Discover As drop-down menu.

17 Click *Start*.

When the Discovery process is finished, click *Close*.

18 Exit the IP Discovery tool by closing all the windows and returning to the MDM main window.

19 Repeat step 12 to step 18 on the other server.

20 Configure a trap receiver for each MDM server on each node.

For details on configuring a trap receiver, see the Configuring SNMP settings in ERS 8600 NTP 315545-B *Managing Platform Operations and Using Diagnostic Tools*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

—End—

Note: The new configuration can be de-activated by stopping the *idi_PP8600DCD* process.

Variable values

Variable	Value
`<filename>`	The <filename> is the name of the file containing the DCD cartridge software.
`<host>`	The <host> is the name of the server on which the MDM application is currently running.

Verifying MDM configuration for ERS 8600 fault management

After completing the procedures for downloading the ERS 8600 DCD cartridge and configuring Nortel MDM servers to receive SNMPv2c traps from the nodes, verify that the servers are set up properly for fault management by using the MDM Network Model.

- "Prerequisites" (page 144)
- "Procedure steps" (page 144)

Prerequisites

- You need to know a password to enable the Network Model Editing feature.

Procedure steps

Step	Action
1	From the MDM Fault menu, select *Network Viewer*. Verify that the icon for the node appears in the display of the Network Model.
2	From the Network Model Edit menu, select *Enable Network Model Editing*. An Enable Editing dialog opens and prompts you for a password.
3	Enter the password at the prompt to enable Network Model editing.
4	From the Network Model Edit menu, select *Show Excluded Modules ...* to list the unassigned network elements.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The unassigned network elements appear in the Excluded Modules window in the Component List dialog.

5 Assign the new nodes to the appropriate site using drag and drop in the Network Viewer display.

6 Position the node icons in the network using the Network Viewer display.

7 From the File menu, select *Save View* to save the Network Model.

8 From the File menu, select *Exit* to close the Network Viewer display.

9 Repeat step 1 to step 7 on the other MDM server.

10 New router - green (on) & grey (no connectivity)

—End—

Disabling syslog parameter for non-SPFS based MDM servers delivering fault events to IEMS

The syslog message ID parameter (msgid) for all non-SPFS based MDM servers that deliver fault events to IEMS must be disabled.

Disabling syslog parameter (msgid = 0)

Step	Action
1	Log in to the MDM.

2	Execute:
	`cd /kernel/drv/`
	`vi log.conf`

3	Add the parameter: `msgid=0` *in log.conf*
4	Reboot the MDM server. `init.6`

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Deploying MDM servers with Server Platform Foundation Software (SPFS)

The Server Platform Foundation Software (SPFS) package consists of the base operating system and third-party application tools. Service applications are provided in the main package such as the Resource monitor (RESMON), Service application monitor (servman), and EMS proxy services. Sub-packages such as the Network Patch Manager, which contains the patch management application, are included as separate packages. The SPFS packages required by MDM are defined in a profile, and only these software packages are installed on MDM servers.

SPFS is installed only on the Sun Netra 240 platform configured to run in simplex mode. SPFS installation and configuration is done as part of the greenfield installation of a Netra 240 server.

The following sections describe the options selected during the installation and configuration of the Server Platform Foundation Software, and changes that must be made to the MDM application.

- "SPFS packages installed on MDM servers" (page 146)
- "SPFS configuration options" (page 147)
- "Changes to MDM when SPFS is installed" (page 149)
- "SPFS processes running on MDM servers" (page 183)

Managing patching of Server Platform Foundation Software is described in:

- "Patch management for SPFS" (page 152)

SPFS packages installed on MDM servers

"SPFS packages included with the MDM profile" (page 146) lists the SPFS packages that are installed on MDM servers.

SPFS packages included with the MDM profile

Package description
Solaris 9 operating system plus • latest jumbo and security patches • NSCPCom package for the Netscape browser
SunScreen 3.2
X11, CDE
JRE 1.4.2-08
IPSec, AES, SSH
Sun Solaris 9 Data Encryption Supplement 1.0.1
NTProftpd

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Package description
Resource Monitor (RESMON)
NTnpm, NTpse
NTDeleGate
NTApache 2.0.51, NTTomcat 5.0.28
Note 1: The Network Patch Manager (NTnpm) will only be configured in certain configurations.
Note 2: SPFS uses OpenSSH software.

SPFS configuration options

Review the following information to understand the initial configuration of Server Platform Foundation Software (SPFS) performed during the SPFS installation sequence.

SPFS configuration prompts and values for Multiservice Data Manager

Prompts	Configured values	Notes
Select a server profile	mdm	The server profile identifies the SPFS software packages to be installed for use with Multiservice Data Manager.
Will this system be a cluster?	no	The server runs in simplex mode.
Use factory default network configuration?	no	
Enter the hostname for this system	<aaaaa>	This is the hostname for the MDM system.
Enter ip address for <aaaaa>	<xx.xxx.xxx.xxx>	This is the IP address of the MDM system.
Configure additional ip address?	no	As server is running in simplex mode, only one IP address is configured.
Enter the subnet mask for this network	255.255.255.0	This is the subnet mask.
Enter ip address for the network's router	<zz.zzz.zzz.zzz>	The is the IP address of the router used by this network.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Prompts	Configured values	Notes
Enter the timezone for this system	<time zone name>	This is the name of the time zone or the offset from GMT where the MDM server is located, for example, eastern time has an offset of +5. Select the appropriate time zone value from the list. ***Note:*** If MDM servers in the network are operating across timezones, then universal time is recommended.
Will this system use DNS?	yes	
Enter the DNS domain for this system	<domain name>	This is the domain name used by the system.
Enter the ip address of a DNS server	<DNS ip address>	This is the IP address of a domain name server for the network.
Enter a DNS search domain	<search domain name> or return	A single search domain is specified. An entry of "return" ends the entry sequence.
Accept current settings?	yes	This input proceeds to install the SPFS software from the installation disks.

The root user uses the SPFS command line interface (CLI) options for initial configuration.

SPFS CLI options used during initial configuration

cli entry	Comments
1-NTP Configuration	This option can be used to configure a timing provider on consolidated management (CM) servers or client-set servers with SPFS installed. Nortel recommends that server-set pairs be synchronized as peers, which this option does not support. For more information on configuration of the Solaris NTP daemon, see "Network Time Synchronization system configuration" in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
2-Apache Proxy Configuration	not used
3-DCE Configuration	not used
4-OAMP Application Configuration	This option is used if NPM is installed on an MDM N240 server deployed in a CO.
5-CORBA Configuration	not used

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

cli entry	Comments
6-IP Configuration	not used. The MDM IP name and address are set up during SPFS installation.
7-DNS Configuration	not used. Access to the DNS is set up during SPFS installation.
8-Syslog Configuration	not used
9-Database Configuration	not used. MDM does not use the Oracle database.
10-NFS Configuration	not used
11-Bootp Configuration	not used
12-Restricted Shell Configuration	not used
13-Security services Configuration	not used
14-Login Session	not used
15-Location Configuration	not used. Timezones are configured during initial installation.
16-Cluster Configuration	not used
17-Succession Element Configuration	This option is used to configure NPM, PSE, and RESMON.
18-SNMP Poller Configuration	not used
19-Backup Configuration	not used

Changes to MDM when SPFS is installed

To enable MDM software to utilize SPFS functionality, the following MDM aspects are changed when SPFS is installed on the MDM server.

MDM port changes

As there is a conflict between the port usage of the MDM Apache and Tomcat servers and the SPFS WEBSERVICES and WEBSERVER, the MDM port assignments for these servers have been changed. These changes are shown in "MDM port changes for Netra 240 servers with SPFS" (page 149).

MDM port changes for Netra 240 servers with SPFS

MDM server	port assignment without SPFS installed	Port assignment with SPFS installed
Apache	8080	8090
Tomcat	8005, 8009	8006, 8010

Copyright © 2006, Nortel Networks Nortel Networks Confidential

For a complete list of MDM ports and SPFS ports, see the section "Firewall configuration" in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Note 1: Due to the port conflict between the SPFS Tomcat and MDM Apache servers, the MDM Apache web server default port must be changed (manually) to a different port for VoIP and VoA

Note 2: Changing the Apache port number on SPFS affects the launching of the Operator Client. See “Launching the Operator Client application from the operator’s desktop” (page 171).

Changing the Apache webserver default port

Central authentication for VoIP with IEMS If you are using central authentication for VoIP with IEMS, perform steps 1 - 7 in the procedure ’Changing the Apache web server default port’ in the 241-6001-303 Nortel Multiservice Data Manager Administration. In step 7 of the ’Changing the Apache web server default port’ procedure; you only need to search and change the port number 8080 to 8090 in the following file:

/opt/nortel/config/applications/desktop/jws/mft/resources/desktop/DesktopGUI.jnlp

Launching the Operator Client application from the operator desktop To launch the Operator Client application from the operator’s desktop, use the following URLs.

1. For MDM Servers using the Sun Fire V480 platform: http://<MDM Server name>:8080/UI
2. For MDM Servers using the Sun Netra 240 platform: http://<MDM Server name>:8090/UI
3. Select a heap size of 256MB when prompted.

For more information on launching the Operator Client application, see the section “Starting Operator Client” in 241-6001-122 *Nortel Multiservice Data Manager Using Toolset and Operator Client Interfaces*.

MDM AAA central authentication If you are using MDM AAA central authentication, follow all the steps in the procedure ’Changing the Apache web server default port’ in the 241-6001-303 *Nortel Multiservice Data Manager Administration*. In step 7 of the procedure, you need to search and change the port number 8080 to 8090 in all of the specified files.

Changing the Tomcat server default port

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Step	Action
1	Edit file /opt/nortel/3rd_party/apache/current_tomcat/conf/server.xml a. Replace all occurrences of 8005 with 8006. b. Replace all occurrences of 8009 with 8010.

2	Restart the Tomcat server:
	`/opt/nortel/3rd_party/apache/current_tomcat/bin/shutdown.sh`
	`/opt/nortel/3rd_party/apache/current_tomcat/bin/startup.sh`

—End—

ATTENTION
If you want the MDM Tomcat server to start automatically after a reboot of MDM on SPFS, you must run a script manually.

1. Execute the following:

```
ln -s /opt/nortel/MDMHelp/bin/tomcat_boot.sh /etc/rc3.d/S86mdm_tomcat

link run level shutdown script

ln -s /opt/nortel/MDMHelp/bin/tomcat_boot.sh

/etc/ rc2.d/K04tomcat_boot
```

SSH directory changes

SPFS provides OpenSSH software which uses a different directory structure. See the section "Activating SSH on an MDM Server" in *NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements* for more information.

MDP changes

Since MDP uses proxy FTP, the following changes have been made:

- The proxy FTP configuration file /opt/proftpd/etc/proftpd.conf has the parameter *AllowForeignAddress* set to "on".
- The file /etc/ftpd/ftpaccess is modified to remove:
  - port-allow of realusers and guestusers
  - pasv-allow of realusers and guestusers

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Required SPFS processes

"Required SPFS processes for MDM servers" (page 152) lists the SPFS processes that are required to be running to support MDM.

Required SPFS processes for MDM servers

SPFS process	
BACKUP_MANAGER	supports the SPFS backup system
WEBSERVICES	SPFS Tomcat server
WEBSERVER	SPFS Apache server
CORBA	supports communication between the NPM BUI/CLUI and the NPM server

Other processes that are not used by MDM may also be running.

For more information on displaying the SPFS processes, see the section "SPFS display utilities" in *NN10180-611 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP/PT-IP*.

Patch management for SPFS

The Network Patch Manager (NPM) is a patch management solution for Nortel network-based products. The NPM software package is delivered with the Server Platform Foundation Software (SPFS). The NPM is used to provide patches for Server Platform Foundation Software. This includes the operating system and third party software application software, and the service application packages. Multiservice Switch software and MSS/MG15000 switch software continues to be patched using current procedures.

Only one instance of the NPM can be installed and enabled in an office. Depending on your office configuration, your choices are as follows:

- IEMS, which is the most preferred location
- CS 2000 Management Tools (CS2000 MT) server when IEMS is not present in the network
- Nortel Multiservice Data Manager (MDM) when IEMS and the CS 2000 Management Tools Server are not present in the network.

The NPM uses the Patch File Receipt System (PFRS) and the Patching Server Element (PSE) device.

NPM deployment scenarios

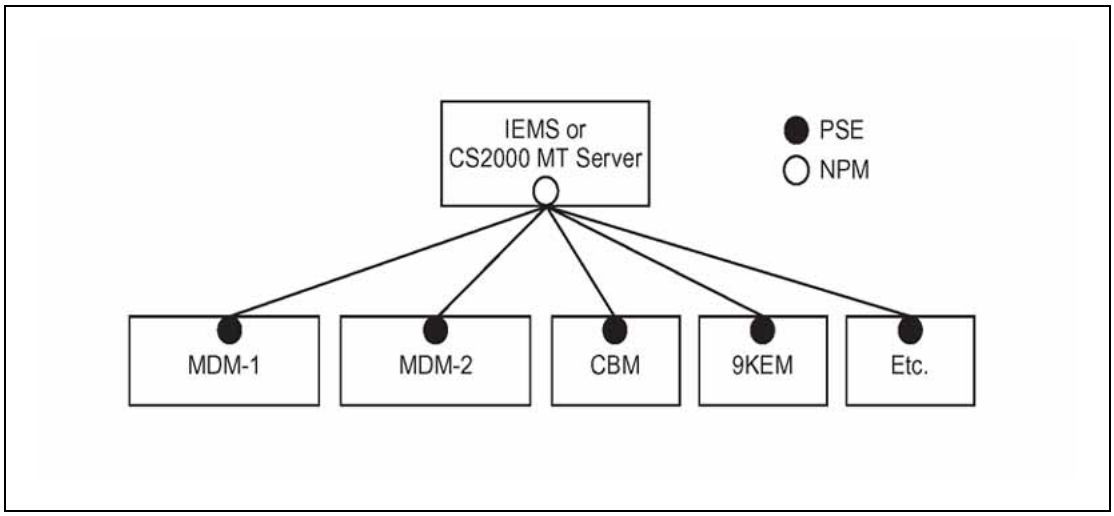
The Network Patch manager is hosted on an MDM server only in certain network configurations.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Central office deployments

"NPM and PSE deployment in the office with IEMS or CS 2000 Management Tools server" (page 153) shows a typical office configuration with the Network Patch Manager already located on the IEMS or the CS2000 Management Tools. The Patching Server Element resides on the MDM servers.

NPM and PSE deployment in the office with IEMS or CS 2000 Management Tools server



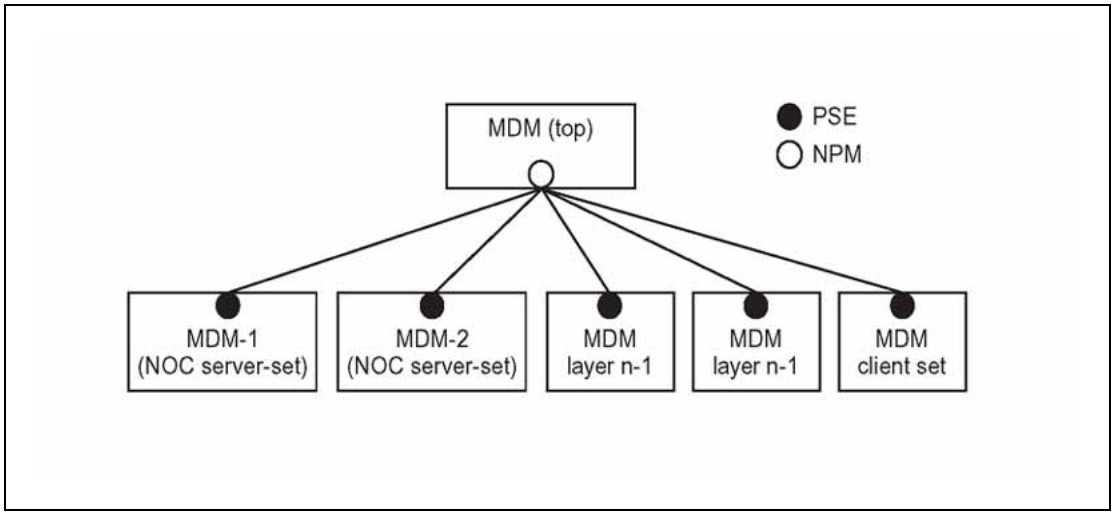
NPM uses unsecured communication protocols to transfer patch files to the PSE as no communications security is required within a central office.

The PSE on each of the MDM servers in the central office is configured to communicate with the NPM on the IEMS.

"NPM and PSE deployment using MDM N240 servers in the office" (page 154) shows a network configuration in which the MDM servers do not have access to another element manager platform that is already hosting NPM.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

NPM and PSE deployment using MDM N240 servers in the office



In this scenario, one of the MDM servers would host the NPM and communicate with the PSEs on the other MDM servers. The NPM is configured with the office CLLI.

Only one instance of NPM can be installed and enabled in an office. If the MDM server hosting the NPM fails, NPM is unavailable to patch the other MDM servers. In this case, an alarm/log from SFM is the trigger to take action to restore the NPM capability.

NPM uses MDM-based security for authentication and authorization, but continues to use unsecured FTP and TCP socket communication to communicate with other parts of the patching system such as PSEs and the drop box.

Deployments outside the central office

In this case, the MDM N240 server that hosts the NPM is located outside the CO. This MDM server may be configured as a server-set, client-set or consolidated management server.

NPM uses unsecured FTP and TCP socket communication to communicate with the other parts of the patching system. In secured VoIP networks, IPSec is used to secure communications between MDM servers.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Overview of the EdgeLink 100 multiplexor to Multiservice Switch 15000 interface configuration

The EdgeLink 100 multiplexor (MUX) is a Telco Systems broadband multiplexor. For more general information about the EdgeLink 100 MUX, see *NN10028-111 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Product and Technology Basics PT-AAL1/UA-AAL1/UA-IP/PT-IP*. For information on connecting a Nortel Multiservice Switch 15000 node to an EdgeLink 100 MUX, see *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.

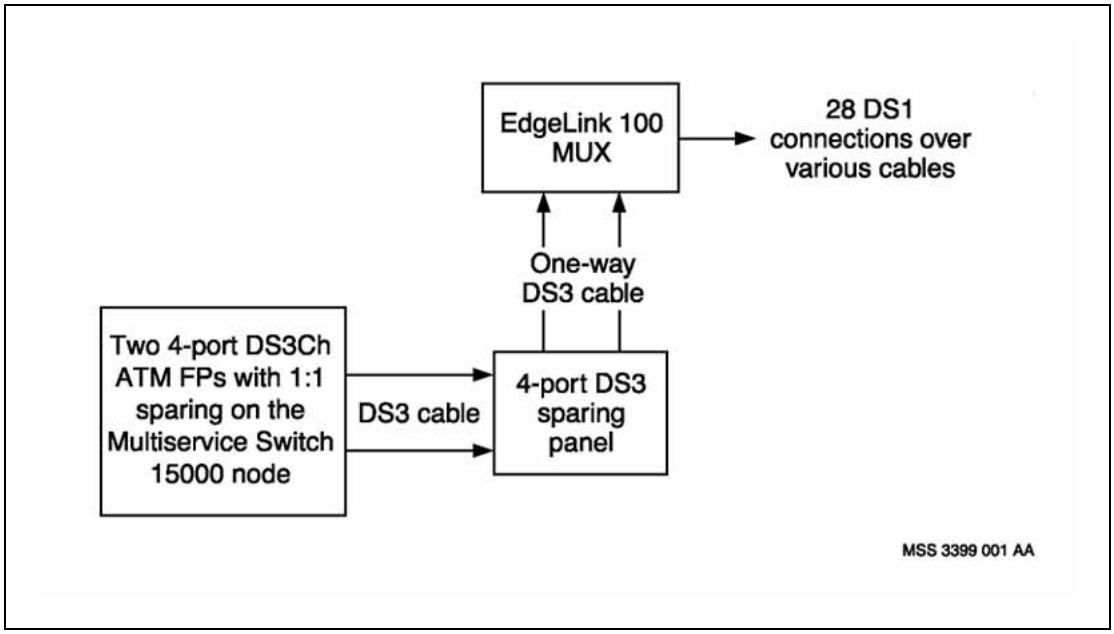
For diagrams depicting a logical view of the connection between the EdgeLink 100 MUX and a pair of 4-port DS3Ch ATM FPs and DS3 sparing panel on a Multiservice Switch 15000 node, see the following figures:

- "Connection between one EdgeLink 100 MUX and a Multiservice Switch 15000 node" (page 156)
- "Connection between four EdgeLink 100 MUXs and a Multiservice Switch 15000 node" (page 157)

Note: You can also support two or three EdgeLink 100 MUXs from the same pair of 4-port DS3Ch ATM FPs and DS3 sparing panel.

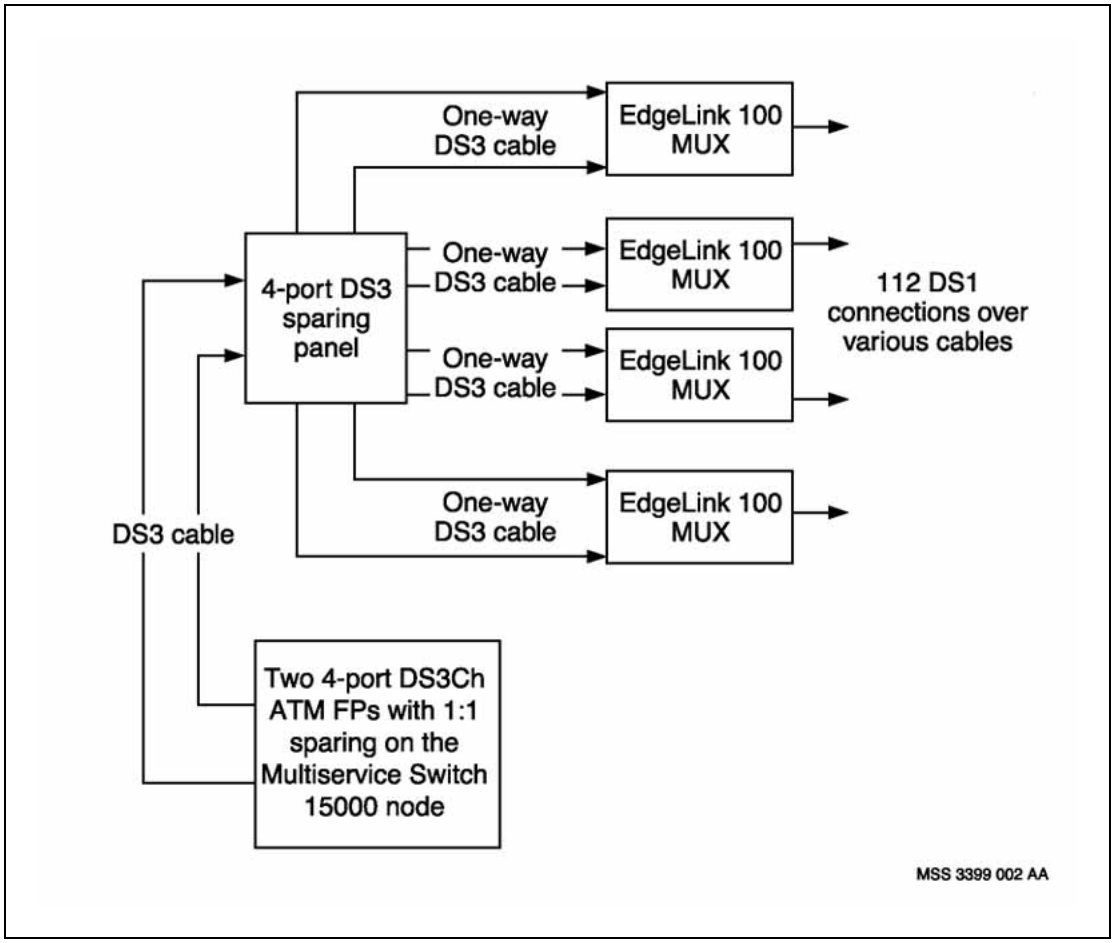
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Connection between one EdgeLink 100 MUX and a Multiservice Switch 15000 node



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Connection between four EdgeLink 100 MUXs and a Multiservice Switch 15000 node



To configure the EdgeLink 100 MUX to interface with a Multiservice Switch 15000 node, refer to the following tables:

- "DS1 provisioning parameters" (page 157)
- "DS3 provisioning parameters" (page 158)

DS1 provisioning parameters

DS1 interface status	Options
channel name = default	none
line code = B8ZS	ami or B8ZS
line buildout = 0-133 feet	0-133 feet, 133-266 feet, 266-399 feet, 399-533 feet, or 533-655 feet
loopback = none	none
service mode = in-service	in-service or out-of-service
equipped state = equipped	equipped, unequipped, or disabled

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

DS1 interface status	Options
input activity = activity present	cannot be set because it is operational or out-of-service
mask state = monitoring	cannot be set because it is operational

DS3 provisioning parameters

DS3 interface status	Options
operation mode = c-bit parity mode (data link disabled)	c-bit parity mode (data link enabled), c-bit parity mode (data link disabled), or M13 mode
line code = B3ZS	cannot be set
line buildout = 0-100 feet	0-100 feet, 100-200 feet, or 200-450 feet
transmit timing = local	local or loop
BER threshold = 10^{-9}	10 -9, 10 -8, 10 -7, or 10 -6
BER value = 7.5E - 11	none
loopback = none	none
service mode = in-service	in-service or out-of-service

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Use cases for Network incremental growth

This section presents use cases for Network incremental growth. It gives a high-level overview of the steps for adding new components to an existing network solution as follows:

- Packet Trunking - AAL1 (PT-AAL1)
- Universal Access - AAL1 (UA-AAL1)
- Packet Trunking - AAL2 (PT - AAL2)
- Universal Access - IP (UA-IP)

This chapter includes the following sections:

- "Use cases for incremental growth of a Carrier VoIP network (PT-AAL1/UA-AAL1)" (page 159)
- "Use cases for incremental growth of a PT-AAL2 network" (page 179)
- "Use cases for incremental growth of a UA-IP network" (page 184)

Use cases for incremental growth of a Carrier VoIP network (PT-AAL1/UA-AAL1)

This section presents use cases for incremental growth of an existing Packet Trunking - AAL1 (PT-AAL1) or Universal Access - AAL1 (UA-AAL1) solution. It gives a high-level overview for the addition of new components to a network.

This section includes the topics as follows:

- "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160)
- "Addition of new node-to-node ATM interface (PT-AAL1/UA-AAL1)" (page 162)
- "Addition of new MG4000 to Carrier VoIP network (PT-AAL1/UA-AAL1)" (page 164)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Addition of new MG9000 with OC-3 to Carrier VoIP network (UA-AAL1)" (page 166)
- "Addition of new MG9000 with DS1 IMA to Carrier VoIP network (UA-AAL1)" (page 169)
- "Addition of new MG9000 with DS3 ATM (UA-AAL1)" (page 172)
- "Addition of new IW-SPM (PT-AAL1/UA-AAL1)" (page 174)
- "Addition of new DPT-SPM (PT-AAL1/UA-AAL1)" (page 177)

Note: The installation, configuration, and connectivity of the component hardware is beyond the scope of this chapter.

Addition of new FP pair (PT-AAL1/UA-AAL1)

Nortel assumes that the new FP pair is being added to a Nortel Multiservice Switch 15000 node configured as part of an existing PT-AAL1 or UA-AAL1 network.

- "Prerequisites to adding a new FP pair" (page 160)
- "Adding a new FP pair to a node" (page 161)
- "Considerations for adding a new FP pair to a node" (page 161)

Prerequisites to adding a new FP pair

- Prior to starting to add the new FP pair, consult your completed network and site plans. Network planning is usually performed by the customer with assistance from representatives from the Nortel network engineering group. Record the type and version of the FPs that are being installed as well as the slot numbers in the site plan. For more information on choosing FP slots, see *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel Multiservice Data Manager Nodal Provisioning templates to configure the new FP pair is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding a new FP pair to a node
Procedure steps

Step	Action
1	Identify the available slots for a new pair of FPs. Once you have installed the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the new FPs on the Multiservice Switch 15000 node by applying any of the templates as follows: a. *PT-AAL1/WUA-AAL1 FP-4pOC3SmIrAtm* b. *PT-AAL1/WUA-AAL1 FP-4pOC12SmIrAtm* c. *WUA-AAL1 FP-4pDS3ChAtm* d. *PT-AAL1/WUA-AAL1 FP-16pOC3SmIrAtm* e. *WUA-AAL1 FP-12pDS3Atm*
3	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
4	If you are adding more than one new FP pair, repeat step 1 to task 3 for each new pair of FPs added to the node.
5	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.
6	Using the MDM Network Model tool, regenerate the Network Model for the modified nodes and save the new model.

—End—

Considerations for adding a new FP pair to a node

The following considerations were kept in mind by Nortel network engineering group when adding a new FP pair to a node:

- At initial installation of the node, FP pairs can be put through the full suite of available card or port tests. However, when adding an FP pair to an existing shelf that is currently providing service, the set of recommended card or port tests should be limited to those that are guaranteed not to effect other parts of the system.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- Adding a 16-port OC3 ATM FP pair with in-band connections over an ATM PNNI link requires different configuration procedures than those used when adding any other FP pair.
- Both types of 4-port OC-12c/STM-4 FP, NTHW11 and NTHW86, can be deployed in a mixed pair of redundant FPs. The ipRoutesPoolCapacity attribute for the FP needs to be configured with a value of zero before the NTHW11 FP is installed as a replacement FP. For more details on the required configuration for this deployment, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

  Note: The NTHW11 version of the 4-port OC-12 FP cannot be deployed in Carrier VoIP Network configurations employing in-band OAM.

Addition of new node-to-node ATM interface (PT-AAL1/UA-AAL1)

This section is a high-level overview of the steps involved in adding a new node-to-node ATM link to an existing PT-AAL1 or UA-AAL1 network.

- "Prerequisites to adding a new Multiservice Switch ATM PNNI" (page 162)
- "Adding a new Multiservice Switch ATM PNNI" (page 163)
- "Considerations for adding a new Multiservice Switch ATM PNNI" (page 163)

Prerequisites to adding a new Multiservice Switch ATM PNNI

- Prior to starting to add a new Nortel Multiservice Switch ATM PNNI, consult your completed network and site plans. Network planning is usually performed by the customer with assistance from representatives from the Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure new FPs is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding a new Multiservice Switch ATM PNNI
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port or 16-port OC-3, 4-port OC-12 or 12-port DS3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Once you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the new interfaces on the Multiservice Switch 15000 node by applying any of the templates for ATM PNNI interfaces, as follows: a. *PT-AAL1/WUA-AAL1 ATM PNNI Interface-4pOC3* b. *PT-AAL1/WUA-AAL1 ATM PNNI Interface-16pOC3* c. *WUA-AAL1 ATM PNNI Interface-12pDS3*
3	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
4	If you are adding more than one new ATM PNNI, repeat step 1 to step 3 for each new ATM PNNI.
5	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.
6	Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

—End—

Considerations for adding a new Multiservice Switch ATM PNNI

The following considerations were kept in mind by the Nortel network engineering group when adding a new Nortel Multiservice Switch ATM PNNI:

- If you are using in-band management over the PNNI link, additional configuration is required.
- You may wish engineer bandwidth pools rather than accept the default values.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- Engineer the virtual path connection (VPC) space if you are running digital subscriber line (DSL) virtual paths (VPs).
- Adding a 16-port OC3 ATM FP pair with in-band connections over an ATM PNNI link requires different configuration procedures than those used when adding any other FP pair.
- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "EM/<remoteNodeName> ATMIF/<remote AtmIfinstance>", where <remoteNodeName> and <remote AtmIfinstance> are customer-defined.

Addition of new MG4000 to Carrier VoIP network (PT-AAL1/UA-AAL1)

Nortel assumes that the new MG4000 is being added to an existing network that includes a Nortel Multiservice Switch 15000 node already loaded with either a 4-port OC-3 or 16-port OC-3 function processor (FP) pair with an available pair of protected ports.

- "Prerequisites to adding a new MG4000" (page 164)
- "Adding a new MG4000" (page 165)
- "Considerations for adding a new MG4000" (page 166)

Prerequisites to adding a new MG4000

- Prior to starting to add the new MG4000, you need to have completed your network planning. Network planning is usually performed by the customer with assistance from representatives from the Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure the new MG4000 is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity between MDM servers and Multiservice Switch 15000 nodes is assumed to have been established before the new MG4000 is added to the network.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- Before a new MG4000 is added to the network both the MDM servers and Multiservice Switch 15000 nodes are assumed to be running compatible software loads. For more information, see Nortel GIS Installation Methods documents.
- MDM servers need to have downloaded the most recent patches for the software release running on the server.

