Carrier VoIP

MSS15K, MG15K, and MDM in Succession Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP

NN10198-912

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

Contents

New in this release 7

Carrier Voice over IP troubleshooting overview 9
General troubleshooting strategy 9
Carrier Voice over IP network overview 9
Troubleshooting strategy 11
When to call Nortel for help 14
Information to collect about a problem 14

Multiservice Switch 15000 / Media Gateway 15000 common hardware problems 19
Hardware failures 19
Shelf failures 19
Control processor failures 21
Function processor failures 23
Link failures 26
Sparing panel failures 35
Hardware-related service degradations 37
Service degradations due to fabric card problems 37
Service degradations due to line automatic protection switching problems 40
Service degradations due to control processor problems 42
Service degradations due to function processor problems 43

Multiservice Switch 15000 / Media Gateway 15000 common software problems 47
Base software failures 47
File system failures 47
Data collection failures 50
FTP session failures 55
User ID and password failures 58
User ID and password failures in VoIP networks with IEMS providing central user authentication and authorization 60
Base software service degradations 61
Service degradations due to network synchronization problems 61
Service degradations due to network time server problems 63

Software upgrade problems 66

Multiservice Switch 15000 / Media Gateway 15000 management problems 67

Overview of management information flow in a Carrier Voice over IP solution network 68

PT-AAL1 / UA-AAL1 troubleshooting 89

PT-AAL1 / UA-AAL1 call processing problems 89

Call processing failures due to ATM framework problems 89

PT-AAL1 / UA-AAL1 call quality problems 91

Call quality problems due to ATM framework problems 91

ATM service problems 93

ATM backbone failures due to ATM routing problems 93

Service degradations due to ATM routing problems 98

UA-IP/PT-IP troubleshooting 105

UA-IP/PT-IP call processing problems 105

H.248 packet forwarding problems 105

Media Gateway 15000 call processing problems 108

UA-IP/PT-IP call quality problems 110

Bearer packet forwarding problems 110

Media Gateway 15000 call quality problems 113

IP service problems 114

IP addressing problems 114

IP security attack 116

OSPF problems 117

Corrective action procedures 121

Common corrective action procedures 121

Correcting data collection problems 122

Correcting file system problems 124

Correcting provisioning view problems 124

Correcting line automatic protection switching problems 126

Correcting network clock synchronization problems 129

Correcting fabric firmware problems 131

Collecting crash data 131

Correcting problems with the Multiservice Switch software and patches 136

Correcting problems with Multiservice Data Manager servers 137

Verifying the status of the link layer 142

Testing Vt1dot5 links 172

PT-AAL1/UA-AAL1 corrective action procedures 174

Correcting call processing problems 174

UA-IP/PT-IP corrective action procedures 183

Verifying the forwarding path between two IP addresses 184

Checking for node-level IP packet discards 185

Isolating IP packet discards to an interface 186
Checking for layer 2 interface-level packet discards 189
Checking for node-level ICMP packet generation/reception 195
Verifying the configured IP address 196
Verifying the ARP table 198
Verifying the forwarding and routing tables 198
Verifying the statistics for locally destined/generated packets 200
Locking out packet traffic 203
Verifying the statistics for the MSS/MG15000 RADIUS server 204
Viewing IPSec general statistics on the MSS/MG15000 206
Verifying IPSec statistics for a specific connection on the MSS/MG15000 206
Viewing IPSec and SSH error logs on the MDM workstation 207

Appendix A Cause code reference for PT-AAL1 / UA-AAL1 call processing 209

Appendix B Connecting to Multiservice Data Manager tools 215

Appendix C Using the PVG DS0 visibility tool 217

Appendix D Using safe shell debug commands 219

Appendix E SVC Failure Alarms 225

New in this release

There have been no updates to the document in this release.

Carrier Voice over IP troubleshooting overview

This troubleshooting guide identifies typical problems that may occur on Nortel Multiservice Switch 15000 nodes, Nortel Media Gateway 15000 nodes, and Nortel Multiservice Data Manager servers within PT-AAL1, UA-AAL1, UA-IP, and PT-IP solutions. A set of tasks and related procedures have been identified to help resolve each of these problems.

This chapter discusses the following topics:

- "General troubleshooting strategy" (page 9)
- "When to call Nortel for help" (page 14)