Adding a new MG4000
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port or 16-port OC-3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Once you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the interface between the MG4000 and the Multiservice Switch 15000 node by applying either the *PT-AAL1/WUA-AAL1 MG4000 ATM Interfaces 4pOC3 or PT-AAL1/WUA-AAL1 MG4000 ATM Interfaces 16pOC3* template.
3	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
4	Repeat step 1 to step 3 for each new MG4000 ATM Interface added to the Multiservice Switch 15000 node.
5	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.
6	Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG4000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG4000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
7	Link the newly created MG4000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see

Copyright © 2006, Nortel Networks Nortel Networks Confidential

241-6001-015 Nortel Multiservice Data Manager Network Model Administration.

8 Using the MDM Network Model tool, create an entry or icon for the new MG4000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

10 Using the MDM Nodal Provisioning tool, create two control PVCs connecting the Multiservice Switch 15000 node and the CS2000. Perform any necessary modifications to the Multiservice Switch 15000 nodes in the network after creating these PVCs.

11 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

—End—

Considerations for adding a new MG4000

The following considerations were kept in mind by the Nortel network engineering group when adding a new MG4000:

- The signaling PVCs connected to the MG4000 need to be routed as diversely as possible.
- On 16-port OC3 FP pairs with in-band connections, MG4000 connection space must be engineered to remain within the connection space capacity for this FP.
- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/MG4K-<SPMID> -<CLLI>", where <SPMID> and <CLLI> are customer-defined.

Addition of new MG9000 with OC-3 to Carrier VoIP network (UA-AAL1)

Nortel assumes that the new MG9000 is being added to an existing Carrier VoIP UA-AAL1 solution that includes a Nortel Multiservice Switch 15000 node already loaded with either a 4-port OC-3 or 16-port OC-3 function processor (FP) pair with an available pair of protected ports.

- "Prerequisites to adding a new MG9000 with OC-3" (page 167)
- "Adding a new MG9000 with OC-3" (page 167)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "Considerations for adding a new MG9000 with OC-3" (page 169)

Prerequisites to adding a new MG9000 with OC-3

- Prior to starting to add the new MG9000, you need to have completed your network planning. Network planning is usually performed by the customer with assistance from representatives from the Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure the new MG9000 is contained in the Nortel GIS Installation Methods documents and the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity between MDM servers and Multiservice Switch 15000 nodes is assumed to have been established before the new MG9000 is added to the network.
- Before a new MG9000 is added to the network both the MDM servers and Multiservice Switch 15000 nodes are assumed to be running compatible software loads.
- MDM servers need to have downloaded the most recent patches for the software release running on the server.

Adding a new MG9000 with OC-3
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-3 or 16-port OC-3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). After you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node by applying either the *WUA-AAL1 MG9000 ATM Interfaces-4pOC3* or *WUA-AAL1 MG9000 ATM Interfaces-16pOC3* template.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

3 Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. Consult the table with values for MG9000 non-IMA interfaces.

4 Repeat step 1 to step 3 for each new MG9000 ATM interface added to the Multiservice Switch 15000 node.

5 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

6 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

7 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

8 Using the MDM Network Model Editor tool, choose either the FDMOD or GEN icon to represent the new MG9000 in the Carrier VoIP network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Considerations for adding a new MG9000 with OC-3

The following considerations were kept in mind by the Nortel network engineering group when adding a new MG9000:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/MG9K-<SPMID>-<CLLI>", where <SPMID> and <CLLI> are customer-defined.
- Internode ESA must be defined for each MG9000, if required.

Addition of new MG9000 with DS1 IMA to Carrier VoIP network (UA-AAL1)

Nortel assumes that the new MG9000 with inverse multiplexing for ATM (IMA) is being added to an existing UA-AAL1 solution that includes a Nortel Multiservice Switch 15000 node already loaded with 4-port DS3ChAtm FPs and available DS3 ports.

- "Prerequisites to adding a new MG9000 with DS1 IMA" (page 169)
- "Adding a new MG9000 with DS1 IMA" (page 170)
- "Considerations for adding a new MG9000 with DS1 IMA" (page 171)

Prerequisites to adding a new MG9000 with DS1 IMA

- Prior to starting to add the new MG9000, you need to have completed your network planning. Network planning is usually performed by the customer with assistance from representatives from the Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure the new MG9000 is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity between the MDM servers and the Nortel Multiservice Switch 15000 nodes is assumed to have been established before the new MG9000 is added to the network.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- Before a new MG9000 is added to the network both the MDM servers and Multiservice Switch 15000 nodes are assumed to be running compatible software loads.
- MDM servers need to have downloaded the most recent patches for the software release running on the server.

Adding a new MG9000 with DS1 IMA
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port DS3ChAtm FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Once you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the required DS3 ports on the 4-port DS3ChAtm FP. You need to configure the DS3 port first using the *WUA-AAL1 DS3 port - 4pDS3ChAtm* template and values from the Network Engineering Specification Book before configuring the IMA interface. Repeat this step for each DS3 port that needs to be configured.
3	Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node by applying the *WUA-AAL1 MG9000 2xDS1 - IMA ATM Interface - 4pDS3ChAtm* template once and the *WUA-AAL1 1xDS1- IMA Link - 4pDS3ChAtm* template for each additional interface. ***Note:*** The *WUA-AAL1 MG9000 2xDS1 - IMA ATM Interface* template configures a 2xDS1 IMA MG9000 link to another Multiservice Switch 15000 node using a DS3 port on a 4-port DS3ChAtm FP. The *WUA-AAL1 1xDS1-IMA Link - 4pDS3ChAtm* template provisions a DS1-IMA link on the IMA virtual port of a DS3 port of a 4-port DS3ChAtm FP.
4	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. Consult the table with values for MG9000 ATM IMA interfaces.
5	Repeat step 1 to step 4 for each new MG9000 ATM IMA interface added to the Multiservice Switch 15000 node.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

6 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

7 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

8 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

9 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

11 Using the Command Console, activate and commit the service data changes.

—End—

Considerations for adding a new MG9000 with DS1 IMA

The following considerations were kept in mind by Nortel network engineering group when adding a new MG9000 with ATM IMA:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/MG9K-<SPMID> -<CLLI>", where <SPMID> and <CLLI> are customer-defined.
- Internode ESA must be defined for each MG9000, if required.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Addition of new MG9000 with DS3 ATM (UA-AAL1)

This section gives an overview of the steps for adding a new MG9000 with a 12pDS3 user-to-network interface (UNI) interface to an existing UA-AAL1 network.

The network must include a Nortel Multiservice Switch 15000 node already loaded with 12-port DS3 ATM type FP cards, with an available pair of DS3 ports.

- "Prerequisites to adding a new MG9000 with DS3 ATM" (page 172)
- "Adding a new MG9000 with DS3 ATM" (page 172)
- "Considerations for adding a new MG9000 with DS3 ATM" (page 174)

Prerequisites to adding a new MG9000 with DS3 ATM

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel's network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of Nortel Multiservice Data Manager, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity must exist between MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- You must download the most recent patches for the software release running on the MDM servers.

Adding a new MG9000 with DS3 ATM
Procedure steps

Step	Action
1	Identify the available ports on a pair of 12-port DS3 Atm FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Install and configure the new FP pair, then continue to the next step.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

2 Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node. Do this by applying the *WUA-AAL1 MG9000 DS3 ATM Interface-12pDS3Atm* template.

3 Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the table that contains values for MG9000 DS3 ATM interfaces.

4 Repeat step 1 to step 3 for each new MG9000 DS3 ATM interface you add to the Multiservice Switch 15000 node.

5 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

6 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

7 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

8 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Using the Command Console, activate and commit the service data changes.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Considerations for adding a new MG9000 with DS3 ATM

Nortel network engineering group considers the following when adding a new MG9000 with DS3 ATM:

- This interface requires use of a 4pDS3 sparing panel (code NTHR79xx-xx). Use only ports 0 through 3, and connect a single panel to P0 (data), and P3 (control). Therefore, one FP is deployed with one NTHR79 4-port 1:1 sparing panel.
- Unlike the DS3 private network-to-network (PNNI) interface between Nortel Multiservice Switch 15000 nodes, with this interface only one channel can exist between the MG9000 and the Multiservice Switch 15000 node. If that channel is lost, the MG9000 is in ESA until the channel is returned to service.
- You can use deployed 12pDS3 cards on which PNNI interfaces are already provisioned to provision new MG9000 interfaces.
- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/MG9K-<SPMID> -<CLLI>", where <SPMID> and <CLLI> are customer-defined.
- Internode ESA must be defined for each MG9000, if required.

Addition of new IW-SPM (PT-AAL1/UA-AAL1)

Nortel assumes that you are adding the new Interworking-Spectrum Peripheral Module (IW-SPM) to an existing Carrier VoIP solution.

The network must include a Nortel Multiservice Switch 15000 node already loaded with an 4-port OC-3 or 16-port OC-3 function processor (FP) pair, with an available pair of protected ports.

- "Prerequisites to adding a new IW-SPM" (page 174)
- "Adding a new IW-SPM" (page 175)
- "Considerations for adding a new IW-SPM" (page 176)

Prerequisites to adding a new IW-SPM

- Prior to starting to add the new IW-SPM, you need to have completed your network planning. Network planning is usually performed by the customer with assistance from representatives from Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure the new IW-SPM is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity between MDM servers and Multiservice Switch 15000 nodes is assumed to have been established before the new IW-SPM is added to the network.
- Before a new IW-SPM is added to the network both the MDM servers and Multiservice Switch 15000 nodes are assumed to be running compatible software loads.
- MDM servers need to have downloaded the most recent patches for the software release running on the server.

Adding a new IW-SPM
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-3 or 16-port OC-3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Once you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the interface between the IW-SPM and the Multiservice Switch 15000 node by applying either the *PT-AAL1/WUA-AAL1IW-SPM Interface 4pOC3* or *PT-AAL1/WUA-AAL1 IW-SPM Interface 16pOC3* template.
3	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
4	Repeat step 1 to step 3 for each new IW-SPM Interface added to the Multiservice Switch 15000 node.
5	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

6 Using the MDM Network Model tool, create an entry or icon for the new IW-SPM and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

7 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

8 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new IW-SPM in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the IW-SPM while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Link the newly created IW-SPM icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

—End—

Considerations for adding a new IW-SPM

The following considerations were kept in mind by Nortel network engineering group when adding a new IW-SPM:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/IW-SPM-<SPMID> -<CLLI>", where <SPMID> and <CLLI> are customer-defined.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Addition of new DPT-SPM (PT-AAL1/UA-AAL1)

Nortel assumes that the new Dynamic Packet Trunking-Spectrum Peripheral Module (DPT-SPM) is being added to an existing solution that includes a Nortel Multiservice Switch 15000 node already loaded with either a 4-port OC-3 or 16-port OC-3 function processor (FP) pair with an available pair of protected ports.

- "Prerequisites to adding a new DPT-SPM" (page 177)
- "Adding a new DPT-SPM" (page 178)
- "Considerations for adding a new DPT-SPM" (page 179)

Prerequisites to adding a new DPT-SPM

- Prior to starting to add the new DPT-SPM, you need to have completed your network planning. Network planning is usually performed by the customer with assistance from representatives from Nortel network engineering group.
- You will need to refer to some customer-specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between the customer and Nortel network engineering group.
- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel MDM Nodal Provisioning templates to configure the new DPT-SPM is contained in the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- Connectivity between MDM servers and Nortel Multiservice Switch 15000 nodes is assumed to have been established before the new DPT-SPM is added to the network.
- Before a new DPT-SPM is added to the network both the MDM servers and Multiservice Switch 15000 nodes are assumed to be running compatible software loads.
- MDM servers need to have downloaded the most recent patches for the software release running on the server.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding a new DPT-SPM
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-3 or 16-port OC-3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (PT-AAL1/UA-AAL1)" (page 160). Once you have installed and configured the new FP pair, continue this task.
2	Using the MDM Nodal Provisioning tool, configure the interface between the DPT-SPM and the Multiservice Switch 15000 node by applying either the *PT-AAL1/WUA-AAL1 DPT-SPM Interfaces-4pOC3* or *PT-AAL1/WUA-AAL1 DPT-SPM Interfaces-16pOC3* template.
3	Perform any necessary additional network-specific configuration using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
4	Repeat step 1 to step 3 for each new DPT-SPM interface added to the Multiservice Switch 15000 node.
5	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.
6	Using the MDM Network Model tool, create an entry or icon for the new DPT-SPM and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
7	Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.
8	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Considerations for adding a new DPT-SPM

The following considerations were kept in mind by Nortel network engineering group when adding a new DPT-SPM:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/DPT-SPM-<SPMID> -<CLLI>", where <SPMID> and <CLLI> are customer-defined.

Use cases for incremental growth of a PT-AAL2 network

This section presents use cases for the incremental growth of an existing Packet Trunking- AAL2 (PT-AAL2) solution. It gives an overview of the steps for adding new FPs to the network.

Nortel assumes that the new FPs are being added to a Media Gateway 15000 node configured as part of an existing PT -AAL2 network. Supported 4pOC12 FPs must be configured as pairs. An exception to the rule that FPs must be configured as pairs exists in the PT-AAL2 solution, such that, in the PT-AAL2 solution the 4pOC3 is configured unprotected.

Adding new Function Processors to the MG15000

For each pair of additional function processors (FP) that you add, apply the corresponding FP template and activate the changes. After adding the FPs using the appropriate template you will add the interfaces. The VSP3-o FP's have a TDM interface on which only port 0 is supported. The interface to the MGC and all 84 TDM trunks are added 28 at a time.

The 2pVSP4e FPs have a TDM interface in which both ports 0 and 1 are supported. The interface to the MGC and all 168 TDM trunks are added 28 at a time.

Prerequisites

- Before starting to add the new FP pair, consult your completed network and site plans. Network planning is usually performed by you with assistance from representatives of the Nortel network engineering group. Record the type and version of the FPs that are being installed, as well as, the slot numbers in the site plan. For more information on choosing FP slots, see *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.
- You will need to refer to some specific values that are found in the Network Engineering Specification Book. This book is the product of co-operation between your company and the Nortel network engineering group.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Note: The data values entered for a shelf are typically provided in a Network Engineering Specification Book. When a field shows an editable default value in a template, it is the template user's responsibility to ensure it is consistent with the Specification Book.

- You will need to refer to some specific values that are found in *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- Information on using Nortel Multiservice Data Manager Nodal Provisioning templates to configure the new FP pair is contained in the *241-6001-023 Nortel Multiservice Data Manager Configuration Tools*.
- The initial CP and Shelf-level parameters setup must have been previously executed.

  In the base commissioning steps, the FP's that were inserted in the shelf were created with a base feature set that was sufficient to run some diagnostic tests after being physically installed, but would not typically have included any carrier grade configuration.
- Ensure you have deleted the FP configuration that resulted from the initial base commissioning. You will replace it using the NP template-based FP configuration.

Adding new functional processors to a node
Procedure steps

Step	Action
1	Identify the available slots for the new FPs.
2	Manually delete the LP for each LP other than 0 (LP/0 is the CP) that existed after the base commissioning steps using the NP tool but do not activate.
3	Apply the appropriate template as follows for the new FPs that you add using the MDM Nodal Provisioning tool: a. Apply the *PT-AAL2 FP-4pOC3SmIrAtm_Unprotected* template for each 4pOC3SmIrAtm FP that you add. b. Apply the *PT-AAL2 FP-4pOC12SmIrAtm* template for each 4pOC12SmIrAtm FP pair that you add. c. Apply the *PT-AAL2 FP-2pOC3ChSmIrVsp* template for each 2pOC3ChSmIrVsp3-o or 2pOC3ChSmIrVsp4e FP pair that you add.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Note: The 2pOC3ChSmIrVsp template provisions 63 E1 TDM ISUP trunks on 2pOC3ChSmIrVsp3-o and 2pOC3ChSmIrVsp4e FPs. All the Vc12 trunks under this Vc4 hierarchy must not have been previously configured.

4 Set the Collection/accounting Spooler spooling component to off.

5 Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

Note: As you perform the steps of this procedure, it is good practice to issue a "save" to the switch on a regular basis to save the provisioning. The use of templates should not cause one to avoid this practice. If you encounter a data entry error that is not easily repaired, you can go back to the last saved view to fix the error.

When you activate the changes, all the required data model files for subsequently applied templates are pulled in to create any possible type of component on the particular FP.

6 Add the VSP and TDM interfaces.

Adding the VSP and TDM physical interfaces create the component infrastructure for the VSP pair, including its packet interfaces to the MGC. Standards-based H.248 protocol is used and VRAP is the connectivity scheme. When you create these interfaces you are creating physical interfaces to which you can add TDM trunks. When the template drop-site is an LP, and the target is a pair of optical cards (there are two LPs one for each card) apply the template against the lower numbered LP. In all cases of 1+1 protection, the template configures both LP's.

a. Apply the *PT-AAL2 IF-TDM-2pOC3ChSmIrVsp* template for each VSP3-o pair in the Network Engineering Specification Book.

b. Apply the *PT-AAL2 IF-MGC-H248-2pOC3ChSmIrVsp3-o* template for each VSP3-o pair in the Network Engineering Specification Book.

c. If required, manually create other associated IP routing (e.g., static route) entries specified in the Network Engineering Specification Book.

d. Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

7 Add the TDM Trunk Interfaces

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding TDM Trunk interfaces create DS1-based TDM ISUP trunks. In this release, the 84 trunks on a VSP3-o pair are added 28 at a time.

a. Ensure the VSP and TDM interfaces have been applied and activated.

b. Apply the *PT-AAL2 TT-28ISUPTrunks-2pOC3ChSmIrVsp3-o* template for STS/0 on each VSP3-o, as specified in the Network Engineering Specification Book.

c. Apply the *PT-AAL2 TT-28ISUPTrunks-2pOC3ChSmIrVsp3-o* template for STS/1 on each VSP3-o, as specified in the Network Engineering Specification Book.

d. Apply the PT-AAL2 TT-28ISUPTrunks-2pOC3ChSmIrVsp3-o template for STS/2 on each VSP3-o, as specified in the Network Engineering Specification Book.

e. Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

8 Add the PNNI Interfaces.

Adding PNNI interfaces create PNNI trunks to other MG15000's. PNNI interfaces must be added on each end.

a. Ensure the 4pOC12 FP pair has been applied and activated.

b. Apply the IF-PNNI-4pOC12SmIrAtm template, as specified in the Network Engineering Specification Book.

c. Delete the following components that were added by the template using the NP tool, if, according to the Specification book, there is no IP over ATM traffic on the PNNI links between nodes:

i. Delete the VCC (default instance 0.32) from the ATMIF that was just added.

ii. Delete the ATMMPE that was just added.

iii. Delete the ProtocolPort (default instance <AGGn/MGn>) just added under the call processing VR (default instance CALLP).

iv. Manually change the ATMIF VCC VCD TM forceTagging attribute to disabled using the NP tool if specified in the Specification Book.

d. Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

9 Add the MGX Interfaces.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding MGX interfaces create interfaces to the 3rd party core ATM switches. MGX interfaces are added in order, as specified in the Specifications Book and the template assumes that at most one MGX interface is required per shelf.

a. Ensure the 4pOC12 FP's has been applied and activated.

b. Apply the IF-MGX-4pOC12SmIrAtm template, as specified in the Network Engineering Specification Book.

c. Manually change the ATMIF oamSegmentBoundary to Yes using the NP tool if Yes is specified in the Specification Book.

d. Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

10 Add the Audio Server (AS) Interfaces as required.

Adding AS interfaces create links to the audio server equipment. AS interfaces can be added in order, as specified in the Specifications Book.

a. Ensure the 4pOC3 FP (unprotected) has been applied and activated.

b. Apply the IF-AS-4pOC3SmIrAtm template, as specified in the Network Engineering Specification Book.

c. Activate the service data changes using the MDM Nodal Provisioning tool or Command Console.

11 Perform any necessary additional network-specific configuration such as Userids, static routes, OC3 interfaces to the ERS 8600, etc. using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

12 If you are adding more than one new set of FP's, repeat step 1 to step 11 as required for each new set of FPs added to the node.

13 If none of the changes in the above steps involve critical attributes, set the Prov Am hitlessActivation attribute to enabled. Otherwise, an additional activation with the hitlessActivation attribute set to disabled is required.

14 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

15 Using the MDM Network Model tool, regenerate the Network Model for the modified nodes and save the new model.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

—End—

Considerations for adding a new FP pair to a node

The following considerations were kept in mind by Nortel network engineering group when adding a new FP pair to a node:

- At initial installation of the node, FP pairs can be put through the full suite of available card or port tests. However, when adding an FP pair to an existing shelf that is currently providing service, the set of recommended card or port tests should be limited to those that are guaranteed not to effect other parts of the system.
- For more details on the required configuration for this deployment, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Use cases for incremental growth of a UA-IP network

This section presents use cases for incremental growth of an existing Universal Access - IP (UA-IP) solution. It gives an overview of the steps for adding new components to a network.

This section includes the topics as follows:

- "Addition of new FP pair (UA-IP)" (page 185)
- "Addition of new MG9000 with OC-3 (UA-IP)" (page 186)
- "Addition of new MG9000 with STS-1/DS3 (UA-IP)" (page 189)
- "Addition of new MG9000 with DS1 IMA (UA-IP)" (page 191)
- "Addition of new Multiservice Switch inter-shelf IP interface to Carrier VoIP network (UA-IP)" (page 194)
- "Addition of new CS-LAN with GE (LAG and no LAG) (UA-IP)" (page 197)
- "Addition of new CS-LAN with OC-12 (UA-IP)" (page 199)
- "Addition of new VSP and TDM physical interface (UA-IP)" (page 202)
- "Addition of new TDM trunk interface (UA-IP)" (page 205)

Note: The installation, configuration, and connectivity of the component hardware is beyond the scope of this chapter.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Addition of new FP pair (UA-IP)

This section is an overview of the steps for adding a new FP pair to a Nortel Multiservice Switch 15000 node in an existing UA-IP network.

This section includes the topics as follows:

- "Prerequisites to adding a new FP pair" (page 160)
- "Adding a new FP pair to a node" (page 161)
- "Considerations for adding a new FP pair to a node" (page 161)

Prerequisites for adding a new FP pair to a node

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- Consult your completed network and site plans. Record the type and version of the FPs that you are installing, as well as the slot numbers in the site plan. For more information on choosing FP slots, see *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*.
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.

Adding a new FP pair to a node
Procedure steps

Step	Action
1	Identify the available slots for a new pair of FPs. Install the new FP pair, then continue to the next step.
2	Using the MDM Nodal Provisioning tool, configure the new FPs on the Multiservice Switch 15000 node. Apply any of the templates as follows: a. *UA-IP FP-4pOC3SmIrAtm* b. *UA-IP FP-4pOC12SmIrAtm* c. *UA-IP FP-12pDS3Atm*

Copyright © 2006, Nortel Networks Nortel Networks Confidential

d. *UA-IP FP-4pDS3ChAtm*

e. *UA-IP FP-4pGE*

f. *UA-IP FP-4pOC3ChSmIr-TDM*

g. *UA-IP FP-2pGeMmSrVsp3*

h. *UA-IP FP-2pOC3ChSmIrVsp*

3 Configure the network, as required. Use values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

4 To add more than one new FP pair to the node, repeat step 1 through step 3 for each new pair of FPs added.

5 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

6 Using the MDM Network Model tool, regenerate the Network Model for the modified nodes and save the new model.

—End—

Considerations for adding a new FP pair to a node

The network engineering group at Nortel considers the following when adding a new FP pair to a Nortel Multiservice Switch 15000 node:

- At initial installation of the Multiservice Switch shelf, FP pairs can be put through the full suite of available card or port tests. However, when adding an FP pair to an existing shelf that is currently providing service, limit the set of recommended card or port tests to those that are guaranteed not to affect other parts of the system.

Addition of new MG9000 with OC-3 (UA-IP)

This section is an overview of the steps for adding a new MG9000, with an OC-3 interface, to an existing UA-IP network.

The network must include a Nortel Multiservice Switch 15000 node already loaded with a 4-port OC-3 function processor (FP) pair, with an available pair of protected ports.

In UA-IP, the MG9000 is supported on the same interfaces as in PT-AAL1 and UA-AAL1. However, the 12pDS3Atm and 4pDS3ChAtm FP cards do not support IP. Therefore, when configuring interfaces to the MG9000 on these cards, you must set up an optical hairpin. The optical hairpin terminates the IP from the MG9000.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Note: This procedure creates two host entries only, one for MG9000 OAM, and another for MG9000 Call Control. You must create the other 16 entries manually.

This section includes the topics as follows:

- "Prerequisites to adding a new MG9000 with OC-3" (page 187)
- "Adding a new MG9000 with OC-3" (page 187)
- "Considerations for adding a new MG9000 with OC-3" (page 189)

Prerequisites to adding a new MG9000 with OC-3

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- You must download the most recent patches for the software release running on the MDM servers.

Adding a new MG9000 with OC-3
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-3 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair. Then continue to the next step.
2	Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node. Do this by applying the *UA-IP IF-MG9000-4pOC3SmIrAtm* template.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

3 Configure the network, as required. Use values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the Attribute Summary, consult the table that contains values for MG9000 OC-3 interfaces.

4 For each new MG9000 OC-3 interface you add to the Multiservice Switch 15000 node, repeat step 1 to step 3.

5 Manually create the remaining address resolution protocol (ARP) Host entries.

6 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

7 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

8 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

9 Using the MDM Network Model Editor tool, choose either the FDMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Considerations for adding a new MG9000 with OC-3

The network engineering group at Nortel considers the following when adding a new MG9000 with OC-3:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. For the MG9000, Nortel recommends a name format of "GEN/MG9K_<id>", where <id> is customer-defined. For the optical hairpin, Nortel recommends a name format of "EM/<remoteNodeName> atmif/<remote AtmIf instance>", where <remoteNodeName> and <remote AtmIf instance> are customer-defined.

Addition of new MG9000 with STS-1/DS3 (UA-IP)

This section is an overview of the steps for adding a new MG9000 with STS-1/DS3 interface to an existing UA-IP network.

The network must include a Nortel Multiservice Switch 15000 node already loaded with 12-port DS3 ChAtm FPs and available DS3 ports.

This section includes the topics as follows:

- "Prerequisites to adding a new MG9000 with STS-1/DS3" (page 189)
- "Adding a new MG9000 with STS-1/DS3" (page 190)
- "Considerations for adding a new MG9000 with STS-1/DS3" (page 191)

Prerequisites to adding a new MG9000 with STS-1/DS3

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel's network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of the Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Multiservice Switch 15000 nodes.
- Both the MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- You must download the most recent patches for the software release running on the MDM servers.

Adding a new MG9000 with STS-1/DS3
Procedure steps

Step	Action
1	Identify the available ports on a pair of 12-port DS3Atm FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step.
2	If required by the Network Engineering Specification Book only, add a new hairpin interface. To configure a new hairpin interface, use the MDM Nodal Provisioning tool. If the optical hairpin is on a 4pOC3 FP, apply the *UA-IP IF-Hairpin-4pOC3SmIrAtm* template. If the optical hairpin is on a 4pOC12 FP, apply the *UA-IP IF-Hairpin-4pOC12SmIrAtm* template.
3	Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node. Do this by applying the *UA-IP IF-MG9000-12pDS3Atm* template. Apply it for each of the MG9000 DS3 interfaces in the Network Engineering Specification Book. ***Note:*** The *UA-IP IF-MG9000-12pDS3Atm* template creates an interface to an MG9000 on 12psDS3Atm FPs. It provisions DS3s with an ATMIF on 12pDS3Atm FPs. The DS3s, ATMIF, and so on must not be configured previously.
4	Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the tables that contain values for Hairpin ATM/IP interfaces, and for MG9000 STS-3/DS1 interfaces.
5	Repeat step 1 to step 5 for each new MG9000 STS-1/DS3 interface you add to the Multiservice Switch 15000 node.
6	Manually create the remaining address resolution protocol (ARP) Host entries.
7	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

8 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

10 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

11 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

12 Using the Command Console, activate and commit the service data changes.

—End—

Considerations for adding a new MG9000 with STS-1/DS3

The network engineering group at Nortel considers the following when adding a new MG9000 with STS-1/DS3:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. For the MG9000, Nortel recommends a name format of "GEN/MG9K_<id>", where <id> is customer-defined. For the optical hairpin, Nortel recommends a name format of "EM/<remoteNodeName> atmif/<remote AtmIf instance>", where <remoteNodeName> and <remote AtmIf instance> are customer-defined.

Addition of new MG9000 with DS1 IMA (UA-IP)

This section is an overview of the steps for adding a new MG9000 with DS1 IMA to an existing Carrier VoIP UA-IP network.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

The network must include a Nortel Multiservice Switch 15000 node already loaded with 4-port DS3 ChAtm FPs and available DS3 ports, with at least 8xDS1 available within the DS3 port.

This section includes the following topics:

- "Prerequisites to adding a new MG9000 with DS1 IMA" (page 192)
- "Adding a new MG9000 with DS1 IMA" (page 192)
- "Considerations for adding a new MG9000 with DS1 IMA" (page 194)

Prerequisites to adding a new MG9000 with DS1 IMA

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of the MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between the MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- You must download the most recent patches for the software release running on the MDM servers.

Adding a new MG9000 with DS1 IMA
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port DS3ChAtm FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step.
2	If required by the Network Engineering Specification Book only, add a new hairpin interface. Use the MDM Nodal Provisioning tool to configure the new hairpin. If the hairpin is on a 4pOC3 FP, apply the

Copyright © 2006, Nortel Networks Nortel Networks Confidential

UA-IP IF-Hairpin-4pOC3SmIrAtm template. If the hairpin is on a 4pOC12 FP, apply the *UA-IP IF-Hairpin-4pOC12SmIrAtm* template,

3 Using the MDM Nodal Provisioning tool, configure the required DS3 ports on the 4-port DS3ChAtm FP. Configure the DS3 port first using the *UA-IP IF-DS3port- 4pDs3ChAtm* template and values from the Network Engineering Specification Book. Click Multiple creations to create all required DS3 ports, as per the Network Engineering Specification Book.

4 Using the MDM Nodal Provisioning tool, configure the interface between the MG9000 and the Multiservice Switch 15000 node. Do this by applying the *UA-IP IF-MG9000-8xDS1-4pDS3ChAtm* template. Apply it for each of the MG9000 DS1 IMA interfaces in the Network Engineering Specification Book.

5 Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the table that contains values for MG9000 DS1 IMA interfaces.

6 Repeat step 1 to step 5 for each new MG9000 DS1 IMA interface you add to the Multiservice Switch 15000 node.

7 Manually create remaining address resolution protocol (ARP) Host entries.

8 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

9 Using the MDM Network Model tool, create an entry or icon for the new MG9000 and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 node and save the new model.

11 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see

Copyright © 2006, Nortel Networks Nortel Networks Confidential

241-6001-015 Nortel Multiservice Data Manager Network Model Administration.

12 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Considerations for adding a new MG9000 with DS1 IMA

The network engineering group at Nortel considers the following when adding a new MG9000 with DS1 IMA:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/MG9K_<id>", where <id> is customer-defined.

Addition of new Multiservice Switch inter-shelf IP interface to Carrier VoIP network (UA-IP)

This section gives an overview of the steps for adding a new remote Nortel Multiservice Switch 15000 node, linked with IP over ATM to another Multiservice Switch 15000 node at the CS2000 site, in a UA-IP solution. This is known as a Multiservice Switch IP over ATM inter-shelf trunk interface.

Generally, in a UA-IP solution, one primary Multiservice Switch 15000 node is situated in the office with the CS-LAN. It is connected to the CS-LAN via Gigabit Ethernet (GE), or OC-12. Other Multiservice Switch 15000 nodes can also be in the CS-LAN site, but are not necessarily connected to the CS-LAN for IP control/bearer traffic. The remaining Multiservice Switch 15000 nodes are situated in Remote Wire Centres (RWCs).

The primary Multiservice Switch 15000 node connected to the CS-LAN likely has an inter-shelf IP interface to each of the other Multiservice Switch 15000 nodes. Each of the other nodes is not necessarily directly linked to another RWC. However, in most cases, an IP over ATM connection exists that is used for bearer path IP between each RWC and every other RWC.

This section includes the topics as follows:

- "Prerequisites to adding a new Multiservice Switch IP over ATM inter-shelf trunk interface" (page 195)
- "Adding a new Multiservice Switch IP over ATM inter-shelf trunk interface" (page 195)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

- "Considerations for adding a new Multiservice Switch IP over ATM inter-shelf trunk interface" (page 196)

Prerequisites to adding a new Multiservice Switch IP over ATM inter-shelf trunk interface

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel . Consult the completed network and site plans.
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of the Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.

Adding a new Multiservice Switch IP over ATM inter-shelf trunk interface
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-3 or 4-port OC-12 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step.
2	Add the interface to the CS2000 site end of the new link. Use the MDM Nodal Provisioning tool to configure the new interfaces on the Multiservice Switch 15000 node. Configure each of the inter-shelf Multiservice Switch IP over ATM interfaces in your Network Engineering Specification Book. If the interface is on a 4pOC3 FP, apply the *UA-IP IF-MSS-IPoATM-4pOC3SmIrAtm* template. If the interface is on a 4pOC12 FP, apply the *UA-IP IF-MSS-IPoATM-4pOC12SmIrAtm* template.
3	Add the interface to the remote site end of the new link, using the same templates as in step 2.
4	Using the MDM Nodal Provisioning tool, configure the *UA-IP AC-RWC-Bearer -4pOC3SmIrAtm* template for each of the RWC-to-RWC bearer path connections in your Network Engineering Specification Book.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Alternatively, apply the *UA-IP AC-RWC-Bearer-4pOC12SmIrAtm* template if the inter-shelf link is on a 4pOC12 FP.

5 Manually create the nailed-up relay points (NRPs) on the CS2000-site Multiservice Switch 15000 shelf.

6 Manually create the IP routing (for example, static route) entries on the CS2000-site Multiservice Switch shelf, as specified in the Network Engineering Specification Book.

7 Perform additional network configuration, as required. Use values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

8 To add more than one new Multiservice Switch IP over ATM inter-shelf trunk interface, repeat step 1 to step 6 for each new interface.

9 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the service data changes.

10 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

—End—

Considerations for adding a new Multiservice Switch IP over ATM inter-shelf trunk interface

The network engineering group at Nortel considers the following when adding a new Multiservice Switch IP over ATM inter-shelf trunk interface:

- If you are using in-band management over the private network-to-network interface (PNNI) link, additional configuration is required.
- You can engineer bandwidth pools rather than accept the default values.
- Engineer the virtual path connection (VPC) space if you are running digital subscriber line (DSL) virtual paths (VPs).
- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "EM/<remoteNodeName> ATMIF/<remote AtmIf

Copyright © 2006, Nortel Networks Nortel Networks Confidential

instance>", where <remoteNodeName> and <remote AtmIf instance> are customer-defined.

Addition of new CS-LAN with GE (LAG and no LAG) (UA-IP)

This section is an overview of the steps for adding a new CS-LAN with Gigabit Ethernet (GE), to an existing UA-IP network. The interface can either use, or not use, a Link Aggregation Group (LAG).

The purpose of this procedure is to provide IP connectivity from a Nortel Multiservice Switch 15000 node to the CS-LAN. A CS-LAN consists of a pair of Passport 8600 nodes, connected to a Multiservice Switch 15000 node.

Multiservice Switch 15000 nodes support GE links to a CS-LAN, using either of the configurations as follows:

- Single GE links on separate 4pGE FP cards, on a single Multiservice Switch 15000 node, using Protected Routes.
- Pairs of GE links in a Link Aggregation Group (LAG), with each pair on separate 4pGE cards, on a single Multiservice Switch 15000 node, using Protected Routes.

The existing network must include a Multiservice Switch 15000 node already loaded with 4-port GE FPs and available GE ports.

Generally, in the UA-IP solution, one primary Multiservice Switch 15000 node is situated in the office with the CS-LAN. It is connected to the CS-LAN via GE or OC-12. Other Multiservice Switch 15000 nodes are also in the CS-LAN site. However, they are not necessarily connected to the CS-LAN for IP control/bearer traffic. The remaining nodes are in Remote Wire Centres (RWCs).

This section includes the topics as follows:

- "Prerequisites to adding a new CS-LAN GE interface" (page 197)

Note: This section does not discuss how to convert from single GE links without LAG, to two or more GE links in a LAG.

Prerequisites to adding a new CS-LAN GE interface

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- For information on using the Nodal Provisioning application of Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- You must download the most recent patches for the software release running on the MDM servers.

Adding a new CS-LAN GE interface
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port GE FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step.
2	For GE links without LAG, using the MDM Nodal Provisioning tool, configure the interface to the CS-LAN on the Multiservice Switch 15000 node. Do this by applying the *UA-IP IF-CSLAN-noLAG-4pGE* template for each of the CS-LAN GE interfaces in the Network Engineering Specification Book.
3	For pairs of GE links in a LAG, using the MDM Nodal Provisioning tool, configure the interface to the CS-LAN on the Multiservice Switch 15000 node. Do this by applying the *UA-IP IF-CSLAN-LAG-4pGE* template for each of the CS-LAN GE with LAG interfaces in the Network Engineering Specification Book. If you require a third GE link in the LAG, add it manually.
4	Manually create IP routing (for example, static route) entries specified in the Network Engineering Specification Book.
5	Manually create OSPF including export rules for advertising local address and static routes to the CS-LAN.
6	Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the table that contains values for CS-LAN GE interfaces, with or without LAG.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

7 Repeat step 1 to step 6 for each new CS-LAN GE interface you add to the Multiservice Switch 15000 node.

8 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

9 Using the MDM Network Model tool, create an entry or icon for the new CS-LAN and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

10 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

11 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

12 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Addition of new CS-LAN with OC-12 (UA-IP)

This section is an overview of the steps for adding a new CS-LAN with an OC-12 link, to an existing UA-IP network. A CS-LAN consists of a pair of ERS 8600 nodes.

The existing network must include a Nortel Multiservice Switch 15000 node already loaded with 4-port OC-12 FPs and available OC-12 ports.

Multiservice Switch 15000 nodes support an OC-12 link to a CS-LAN. The interface consists of single OC-12 links, unprotected, from each of two Multiservice Switch 15000 nodes. The nodes are connected with a 1+1 protected IP over ATM inter-shelf link.

Generally, in the UA-IP solution, one primary Multiservice Switch 15000 node is situated in the office with the CS-LAN. It is connected to the CS-LAN via GE or OC-12. Other Multiservice Switch 15000 nodes are also in the

Copyright © 2006, Nortel Networks Nortel Networks Confidential

CS-LAN site. However, they are not necessarily connected to the CS-LAN for IP control/bearer traffic. The remaining nodes are in Remote Wire Centres (RWCs).

> ***Note:*** For OC-12 CS-LAN links, the *UA-IP FP-4pOC12SmIrAtm* template configures a pair of OC-12 cards with default connectionPoolCapacity settings. You must override these settings to create the unprotected VCCs required by the CS-LAN interface. If you apply the FP template initially without overriding these settings, and then change those parameters manually, an outage of both OC-12 cards occurs. If the manual override is required during incremental commissioning, coordinate the change to minimize or eliminate traffic outages on any interfaces currently in use on the OC-12 cards.

This section includes the topics as follows:

- "Prerequisites to adding a new CS-LAN with OC-12" (page 200)
- "Adding a new CS-LAN with OC-12 link" (page 201)
- "Considerations for adding a new CS-LAN with OC-12 link" (page 202)

Prerequisites to adding a new CS-LAN with OC-12

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using Nortel MDM Nodal Provisioning templates to configure the new CS-LAN with optical link, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- You must download the most recent patches for the software release running on the MDM servers.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding a new CS-LAN with OC-12 link
Procedure steps

Step	Action
1	Identify the available ports on a pair of 4-port OC-12 FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step. ***Note:*** In this case, a pair of 4pOC12 FPs must have other ports with LAPS-protected interfaces, in order for the HSM and EP switchovers to meet carrier-grade standards.
2	Using the MDM Nodal Provisioning tool, configure the interface to the CS-LAN on the Multiservice Switch 15000 node. Apply the *UA-IP IF-CSLAN-4pOC12SmIrAtm* template.
3	Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the table that includes values for CS-LAN OC-12 interfaces.
4	Repeat step 1 to step 4 for each new CS-LAN OC-12 interface you add to the Multiservice Switch 15000 node.
5	Manually create IP routing (for example, static route) entries specified in the Network Engineering Specification Book.
6	Manually create OSPF including export rules for advertising local address and static routes to the CS-LAN.
7	Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.
8	Using the MDM Network Model tool, create an entry or icon for the new CS-LAN and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.
9	Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.
10	Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

11 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Considerations for adding a new CS-LAN with OC-12 link

The network engineering group at Nortel considers the following when adding a new CS-LAN with OC-12 link:

- The reporting for the REMOTEATMIFLABEL NTM statistic field is only useful if you give the *remoteAtmInterfaceLabel* attribute a meaningful name that is consistent with the naming conventions used at your company. MDM surveillance also uses this field. Nortel recommends a name format of "GEN/8600_<ID>", where <ID> is customer-defined.

Addition of new VSP and TDM physical interface (UA-IP)

This section is an overview of the steps for adding new voice services processor (VSP) or time division multiplexing (TDM) physical interfaces, to an existing UA-IP network.

The purpose of adding VSP and TDM physical interfaces is to create the component infrastructure for a VSP pair, including its packet interfaces to the media gateway controller (MGC). This procedure also creates physical interfaces for later adding the TDM trunks. For information about adding TDM trunks, see "Addition of new TDM trunk interface (UA-IP)" (page 205).

For VSP3 FP cards, the TDM interfaces must be on 4pOC3 TDM cards.

For VSP3-o FP cards, the TDM interface must be on VSP3-o FP cards, using port 0 only.

For 2pVSP4e FP cards, the TDM interface must be 2pVSP4e FP cards, using ports 0 and 1 only.

This section includes the topics as follows:

- "Prerequisites to adding a new VSP or TDM physical interface" (page 203)
- "Adding a new VSP or TDM physical interface" (page 203)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Prerequisites to adding a new VSP or TDM physical interface

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- The network must use H.248 as the protocol between the MGC and the Media Gateway 15000, and virtual router access point (VRAP) as the connectivity scheme.
- You must download the most recent patches for the software release running on MDM servers.

Adding a new VSP or TDM physical interface
Procedure steps

Step	Action
1	For a new TDM FP OC-3 interface, identify the available ports on a pair of 4-port OC3ChSmIr FPs. If you are unable to identify any available ports, see "Addition of new FP pair (UA-IP)" (page 185). Install and configure the new FP pair, then continue to the next step.
2	For each of the TDM interfaces in the Network Engineering Specification Book, use the MDM Nodal Provisioning tool to configure the required OC-3 ports on the 4-port OC-3 TDM FPs. To do this, use the *UA-IP IF-TDM-4pOC3ChSmIr* template along with values from the Network Engineering Specification Book. Repeat this step for each OC-3 TDM port to configure.
3	For each of the VSP3-o or 2pVSP4e interfaces in the Network Engineering Specification Book, use the MDM Nodal Provisioning tool to configure the required OC-3 ports on the 2-port OC-3 Vsp3-o/2pVSP4e FP cards. To do this, apply the *UA-IP*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

IF-TDM-2pOC3ChSmIrVsp template along with values from the Network Engineering Specification Book. Repeat this step for each VSP3-o/2pVSP4e port to configure.

4 Configure the network, as required, using values from the Network Engineering Specification Book and *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*. In the *Attribute Summary*, consult the table that includes values for VSP and TDM interfaces.

5 Repeat step 1 to step 5 for each new TDM interface you add to the Multiservice Switch 15000 node.

6 Manually create the associated IP routing (for example, static route) entries specified in the Network Engineering Specification Book.

7 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

8 Using the MDM Network Model tool, create an entry or icon for the new VSP or TDM physical interface and links to the specific pair of ports selected on the Multiservice Switch 15000 node. For more information on creating and editing links in the MDM Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

9 Using the MDM Network Model tool, regenerate the Network Model for the modified Multiservice Switch 15000 nodes and save the new model.

10 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

11 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Addition of new TDM trunk interface (UA-IP)

This section is an overview of the steps for adding a new time division multiplexing (TDM) trunk interface, to an existing UA-IP network. The purpose of adding new TDM trunk interfaces is to create individual profiles and DS1-based TDM trunks. You must add the trunks one at a time.

For some trunk types, you must add profiles before adding the associated trunks. After that, you can add the trunks in order, as specified by the Network Engineering Specification Book.

This section includes the topics as follows:

- "Prerequisites to adding a new TDM trunk interface" (page 205)
- "Adding a new TDM trunk interface" (page 206)

Prerequisites to adding a new TDM trunk interface

- Complete your network planning. For assistance, contact your representatives from the network engineering group at Nortel .
- For customer-specific values, see the Network Engineering Specification Book. The customer and Nortel network engineering group produce this book jointly.
- For specific values, see the *NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.
- For information on using the Nodal Provisioning application of Nortel MDM, see the *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.
- There must be connectivity between MDM servers and the Nortel Multiservice Switch 15000 nodes.
- MDM servers and Multiservice Switch 15000 nodes must be running compatible software loads.
- The network must use H.248 as the protocol between the MGC and the Media Gateway 15000 (MG15000), and virtual router access point (VRAP) as the connectivity scheme.
- You must download the most recent patches for the software release running on the MDM servers.
- The VSP and TDM physical interfaces must be already applied and activated. For more information, see "Addition of new VSP and TDM physical interface (UA-IP)" (page 202).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Adding a new TDM trunk interface
Procedure steps

Step	Action
1	For a new PRI trunk on a VSP3 FP, first create a PRI trunk profile. Apply the *TT-PRIProfile-2pGeMmSrVsp3* template for each of the VSP3s that contain PRI trunks, as specified in the Network Engineering Specification Book.
2	For a new PRI trunk on a new VSP3-o or 2pVSP4e FP card, first create a PRI trunk profile. Apply the *TT-PRIProfile-2pOC3ChSmIrVsp* template for each of the VSP3-o or 2pVSP4e FP cards that contain PRI trunks, as specified in the Network Engineering Specification Book.
3	For a new PTS trunk on a VSP3-o or 2pVSP4e FP, first create a PTS trunk profile. Apply the *TT-PTSProfile-2pOC3ChSmIrVsp* template for each of the VSP3-o or 2pVSP4e FP cards that contain PTS trunks, as specified in the Network Engineering Specification Book.
4	Activate the changes.
5	For a new TDM port, first configure the LAPS STS component. Apply the *TT-LapsSts-TDM* template for each of the TDM ports (4pOC3TDM, VSP3-o, or 2pVSP4e) as specified in the Network Engineering Specification Book. You can click Multiple creations to create all the STS components under the LAPS for a port pair. ***Note:*** You cannot activate the changes until you add at least one Trunk under each STS you create.
6	For each ISUP trunk on VSP3, apply the *TT-ISUPTrunk-2pGeMmSrVsp3* template. Repeat this step for each ISUP trunk on VSP3, as specified in the Network Engineering Specification Book.
7	For each PRI trunk on VSP3, apply the *TT-PRITrunk-2pGeMmSrVsp3* template. Repeat this step for each PRI trunk on VSP3, as specified in the Network Engineering Specification Book.
8	For each ISUP trunk on VSP3-o or 2pVSP4e, apply the *TT-ISUPTrunk-2pOC3ChSmIrVsp* template. Repeat this step for each ISUP trunk on VSP3-o, as specified in the Network Engineering Specification Book.
9	For each PRI trunk on VSP3-o or 2pVSP4e, apply the *TT-PRITrunk-2pOC3ChSmIrVsp* template. Repeat this step for each PRI trunk on the VSP3-o or 2pVSP4e, as specified in the Network Engineering Specification Book.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

10 For each PTS trunk on VSP3-o or 2pVSP4e, apply the *TT-PTSTrunk-2pOC3ChSmIrVsp* template. Repeat this step for each PTS trunk on VSP3-o or 2pVSP4e, as specified in the Network Engineering Specification Book.

11 Using the MDM Nodal Provisioning tool or Command Console, activate and commit the new service data.

12 Using the MDM Network Model Editor tool, choose either the FNMOD or GEN icon to represent the new MG9000 in the network and link it to the specific pair of ports selected on the Multiservice Switch 15000 node. The FNMOD supports one link that terminates on the MG9000 while GEN supports multiple links. For more information on creating and editing links in the Network Model, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

13 Link the newly created MG9000 icon to the Multiservice Switch 15000 node in the Network Model. For more information, see *241-6001-015 Nortel Multiservice Data Manager Network Model Administration*.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Copyright © 2006, Nortel Networks

SPFS configuration procedures

This section contains a set of solution-level Server Platform Foundation Software (SPFS) procedures that are relevant to Configuration. Use the information in the following procedures in the context of Note 1 to Note 4:

Note 1: An N240 server with SPFS and MDM runs in a simplex configuration; it is not part of a high-availability cluster configuration. When dual MDM servers are deployed, they are functioning as two distinct one-server systems.

Note 2: In secured systems, SSH is used to log in to the server instead of telnet.

Note 3: As these procedures are used in different contexts in the Carrier Voice over IP suite of documentation, they may contain references to procedures that are not used by Nortel Multiservice Data Manager.

Note 4: Server Platform Foundation Software (SPFS) may alternately be referred to as Succession Server Platform Foundation Software (SSPFS).

- "Network Patch Manager" (page 211)
- "Configuring NPM for automatic patch file delivery" (page 220)
- "Re-establishing the connection between the NPM GUI and the server" (page 227)
- "Accessing the Network Patch Manager CLUI" (page 229)
- "Starting the NPM server application" (page 231)
- "Stopping the NPM server application" (page 233)
- "Initializing the NPM database" (page 235)
- "Cleaning up old data in the NPM database" (page 239)
- "Configuring the Patching Server Element on an SPFS-Based Server" (page 245)
- "Starting the PSE server application on an SPFS-based server" (page 249)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Stopping the PSE server application on an SPFS-based server" (page 252)
- "Setting a limit for login retries on an SPFS-based server" (page 255)
- "Configuring a Timing Provider on an SPFS-Based Server" (page 258)
- "Creating or Modifying the Login Greeting Message on an SPFS-Based Server" (page 262)
- "Configuring the Time Zone on an SPFS-Based Server" (page 265)

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Network Patch Manager

Overview

The Network Patch Manager (NPM) is a patch management solution for Nortel network-based products. Patching using the NPM is supported for the following components:

- Gateway Controller Manager (GWC Manager)
- Media Gateway 9000 (MG 9000)
- Media Gateway 9000 Manager (MG 9000 Manager)
- SAM 21 Manager
- Patching Server Element (PSE)
- Succession Element and Subelement Manager (SESM)
- QoS Collector Application (QCA)
- Server Platform Foundation Software (SPFS)
- Integrated Element Management System (IEMS) and IEMS security component
- Core Element Manager (CEM)
- Network Patch Manager (NPM)

The NPM software package is delivered with the Server Platform Foundation Software (SPFS).

Only one instance of the NPM can be installed and enabled in an office. Depending on your office configuration, your choices are as follows:

- Integrated Element Management System (IEMS), which is the most preferred location
- CS 2000 Management Tools server (CS2M) when IEMS is not present in the network

The NPM uses the Patch File Receipt System (PFRS) and the Patching Server Element (PSE) device.

Patch File Receipt System

The Patch File Receipt System (PFRS) provides an automated means of interacting with an upstream patch administration and delivery system, for example, the Regional Patch Selector (RPS), to make new patch files available to the NPM.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

When installed, PFRS runs each of two tasks once every 24 hours. One task generates a report specifying the patch and load content for each device in the site (report). A second task detects newly available patch files and brings those patches into the NPM system (getpatch). You can schedule these two tasks, report and getpatch, to run at any given time on a daily basis. However, the intent is to schedule the report task at an early time so that the site patch contents are returned to Nortel, and to schedule the getpatch task at a later time to pick up new patch files based on the report information that was returned during the report task.

The PFRS 24-hour cycle typically uses the following schedule:

- PFRS generates the report showing the patch status of the site and puts the report file in the designated dropbox.
- Some time later, the upstream patch administration system gets the report from the dropbox.
- The upstream patch administration system uses the report to "calculate" which newly available patches are needed by the site.
- The upstream patch administration system downloads new patches to the site's dropbox.
- Some time later, PFRS executes the getpatch task which makes the new patches known to the NPM server and database, puts a copy of the each patch file in NPM's "Au" directory, and determines which devices can use the patch (for example, creates a VA status where appropriate).

ATTENTION

PFRS does not automatically apply any patches.

The PFRS has the following requirements for use in the NPM:

- An interface server hosting an FTP server that is accessible using a userid and password with full read, write, and overwrite access, must be available.
- The default directory of the FTP user (1 unique user per site recommended) on the FTP server must provide the location from which patch files are retrieved and to which reports are written.
- The PFRS can be configured at any time after the NPM is installed, configured and running, using the command line interface (CLI) tool.
- A CLLI name is required to configure PFRS. You can retrieve the CLLI name from table OFCENG.
- The IP address or host name of the interface server is required to configure PFRS.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Patching Server Element Device

The patching server element (PSE) device enables communication between the NPM and OAM devices to be patched on the SPFS platform. The PSE also tracks patch data and information on each OAM device.

User interface

The NPM provides a graphical user interface (GUI) and a command line user interface (CLUI). Both interfaces offer the same functionality. Using the NPM GUI or CLUI, you can

- apply and remove patches
- audit devices
- activate and deactivate patches
- restart OAM devices
- image select MG 9000 devices automatically
- perform file management, tracking, and reporting

Users who need to perform patching activities using the NPM GUI or CLUI, need to belong to user group "emsadm". If you are locally managing user accounts, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600. If you are centrally managing user accounts through the Integrated Element Management System (IEMS), refer to procedure "Configuring user settings" in *IEMS Security and Administration*, NN10336-611.

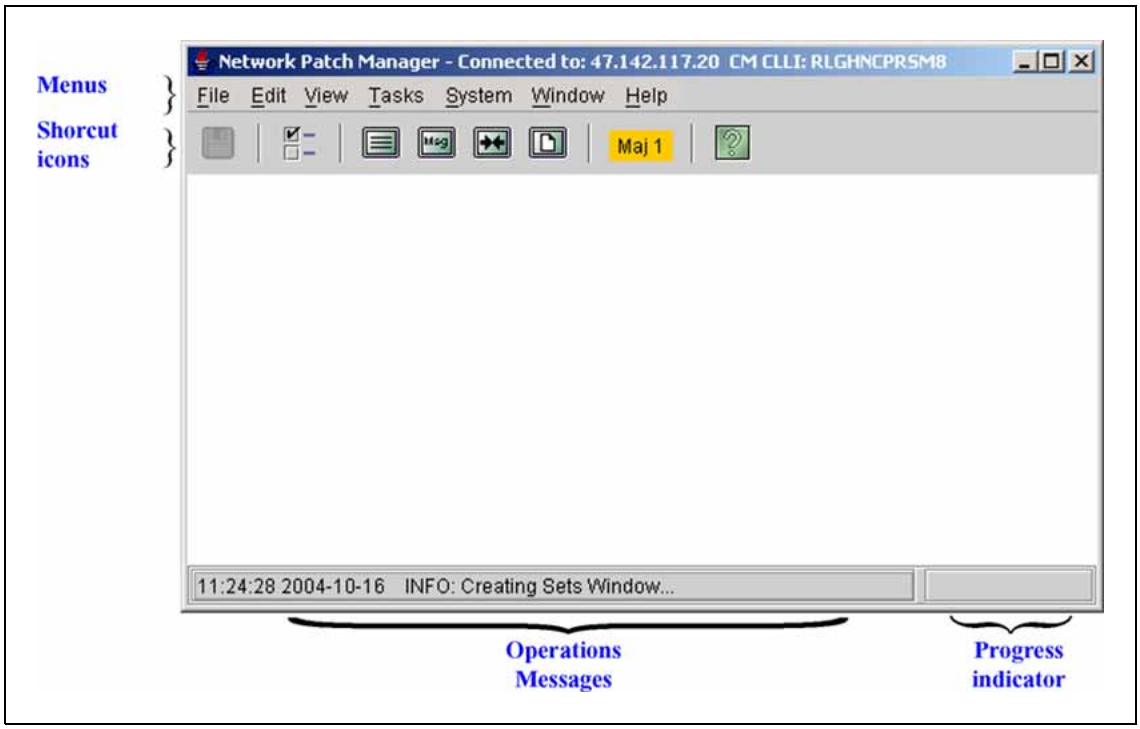
NPM GUI

The NPM GUI is a Java™ Web Start (JWS) application delivered through a web browser that provides full access to all patching functionality. The NPM GUI is accessed through the common launch page as previously described under Common launch page.To access the NPM GUI, refer to procedure "Launching the CS 2000 Management Tools and NPM client applications" in the *ATM/IP Security and Administration* document, NN10402-600.

The following figure shows an example of the NPM GUI.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

The NPM GUI



The GUI provides menus along the top with shortcut icons for some of the following menu items. Placing your cursor over an icon indicates its function. The IP address of the NPM server and the office CLLI are displayed at the top of the window. Operations messages are displayed at the bottom left of the window, and a progress indicator, which shows the progress of patch requests, is provided at the bottom right of the window.

The sections that follow, briefly describe the options available under each menu. More details are provided in the online help for the Network Patch Manager (see "Help" (page 218)).

File

The File menu contains the following options:

- **Save** - save the data of the currently active window to a file
- **Exit** - exit the Network Patch Manager GUI

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

File menu

Edit

The Edit menu contains the **Preferences** option used to set the user preferences (enable or disable the display of patching activity results, and enable or disable debug message), and set the patch file retrieval preferences (PFRS drop box information).

Edit menu

View

The View menu contains following options:

- **Tasks Window** - display maintenance tasks (apply, remove, and audit) and their current status
- **Messages** - display all system messages and responses received during the current session
- **Files** - view details of patch files

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

View menu

Tasks

The Tasks menu contains the following options:

- **Maintenance** - initiate patching tasks such as apply, remove, audit, activate, deactivate, restart, and smart image
- **Set Field Values** - set database field values such as PATCH.HOLD, and DEVICE.HOLD
- **Reports** - define and generate reports

Tasks menu

System

The System menu contains the following options:

- **Alarms** - define and manage alarms
- **Plans** - define, modify or delete a plan, which is a list of one or more tasks such as apply, remove, audit, reports, that can be executed according to a specified schedule

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- **Sets** - define sets, which are groupings of patches and devices used in routine patching tasks
- **Status** - view details for currently active alarms
- **Re-Connect to Server** - reconnect to the server in the event the connection is lost

System menu

Window

The Window menu contains the following options:

- **Next/Previous** - activate the next or previous open window
- **Cascade** - auto-arrange all open windows on the desktop
- **Close All** - close all open windows
- **Windows** - view all open windows, and switch to or close an open window

Window menu

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Help

The Help menu contains the following options:

- **Contents** - display online help information for the NPM
- **About** - display the version of the NPM GUI, NPM server application, and NPM database schema

Help menu

NPM CLUI

The CLUI offers the same functionality as the GUI, but in a command-line approach. Additionally, the CLUI services can be used as an Application Programming Interface (API) for scripts that need to access patching information or functions.

Alarms

The Network Patch Manager (NPM) includes a set of pre-defined system alarms at install. You cannot remove or modify these alarms, however, you can disable them (refer to procedure "Enabling and disabling alarms using the NPM" in the *ATM/IP Fault Management* document, NN10408-900). By default, all system alarms are enabled.

Each time an alarm is raised, log NPM360 is generated. For more details on the alarms that are reported through log NPM360, refer to the *Carrier Voice over IP Fault Management Logs Reference* document, NN10275-909.

In addition to the pre-defined system alarms, you can create your own alarms to match your specific criteria. Refer to procedure "Defining alarms using the NPM" in the *ATM/IP Fault Management* document, NN10408-900.

Logs

The NPM logs are saved into a local file "/data/npm/logs/custlogs", but you can also send them into the customer's log system through an Operations Support Systems Interface (OSSI).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The NPM logs are grouped into logical sets based on the log number as follows:

- NPM300 to NPM399 - Trouble logs
- NPM400 to NPM499 - Service summary logs
- NPM600 to NPM699 - Information logs

Log severity is indicated by a number of asterisks at the beginning of the log.

- <none> - information
- * - minor
- ** - major
- *** - critical

For details on each of the NPM logs, refer to the *Carrier Voice over IP Fault Management Logs Reference* document, NN10275-909.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Configuring NPM for automatic patch file delivery

Application

Use this procedure to configure the Network Patch Manager (NPM) for automatic patch file delivery, which consists of configuring the Patch File Receipt System (PFRS). You can configure PFRS using one of the following two NPM interfaces:

- "Using the NPM CLUI" (page 220)
- "Configure the NPM GUI" (page 223)

Once the PFRS is configured, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

An option is provided to delete patch files from the drop-off server after they have been retrieved.

Prerequisites

To configure the PFRS, you need the following information:

- the hostname or IP address of the patch file drop-off server
- the user ID and password to connect to the patch file drop-off server

Action

Perform the following steps to complete this procedure.

Using the NPM CLUI

Step	Action
	At your workstation
1	Access the NPM CLUI. `# npm` When prompted, enter your **`username`** and **`password`**. If required, refer to the Accessing the Network Patch Manager CLUI procedure for more information.
	At the NPM CLUI
2	Configure the PFRS by typing **`npm> setpfrs <drop-off server> <userID> <delete patches>`** and pressing the Enter key.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

where

drop-off server is the IP address or hostname of the drop-off server where patch files are to be delivered
userID is the user ID that will be used to connect to the drop-off server
delete patches is either Y or N to indicate whether you want the patch files to be deleted from the drop-off server after they have been retrieved

The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

Example response:

```
Enter password for drop box:
```

3 When prompted, enter the password associated with the user ID that will be used to connect to the drop-off server.

Example response:

```
WARNING: You are about to set/reset the Patch File
Retrieval System settings.  If these values are
incorrect they may interfere with automatic delivery of
patches to this site.
Do you wish to continue Yes (Y) or N (N)?
```

4 When prompted, confirm you want to continue if acceptable by typing

y

and pressing the Enter key.

5 Review the PFRS settings if required by typing

npm> viewpfrs

and pressing the Enter key.

6 Enable the GENREPORT plan by typing

npm> enableplan genreport

and pressing the Enter key.

Ensure that the response is:

```
Plan enabled successfully.
```

If you receive any other response, contact your next level of support.

7 Check the plan status for genreport by typing

```
npm> vplan genreport
```

and pressing the Enter key.

The value for **Enabled** must be set to **Y**.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Expected response:

```
Name            : GENREPORT
Description     : PFRS Inform list report generation
Status          : SCHED
Enabled         : Y
Frequency       : Daily
Execute Time    : Wed Jan 25 12:00:00 GMT-03:00 2006
Max Execut Time:  No_Limit
Tasks/Reports   : [TASK:PFRSGENREPORT]
System Defined :  true
```

If genreport is not enabled, contact your next level of support.

8 Enable the GETPATCH plan by typing

```
npm> enableplan getpatch
```

and pressing the Enter key.

Ensure that the response is:

```
Plan enabled successfully.
```

If you receive any other response, contact your next level of support.

9 Check the plan status for getpatch by typing

```
npm> vplan getpatch
```

and pressing the Enter key.

The value for **Enabled** must be set to **Y**.

Expected response:

```
Name            : GETPATCH
Description     : Patch file retrieval
Status          : SCHED
Enabled         : Y
Frequency       : Daily
Execute Time    : Thu Jan 26 01:00:00 GMT-03:00 2006
Max Execut Time:  No_Limit
Tasks/Reports   : [TASK:PFRSGETPATCH]
System Defined :  true
```

If getpatch is not enabled, contact your next level of support.

10 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configure the NPM GUI

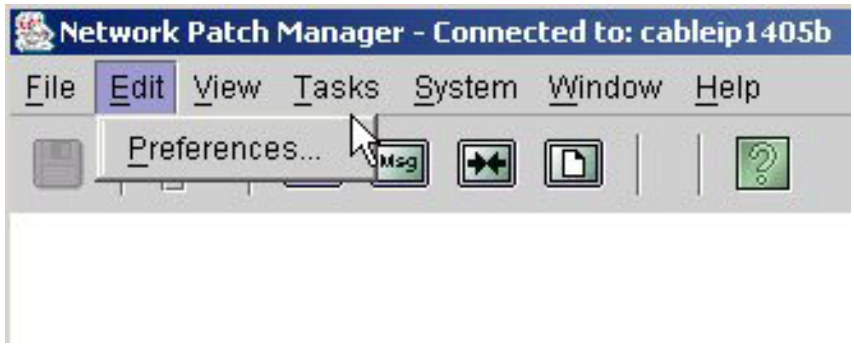
Step	Action

At your workstation

1 Access the NPM GUI. If required, refer to procedure Launching CS 2000 Management Tools and NPM Client Applications.

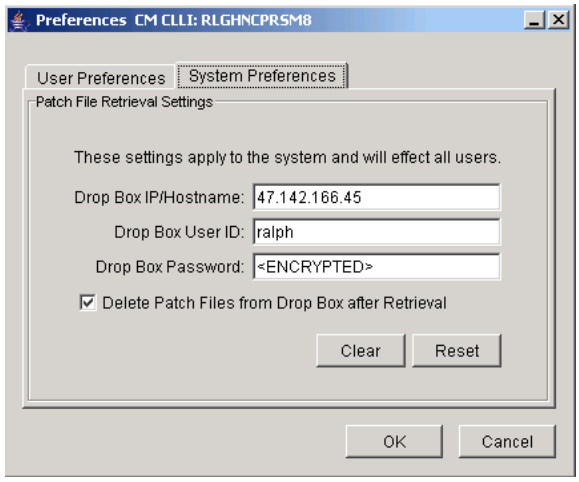
At the NPM GUI

2 On the Edit menu, click **Preferences...**.



The Preferences window is displayed.