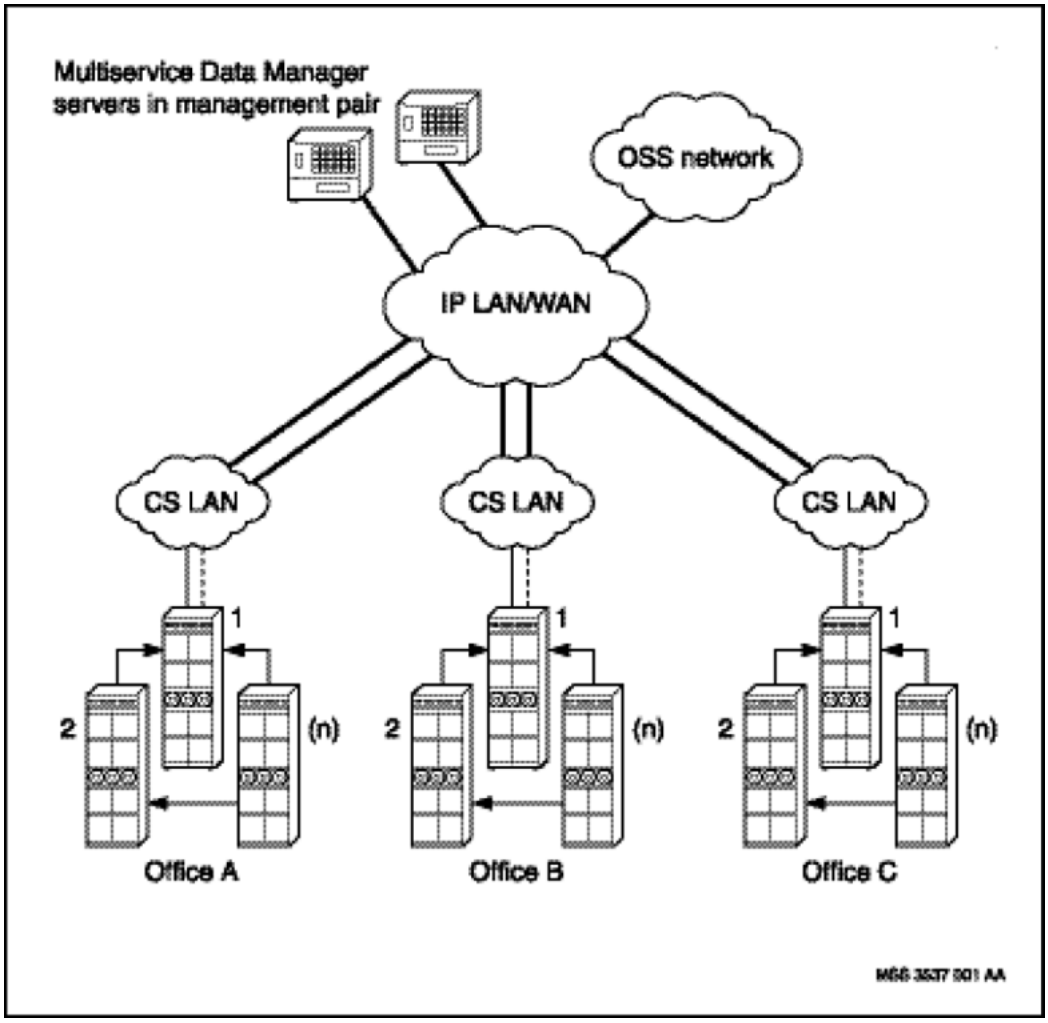
General troubleshooting strategy

In order to troubleshoot problems in a PT-AAL1 / UA-AAL1/ UA-IP/PT-IP solutions network, it is important to understand where the Nortel Multiservice Switch / Media Gateway nodes and Multiservice Data Manager servers are located in the overall network structure, and to have a strategy to detect and isolate faults in preparation for correcting them.

Carrier Voice over IP network overview

"PT-AAL1 / UA-AAL1 / UA-IP / PT-IP network structure" (page 10) shows a high-level view of a PT-AAL1 / UA-AAL1 / UA-IP/ PT-IP network. In this figure, Nortel Multiservice Data Manager servers are deployed in a centralized network management configuration.

PT-AAL1 / UA-AAL1 / UA-IP / PT-IP network structure



The Nortel Multiservice Switch nodes in each office are dedicated to a single solution, either PT-AAL1, or UA-AAL1, or UA-IP/PT-IP.

The number of Multiservice Data Manager server pairs needed in the network is dependent on several factors:

- performance engineering requirements
- OSS interfaces
- deployed network solutions

Note: The figure "PT-AAL1 / UA-AAL1 / UA-IP / PT-IP network structure" (page 10) just happens to show a single pair deployed for the network.

In PT-AAL1 and UA-AAL1 solutions, the key capability of the Nortel Multiservice Switch 15000 node is ATM signalling and routing.

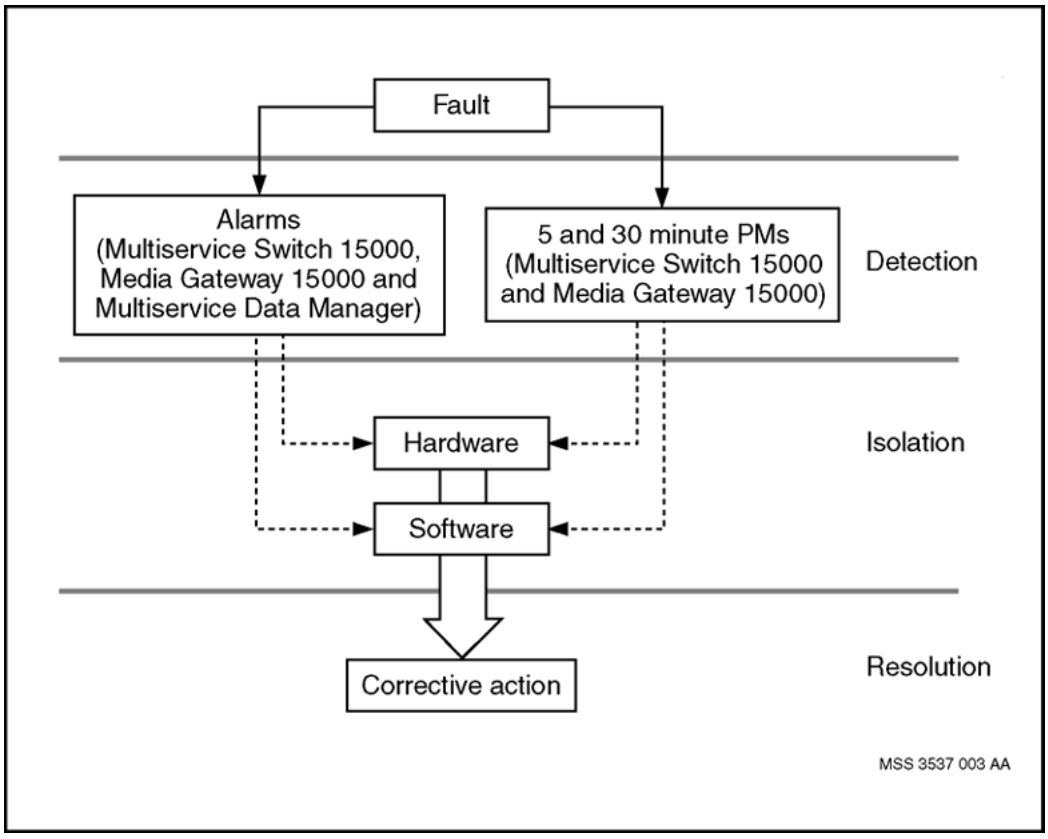
In a UA-IP/PT-IP solution, the node uses Multiservice Switch and Media Gateway capabilities. The Multiservice Switch provides IP routing functionality over both Ethernet and ATM while the Media Gateway provides standard trunk gateway functionality.

For all solutions, IP is used for network management of Multiservice Switch 15000 / Media Gateway 15000 nodes.

Troubleshooting strategy

Before a network fault can be corrected, first it must be detected and then isolated to a specific Nortel Multiservice Switch node or Multiservice Data Manager component or interface within the network. Refer to the figure "Troubleshooting approach" (page 11).

Troubleshooting approach



Types of faults

A fault can be characterized in the following ways:

- hard faults include line or facility failures, circuit pack hardware failures, software resets, etc.
- soft faults include software processing failures or service degradations such as packet loss, overload conditions, misconfigured addressing, etc.

Fault detection

Once a fault occurs, the first step is to detect a potential service-impacting problem as soon as possible. For Multiservice Data Manager server faults, the key detection mechanism is the alarms. For Multiservice Switch 15000/ Media Gateway 15000 nodes, there are two key detection mechanisms: alarms, and 5 and 30 minute performance measurements (PMs). These mechanisms should typically be monitored automatically for detecting fault conditions.

Misconfiguration faults on Multiservice Switch 15000 and Media Gateway 15000 nodes can be detected using the Nodal Provisioning (NP) Template Audit capability. The security audit logs track information about who applied the template, when it was applied, which NP template has been applied, and the applied attribute values. Unauthorized login and configuration changes can be tracked down. Then the NP Template Audit allows the user to compare the configuration on the nodes with the latest NP template. The user can reapply the template with the correct values and set the node to the initially commissioned conditions.

Fault isolation

Once a fault has been detected, the next major step is to isolate the fault to a level where corrective actions can be applied. Referring to the figure "PT-AAL1 / UA-AAL1 / UA-IP / PT-IP network structure" (page 10), a sample fault isolation for a Multiservice Switch 15000 / Media Gateway 15000 node might be as follows:

- office C
- Multiservice Switch (2)
- circuit pack located in slot 6
- specific physical interface on this circuit pack

If the node fault is a hard fault, alarms are the best mechanism to quickly isolate the fault. The alarms give indicators as to whether the problem is with hardware or software.

If the node fault is a soft fault, alarms are still the best starting point for fault isolation. However, since node performance measurements provide key statistics every 5 minutes on a physical interface basis, the

processing of this data for abnormal values can also help to isolate difficult problems such as intermittent failures. For information on performance measurements, and how to use them to assist with fault isolation, refer to *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*.

If the fault is with a Multiservice Data Manager server, alarms and the System Log are the key mechanisms for isolating the fault to hardware or software.

It is often necessary to compile statistical data that shows the operational traffic flow patterns across all the various media connections of the node. These "normal" operational patterns are the basis for identifying abnormalities when they occur. Troubleshooting a difficult problem often requires evaluating various statistical parameters over time, looking at the rates of change of the parameters, and comparing these to the normal operation of the node.

For example, in a UA-IP/PT-IP network, a Multiservice Switch / Media Gateway node that has been engineered to be congestion free during busy hour should not have packet discards. Traffic flow should be a time-varying percentage of the maximum throughput of the various media connections. A sudden increase or decrease in the rates of packet transmission or an increase in the number of packets that are being discarded on a connection is information that can help focus the fault isolation to a particular area of the node.