3 Click the **System Preferences** tab.



4 In the Drop Box IP/Hostname field, enter the host name or IP address of the drop-off server where patch files are to be delivered.

5 In the Drop Box User ID field, enter the user ID that will be used to connect to the drop-off server.

The user ID must have read, write, and overwrite privileges in the FTP default directory for the user on this server.

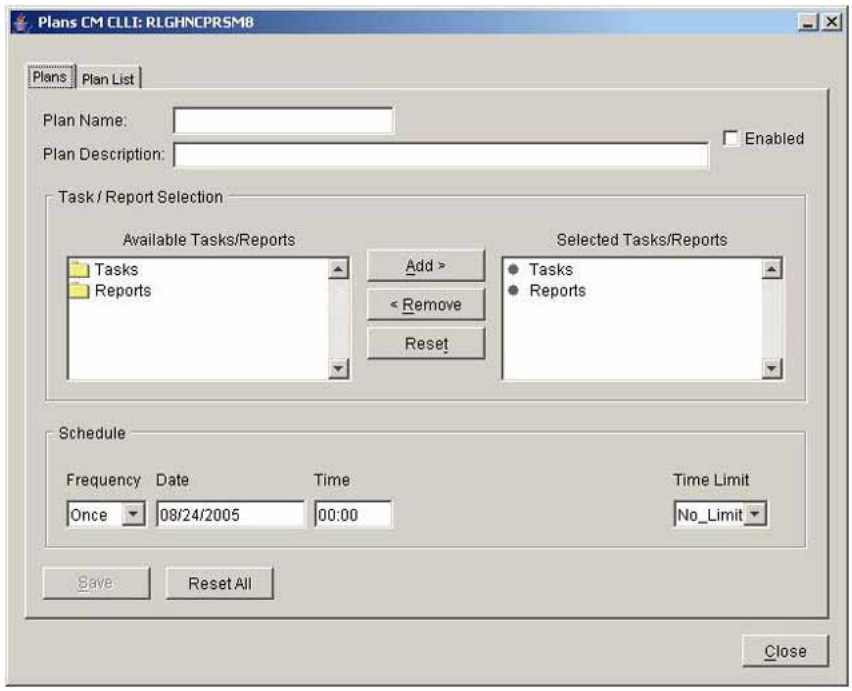
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

6 In the Drop Box Password field, enter the password associated with the user ID that will be used to connect to the drop-off server.

7 Click the Delete Patch Files from Drop Box after Retrieval box if you want the patch files to be deleted from the drop-off server after they have been retrieved, otherwise, leave it blank.

8 Click **OK** to complete the PFRS configuration.

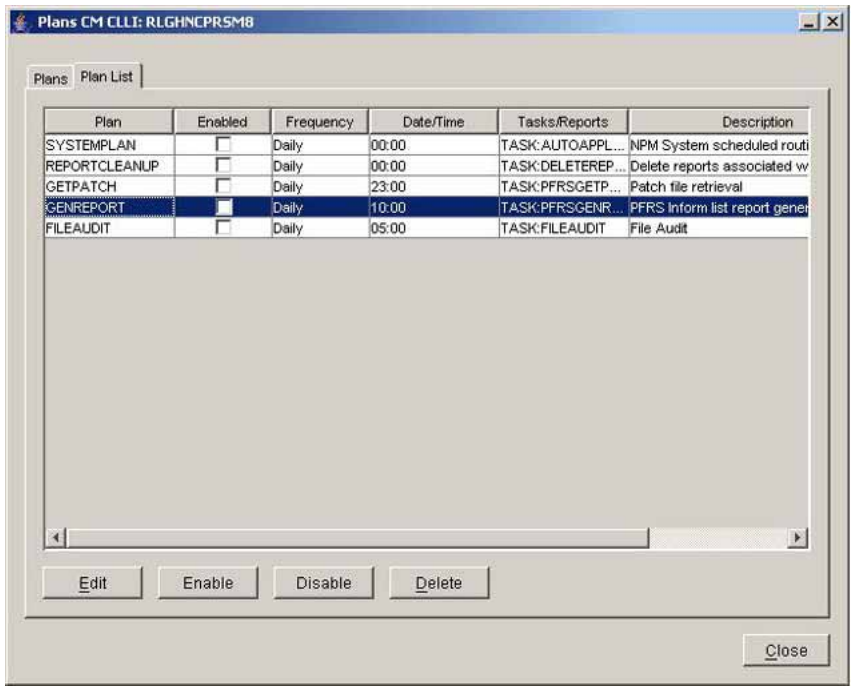
9 On the System menu, select **Plans....**



The Plans window is displayed.

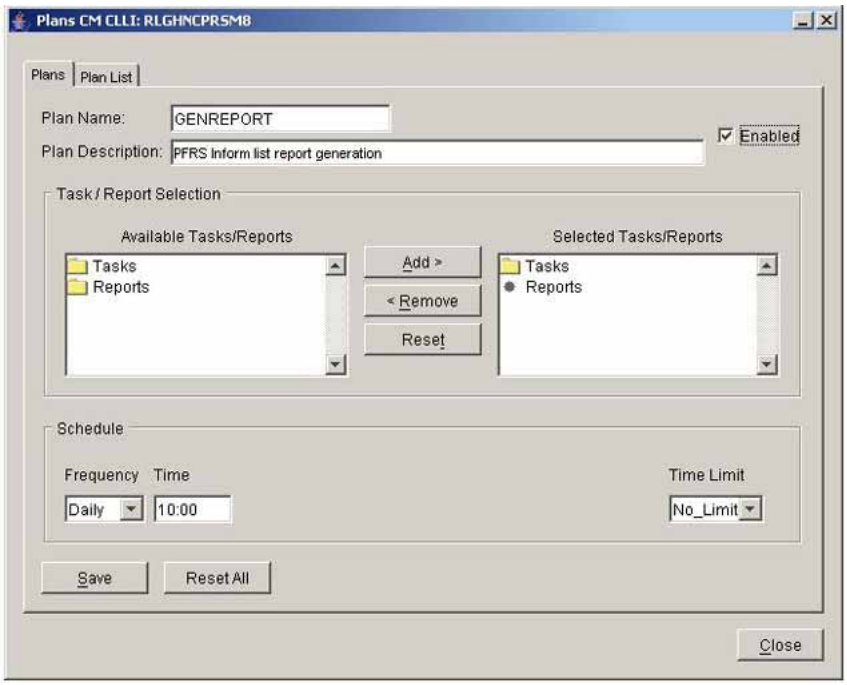
10 Click **Plan List** tab.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



The Plan List window is displayed.

11 Select the GENREPORT task and click **Edit**.



12 Click the Enabled checkbox, verify the schedule for the plan, and then click **Save**.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

13 Repeat step 10 through to step 12 but select the GETPATCH task this time.

14 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Re-establishing the connection between the NPM GUI and the server

Application

Use this procedure to re-establish the connection between the Network Patch Manager (NPM) GUI and the Sun server where the Network Patch Manager (NPM) software resides. The NPM GUI loses server connectivity when the server goes out of service. Once the server returns to service you need to reconnect.

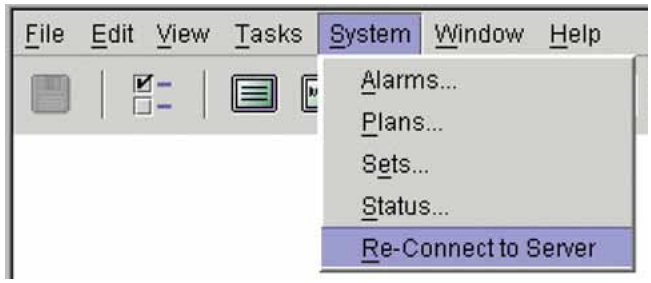
Prerequisites

The server where the NPM software resides must be in service.

Action

Perform the following steps to complete this procedure.

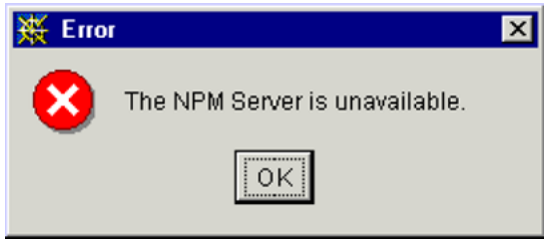
Step	Action
	At the NPM GUI
1	On the **System** menu, click **Re-Connect to Server**.



When the connection is successful, a response similar to the following one is displayed.

When the connection fails, a response similar to the following one is displayed.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



When the connection fails, try to reconnect at a later time. If the connection failure persists, contact your next level of support.

2 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Accessing the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

Note 1: You can also access the NPM CLUI from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to the IEMS Basics document, NN10329-111.

Note 2: The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launching CS 2000 Management Tools and NPM client applications.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure 'Setting up local user accounts on an SPFS-based server' in the ATM/IP Security and Administration document, NN10402-600.

Action

Perform the following steps to complete this procedure.

Step Action

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

Copyright © 2006, Nortel Networks Nortel Networks Confidential

b. When prompted, enter your user ID and password

Proceed to step 4

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l > ssh -l <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

Note: If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

b. When prompted, enter your password.

4 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

5 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode:  Enter npm' commands, help
or quit to exit.
npm>
```

6 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Starting the NPM server application

Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

Action

Perform the following steps to complete this procedure.

ATTENTION
In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server where the NPM server application resides

In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

In a two-server configuration, ensure you are on the Active server by typing ubmstat. If ClusterIndicatorSTBY is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

5 Verify the status of the NPM server application by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
not running	step 6
running	you have completed this procedure

6 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

7 Verify the NPM server application is running by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Stopping the NPM server application

Application

Use this procedure to stop the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

You need root user privileges to perform this procedure.

It is recommended that all users exit the NPM CLUI and GUI before stopping the NPM server application.

Action

Perform the following steps to complete this procedure.

ATTENTION
In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server where the NPM server application resides

In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

In a two-server configuration, ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of

Copyright © 2006, Nortel Networks Nortel Networks Confidential

that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

5 Verify the status of the NPM server application by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
running	step 6
not running	you have completed this procedure

6 Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

7 Verify the NPM server application is no longer running by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Initializing the NPM database

Application

Use this procedure to initialize the Network Patching Manager (NPM) database.

ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

Prerequisites

Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server where NPM resides
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su - root` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Re,ote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response:

```
Succession Element Configuration
1 - SESM Application Configuration
2 - SAM21EM Application Configuration
3 - NPM Application Configuration
4 - PSE Application Configuration
5 - DDMSProxy Application Configuration
6 - OMPUSH Application Configuration
7 - RESMON Application Configuration
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
X - exit
select -
```

8 Enter the number next to the "NPM Application Configuration" option in the menu.

Example response

```
NPM Application Configuration
1 - CreateDB (Initialize or re-initialize the NPM
database)
X - exit
select -
```

9 Enter the number next to the "CreateDB" option in the menu.

10 Exit each menu level of the command line interface to eventually return to the root level, by typing

```
select - x
```

and pressing the Enter key.

11 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:

- for reports, refer to procedure "Defining reports using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211)
- for tasks, refer to procedure "Defining a task using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211)
- for sets, refer to procedure "Defining sets using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211)
- for plans, refer to procedure "Defining a plan using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211)
- for alarms, use procedure "Defining alarms using the NPM" in the ATM/IP solution-level Fault Management document, NN10408-900.*Packet MSC Security and Administration* (NN-20000-216)

12 If any patches or devices were on hold prior to this procedure, place them back on hold using procedure "Setting field values using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

13 If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure "Modifying a plan using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450*Packet MSC Upgrades* (NN-20000-211).

14 If PFRS was configured prior to this procedure, re-configure it using procedure "Configuring the NPM for automatic patch file delivery" in the ATM/IP solution-level Configuration document, NN10409-500*Packet MSC Configuration* (NN-20000-213).

If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Cleaning up old data in the NPM database

Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

ATTENTION

This procedure includes stopping and starting the NPM, which has the NPM re-discover the patches on the system when the NPM is brought back into service. This can take up to one hour depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Generate and save a patchlist report using the NPM CLUI or GUI.

The patchlist report may be useful in the event the apply time information is required at a later time.

If using the	Do
CLUI	step 2
GUI	step 14

2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password

Copyright © 2006, Nortel Networks Nortel Networks Confidential

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server

For detailed steps, refer to Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

3 Change directory to /data/npm by typing:

```
# cd /data/npm
```

and pressing the Enter key

4 Determine if a tmp directory exists in the npm directory by typing:

```
# ls -l
```

and pressing the Enter key.

5 Use the following table to determine your next step

If	Do
a tmp directory exists	step 7
otherwise	step 6

6 Create a tmp directory by typing

```
# mkdir tmp
```

and pressing the Enter key

7 Change directory to the tmp directory by typing:

```
# cd tmp
```

and pressing the Enter key.

8 Generate the patchlist report by typing

```
# npm q patchlist output <filename>.list
```

and pressing the Enter key.

where

filename is the name you want to give to the patchlist report

npm q patchlist output aug032004.list
Example response

```
Enter the NPM Succession user id and password.
Login
```

9 When prompted, enter the NPM user ID

Example response

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
password
```

10 When prompted, enter the NPM user password.

Example response

```
Redirecting output to:  aug032004.list
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
Redirecting output to standard I/O
```

11 Display the file by typing

`$ ls`

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

12 If required, display the contents of the file by typing:

`# cat <filename> |more`

and pressing the Enter key.

where

`filename` is the name you gave to the patchlist report file

cat aug032004.list

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

13 Proceed to step 25

Access the NPM GUI. If required, refer to procedure.

14 Access the NPM GUI.

For detailed steps, refer to Launching CS 2000 Management Tools and NPM Client Applications

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

At the NPM GUI

15 On the **Tasks** menu, click **Reports...**

16 Click the **Report List** tab to display the list of defined reports.

17 Click on **PATCHLIST**, and then click **Execute** to generate the PATCHLIST report.

The Reports Results window is displayed.

18 Click **Save**, to save the results of the PATCHLIST report and specify the filename and location to save the report.

The Save window is displayed.

19 Enter a name for the saved report in the File name field and then click **Save**

20 Click **Close** to close the Reports Results window.

21 Click **Close** to close the Reports window.

22 On the Edit menu, Click **Preferences**.

23 Click on the **System Preferences** tab.

Copy and paste the data on display including that in the Delete Patches from the Drop Box after Retrieval checkbox

At your workstation

24 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

25 Stop the NPM server application by typing:

```
# servstop NPM
```

and pressing the Enter key.

26 Access the command line interface by typing:

```
# cli
```

and pressing the Enter key.

27 Enter the number next to the “Configuration” option in the menu.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

28 Enter the number next to the “Succession Element Configuration” option in the menu.

29 Enter the number next to the “NPM Application Configuration” option in the menu.

30 Enter the number next to the “CreateDB” option in the menu.

Allow to complete.

31 Exit each menu level of the command line interface to eventually return to the root level by typing:

```
select - x
```

and pressing the Enter key.

32 Start the NPM server application by typing:

and pressing the Enter key.

33 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, redefine them using the corresponding procedure.

- for reports, use procedure Defining NPM patching reports
- for tasks, use procedure Defining NPM patching tasks
- for sets, use procedure Defining NPM patching sets
- for plans, use procedure Defining NPM patching plans
- for alarms, use procedure “Defining alarms using the NPM” in document ATM/IP Fault Management, NN10408-900.

34 If any patches or devices were on hold prior to this procedure, place them back on hold using procedure Setting field values using the NPM

35 If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure Modifying NPM patching plans

36 If PFRS was configured prior to this procedure, re-configure it using procedure "Configuring NPM for Automatic Patch File Delivery" in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

If any users were logged in to the NPM GUI prior to this procedure, they must exit and launch the GUI again. A reconnect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

37 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring the Patching Server Element on an SPFS-Based Server

Application

Use this procedure to configure the Patching Server Element (PSE) on a Server Platform Foundation Software (SPFS) based server. Configuring the PSE involves specifying the location of the NPM server application so the PSE can communicate with the NPM server application.

ATTENTION

Only perform this procedure after an upgrade if a new SPFS-based server is added to the network with the PSE on it, or the NPM is moved to another SPFS-based server.

Prerequisites

The SPFS upgrade is complete.

Action

Perform the following steps to complete this procedure.

Configure the Patching Server Element

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you are configuring PSE
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing `# cli`

Copyright © 2006, Nortel Networks Nortel Networks Confidential

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - DCE Configuration
  4 - OAMP Application Configuration
  5 - CORBA Configuration
  6 - IP Configuration
  7 - DNS Configuration
  8 - Syslog Configuration
  9 - Remote Backup Configuration
 10 - Database Configuration
 11 - NFS Configuration
 12 - Bootp Configuration
 13 - Restricted Shell Configuration
 14 - Security Services Configuration
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
 10 - RESMON Application Configuration
X - exit
select -
```

8 Enter the number next to the “PSE Application Configuration” option in the menu.

Example response

```
PSE Application Configuration
1 - View_NPM_host_or_ip <View NPM hostname/ip address
location>
2 - Update_NPM_host_or_ip <Update NPM hostname/ip
address location>
3 - Create_PSE_Database (Initialize or re-unitize the
PSE database)
4 - Update_Patch_Corba_Mirroring (Mirror the NPM patch
CORBA name reference)
5 - Remove_Patch_Corba_Mirroring (Remove the NPM patch
CORBA name mirror re...)
6 - Unconfigure_PSE (Remove PSE as a system process.)
X - exit
select -
```

9 Enter the number next to the "Update_NPM_host_or_ip" option in the menu.

Example Response:

```
Enter the hostname (preferred) or the IP address
of the SPFS-based machine that contains the Network
Patch Manger (NPM) server.  If this machine is part
of a duplex/clustered configuration, please enter the
cluster hostname or IP address.
Enter NPM hostname or IP address:
```

10 When prompted, enter the host name or IP address of the SPFS-based server where the NPM resides.

If the NPM is installed on a server in a cluster (two-server configuration), enter the host name or IP address of the cluster.

Example response:

```
Checking communication to 124.12.54.3.  This may take
up to ten seconds.
Is host/ip 124.12.54.3 acceptable?  [y] [y,n,?,q]
```

11 When prompted, confirm the host name or IP address by typing

y

and pressing the Enter key.

Example response:

```
==="Update_NPM_host_or_ip" completed successfully
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

12 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Starting the PSE server application on an SPFS-based server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION
In a two-server configuration, perform the steps that follow on the active server.

Step	Action

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

5 Verify the PSE server application started by typing

```
# pse status
```

and pressing the Enter key.

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Stopping the PSE server application on an SPFS-based server

Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION
In a two-server configuration, perform the steps that follow on the active server.

Step	Action

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **`yes`** at the prompt.

b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Stop the PSE server application by typing

```
# pse stop
```

and pressing the Enter key.

5 Verify the PSE server application stopped by typing

```
# pse status
```

and pressing the Enter key.

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Setting a limit for login retries on an SPFS-based server

Application

Use this procedure to set a limit on the number of login retries on a Server Platform Foundation Software (SPFS)-based server. When a user exceeds the number of login retries specified, the user loses connection to the host.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to modify the login greeting
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su -`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Login Session" option in the menu.

Example response

```
Login Session
1 - login_session_timeout (User Inactivity Timeout
Configuration)
2 - login_session_termination (User Termination Timeout
Configuration)
3 - login_session_reauthentication (User Reauthenticat
ion Disable Timeout Configuration)
4 - login_session_server (Login Session Master Server
Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
X - exit
select -
```

8 Enter the number next to the "login_retries" option in the menu.

Example response

```
===Executing "login_retries"
Current value for Login Retries is:
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
RETRIES=3
Enter the Login Retries Limit Value (1->15):
```

9 When prompted, enter the limit value for login retries.

Example response

```
==="login_retries" completed successfully
```

Exceeding the range of the login retries limit value generates the error message "ERROR - Login Retries Limit Value Out Of Range", at which point you are prompted to enter a value between 1 and 15.

10 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Configuring a Timing Provider on an SPFS-Based Server

Application

Use this procedure to configure a timing provider for a Server Platform Foundation Software (SPFS) based server. The timing provider is a Network Timing Protocol (NTP) server supplied by the customer. Perform the steps under "Configure a timing provider on an SPFS server" (page 258).

For a cluster (two-server configuration), the Active server can serve as the master time provider for the Inactive server in the event that an NTP server is not provisioned. Perform the steps under "Configure the active server in a cluster as the timing provider" (page 260).

CAUTION
To avoid server configuration being overwritten, do not use this procedure to configure a timing provider for a CO-based MDM on an SPFS server. Instead, follow the Configuring Solaris NTP software sections in *MSS 15000, MG 15000 & MDM Configuration Attribute Summary* (NN10225-512).

Prerequisites

You must have the IP address of the customer-supplied NTP server.

Action

Perform the following steps to complete this procedure.

Configure a timing provider on an SPFS server

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to configure an NTP server
2	When prompted, enter your user ID and password.
3	Change to the root user by typing

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number that corresponds to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "NTP Configuration" option in the menu.

Example response

```
NTP Configuration
1 - ntp_conf (Configure the NTP daemon)
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
2 - ntp_unconf (Unconfigure the NTP daemon)
3 - ntp_remove (Remove an NTP server)
4 - ntp_view (View NTP configuration information.)
X - exit
select -
```

8 Enter the number next to the "ntp_conf" option in the menu.

9 When prompted, enter IP address of the time server.

The system attempts to verify the IP address. If the IP address verification fails, check the IP address and try again.

You can specify up to three NTP servers.

10 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Configure the active server in a cluster as the timing provider

Step	Action

At your workstation

1 Log in to the Active server by typing

`> telnet <server>`

and pressing the Enter key.

where

`server` is the physical IP address of the Active server in the cluster

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

`$ su -`

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify the time is correct on the Active server by typing

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
# date
```

and pressing the Enter key.

If the time	Do
is not correct	step 6
is correct	step 7

6 Adjust the time on the Active server using the "date" command. If required, refer to the man pages on the "date" command to adjust the time.

7 Synchronize the time on the Active server with the time on the Inactive server by typing

```
# synctime
```

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Creating or Modifying the Login Greeting Message on an SPFS-Based Server

Use this procedure when logging in to the server through Telnet.

Application

Use this procedure to create or modify the login greeting message on a Server Platform Foundation Software (SPFS) based server. This message is presented to the user who logs in to the server through Telnet.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Create (modify) the login greeting message

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to modify the login greeting
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`

Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
  Select -
```

7 Enter the number next to the "Login Session" option in the menu.

Example response

```
Login Session
1 - login_session_timeout (User Inactivity Timeout
Configuration)
2 - login_session_termination (User Termination Timeout
Configuration)
3 - login_session_reauthentication (User Reauthenticat
ion Disable Timeout Configuration)
4 - login_session_server (Login Session Master Server
Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
X - exit
select -
```

8 Enter the number next to the "telnet_greeting" option in the menu.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Example response

```
===Executing "telnet_greeting"
Telnet Login Greeting Message:
Authorized use only, activities logged.
Enter the Telnet Login Greeting Message.
Enter a blank line to end the message:
```

9 When prompted, enter the message. End the message with a blank line.

Example response

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

10 When prompted, commit the change by typing

`ok`

and pressing the Enter key.

Example response

```
==="telnet_greeting" completed successfully
```

11 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Configuring the Time Zone on an SPFS-Based Server

Application

Use this procedure to configure the time zone on a Server Platform Foundation Software (SPFS) based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server on which you want to configure the time zone

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Location Configuration" option in the menu.

Example response

```
Location Configuration
1 - Chg_tz (Change Timezone
2 - sys_loc (System Location)
X - exit
select -
```

8 Enter the number next to the "chg_tz" option in the menu.

Example response

```
=== Executing "chg_tz"
WARNING: Changing the timezone will require a reboot
Current setting:
Timezone:       US/Eastern
Enter the timezone for this host <default:  US/Easter
n>:
```

9 When prompted, enter the correct time zone and press the Enter key.

Example response

```
New setting:
Timezone:       US/Eastern
Enter "ok" to commit changes
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
Enter "quit" to exit
Enter anything else to re-enter settings
```

10 When prompted, confirm the change by typing

`ok`

and pressing the Enter key.

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Appendix A Time-of-day updates for seasonal time changes

Seasonal time changes, such as the change from Standard Time to Daylight Saving Time (DST) or back again, require that the time kept by the Nortel Multiservice Switch ATM Core and Packet Core networks be updated using the procedure documented here. Typically in North America, seasonal time changes occur at approximately 2:00 AM on a Sunday in the spring and fall.

- "Prerequisites to updating the time of day for seasonal time changes" (page 269)
- "Updating the time of day for seasonal time changes task flow" (page 270)
- "Updating the time of day for seasonal time changes" (page 271)
- "Monitoring the script" (page 275)

Prerequisites

- Nortel Multiservice Switch ATM Core network needs to use a supported version of the Network Time Protocol (NTP) to synchronize the network time of day.
- Ensure that the ppautopatch script is not currently running and that you have inhibited the ppautopatch script from running at its scheduled time if it has been scheduled to run during the time planned for tod changes. See "Controlling the auto-patch process" (page 136).
- It is recommended that you suspend the Media Gateway 15000 periodic routine exercise (REX) feature (rexScheduled=NO) for the days on which time-of-day changes will occur.
- All Nortel MDM servers and Multiservice Switch nodes must be configured according to the standard configuration and recommendations specified in the documentation.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

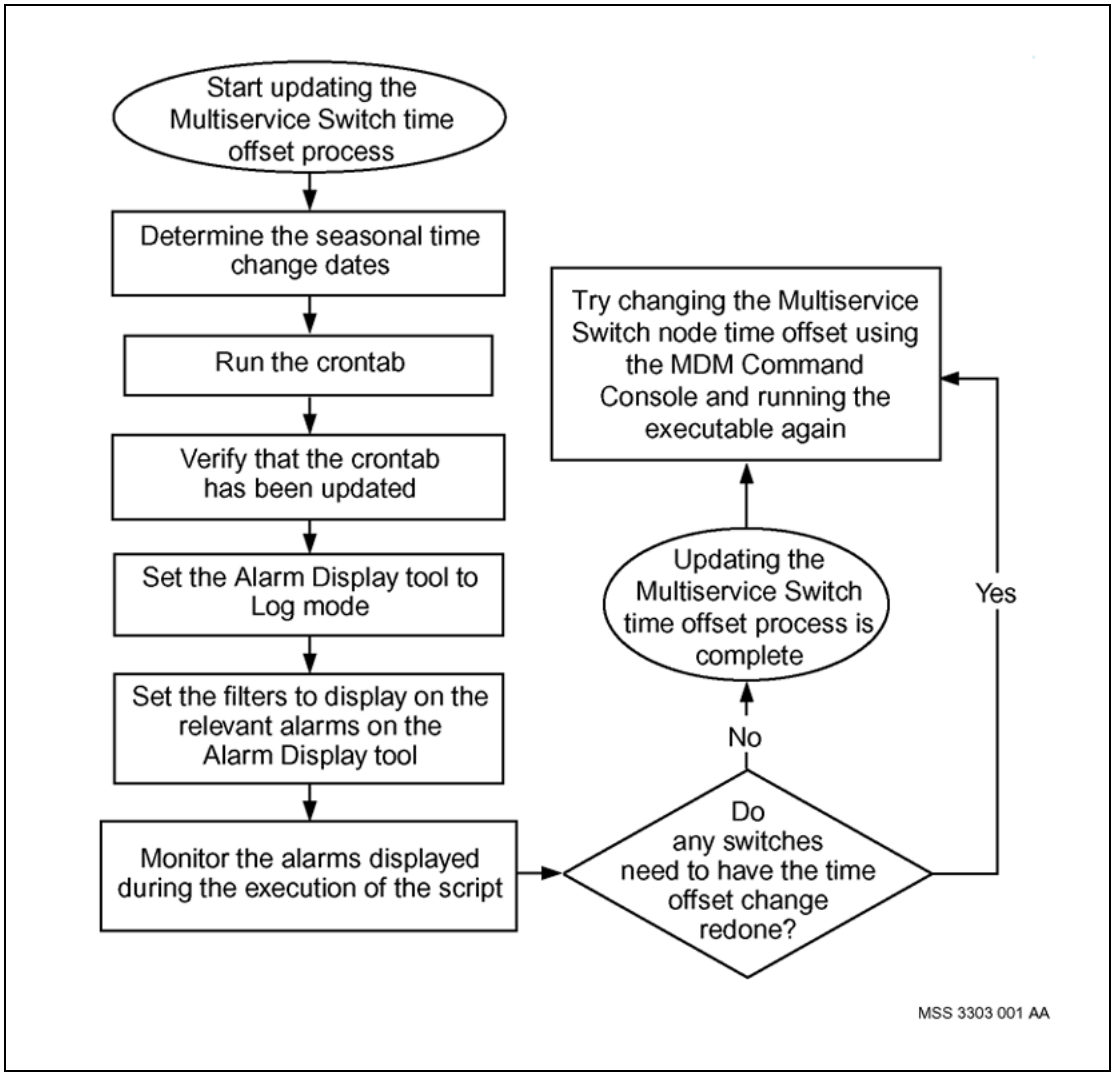
- MDM servers need to be configured with a valid time zone that has an enabled seasonal time changeover capability. Such a configuration ensures that the server's local time will handle the time change automatically, using the standard Solaris-based mechanism.
- All MDM servers and Multiservice Switch nodes within a region need to belong to the same time zone.
- The script needs to be installed on both MDM servers. Installing the script on both servers provides redundancy in case one of the servers is unavailable while the script is executing. If you are installing the script on more than one server, Nortel recommends leaving an interval of one minute before running the script on each server. The exception to this rule is MDM servers running as client-servers. MDM client-servers do not require the script to be installed.
- During the execution of the script, no configuration or operational tasks can run on the Multiservice Switch nodes or MDM servers. For example, there should not be a software migration nor disk cleanup running while the script is executing.
- This procedure needs to be repeated on a regional-basis in order to ensure all the MDM servers and Multiservice Switch nodes are updated.

Updating the time of day for seasonal time changes task flow

This task flow displays the sequence of tasks you need to perform to update the time-of-day on Nortel Multiservice Switch nodes for seasonal time changes. To link to any task, go to "Task flow navigation" (page 271).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Updating the time of day for seasonal time changes task flow



Task flow navigation

- "Updating the time of day for seasonal time changes" (page 271)
- "Monitoring the script" (page 275)

Updating the time of day for seasonal time changes

Nortel recommends that a System Administrator ("root") perform the procedures that comprises this task.

- "Prerequisites" (page 272)
- "Configuration" (page 272)
- "Execution" (page 273)
- "Example steps" (page 274)

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- "Variable values" (page 275)

Prerequisites

Prior to executing the script, perform the following recommended steps to ensure no system surveillance outage occurs:

- Start the nmstool application and configure it to be administering the session servers. If the system administrator is remotely accessing the system the correct settings for the display variables must be met.
- Enable Log mode in the Alarm Display tool and make the alarms for all nodes in the region viewable by removing all filters.
- Verify that the seasonal time change has occurred in the region in question. Typically in North America, seasonal time changes occur at approximately 2:00 AM on a Sunday in the spring and fall.

Have the following information available before executing the script:

- The new offset value for the *todchangeover* attribute. For example, -300 is Eastern Standard Time (5 hours earlier than UTC) and -240 is Eastern Daylight saving time (4 hours earlier than UTC).
- The name of the HGDS group to be specified in the procedure. This information is only needed if you are not using the default HDGS group name.
- A valid Nortel Multiservice Switch user ID and password with an impact-level of at least service is needed for MDM group authentication.

Configuration

Configuration needs to be performed annually per server.

Step	Action
1	Determine the dates of the seasonal time change. For example, during the fall of 2002, October 27th was the date of the seasonal time change and Nortel recommended running the script at 2:01 AM. During the spring of 2003, April 6th was the date of the seasonal time change and Nortel recommended running the script at 3:01 AM. On each subsequent MDM server upon which the script is run, add one minute to the time when you set it to begin running originally.
2	Run the crontab editor (crontab -e) to edit the crontab entry under your administration userid: `<minute hour day month> /opt/MagellanNMS/bin/todchangeover <new offset value> -auth <Passport group> <Passport userid for groupname> <Passport password for groupname>`

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Note: You must specify the entire executable path to the todchangeover script, as follows:

```
/opt/MagellanNMS/bin/todchangeover
```

Note: This step needs to be repeated annually. Nortel recommends that you program the time change each year on January 1st for both the spring and fall time-of-day change.

For an example of the command used in this step complete with sample values that reset the time offset for the spring and fall seasonal change, see "Example steps" (page 274).