Fault correction

After the fault is isolated, the last step is to recover from any service outage, service degradation, or service loss of protection condition by taking the appropriate corrective action.

Recovery from configuration errors can be accomplished through the Nodal Provisioning Template Audit capability which allows Nodal Provisioning to verify if the on-switch provisioned data matches the data produced by a selected template and user inputs. 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 *241-6001-610 Nortel Multiservice Data Manager Nodal Provisioning User Guide*.

When to call Nortel for help

There may be times when you will be unable to use this document to troubleshoot and resolve problems on your equipment. If this happens, contact Nortel Global Networks Technical Support (GNTS) at the following number and provide them with as much information as you can about the problem:

1 - 800 - 4Nortel

When prompted for the Express Routing Code:

- for Multiservice Switch 15000 problems, enter ERC - 555
- for Multiservice Data Manager problems, enter ERC - 186
- for Media Gateway 15000 specific problems, enter ERC - 563

Information to collect about a problem

Use the following tables to ensure that you have collected as much data as possible about your problem. Using this information, GNTS will be able to more quickly help you correct the problems you are experiencing.

Multiservice Switch problem-related information required by GNTS

Collect the following information:	Notes
Alarms	Collect alarms that were raised in the hour preceding the problem for the affected node. To collect information on current active alarms, use the Multiservice Data Manager Alarm Display tool. For more information on using the Alarm Display tool, refer to "Alarm Display" in *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*. To collect information on all alarms that have occurred in the interval of interest, use the Multiservice Data Manager Query Historical Alarms tool. For more information on using the Query Historical Alarms tool, refer to "Query Historical Alarms" in *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*. If you suspect that there has been a loss of connectivity between the MSS/MG 15000 nodes and the Multiservice Data Manager servers, then use the Multiservice Data Manager Data Viewer tool to view alarms in the MDP spooled data. For more information on using the Data Viewer tool,

Collect the following information:		Notes
		refer to "Data Viewer basic procedures" in *241-6001-031 Nortel Multiservice Data Manager Performance Management Tools*.
	State change notifications (SCNs)	Collect SCN entries that occurred in the hour preceding the problem for the affected node. To view current state change notifications, use the Alarm Display tool to view active 0999 0012 proxy alarms on the Multiservice Data Manager active alarm display. Note that the 0999 0012 proxy alarm is used to present MSS/MG 15000 SCNs on the Multiservice Data Manager server. For more information on using the Alarm Display tool, refer to "Alarm Display" in *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*. To collect information on all SCNs that have occurred in the interval of interest, use the Multiservice Data Manager Query Historical Alarms tool to view 0999 0012 proxy alarms. For more information on using the Query Historical Alarms tool, refer to "Query Historical Alarms" in *241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*. If you suspect that there has been a loss of connectivity between the MSS/MG 15000 nodes and the Multiservice Data Manager servers, then use the Multiservice Data Manager Data Viewer tool to view SCNs in the MDP spooled data. For more information on using the Data Viewer tool, refer to "Data Viewer basic procedures" in *241-6001-031 Nortel Multiservice Data Manager Performance Management Tools*.
	Security logs	Collect security log information on the most recent provisioning or service changes made on the node. Using the Log Browser tool, note any operator activities that occurred on the node just before the problem or while the problem was occurring.

Collect the following information:		Notes
		For more information on using the Log Browser tool to review security log information, refer to "Viewing security logs" in *NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals*.
	Service degradation and service interruption records	Collect information on any degradations or service disruptions that you observed on the card either before or after the problem.
	Problem frequency records	If this is not the first time the problem has occurred, collect information about previous problems, including frequency and the time of day at which they occurred.
	List of cards with recoverable errors	
	Detailed information for all recoverable errors	
	List of installed software List of installed patches List of active software List of active disruptive patches List of active non-disruptive patches	Capture shelf-specific data, such as current software and patch level, the time since the last outage, the current committed file, a list of function processors that are currently inserted, and the control processor disk status. Using the Multiservice Data Manager Command Console, enter the following commands: **`display -current sw avl`** **`display -current -oper provisioning`** **`display -current -oper fs`** **`display -current sw patch`**
	Operational data for each function processor	Capture card-specific data, such as CPU utilization, memory usage, and software features. Using the Multiservice Data Manager Command Console, enter the following commands: **`display -notab -prov lp/*`** **`display -prov sw lpt/*`** **`display -notab -oper lp/*`** **`display -notab -oper shelf card/*`**

Collect the following information:		Notes
		Capture DS0 specific data, such as signaling and/or bearer path data. Using the Component Administration System or rlogin CLI, enter the following commands: `start Nsta/x Vgs SigTrace` `stop Nsta/x Vgs SigTrace` `start Nsta/x Vgs MediaTrace` `stop Nsta/x Vgs MediaTrace`
For crash data collection, collect the following:		
	Collect all the information described in this table, and the crash data	
	Complete list of cards and detailed crash data for each card listed	Capture data logged on the node during the crash. Using the Multiservice Data Manager Command Console, enter the following commands: `display -notab shelf card/* diagnostics recoverableerror line/*` `display -notab shelf card/* diagnostics trapdata line/*`

Multiservice Data Manager problem-related information required by GNTS

Collect the following information:		Notes
	Collect information on Multiservice Data Manager system activity that occurred in the hour preceding the problem.	Using the Log Browser tool, scan Multiservice Data Manager logs, and note any operator activities that occurred on the Multiservice Data Manager server just before the problem or while the problem was occurring. Using the Server Admin tool and the System Log Display tool, collect information on: • which servers are running • alarms or other log information about server activity during the interval of interest For more information on using the Log Browser tool, refer to "Viewing security logs" in *NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals*.

Collect the following information:		Notes
		For more information on using the Server Admin and System Log Display tools, refer to *241-6001-303 Nortel Multiservice Data Manager Administration*.
	List of installed software	Capture information about the current software level of Multiservice Data Manager server. Using the Multiservice Data Manager Command Console, enter the following commands: **`/opt/MagellanNMS/system/inst/nmsLinks`** **`/opt/MagellanMDP/system/init/mdpLinks`**
	List of installed patches	Using a Unix window, enter the following commands to capture information about the current patch level of the Multiservice Data Manager workstation. **`showrev -p | grep MDM`** **`showrev -p | grep MDP`**

Multiservice Switch 15000 / Media Gateway 15000 common hardware problems

For more information on Multiservice Switch 15000 and Media Gateway 15000 common hardware problems, refer to:

- "Hardware failures" (page 19)
- "Hardware-related service degradations" (page 37)

Hardware failures

Refer to one of the following sections for more information about how to correct Nortel Multiservice Switch 15000 / Media Gateway 15000 hardware failures:

- "Shelf failures" (page 19)
- "Control processor failures" (page 21)
- "Function processor failures" (page 23)
- "Link failures" (page 26)
- "Sparing panel failures" (page 35)

Shelf failures

Nortel Multiservice Switch 15000 / Media Gateway 15000 shelf failures may be caused by one of the following:

- a loss of power to the node
- a power supply failure
- a cooling unit failure
- a corrupt MAC address card
- a failure on the Alarm/BITS card
- control processor failures

Problem indicators

- hardware not accessible or not responding
- 7012 00xx shelf-specific alarms are displaying on the OSS and on Multiservice Data Manager servers
- LED indicator on the faceplate changes from green to red

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct shelf failures. The task table references procedures contained in this document or located in other Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Multiservice Switch 15000 shelf failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	On the node, verify that the cabinet has power.	"Troubleshooting the node"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
5.	If the alarms indicate a power supply failure, check the power LED status indicators on the node.	"Power LED status indicators for the BIP alarm module" "Power LED status indicators for each PIM"	*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description*

Task		Use the section...	in...
		"Power-and-ground hardware for a Multiservice Switch"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
6.	Check for and correct any cooling unit problems.	"Status LEDs of a cooling unit fan"	*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description*
		"Cooling unit replacement" "Fan controller replacement" "Replacing a cooling unit alarm cable" "Replacing a cooling unit power cable" "Replacing an air filter" "Temperature sensor replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
7.	If the alarms indicate a MAC address problem, contact Nortel GNTS to confirm that the MAC address module is faulty. If it is faulty, then replace it.	"MAC address module replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
8.	If the alarms indicate a problem with the alarm/BITS card, contact Nortel GNTS to confirm that the alarm/BITS card is faulty. If it is faulty, then replace it.	"Alarm/BITS module replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
9.	If the alarms indicate a problem with the control processor, follow the task table steps for control processor failures.	"Control processor failures" (page 21)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Control processor failures

Control processor (CP) failures may be caused by one of the following:

- a CP or a standby CP did not load its software

- a CP that has crashed
- faulty hardware

Problem indicators

- one of the CPs did not load
- hardware not accessible or not responding
- 7012 01xx control processor alarms against a control processor (`shelf card/0 or shelf card/1`) are displaying on the OSS and on Multiservice Data Manager servers
- LED indicator on the faceplate changes from green to red

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct control processor failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Control processor failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	Determine if the CP is having problems loading its software.	"Determining why a control processor does not load"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
5.	Determine if the standby CP is having problems loading its software. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Determining why the standby control processor does not load"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Collect diagnostic information for root cause analysis and to determine if the CP needs to be replaced.	"Determining the cause of a control processor crash"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
		"Isolating the problem that causes a crash" (page 132)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
7.	If required, replace the CP.	"Prerequisites to failed CP replacement" "Installing a CP" "CP upgrade" "Failed CP replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
		"Probable causes and corrective measures for troubleshooting control processor problems"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*

Function processor failures

Function processor (FP) failures may be caused by one of the following:

- an FP or standby FP did not load its software
- an FP that has crashed
- faulty hardware

Problem indicators

- one of the FPs did not load
- hardware not accessible or not responding
- 7012 01xx alarms against a function processor (`shelf card/2 up to shelf card/15`) are displaying on the OSS and on Multiservice Data Manager servers
- 7012 0200 alarm against a function processor (`shelf card/2 up to shelf card/15`) is displaying on the OSS and on Multiservice Data Manager servers
- 7056 00xx VSP alarms are displaying on the OSS and on Multiservice Data Manager servers
- LED indicator on the faceplate changes from green to red