3 Verify the crontab has been updated by listing the contents of the cron file:

```
more /var/spool/cron/crontabs/root
```

4 Log out of the MDM server.

5 Repeat step 1 through step 4 on the redundant MDM server. Configuring both servers provides redundancy in case the primary server is not available during the time changeover period specified in the command in step 2. Once you have completed these steps on the second server, configuration is complete.

—End—

Execution

Execution needs to be performed twice annually.

Step	Action
1	Log on to a MDM server just prior to the seasonal time changeover.
2	Select Log mode from the nmstool set menu to set the GUI of the Alarm Display tool. Use this GUI to monitor the execution of the script. ***Note:*** For more information about enabling Log mode in the Alarm Display tool, see *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*.
3	Set the filters for the 70150001 and 301007* series of alarm messages to display using the Alarm Display tool. You can follow the progress of the todchangeover script by viewing the node time change alarms (70150001) and todchangeover script alarms (301007* series).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

4 The 70150001 alarm is the alarm you want to see because it indicates that the node's time offset has changed by more than 100 seconds. You should expect one of these alarms for each node in the group specified on the script command line (see step 2). You will not see the 70150001 alarm when the script executes on the second MDM server if the script running on the first server was successful in changing the node time offset. The 301007* alarm indicates that some sort of error occurred during the execution of the script and intervention by an operator is required to complete the time offset change.

5 Begin monitoring the alarms produced by the script just prior to the seasonal time change. For more information about monitoring the alarms generated by the script, see "Monitoring the script" (page 275).

6 Ensure that the script has successfully executed without any unexpected errors by reviewing the content of the `/tmp/tod_output` file.

Note 1: The records in this temporary file are appended to every time the script or executable is run; however, they are overwritten following a server reboot. To save your records prior to a reboot, create a new non-temporary file for storing them.

Note 2: During the time changeover period during which the server changes its time offset until the node changes its time offset (in the fall, 62 minutes from 1:59 DST to 2:01 EST and in the spring, 1 minute from 2:00 EST to 3:01 DST), Performance Management Stream Processor (PMSP) data is lost. PMSP data will be accurate again at the next 5 or 30 minute interval after the interval featuring the time changeover (in the fall, the 5-minute data from 2:10 EST and 30-minute data from 3:00 EST and in the spring, the 5-minute data from 3:10 DST and 30-minute data from 4:00 DST).

—End—

Example steps

The following steps are examples of Nortel MDM server cron entry for changing the time offset on a node as in the command appearing in step 2 of the "Updating the time of day for seasonal time changes" (page 271). The sample variable values used in these example steps are based on the seasonal time changes mentioned in step 1 of "Updating the time of day for seasonal time changes" (page 271).

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Step	Action
1	Set the values for making the time-of-day change occurring at 2:01 AM on October 27th, 2002 for the Eastern time zone: **1 2 27 10 /opt/MagellanNMS/bin/todchangeover -300 -auth ACCESS fred samsam**
2	Set the values for making the time-of-day change occurring at 3:01 AM on April 6th, 2003 for the Eastern time zone: **1 3 6 4 /opt/MagellanNMS/bin/todchangeover -240 -auth ACCESS fred samsam** ***Note 1:*** These steps are only an example. The values you use in your configuration might differ from the values shown here. Consult your network engineer to ensure the values you are using are accurate for your configuration. ***Note 2:*** Remember that for additional MDM servers the times specified for running the script should be one minute later.

—End—

Variable values

Variable	Value
<minute hour day month>	The exact time, down to the minute, when you want to set the change of the time offset value to occur. It is not necessary to use more digits than necessary for each of these values. For example, represent April with `4` and October with `10`.
<new offset value>	The new time offset value applied to Multiservice Switch nodes. This value is the time in minutes that the node is being offset from UTC. The range of possible is -720 to 720. There is no default value.
<Passport group>	The name of the HGDS group to be used to communicate with the nodes.
<Passport password for groupname>	The node password for the user ID specified in the command
<Passport userid for groupname>	The node user ID for the group specified in the command.

Monitoring the script

The script executes after the time you specified in step 2 of "Updating the time of day for seasonal time changes" (page 271) is passed. This section documents what happens when the script runs. Steps are used in order

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

to break the information down into small units, however, the script runs automatically without input from the system operator. The script provides two types of output, one to a log file, **/tmp/tod_output**, and the other to the Alarm Display tool. For important events occurring during the execution of the script, both types of outputs are shown below in "Script process" (page 276).

- "Prerequisites" (page 276)
- "Script process" (page 276)

Prerequisites

Prior to executing the script, perform the following recommended steps to ensure there is no system surveillance outage:

- In addition to normal operations, open windows for the display of the alarms generated by the execution of the script prior to the 2:00 AM seasonal time change.
- Enable Log mode in the Alarm Display tool and set the filters for the 7015 0001 alarm and the 301007* series of alarms.

Script process

Step	Action
1	The script begins executing.

Sample log output

```
... Welcome to the Time Of Day change tool. This
tool is used to change

... Passports time offset value


... Note that this tool should be run after MDM has
completed its time
... change to/from Daylight Savings Time.

on error

Thu Sep 5 15:27:27 EDT 2002

The UTC time offset value must be specified.
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

Sample Display Alarm tool output

Nothing unless an input parameter error

On error

Warning MSG 30100703 02-07-24 15:27:27 NMS/FT1400-2 APPL/TODCHANGEOVER

ID-FFFFC929 Type: environmental CAUSE:unexpectedInfo

NMS/ft1400-2 TOD script failed to execute due to bad parameters

2 The todchangeover script authenticates the node's group. In the example used here, the group is ACCESS (seen in the output below as "group ACC") as specified in the command line of step 2 of "Updating the time of day for seasonal time changes" (page 271). Successful authentication results in the display of the following messages.

Sample log output

```
No message if authentication successful

on error

Unable to connect to group ACC. Exiting. Operation
failed:

CM: error - APPLICATION_ERROR 1136 Fdtr - Invalid
group requested ACC
```

Sample Display Alarm tool output

No message if authentication is successful

On error

Warning MSG 30100700 02-07-24 15:27:27 NMS/FT1400-2 GROUP/ACC

ID-FFFFC929 Type: security CAUSE:authenticationFailure

3 The todchangeover script displays the current time offset value for each node in the group. If the script is successful, you will see the actual time offset value for each node within the log. If the script is unable to display an time offset value for a node, an alarm is sent to the alarm browser.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Sample log output

```
... Displaying Passports with their current offset.

... If a Passport is missing or showing the wrong
offset it will need to be manually updated or a
different group should be selected. Use the Command
Console tool and use the Passport command 'set time
offset nnnn' to correct.

CHRISPC - time offset = Unable to query the time
offset

SUCCESSION_1 - time offset = -240 minutes
```

Sample Display Alarm tool output

```
WARNING MSG 30110701 02-09-05 15:27:27 NMS/FT1400-
2 PP/CHRISPC

ID: FFFFF8A0 TYPE: communications CAUSE: congestion

CO: TOD script failed to get response from Passport
```

4 The todchangeover script changes the time offset value on each node. If the script is unable to set the new time offset value, an alarm is sent to the alarm browser.

Sample log output

```
... About to change the Passport time to the new
offset

on error
```

Sample Display Alarm tool output

No message if authentication is successful

On error

```
WARNING MSG 30110702 02-09-05 15:27:27 NMS/FT1400-
2 PP/CHRISPC

ID: FFFFF8A0 TYPE: communications CAUSE:
```

5 The todchangeover script displays the results of the setting of the new time offset value. If the time offset value has been successfully changed, you will see the actual offset value of the node within the log. If the script is unable to display an offset time value, an alarm is sent to the alarm browser.

Copyright © 2006, Nortel Networks Nortel Networks Confidential

Sample log output

```
... Displaying Passports with their current offset.

... If a Passport is missing or showing the wrong
offset it will need to be manually updated or a
different group should be selected. Use the Command
Console tool and use the Passport command 'set time
offset <new_offset>' to correct.

CHRISPC - time offset = Unable to query the time
offset

SUCCESSION_1 - time offset = -240 minutes
```

Sample Display Alarm tool output

```
WARNING MSG 30110701 02-09-05 15:27:27 NMS/FT1400-
2 PP/CHRISPC

ID: FFFFF8A0 TYPE: communications CAUSE: congestion

CO: TOD script failed to get response from Passport
```

6 The script terminates. The **`/tmp/tod_output`** log file should be reviewed to ensure that all the nodes had their time offset value changed. The following message indicating that the process is complete is added to the log.

Sample log output

```
... Passport time offset change macro completed.
```

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Appendix B Using the MDM Nodal Provisioning Templates

The MDM NP template application provides a mechanism to do the following:

- add/change/delete any component/attribute in any MG15000 configuration
- apply pre-defined templates into the valid targets in the device component hierarchy and then configure the service in the resulting service form
- input certain variable data manually as it is exposed to the user, (most of configuration tasks are done transparently by the template)

  Note: The Installation Methods provide the order in which the templates are to be applied with the Engineering Specification Book providing the template field values.

See the following sections:

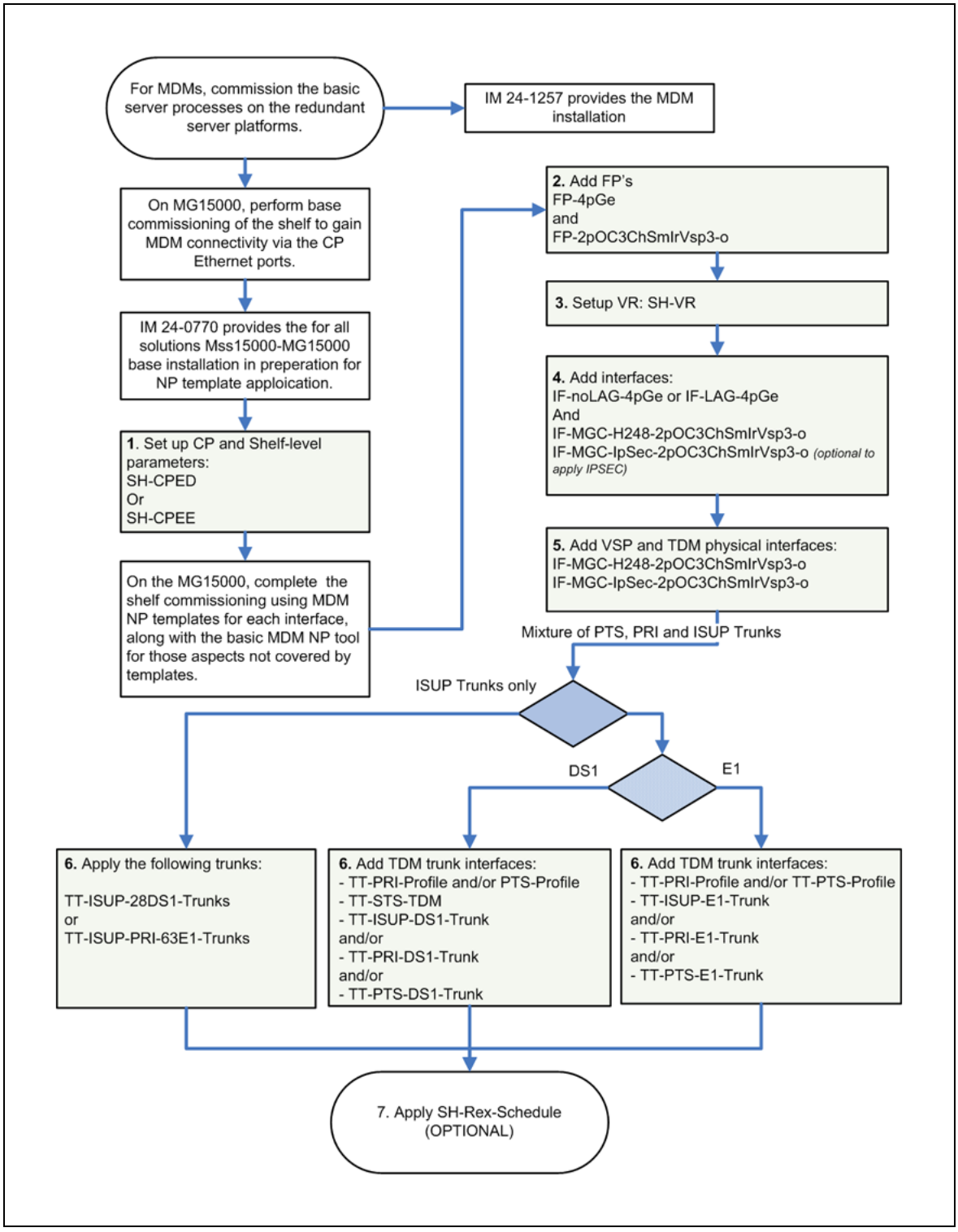
- "NP Template taskflow" (page 281)
- "Accessing and using NP Templates" (page 283)
- "NP Template descriptions for PT-IP" (page 288)
- "Using the periodic routine exercise (REX) templates" (page 313)

NP Template taskflow

The following task flow shows the steps involved for an MG15000 installation that uses Installation Methods (IMs) and Nodal Provisioning Templates for the PT-IP solution. Each major task references either an IM, used for base commissioning, or a sequence of steps that can be provisioned using the Nodal Provisioning Templates which are shown after each step. See "NP Template Task flow" (page 282).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

NP Template Task flow



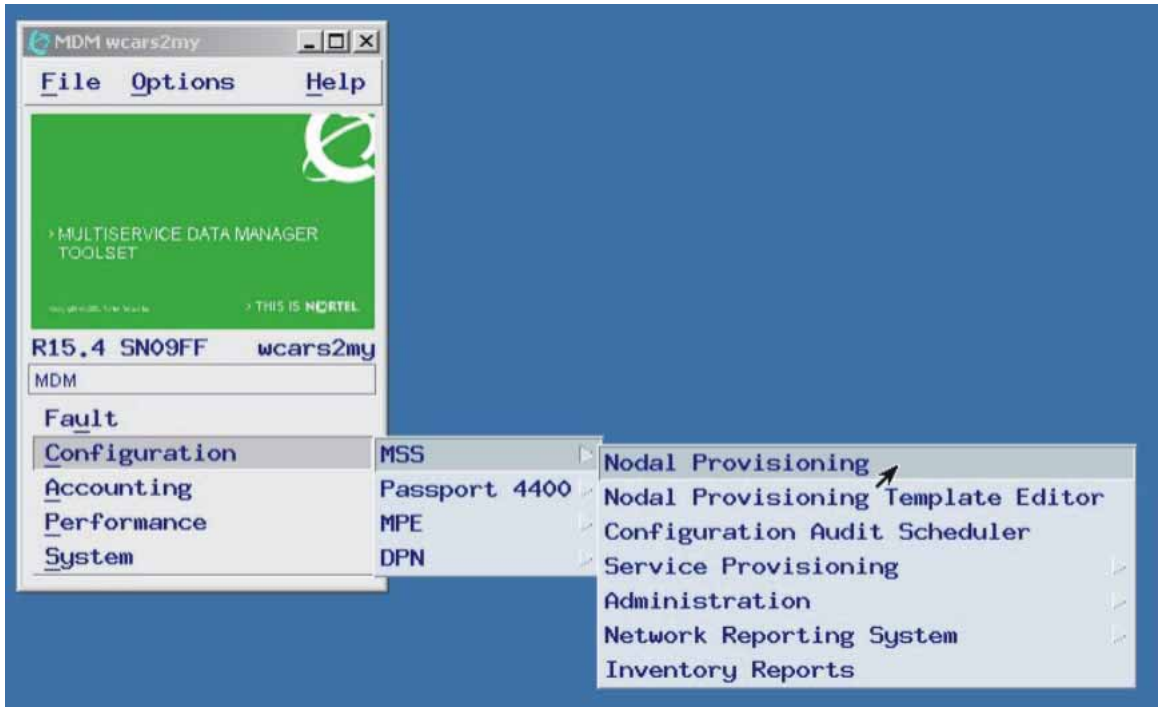
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Accessing and using NP Templates

This procedure describes the steps performed to use the Nodal Provisioning Template tool for configuring an MSS/MG15000 in the CVoIP solution. Specifically, it describes the launch of the NP tool and how to connect to and log in to an MG15000.

Accessing and using NP Templates

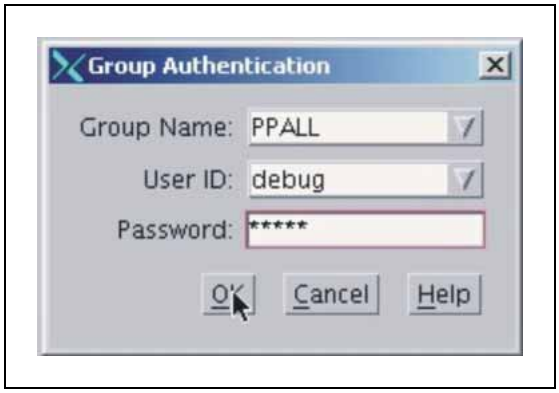
Step	Action
1	Launch the NP tool from the MDM Toolset and connect to the MG15000.



2	Select File > New Device in the Nodal Provisioning tool screen and when the Device selection screen opens select the device name of the MG15000:

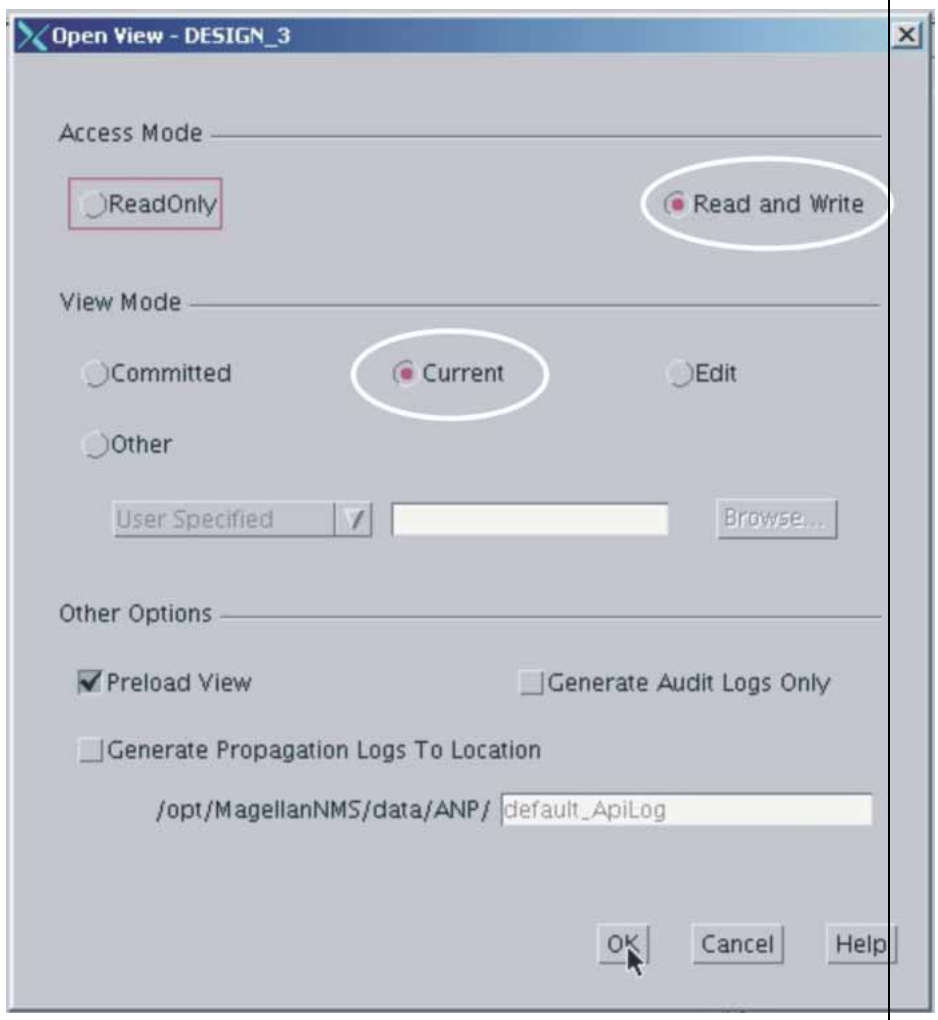
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

3 Enter your Group Name, User ID, and password for authentication in the following screen:



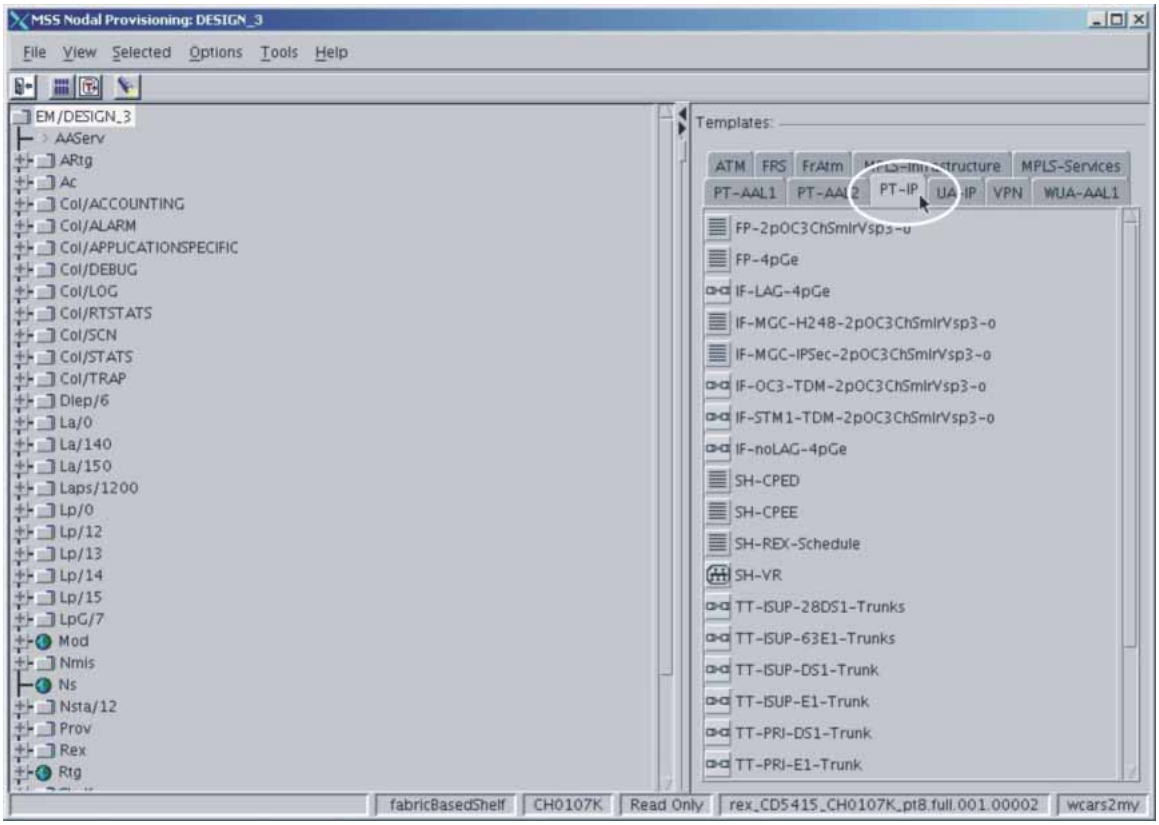
4 Select the current view with read and write privileges as follows:

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



5 Select the tab to display only the relevant templates. In this example the PT-IP tab circled as the chosen tab. The screen displays all the components provisioned on the left hand side, and all the available templates on the right hand side.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

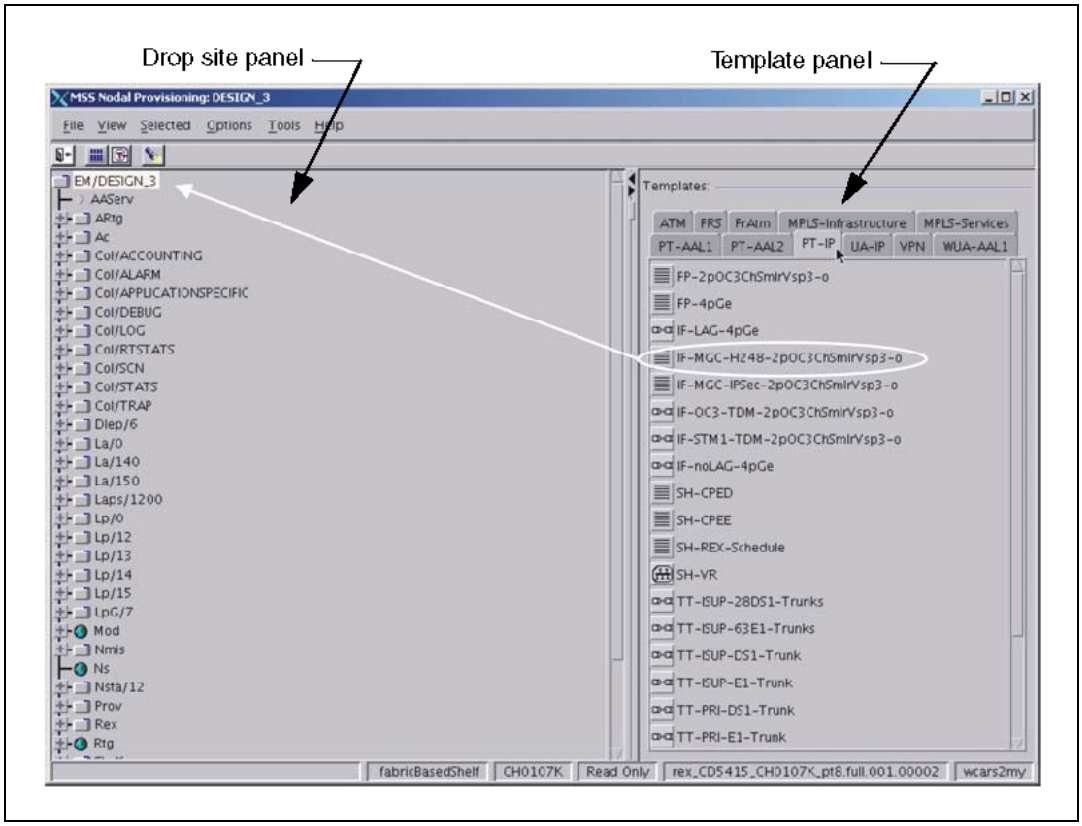


Note: In this screen, PT-IP is used as an example.

6 Drag and drop the appropriate template onto the appropriate drop-site. This is shown with a white arrow in the diagram.

Note: To determine the correct drop-site for a given template, right click->Description on the template and look for “Drop site:” in the template description. This description explains the usage of the template and lists the other templates that need to be applied prior to using the chosen template. Another alternative is to right-click on the drop-site component and select “Apply Template”. This has the advantage of only showing the subset of PT-IP templates that can be applied to that drop site.

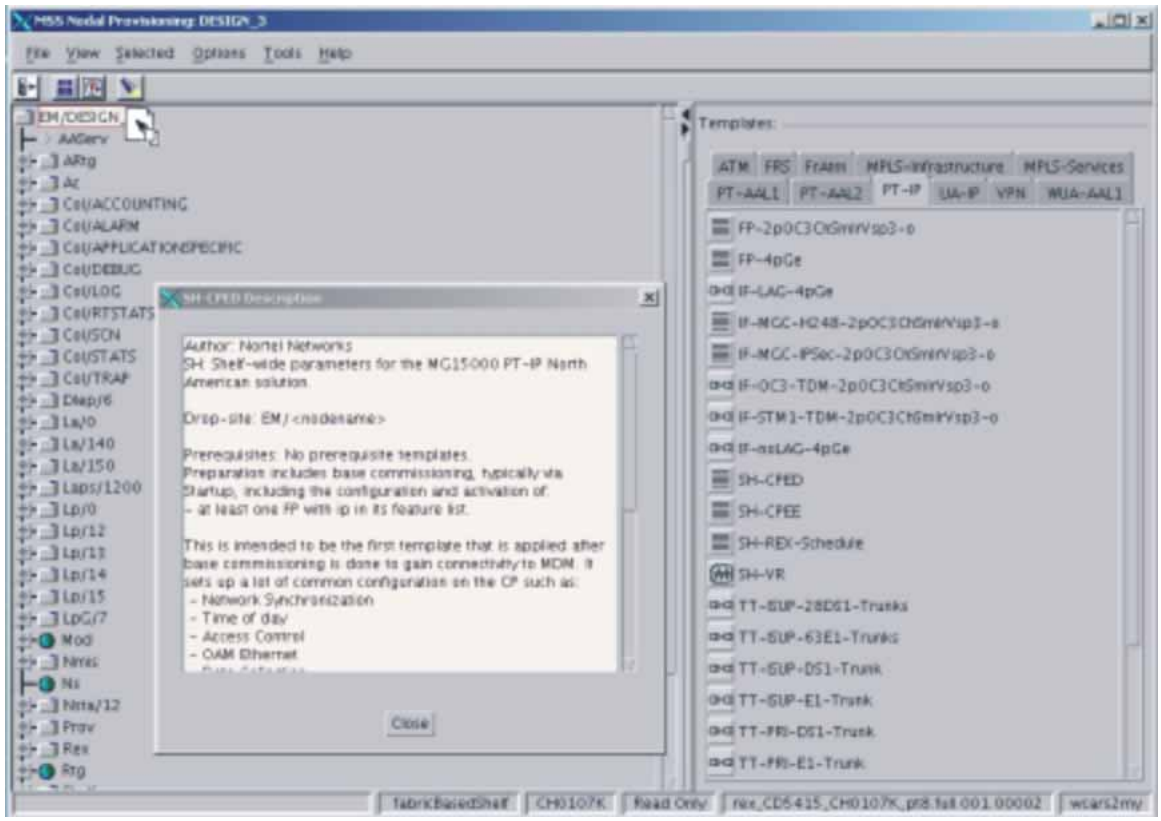
Copyright © 2006, Nortel Networks Nortel Networks Confidential



7 Apply the templates as required for your network.

Note: See "NP Template descriptions for PT-IP" (page 288).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



—End—

NP Template descriptions for PT-IP

SH-CPeD and SH-CPeE templates

CPeD and CPeE templates can be used for base shelf commissioning, however, the SAT tool is the preferred method used for base shelf commissioning and these templates are provided for audit purposes. There is one panel, Template1 for Shelf information (for example, time server IP addresses, BITS DS1 format). See "SH-CPeD template 1, Shelf panel" (page 289)The CPeE template is a variant of the CPeD template that supports the E1 BITS interface and the CPeE card.

The CPeE template is the first template that is applied after base commissioning is done to gain connectivity to MDM. It sets up a lot of common configuration on the CP such as: network synchronization, time of day, OAM Ethernet and data collection.

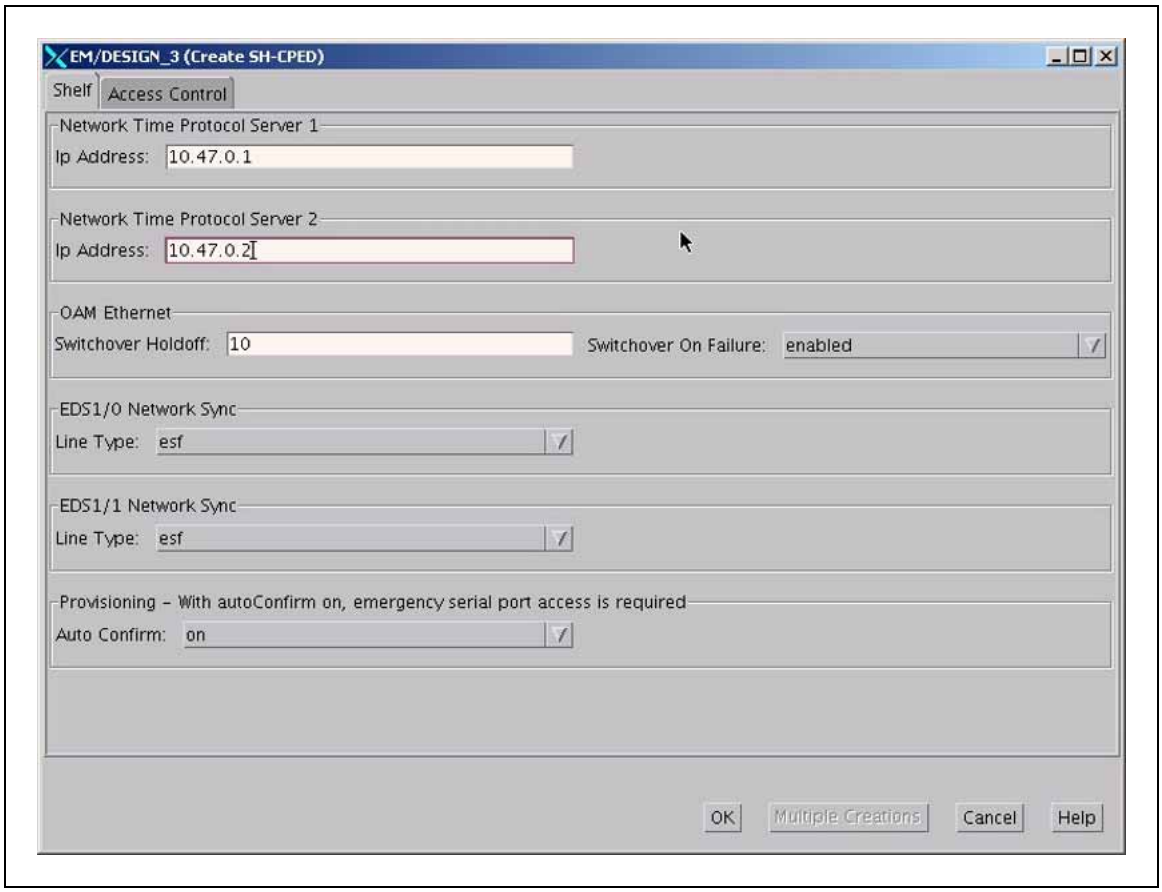
Copyright © 2006, Nortel Networks Nortel Networks Confidential

Prerequisites

No prerequisite templates are required. Preparation includes base commissioning (typically through Startup) including configuration and activation of the CP.

The sw lpt/CP featureList must include IP as well as other required features.

SH-CPeD template 1, Shelf panel

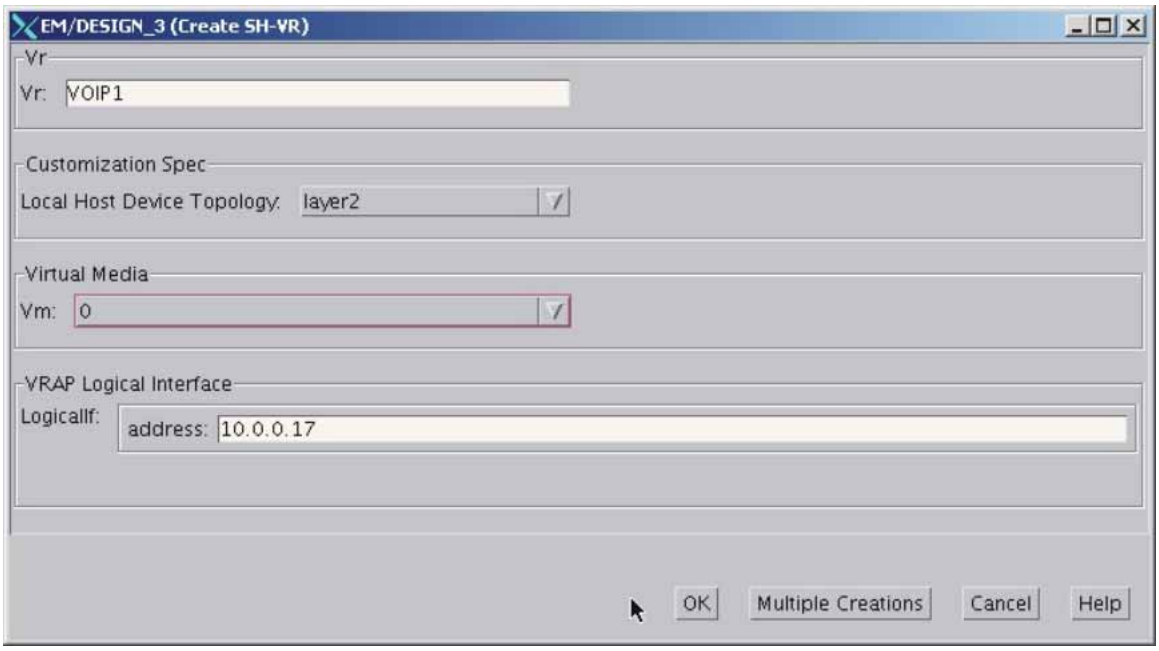


VR template

The VR template is applied to the shelf and creates a user VR with one protocol port and VM media for all the VSP cards to go on that VR. This template must not be applied until at least one GE and one VSP FP card template has been applied. All fields must be filled in, although the layer2 Local Host Device Topology should be left as layer2. The name of the virtual router should be named consistently to avoid confusion if/when further VoIP virtual routers are added for growth. The virtual media value must be unique across all the VoIP VRs that are created. The VRAP logical interface is from the Engineering specification book. It's value depends on the subnet, but is normally set to 10.0.0.17.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

SH-VR



Note: When configuring using the SH-VR template, set the Local Host Device Topology (localHostDeviceTopology) attribute to layer 2.

When layer 3 is supported, the LOS during Migration must be set to enabled.

FP card templates

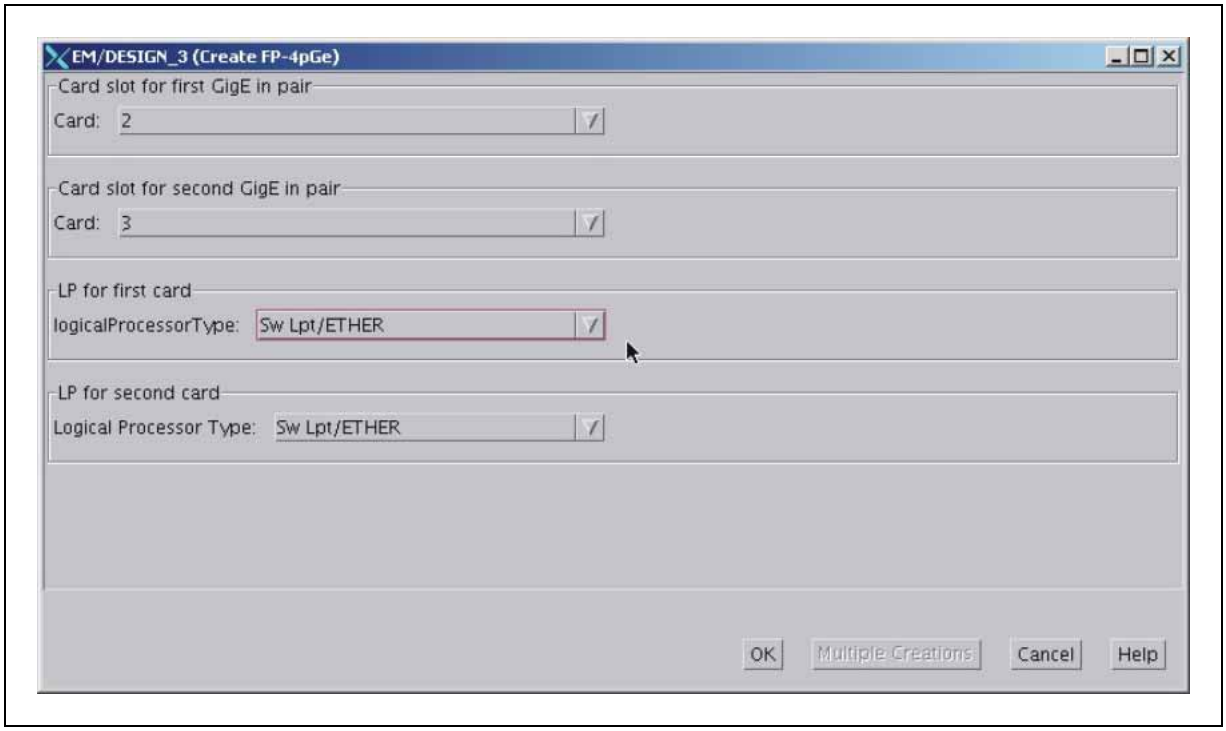
These templates provision the 4pGE, 2pVSP3-o, and 2pVSP4e FP cards on the shelf.

For the 4-port GE template there are only two fields to set. The other fields are automatically set depending on the selection. The two fields are as follows:

- Set the card slot for the first GE card in the pair. This is normally card slot 2. (The second slot will automatically be set to 3.)
- Set the logical processor type for the first LP. It must be set to ethernet. (The second LP is automatically set.) The selection of software types is provisioned before nodal provisioning with templates takes place. See the "4pGE template" (page 291).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

4pGE template



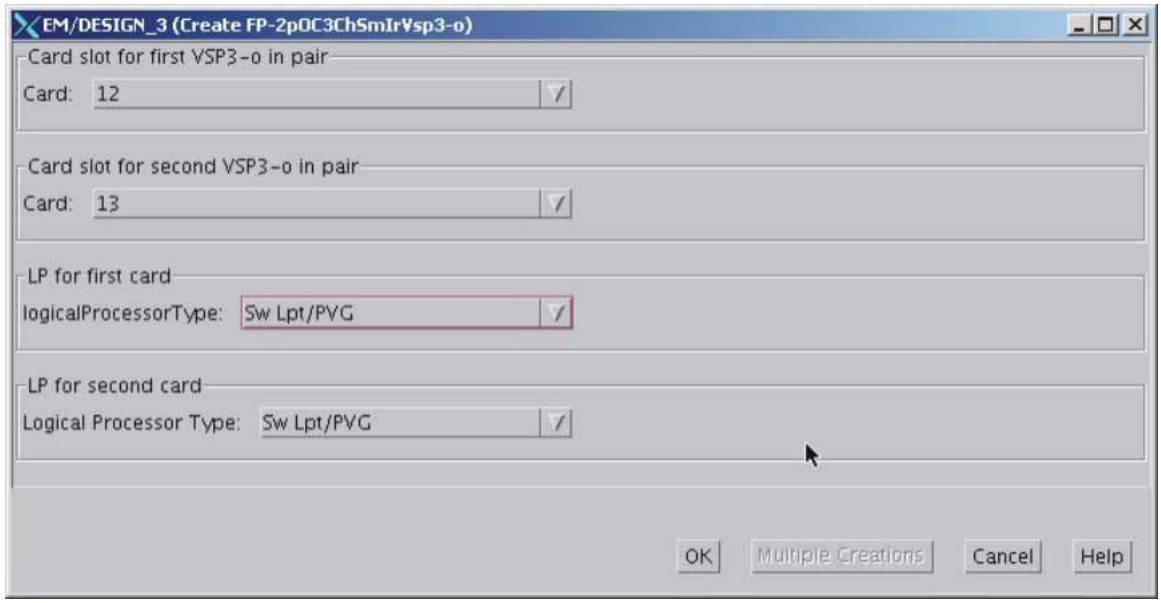
For the 2pVSP3-o there are only two fields to set in the VSP3-o template. The other fields are automatically set depending on the selection. The two fields are as follows:

- Set the card slot for the first VSP3-o card in the pair. This is normally an even-numbered slot from 4-14. (The second slot will automatically be set.)
- Set the logical processor type for the first LP. It must be set to PVG. (The second LP is automatically set.) The selection of software types is provisioned before nodal provisioning with templates takes place. See the "2pVSP3-o template" (page 292).

  Note: If you chose Local Host Device Topology of layer2 when you configured with the SH-VR template, set the LOS during Migration to disabled. When layer3 is supported, the LOS during Migration must be set to enabled.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2pVSP3-o template



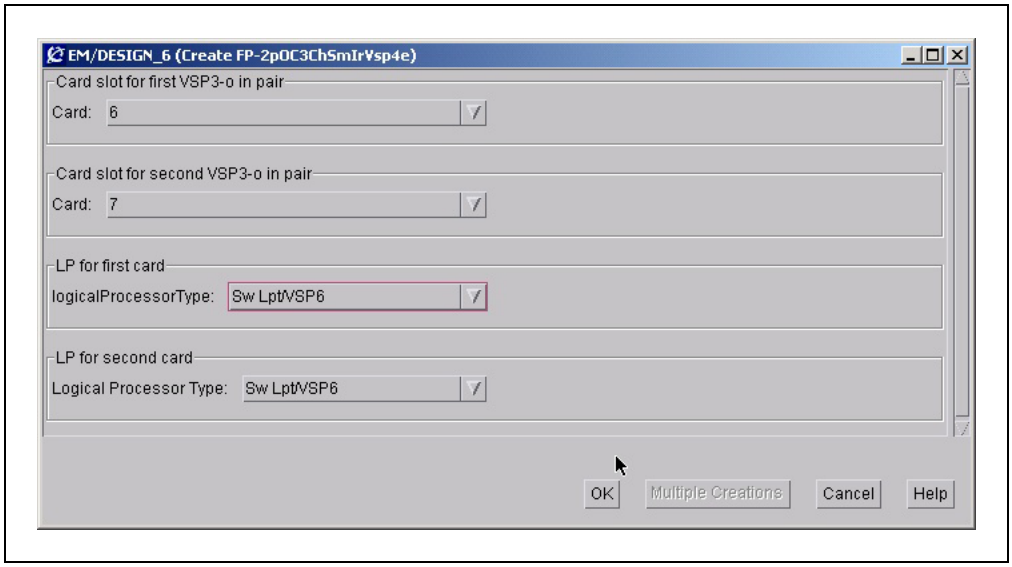
For the 2pVSP4e FP, there are only two fields to set in the 2pVSP4e template. The other fields are automatically set depending on the selection. The two fields are as follows:

- Set the card slot for the first 2pVSP4e card in the pair. This is normally an even-numbered slot from 4-14 (the second slot is automatically set).
- Set the logical processor type to PVG for the first LP (the second LP is automatically set). The selection of software types is provisioned before nodal provisioning with templates takes place. See "2pVSP4e template" (page 293).

  Note: If you chose the local host device topology of layer2 when you configured with the Sh-VR template, set the LOS during Migration to disabled. When layer3 is supported, the LOS during Migration must be set to enabled.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2pVSP4e template



Interface templates

The following are screens for the Gigabit Ethernet template using the no LAG configuration. This is a configuration for PT-IP using VSP3-o cards. (LAG is primarily for future configurations using 2pVSP4e cards.) There are two tabs in the dialog, which the user will need to view.

The only field that normally requires provisioning is the Ethernet port (0-3). The LAN Application is determined from the LP on which you drop the template. You can enter information in the far-end Vendor and Comment Text fields, depending on your requirements. See "GigE No LAG template1" (page 294).

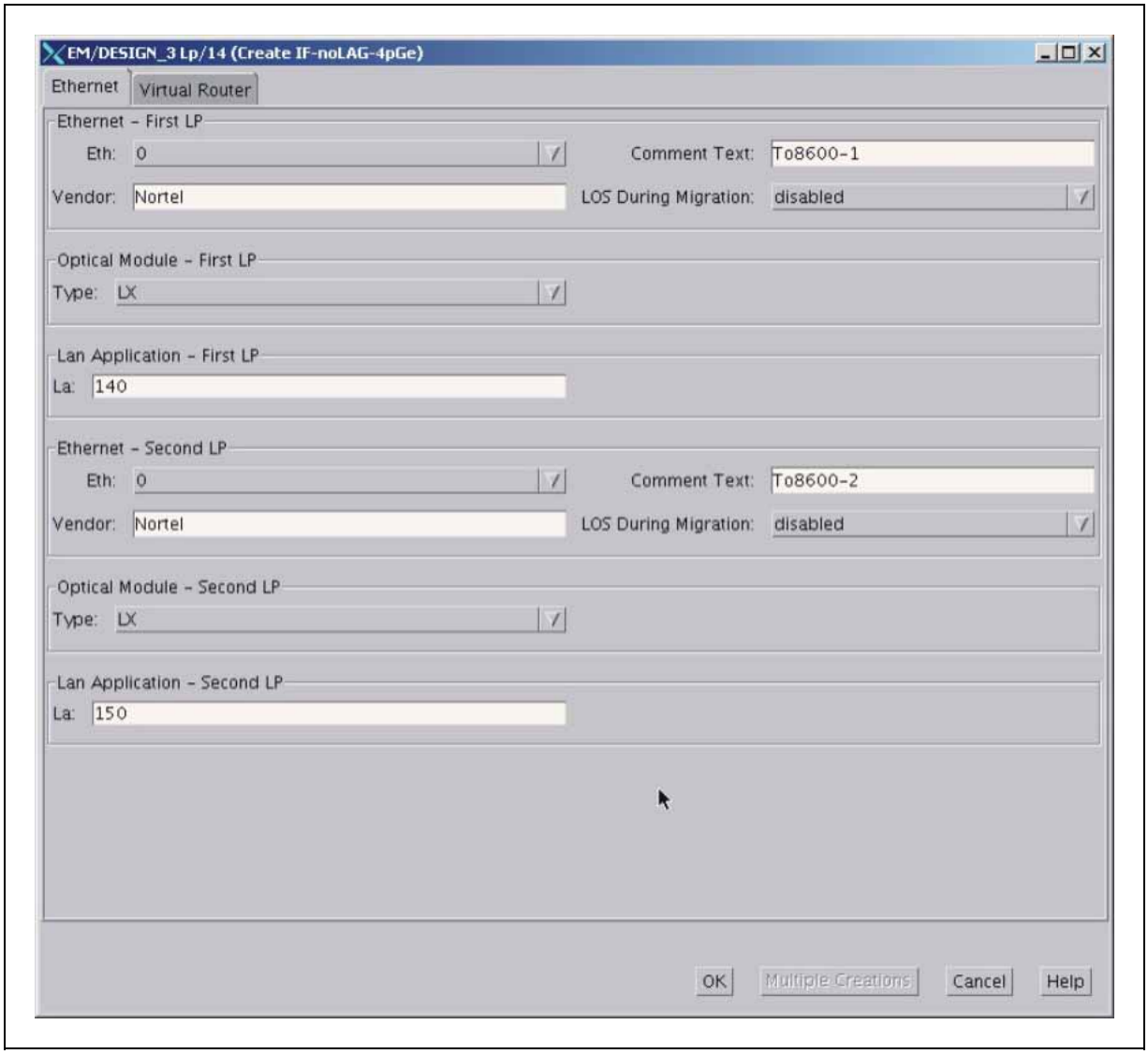
> ***Note:*** You must set the Optical Module type to match the Inserted type. To determine the Inserted type, use the following MSS command

```
d lp/x eth/0 om insertedType
```

If layer3 local host topology is used, select “enabled” for losDuringMigration on both Ethernet ports. The default, however, is disabled for layer2.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

GigE No LAG template1

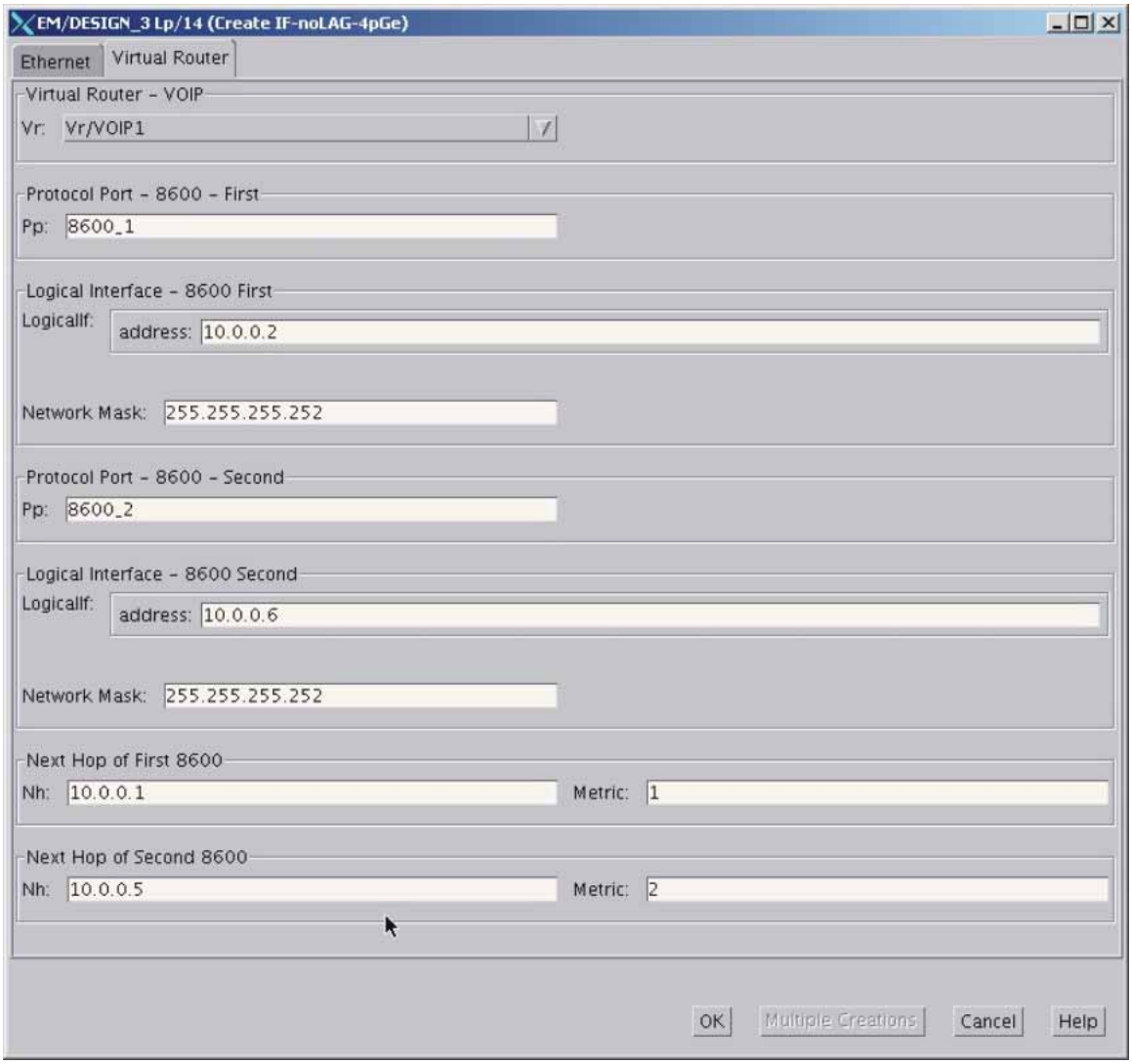


For GigE NoLAG template 2 the user must select the appropriate VoIP virtual router. then you would choose appropriate names for the two 8600s. The values shown in the template are sufficient. Again, if suggested addressing is used, the values of 10.0.0.2 and 10.0.0.6 are appropriate. Enter the logical interfaces. The netmask should be left at the default of 255.255.255.252.

Finally, next hop addresses for routing to the 8600s must be entered. These are normally 10.0.0.1 and 10.0.0.5. Metrics are for routing weighting, and should normally be left as the defaults of 1 and 2.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

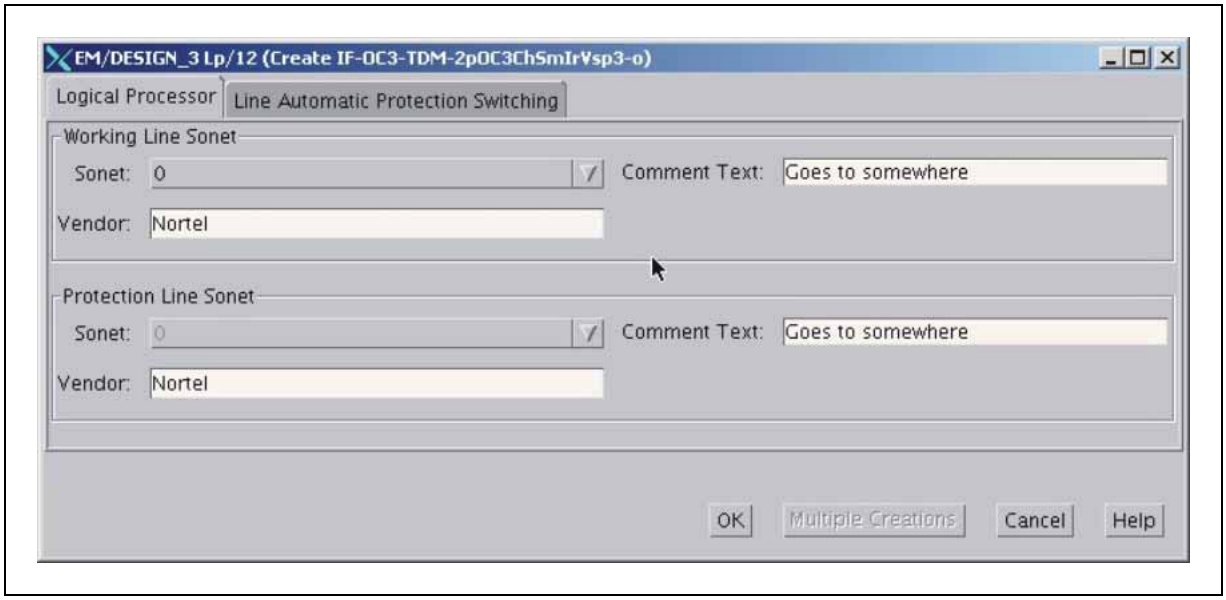
GigE NoLAG template 2



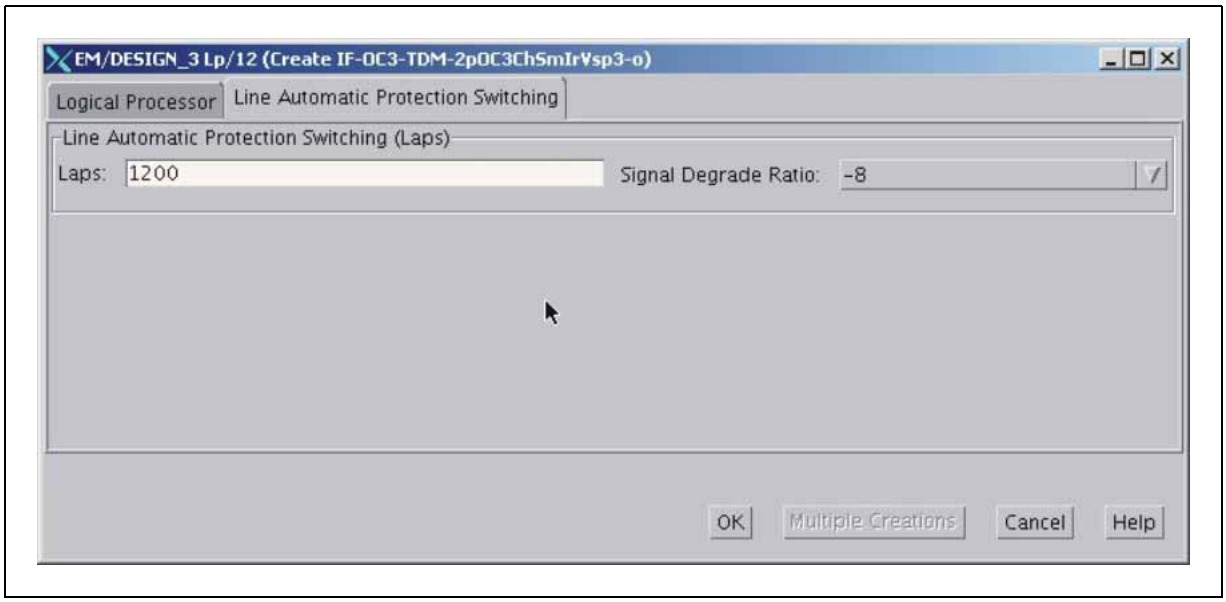
The following two screens show the information in the OC3 TDM provisioning template. This template is used to configure the TDM port on the VSP3-o cards. You must define at least 1 Sts components (value 1 to 3) using the TT-Sts-TDM template, before provisioning trunks. The Sonet port should be set to 0, as there is only 1 TDM port on the VSP3-o. Vendor and Comment text may be set as well. Usually, nothing needs to be changed in the LAPS tab.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

OC3 TDM provisioning template 1



OC3 TDM provisioning template 2



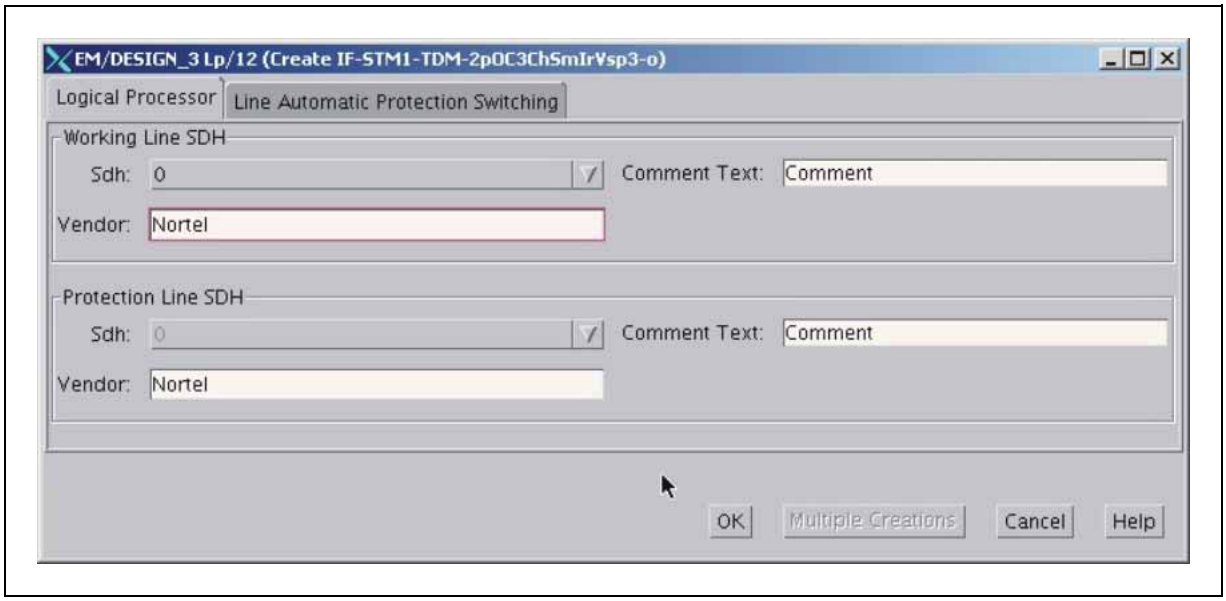
The next two screens are used to provision STM1 ports. The information is identical to the OC3 templates, except it is for the International standards.

The STM1 template, however, does define a VC4 component. Therefore it is not necessary to apply the TT-Sts-TDM template. The reason the subcomponent is added automatically is because a VC4 component uses the entire STM1 bandwidth.

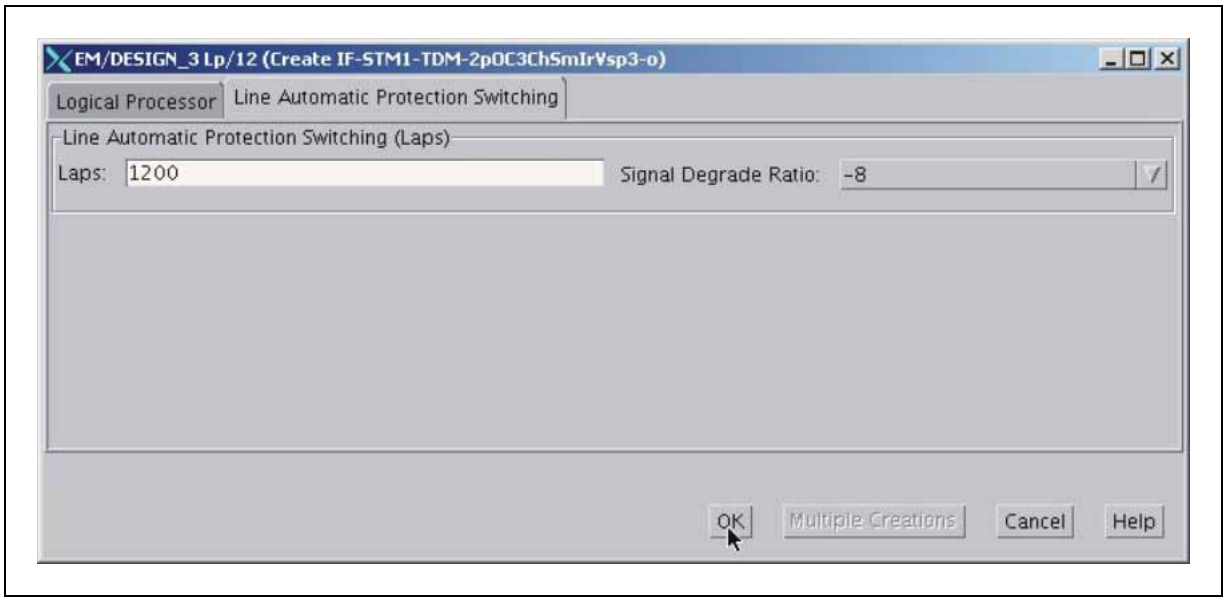
See "STM1 template1" (page 297) and "STM1 template2" (page 297).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

STM1 template1



STM1 template2



Service templates

The Media Gateway Controller templates are used to set up communication between the 2pVSP3-o or 2pVSP4e FP cards on the Media Gateway 15000 and the Media Gateway Controller. In both cases, although the template is only one screen, each template is shown in two figures (H.248-2pOC3ChSmlrVsp3-o templates 1 and 2 for the 2pVSP3-o FP, and H.248-2pOC3ChSmlrVsp4e templates 1 and 2 for the 2pVSP4e FP).

- Protocol port: This is the VRAP protocol port under the VoIP virtual router.

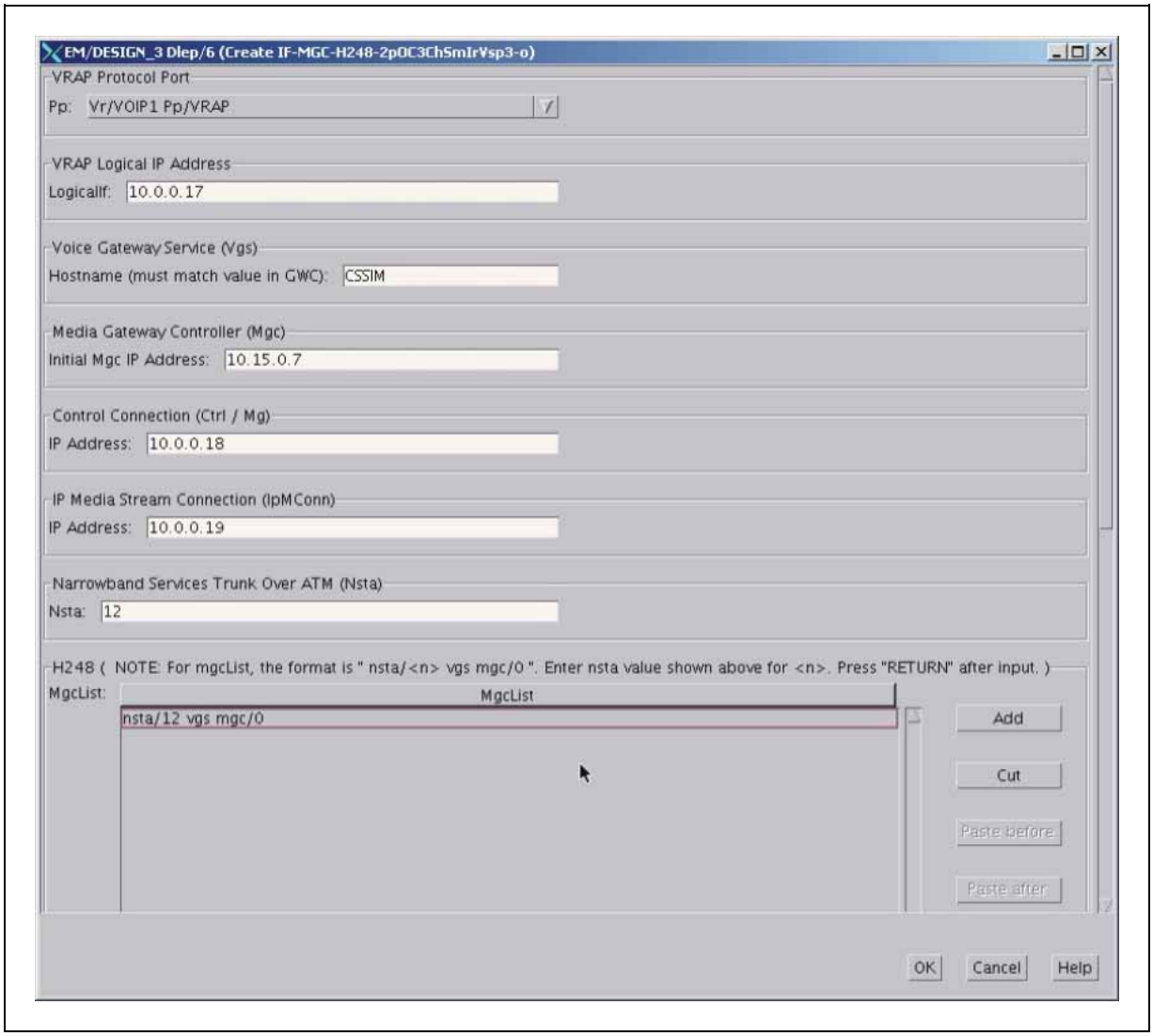
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- VRAP IP address: This is normally set to 10.0.0.17
- VGS hostname: This value must match the value specified in the gateway controller provisioning, so the spec. book will list this value. If this value is ever changed later, it will cause all calls on the gateway to drop.
- Media gateway controller IP address: This must be set to the IP address of the gateway controller. It is likely a 10.x.x.x private address.
- Control connection IP address: This is normally 10.0.0.18.
- IP Media stream IP address: This is normally 10.0.0.19.
- Nsta: This value is set automatically.
- H248 MgcList: This value must be set by the user, by simply copying the Nsta value into the nsta value already defined in the list.
- Mg Mid: Normally, leave this value alone, as it is set automatically when the control connection IP address is defined above.
- The VRAP MG and IpMConn are also set automatically.
- The loss integration period should be left as 0.
- Default codec list. More codecs can be added using the Add button if required.

See "H.248-2pOC3ChSmlrVsp3-o template 1" (page 299), "H.248-2pOC3ChSmlrVsp3-o template 2" (page 300), "H.248-2pOC3ChSmlrVSP4e template 1" (page 301). and the "H.248-2pOC3ChSmlrVSP4e template 2" (page 302)..

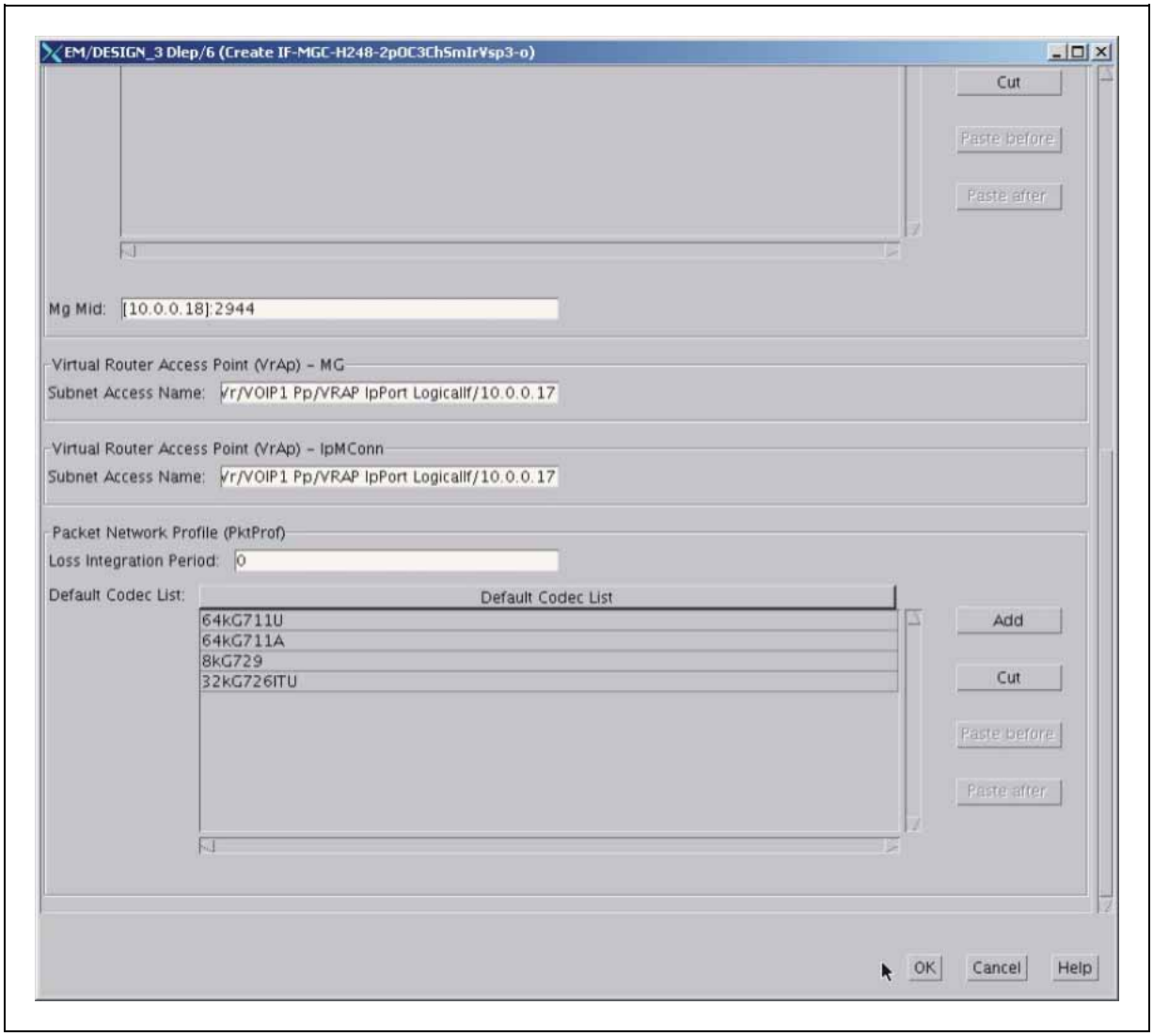
Copyright © 2006, Nortel Networks Nortel Networks Confidential

H.248-2pOC3ChSmlrVsp3-o template 1



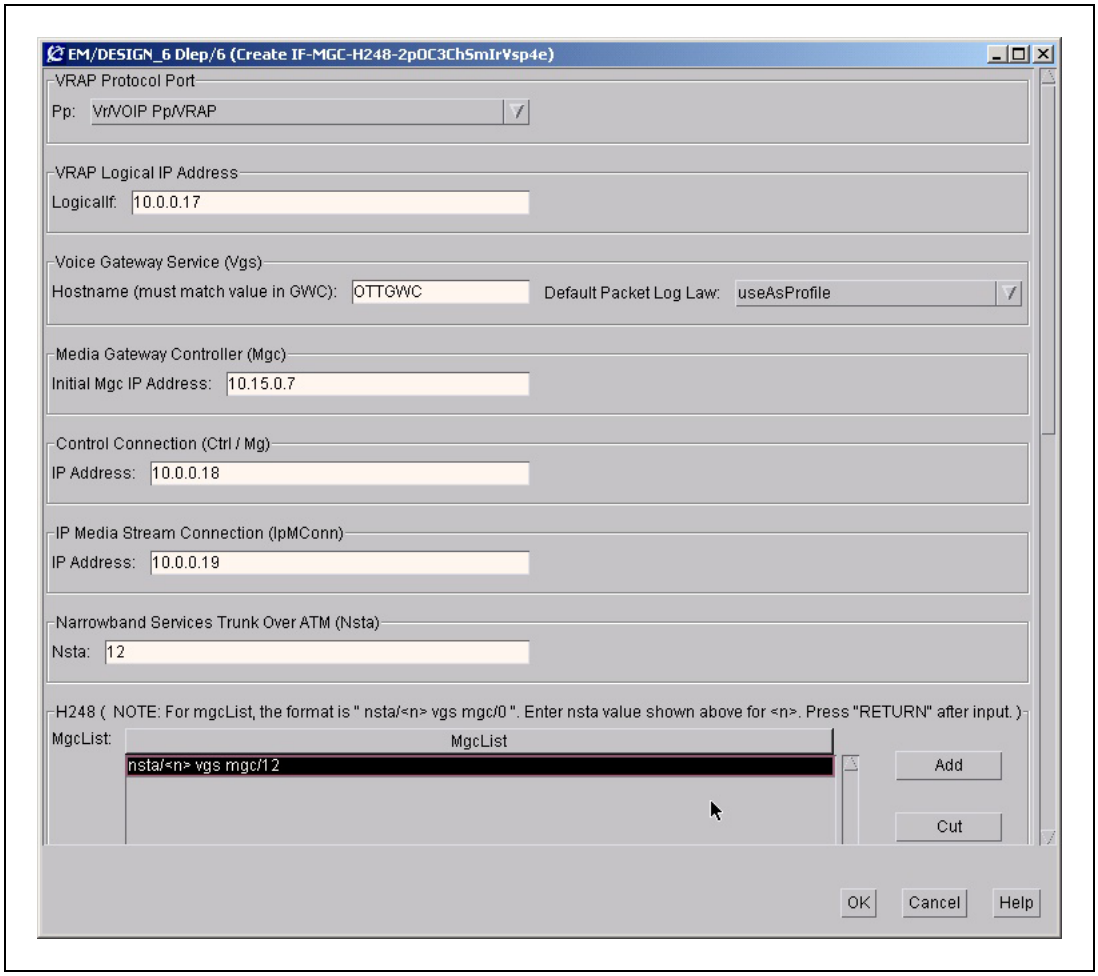
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

H.248-2pOC3ChSmlrVsp3-o template 2



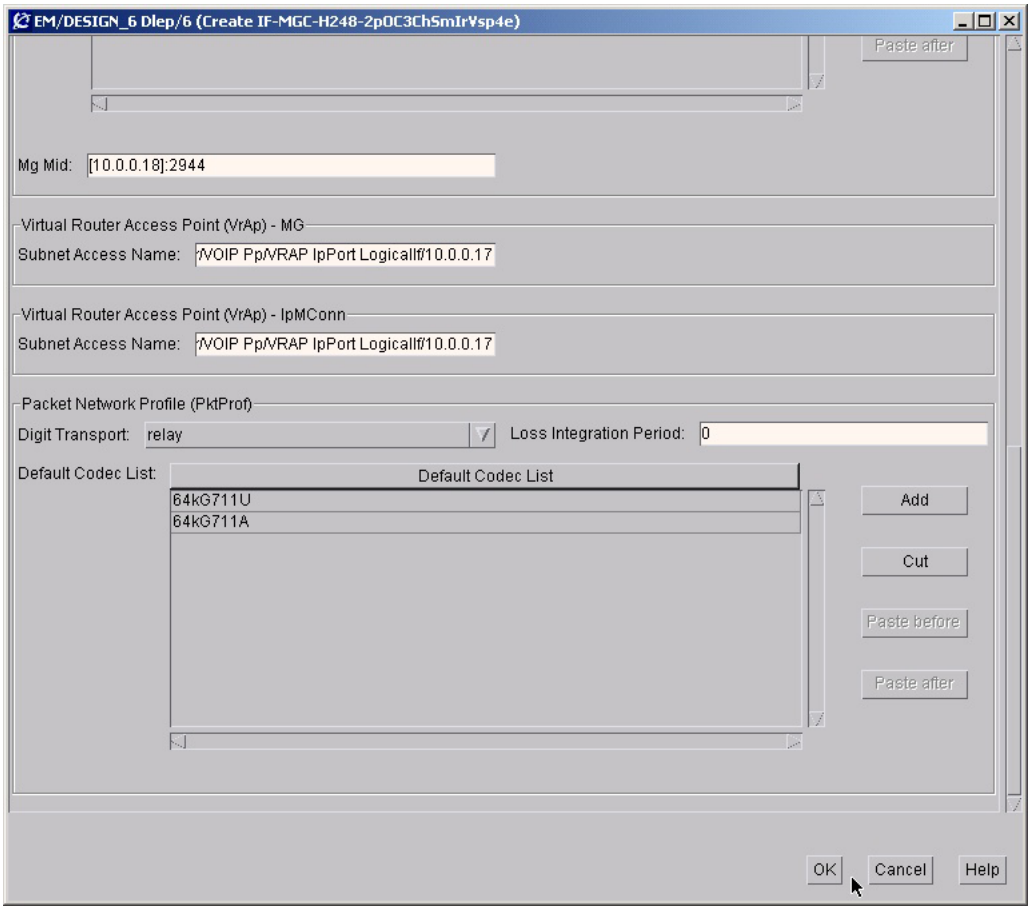
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

H.248-2pOC3ChSmIrVSP4e template 1



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

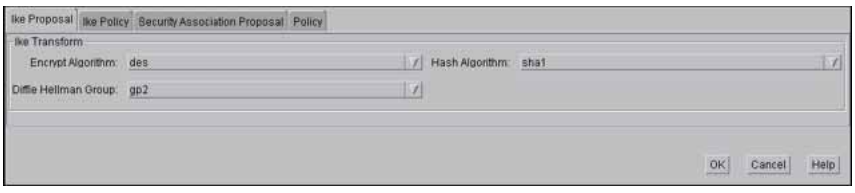
H.248-2pOC3ChSmIrVSP4e template 2



Optionally, the IF-MGC-IPSec-2pOC3ChSmIrVsp3-o template may be applied to give enhanced security in the H.248 signalling traffic between the gateway and gateway controller. The next few figures illustrate the various screens within the template.

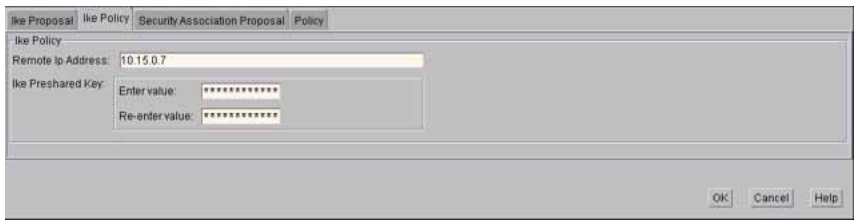
To provision enhanced security, pvgIpSec is needed in the feature list of the VSP3-o LP software.

MGC IPSec template 1

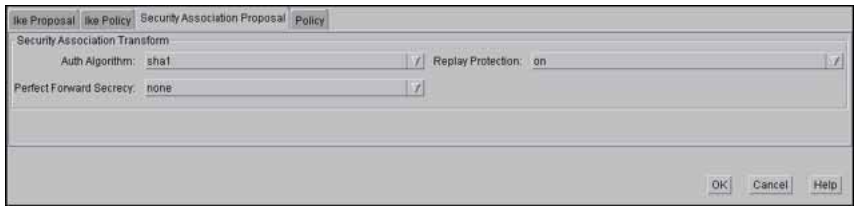


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