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct function processor failures. The task table references procedures contained in this document or located in other Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Function processor failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	Isolate any problems on the FPs.	"Detecting function processor problems" "Card testing"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
5.	Determine if the main FP or the standby FP are having problems loading their software.	"Determining why a function processor does not load software"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Collect diagnostic information for root cause analysis and determine if the FP needs to be replaced.	"Determining the cause of an FP crash" "Collecting diagnostic information" "Isolating the problem that causes a crash" (page 132)	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
7.	If required, replace the FP. ***Note:*** Contact Nortel GNTS before replacing an FP.	"Determining the active function processor and the active lines" (page 127) "Switching between the active lines and the lines providing equipment protection" (page 128) "FP upgrade" "Replacement of a failed FP" "Replacement of an FP with one of a different card type"	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP* *NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
8.	Thermal failures.	"Operational environment" "Power dissipation" "Bulk heat dissipation"	*NN10600-125 Nortel Multiservice Switch 15000/20000 Planning Site Requirements*

Link failures

Link failures may be caused by one of the following:

- a problem with the physical layer
- a problem with a port
- a problem with electrical cables or optical fibers
- faulty hardware

Problem indicators

- 7011 520x, 7011 521x, and 7011 5501 SONET alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7011 5000, 7011 5001, 7011 5002, 7011 5010, and 7011 5293 Vt1dot5 alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7011 51xx, 7011 56xx DS3 alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7011 1100, 7011 12xx IMA alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7011 54xx Gigabit Ethernet alarms are displaying on the OSS and on the Multiservice Data Manager servers
- 7026 3002, 7026 3003, 7026 3006 OAM Ethernet alarms are displaying on the OSS and on Multiservice Data Manager servers

Corrective actions for SONET link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct SONET link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

SONET link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Monitor the status of the SONET link for section, line and path errors.	"Verifying the status of the SONET link layer" (page 142)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
5.	Verify the operation of the physical layer. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"OC-3/STM-1 FP tests for Multiservice Switch 15000 and Multiservice Switch 20000 devices" "OC-12/STM-4 FP tests for Multiservice Switch 15000 and Multiservice Switch 20000 devices" "Testing a port" "Testing an optical port configured with LAPS"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Check the integrity of the optical fiber, and clean or replace as necessary.	"Cleaning LC or SC connectors" "Cleaning MT-RJ connectors" "Replacing a fiber cable in a fiber management unit"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
7.	If required, replace the FP experiencing problems. ***Note:*** Consult Nortel GNTS before replacing an FP card.	"Function processor failures" (page 23)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Corrective actions for Vt1dot5 link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct Vt1dot5 link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Vt1dot5 link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Monitor the status of the Vt1dot5 link for errors.	"Verifying the status of the Vt1dot5 link layer" (page 150)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
5.	Verify the operation of the physical layer and resolve physical problems specific to Vt1dot5 connectivity. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"Testing Vt1dot5 links" (page 172)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
		"Testing a tributary port"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Verify operation of the SONET link and correct problems as required.	"SONET link failures" (page 26), steps 3, 4, 5, and 6.	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Corrective actions for DS3 link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct DS3 link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

DS3 link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	Monitor the status of the DS3 link for line and path errors.	"Verifying the status of the DS3 link layer" (page 153)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
5.	Verify the operation of the physical layer. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"DS3 FP tests for Multiservice Switch 15000 and Multiservice Switch 20000 devices" "12-port DS3 ATM FP tests additional considerations" "Testing a port"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Resolve any physical layer problems with FP cables or sparing panels.	"FP cable replacement" "Sparing panel failures" (page 35)	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade* *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
7.	If required, replace the FP experiencing problems. ***Note:*** Consult Nortel GNTS before replacing an FP card.	"Function processor failures" (page 23)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Corrective actions for IMA link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct IMA link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IMA link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Monitor the status of the IMA link for line and path errors.	"Verifying the status of the IMA link layer" (page 158)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
5.	Resolve IMA specific problems.	"Troubleshooting IMA" "IMA-specific alarms" "IMA link alarms" "The troubleshooting process"	*NN10600-730 Nortel Multiservice Switch 7400/15000/20000 Operations: Inverse Multiplexing for ATM*

Task		Use the section...	in...
6.	Verify the operation of the physical layer. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"DS3 FP tests for Multiservice Switch 15000 and Multiservice Switch 20000 devices" "4-port DS3 channelized ATM FP tests additional considerations" "Testing a channel" "Testing a port"	*NN10600-520 Nortel Multiservice Switch 740 0/15000/20000 Fault and Performance Management: Troubleshooting*
7.	Resolve any physical layer problems with FP cables or sparing panels.	"FP cable replacement" "Sparing panel failures" (page 35)	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade* *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
8.	If required, replace the FP experiencing problems. ***Note:*** Consult Nortel GNTS before replacing an FP card.	"Function processor failures" (page 23)	*NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Corrective actions for Gigabit Ethernet link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct Gigabit Ethernet link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Gigabit Ethernet link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Monitor the status of the Gigabit Ethernet line for errors.	"Verifying the status of the Gigabit Ethernet link layer" (page 165) "Verifying the status of the Link Aggregation (LAG) layer" (page 168)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
5.	Verify the operation of the physical layer. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"4-port Gigabit Ethernet FP tests additional considerations" "Testing a port"	*NN10600-520 Nortel Multiservice Switch 740 0/15000/20000 Fault and Performance Management: Troubleshooting*

Task		Use the section...	in...
6.	Check the integrity of the optical fiber, and clean or replace as required.	"Cleaning an SFP optical module" "SFP module replacement" "Replacing a fiber cable in a fiber management unit"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
7.	If required, replace the FP experiencing problems. ***Note:*** Consult Nortel GNTS before replacing an FP card.	"Function processor failures" (page 23)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Corrective actions for OAM Ethernet link failures

This task table shows you the sequence of tasks you need to perform to isolate and correct OAM Ethernet link failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

OAM Ethernet link failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	Monitor the status of the OAM Ethernet line for errors.	"Verifying the status of the OAM Ethernet link layer" (page 171)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
5.	Verify the operation of the physical layer. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"Testing the OAM Ethernet port"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Correct physical layer problems as required, such as replacing the OAM Ethernet cable.	"Connecting a CP Ethernet cable"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
7.	If required, replace the CP.	"Control processor failures" (page 21)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Sparing panel failures

Sparing panel failures may be caused by one of the following:

- cable connectivity failure
- faulty hardware (sparing panel or FP)

Problem indicators

- 7054 xxxx alarms are displaying on the OSS and on Multiservice Data Manager servers

Corrective actions

This task table shows you the sequence of tasks you need to perform to isolate and correct sparing panel failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Sparing panel failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Verify the connectivity between the FP and the sparing panel.	"Checking the connectivity between FPs and sparing panels"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
5.	Verify the operation of the sparing panel and resolve problems as required.	"Verifying the operation of a sparing panel"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*

Task	Use the section...	in...
	"Sparing panel replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
6. If required, replace the FP experiencing problems. ***Note:*** Consult Nortel GNTS before replacing an FP card.	"Function processor failures" (page 23)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Hardware-related service degradations

Refer to one of the following sections for more information about how to correct service degradations caused by problems with Nortel Multiservice Switch 15000 / Media Gateway 15000 hardware:

- "Service degradations due to fabric card problems" (page 37)
- "Service degradations due to line automatic protection switching problems" (page 40)
- "Service degradations due to control processor problems" (page 42)
- "Service degradations due to function processor problems" (page 43)

Service degradations due to fabric card problems

Service degradations caused by problems with the fabric cards may be caused by one of the following:

- the fabric card is using the wrong version of firmware
- an increase in temperature has occurred on the shelf
- faulty hardware

Problem indicators

- 7002 000x alarms are displaying on the OSS
- disabled fabric alarms are displaying on Multiservice Data Manager servers
- LED indicator on the faceplate changes from green to another color
- the fabric LED is not solid green
- the hardware is not responding

- the hardware is not redundant

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct fabric card problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to fabric card problems

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Isolate the problem with the fabric card. ***Note:*** Contact Nortel GNTS before performing fabric card tests as some tests may cause service interruptions.	"Troubleshooting the fabric card" "Supporting information for troubleshooting the fabric card" "Manually testing a fabric card" "Interpreting fabric card test results"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
5.	Check for and correct any cooling unit problems.	"Status LEDs of a cooling unit fan"	*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description*

Task		Use the section...	in...
		"Cooling unit replacement" "Fan controller replacement" "Replacing a cooling unit alarm cable" "Replacing a cooling unit power cable" "Replacing an air filter" "Temperature sensor replacement"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
6.	Using the appropriate technical bulletin, identify the version of fabric firmware that should be running on the switch.	"Download release notes"	*NN10070-461 Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1* *NN10419-461 Upgrading Nortel Multiservice Switch 15000 and Media Gateway 15000/20000 in Carrier Voice over IP Networks*
7.	Verify that the node is running the correct version of fabric firmware.	"Identifying the firmware that is installed on the fabric card" (page 131)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
8.	If the fabric card is an older version of firmware, upgrade it.	"Fabric replacement may need a firmware upgrade"	*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description*
		"Upgrade the fabric"	*NN10070-461 Upgrading Nortel Multiservice Switch 15000 in Carrier Voice over IP Networks PT-AAL1/UA-AAL1*

Task		Use the section...	in...
9.	If the fabric card needs to be replaced, replace it.	"Fabric replacement can affect system cooling" "Fabric replacement may need a firmware upgrade" "Status LEDs of fabric cards in a Multiservice Switch 15000"	*NN10600-120 Nortel Multiservice Switch 15000/20000 Hardware Description*
		"Removing a fabric card from a Multiservice Switch 15000" "Installing a fabric card into a Multiservice Switch 15000"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*