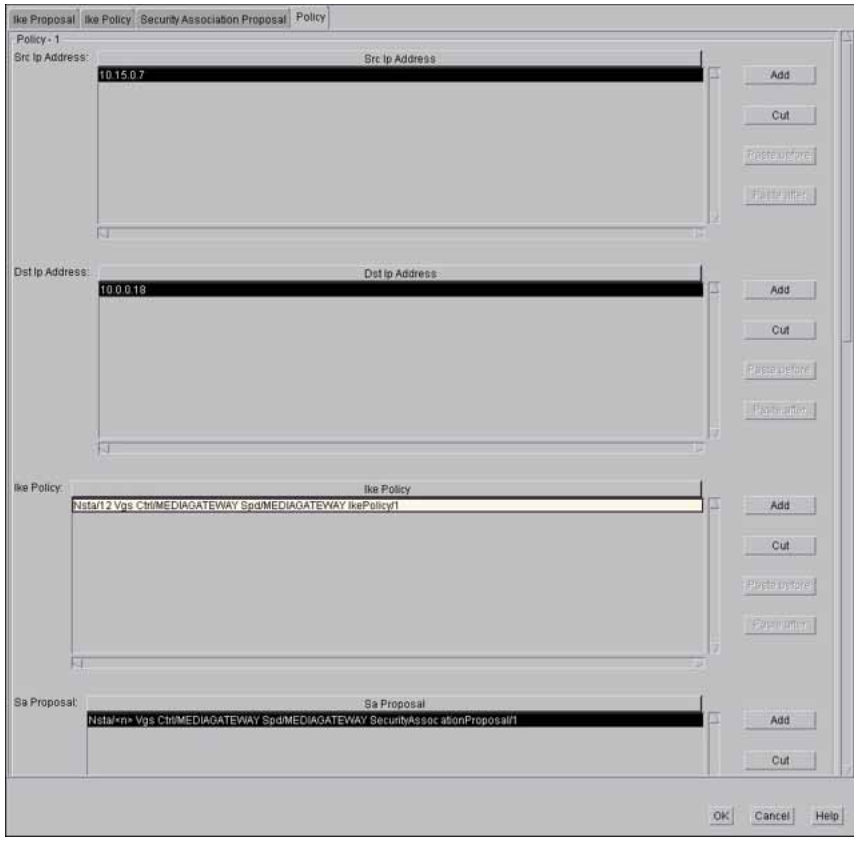
MGC IPSec template 2



MGC IPSec template 3



MGC IPSec template 4

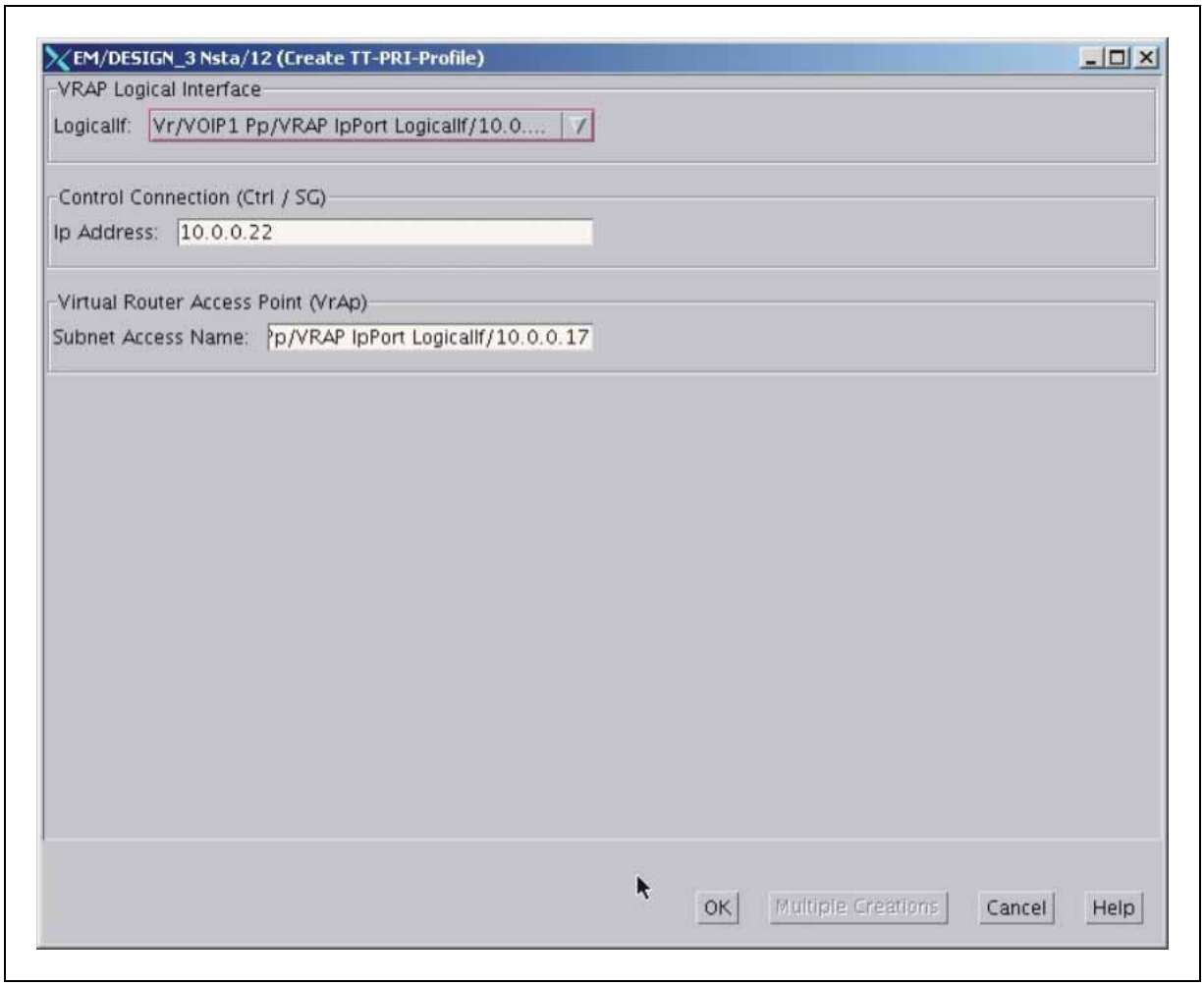


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

PRI Profile Template

This template must be used if PRI trunks are used on the MG15000. The template is used to define the signaling information needed to handle PRI trunks. Select the VRAP interface under the VoIP virtual router, and enter the control connection IP address where required. This value is likely to be 10.0.0.22, but may differ depending on the configuration.

PRI Profile Template



PTS Profile Template

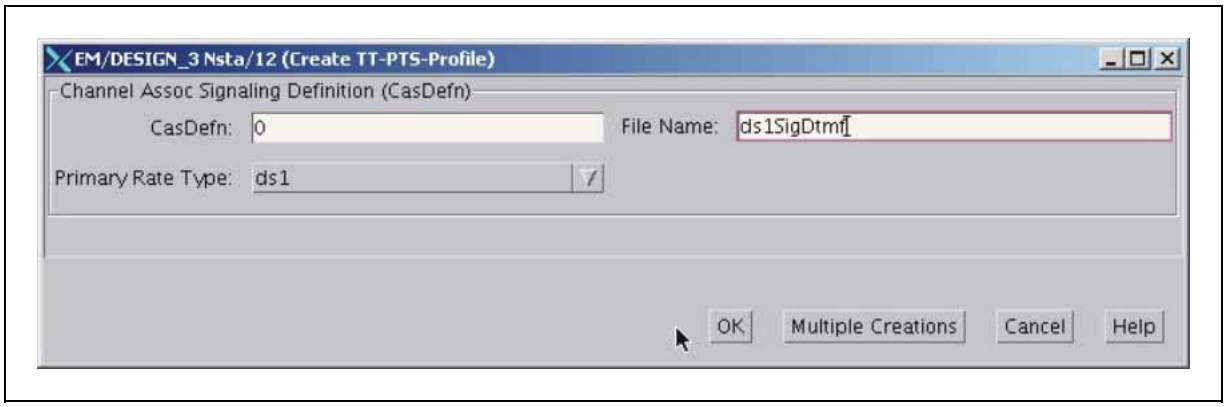
The PTS Profile Template, for both the North-American version and the European version. This template must be used if PTS trunks are used on the MG15000. The template is used to define the signaling information needed to handle PTS trunks. See "North American profile" (page 305) and "International profile" (page 305).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

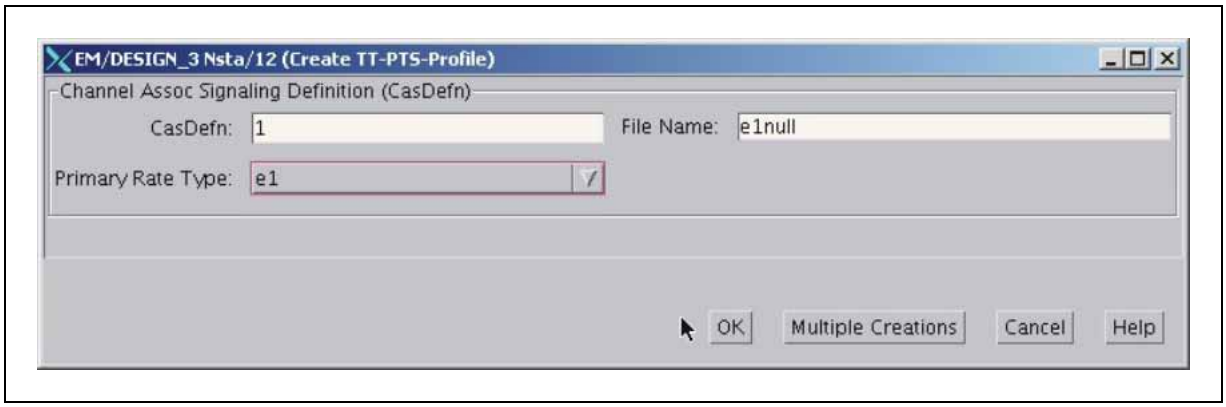
The CasDefinition value should be unique for each PTS profile. Normally, start numbering this from 0. The primary rate type should be set to ds1 or e1, depending on the standard.

Finally, the file name for the profile should be set to “ds1SigDtmf” if using DS1 trunks, or e1null if using E1 trunks.

North American profile



International profile



DS1/E1 ISUP trunk

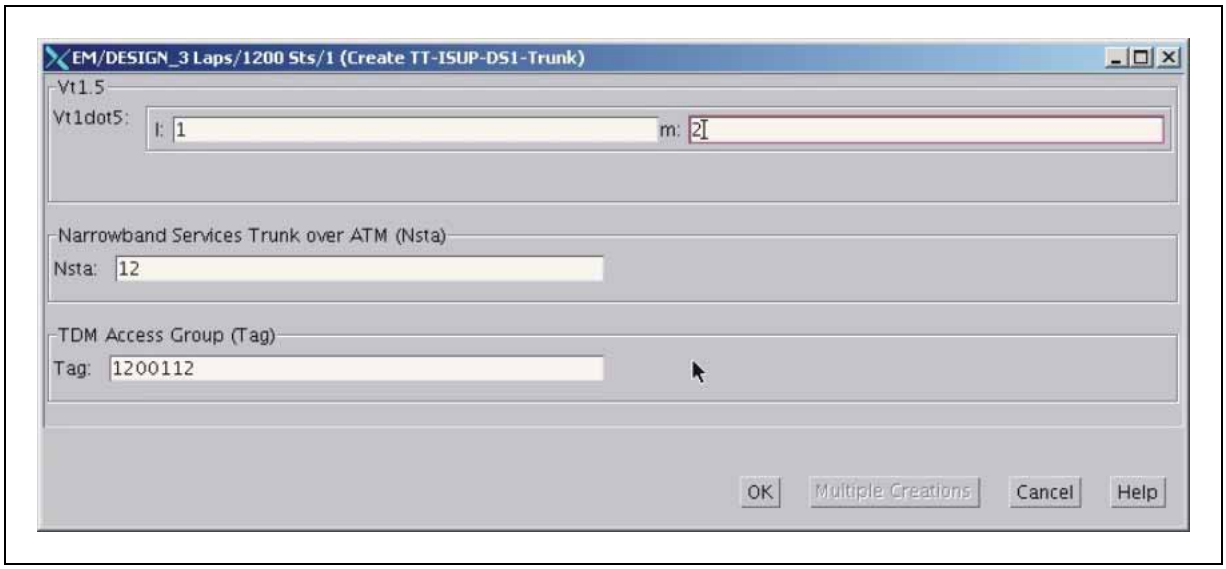
To create a DS1 ISUP trunk, simply drag the template onto a Laps Sts component. (If the Sts component does not exist under the Laps component, create it using the TT-Sts-TDM template.) The only information that needs entering is the “l” and “m” values for numbering the trunk. The “l” is an integer from 1 to 7, and “m” is an integer from 1 to 4. Thus a total of 28 Ds1 trunks can be defined.

To create an E1 ISUP trunk, simply drag the template onto a Laps Vc4 component. The only information that needs to be entered is the “k”, “l”, and “m” values for numbering the trunk. “k” is an integer from 1 to 3. “l” is an integer from 1 to 7, and “m” is an integer from 1 to 3. Thus a total of 63 E1 trunks can be defined.

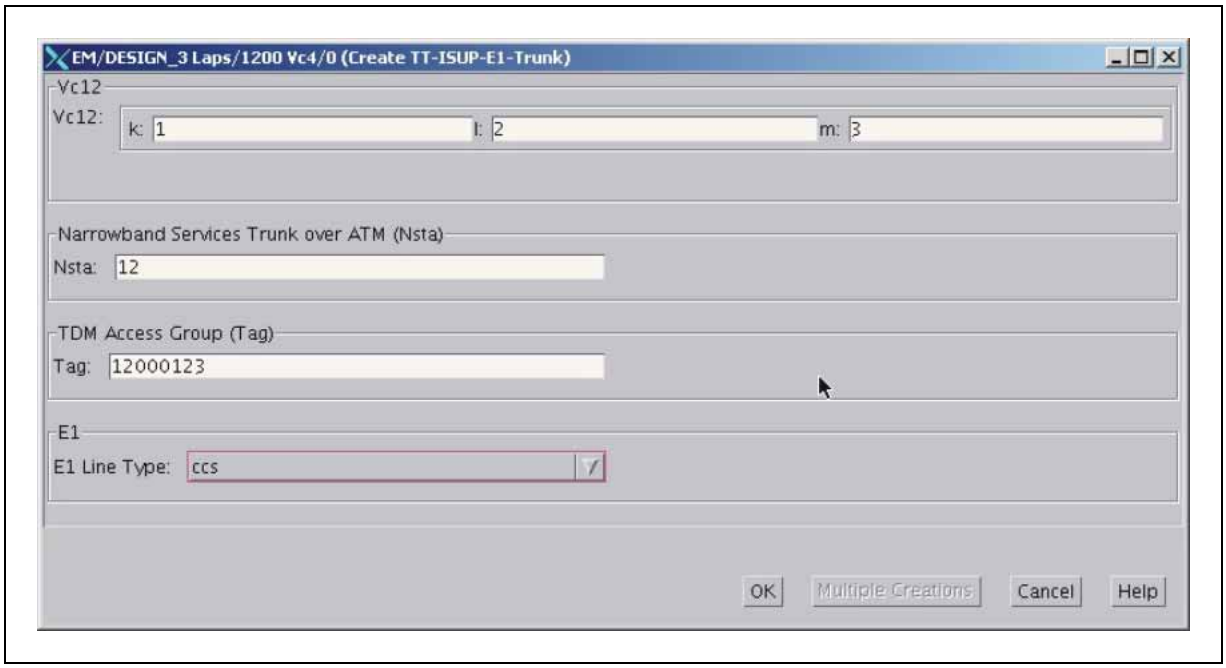
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

See "DS1 ISUP Template" (page 306) or "E1 ISUP Template" (page 306).

DS1 ISUP Template



E1 ISUP Template



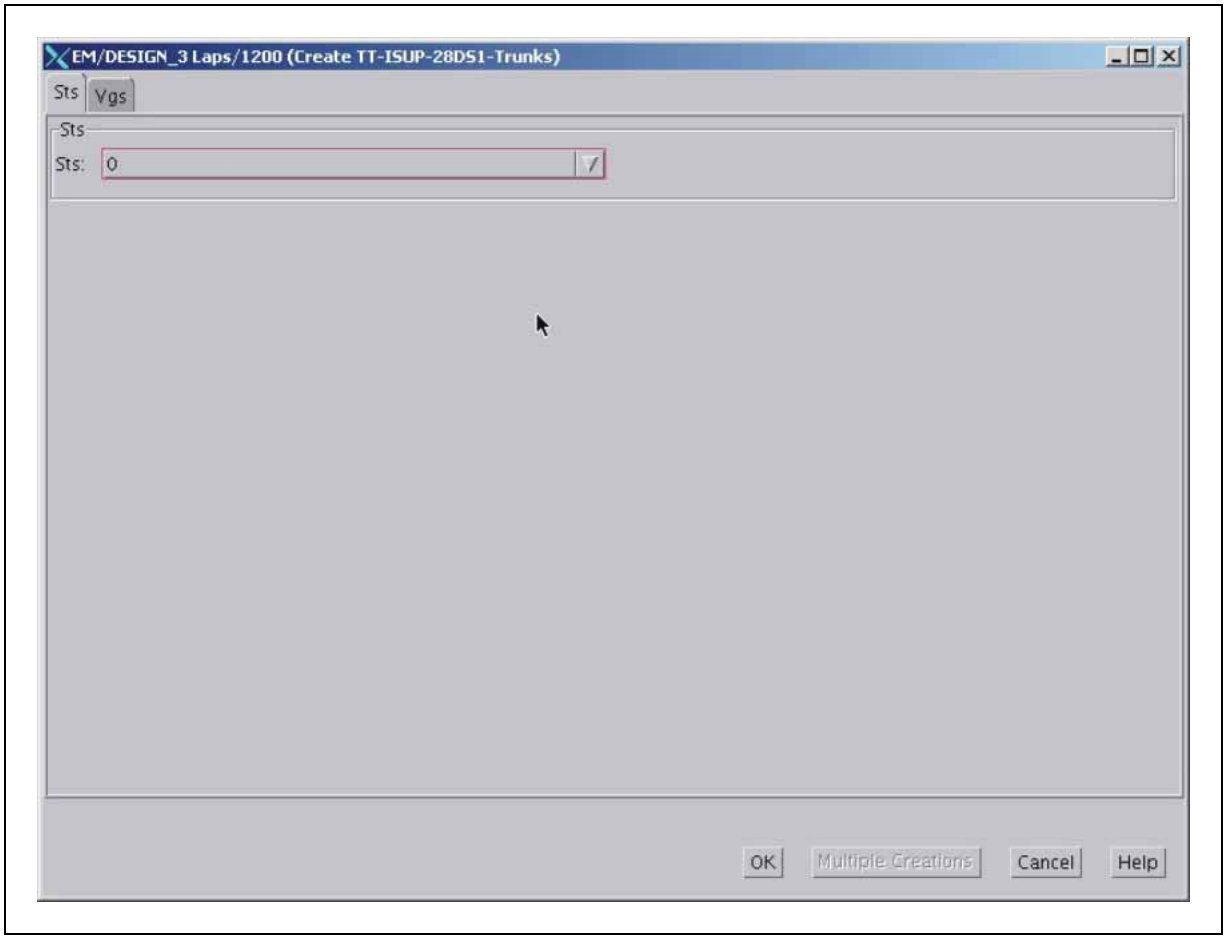
28 DS1 ISUP trunk

Provisioning 28 DS1 trunks and the Sts component under Laps can be achieved using the TT-ISUP-28DS1-Trunks template. The only value that the user needs to enter is the Sts number. It's value is 0, 1, or 2. The

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

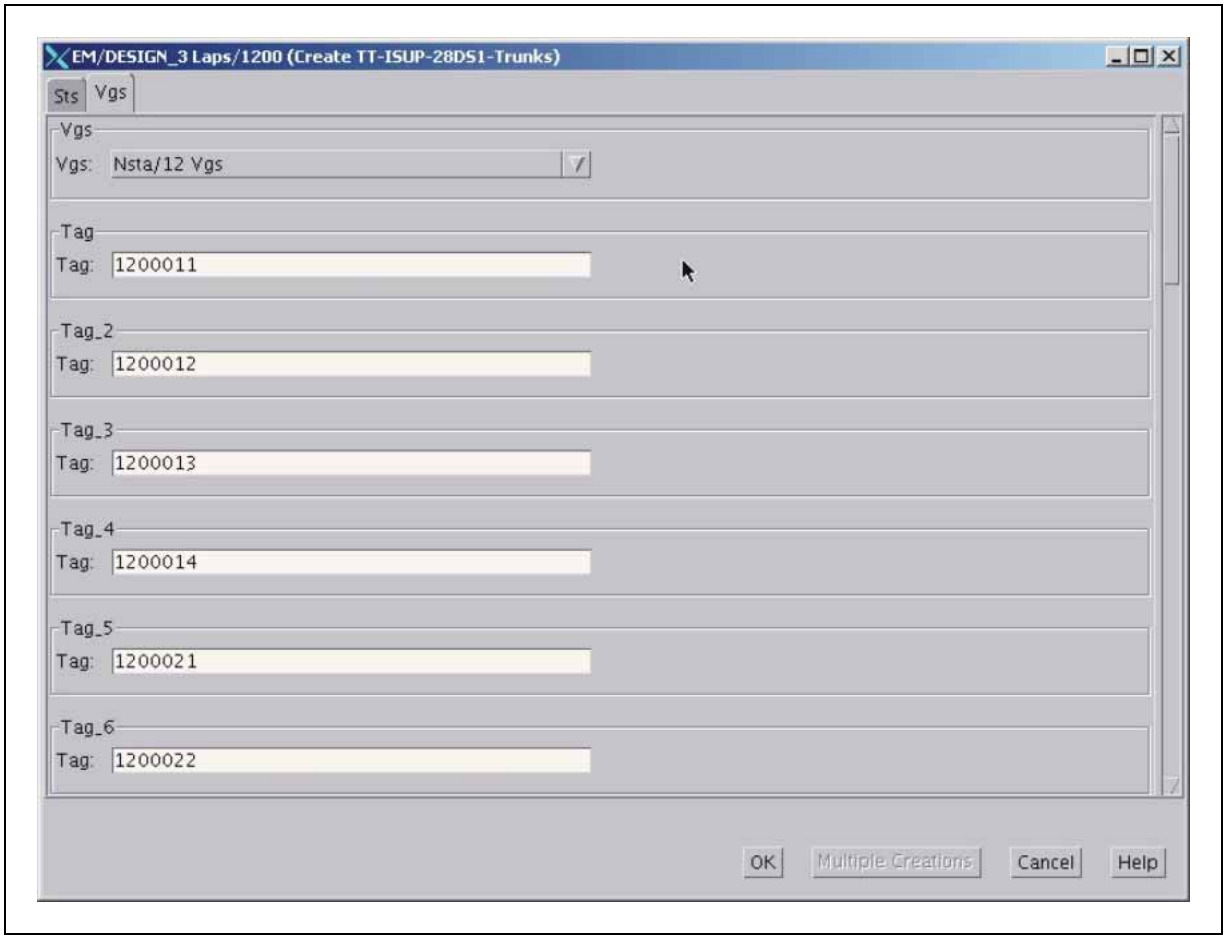
effect is the same as provisioning all 28 DS1 trunks individually, but much quicker. See "28 DS1 ISUP Template (1)" (page 307) and "28 DS1 ISUP Template (2)" (page 308).

28 DS1 ISUP Template (1)



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

28 DS1 ISUP Template (2)

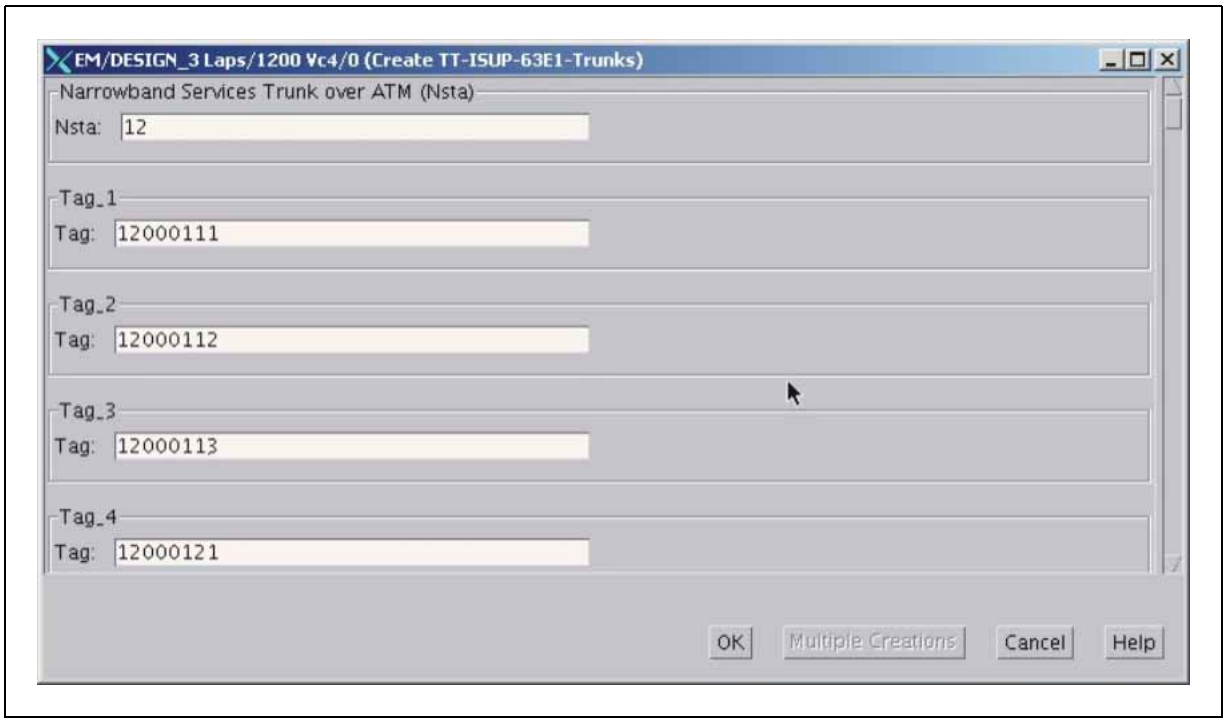


63 ISUP E1 trunks

You can provision 63 ISUP E1 trunks using the TT-ISUP-63E1-Trunks template on 2pOC3ChSmIrVsp3 FPs. All Vc12 trunks under this Vc4 hierarchy must not have been previously configured. This must be dropped on the Vc4 component, under Laps. No further user information is required. See "63 ISUP E1 trunks" (page 308).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

63 ISUP E1 Trunks



PRI trunks

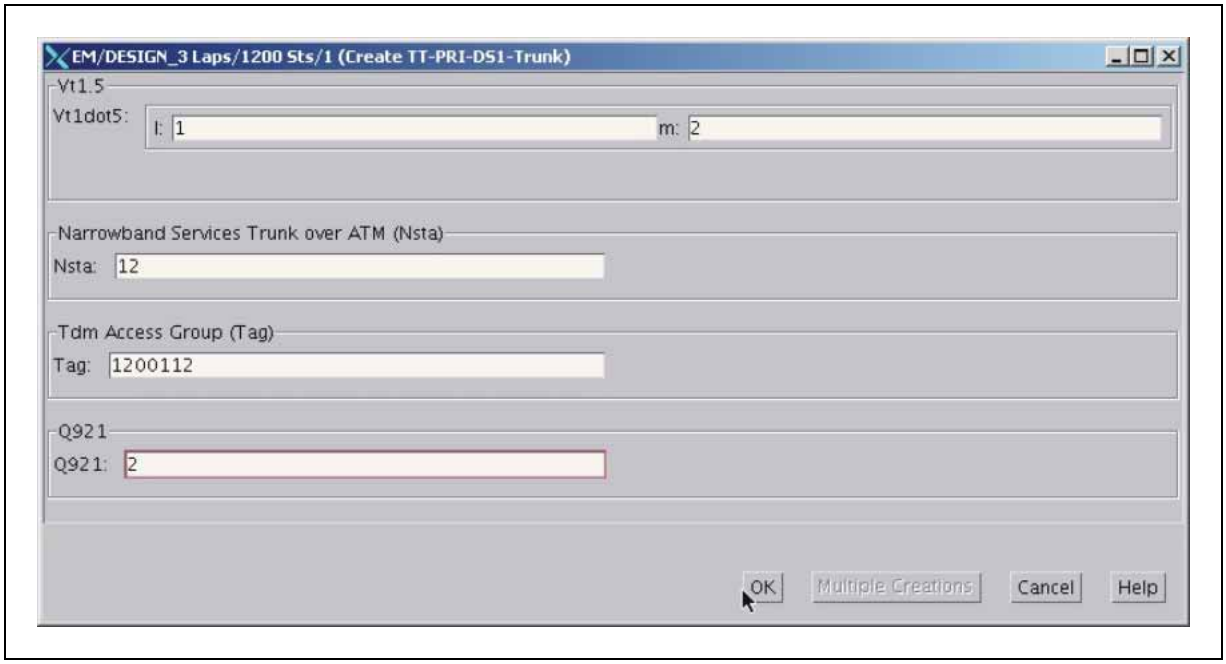
Provisioning PRI trunks is similar to provisioning ISUP trunks, with the following exception.

For the PRI trunk, there is one Q921 component for each trunk group. You must look under Nsta/For the PRI trunk, there is one Q921 component for each trunk group. You must look under Nsta/Vgs to verify the last Q921 instance number used. Set the field in the template to one more instance number.

See "PRI DS1 Template" (page 310) and "PRI E1 Template" (page 311).

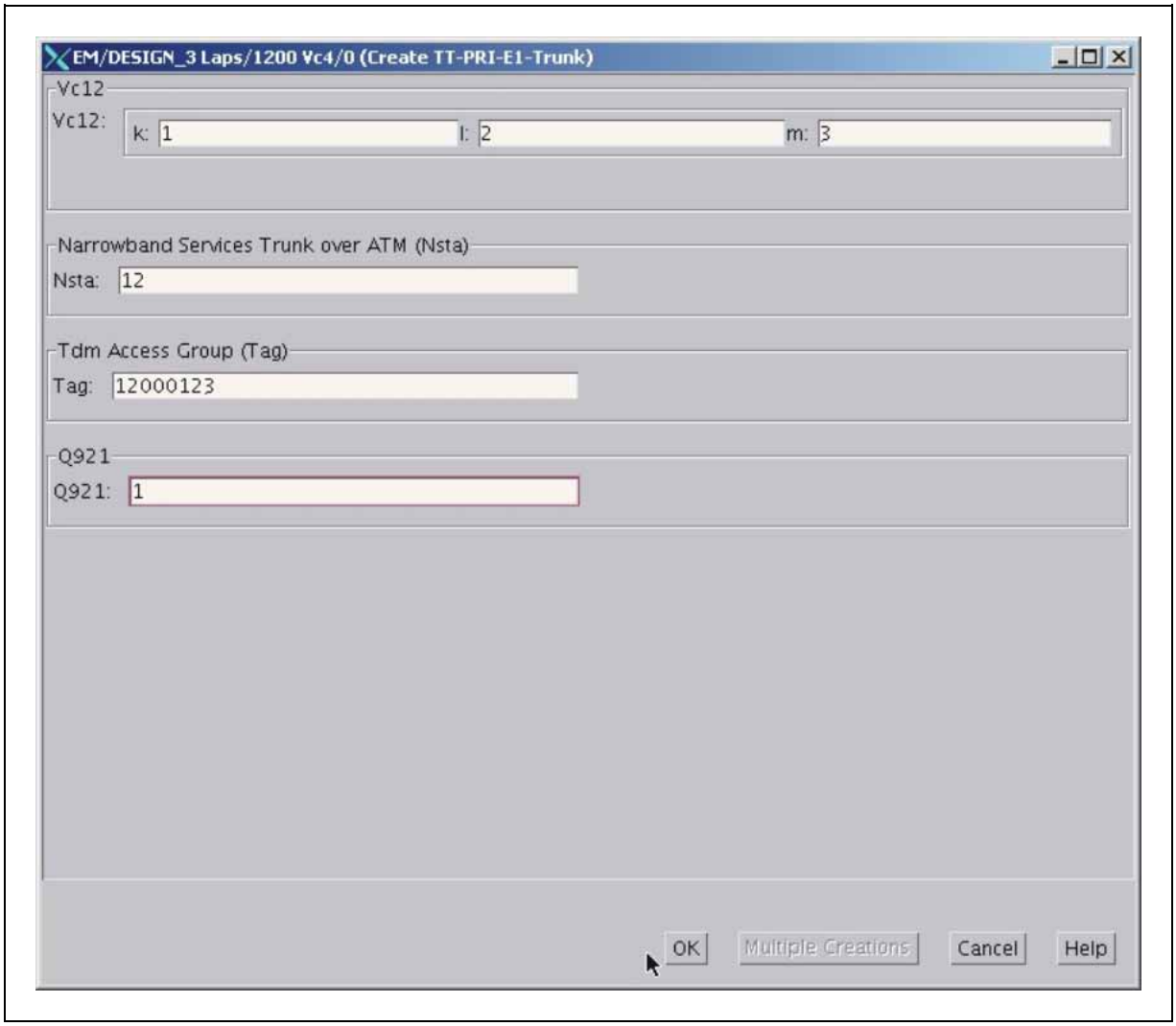
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

PRI DS1 Template



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

PRI E1 Template

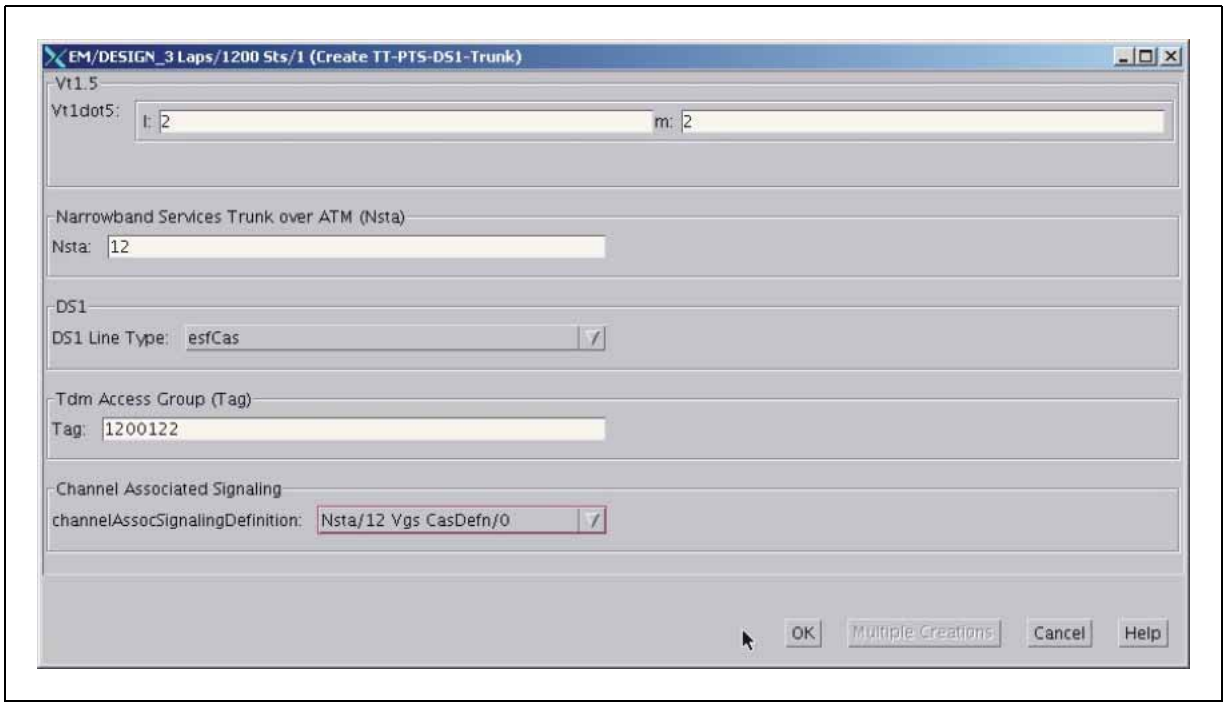


PTS Trunks

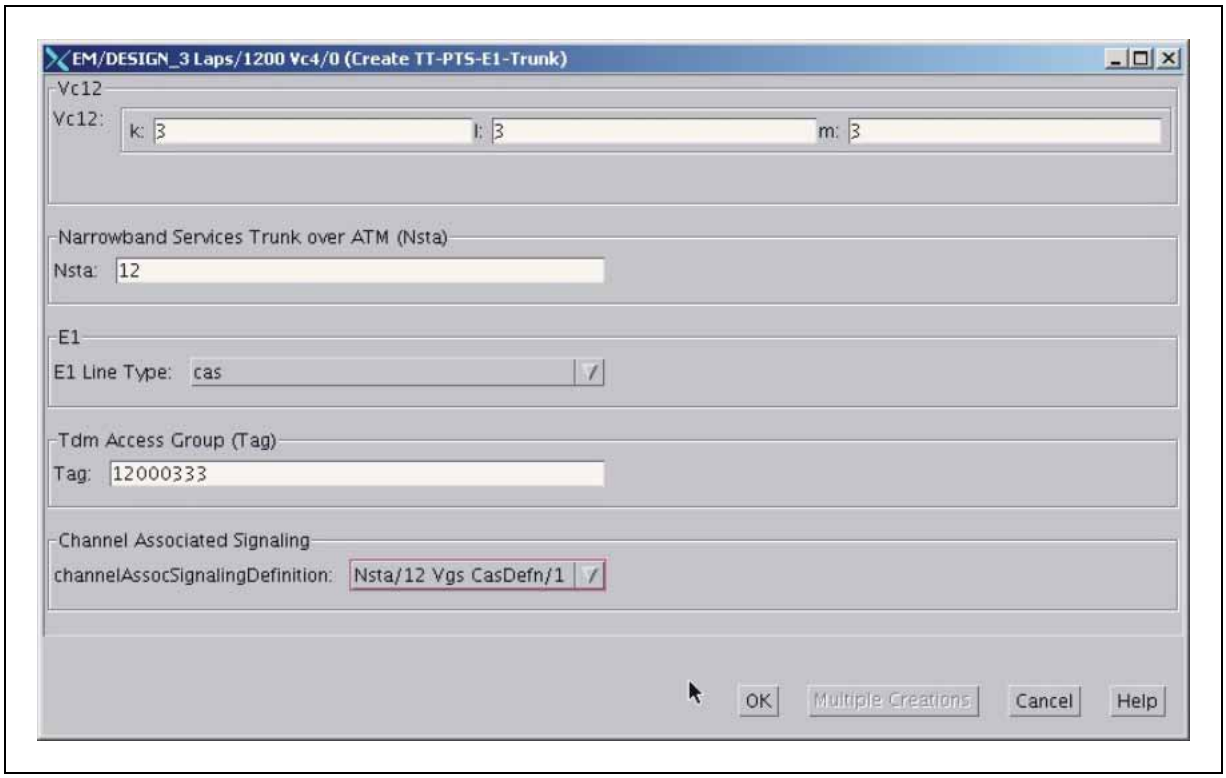
Provisioning PTS trunks is similar to provisioning ISUP trunks, with the exception that you need to provide the channel associated signalling (Cas) definition. This value is chosen from a list, and should be found under the same Nsta as the value listed on the template. See "PTS DS1 trunks" (page 312) and "PTS E1 trunks" (page 312).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

PTS DS1 trunks



PTS E1 trunks



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using the periodic routine exercise (REX) templates

To add REX to the MG15000, first ensure that rex_CXXXXX is loaded on the switch (check the software avl attribute). In order to use the REX component, ensure that lpt/cp fl includes the rex software. For example:

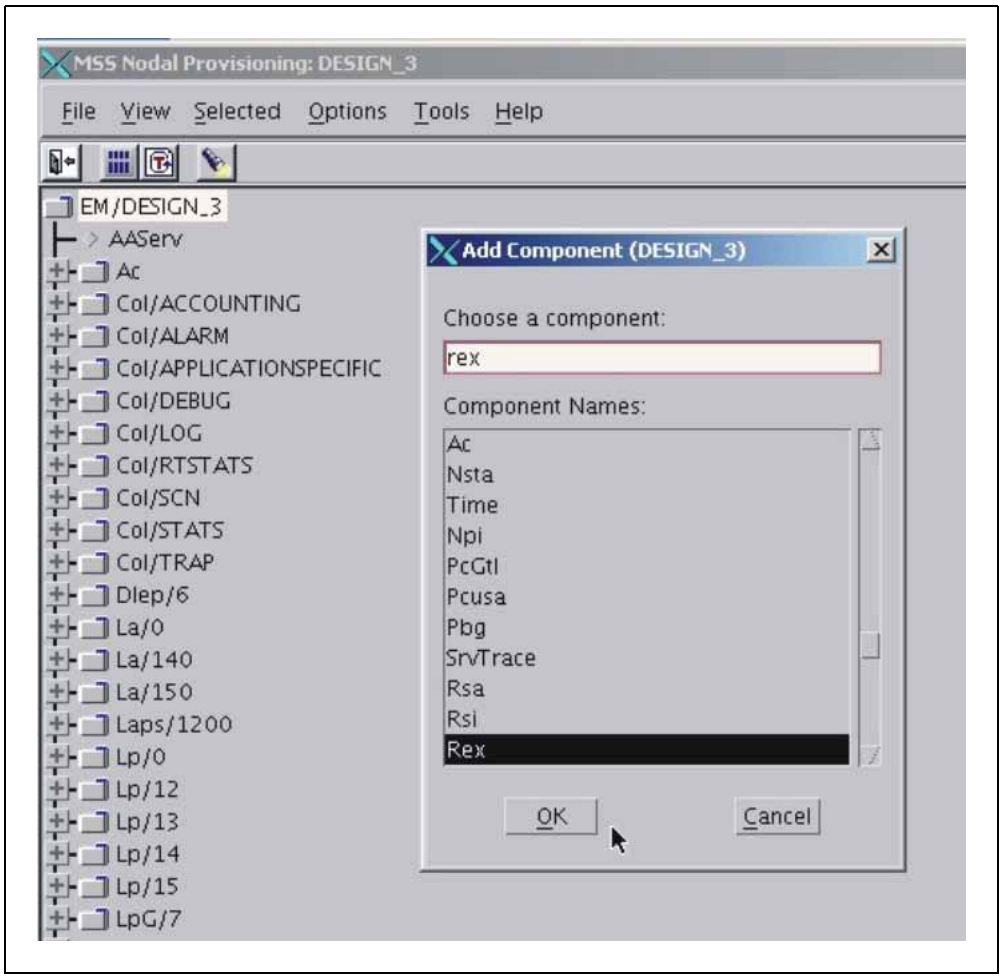
```
d sw lpt/cp fl

d sw avl
```

For more information on these software features, refer to the LP feature configuration for the respective solution.

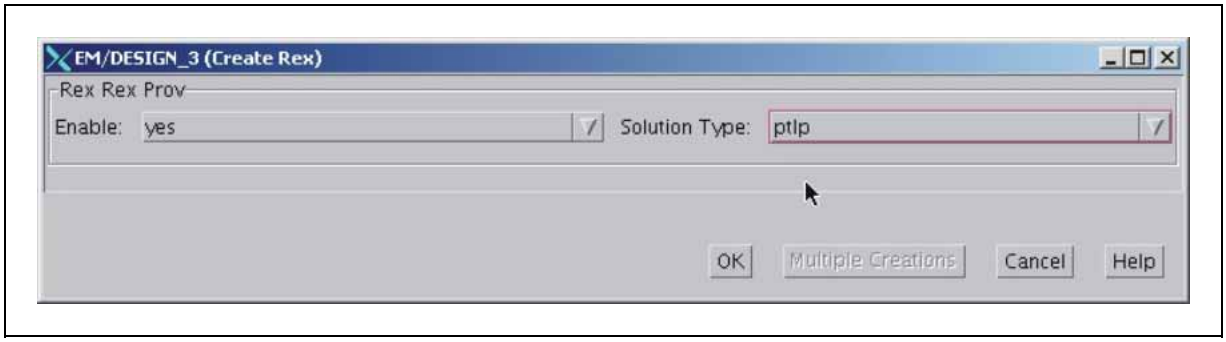
First, the top level “Rex” component must be added manually using the NP tool to enable the tests and set the solution type to PtIp. See "Adding REX template 1" (page 313) and "Adding REX template 2" (page 314).

Adding REX template 1



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding REX template 2

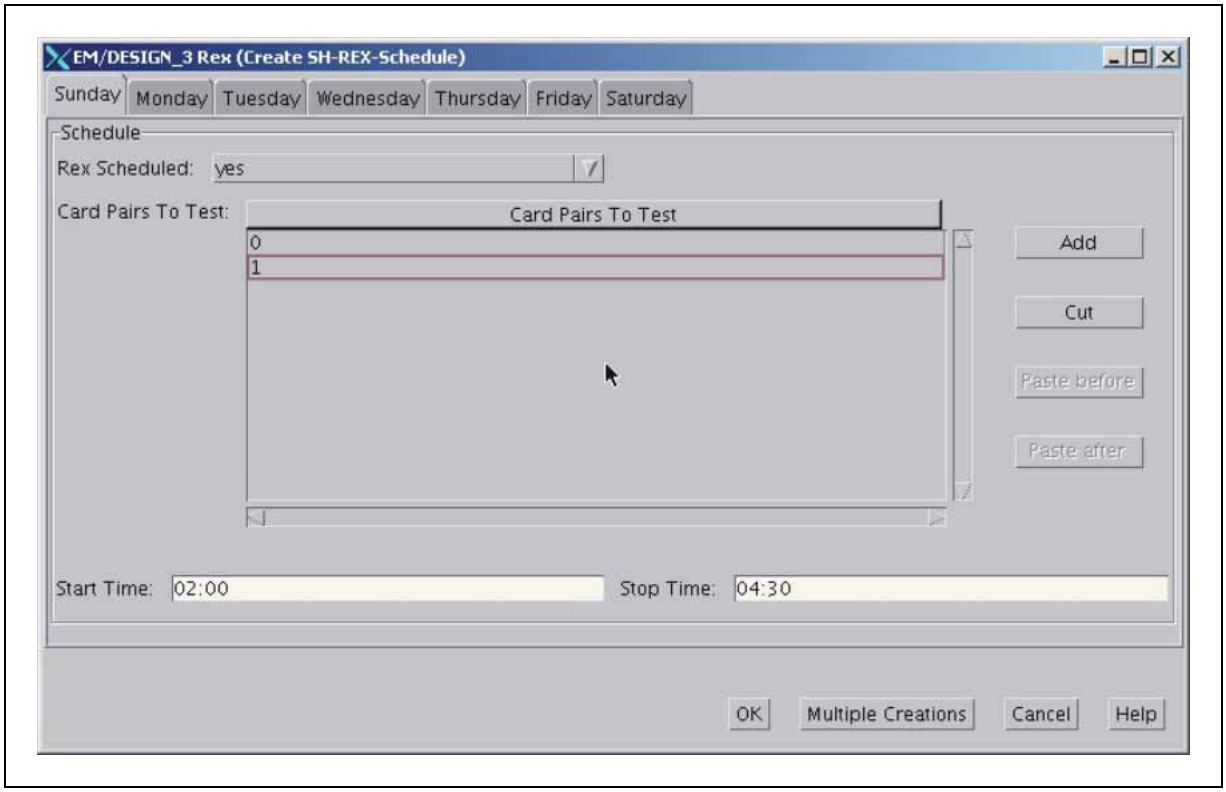


REX scheduler

Once the view has been saved and activated, the REX schedule can be set using the SH-REX-Schedule NP template, see "REX scheduler template" (page 314).

When setting the REX schedule using the SH-REX-Schedule NP template. select only the even-numbered cards or fabricCards listed under “Card Pairs to Test” in the schedule.

REX scheduler template



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Carrier VoIP

MSS15K, MG15K, and MDM Configuration Overview PT-AAL1/UA-AAL1/UA-IP/PT-AAL2

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10114-511
Document status: Standard
Document version: 09.01
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.