Service degradations due to line automatic protection switching problems

Service degradations due to problems with line automatic protection switching (LAPS) may be caused by one of the following:

- problems with a link (refer to "Link failures" (page 26)
- problems with a function processor (FP)
- configuration errors between near end and far end equipment

Problem indicators

- 7011 525x, 7011 526x, 7011 5270...5276 alarms are displaying on the OSS and on Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct LAPS problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to line automatic protection switching problems

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
			Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Verify the appropriate LAPS mode is configured and that both ends to have the same configuration. ***Note:*** Perform this procedure on the near end/far end of an active/inactive link.	"Identifying line automatic protection switching mode mismatch problems" (page 129)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
		"Understanding line and equipment protection for Multiservice Switch 15000 and Multiservice Switch 20000 optical interfaces" "Configuring line and equipment protection for Multiservice Switch 15000 and Multiservice Switch 20000 optical interfaces"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
5.	Compare the configured FP values with the recommended values for your solution. ***Note:*** Perform this procedure on the near end/far end of an active/inactive link.	"Summary of FP configuration"	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
	If the configuration values do not match the recommended values, make configuration changes as necessary. ***Note:*** Consult Nortel GNTS before changing your configuration.		*Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2/PT-IP*
6.	Verify operation of the SONET link and correct problems as required.	"SONET link failures" (page 26), tasks 3, 4, 5, and 6.	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Service degradations due to control processor problems

Service degradations due to problems with the control processor (CP) may be caused by one of the following:

- BITS timing connections
- file system problems
- OAM Ethernet problems
- memory exhaustion, memory crashes
- message block exhaustion
- CPU utilization problems
- provisioning errors on the control processor

Problem indicators

- the spared services of the control processor are degraded or disabled
- 7017 xxxx BITS alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7008 xxxx file system alarms are displaying on the OSS and on Multiservice Data Manager servers
- 7026 3002, 7026 3003, 7026 3006 OAM Ethernet alarms are displaying on the OSS and on Multiservice Data Manager servers

- 0000 300x, 7012 03xx, 7013 00xx 7014 00xx alarms against CP (0) are displaying on the OSS and on Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct CP problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to control processor problems

Task		Use the section...	in...
1.	Check the status of the clock on the CPs by issuing the command display NetworkSynchronization.	"Correcting network clock synchronization problems" (page 129)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
2.	Check for unusual disk activity such as a failing disk.	"Troubleshooting file system problems"	*NN10600-520 Nortel Multiservice Switch 740 0/15000/20000 Fault and Performance Management: Troubleshooting*
3.	Check for Ethernet connections to see if there is any unusual activity.	"Testing the OAM Ethernet port"	*NN10600-520 Nortel Multiservice Switch 740 0/15000/20000 Fault and Performance Management: Troubleshooting*
4.	Check for memory usage or memory crash.	"Collecting problem-related information required" "Troubleshooting control processors" "Determining the cause of a control processor crash"	*NN10600-520 Nortel Multiservice Switch 740 0/15000/20000 Fault and Performance Management: Troubleshooting*

Service degradations due to function processor problems

Service degradations due to problems the function processor (FP) may be caused by one of the following:

- memory exhaustion, memory crashes
- message block exhaustion

- CPU utilization problems
- provisioning errors on the function processor
- hardware resource exhaustion (conflicts between the capacity of the card and the type or volume of traffic)

Problem indicators

- the spared services of the function processor are degraded or disabled
- the provisioning is inappropriate for the function processor
- 0000 300x, 7012 03xx, 7013 00xx, 7014 00xx alarms against a function processor (`shelf card/2 up to shelf card/15`) are displaying on the OSS and on Nortel Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct FP problems and sparing problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to function processor problems

Task		Use the section...	in...
1.	Check for memory usage or memory crash	"Collecting problem-related information required" "Troubleshooting function processor problems" "Determining the cause of a function processor crash"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
2.	Check the physical set up of the card to determine whether its hardware is properly connected and operating.	"Function Processors" "CP and FP cables and associated hardware"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
3.	Check that the provisioning of the card is appropriate for the type of function processor you are using.	"Summary of FP configuration" "Summary of link configuration"	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task	Use the section...	in...
		Configuration Attribute Summary PT-AAL1/UA-AAL 1/UA-IP/PT-AAL2/PT-IP
4. Determine whether the type or volume of traffic is appropriate for the type of card you are using.	"PT-AAL1 / UA-AAL1 troubleshooting" (page 89) "UA-IP/PT-IP troubleshootin g" (page 105)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/U A-AAL1/UA-IP/PT-IP*

Multiservice Switch 15000 / Media Gateway 15000 common software problems

For more information on Multiservice Switch 15000 and Media Gateway 15000 common software problems, refer to:

- "Base software failures" (page 47)
- "Base software service degradations" (page 61)
- "Software upgrade problems" (page 66)

Base software failures

Refer to one of the following sections for more information about how to correct Nortel Multiservice Switch 15000 / Media Gateway 15000 base software failures:

- "File system failures" (page 47)
- "Data collection failures" (page 50)
- "FTP session failures" (page 55)
- "User ID and password failures" (page 58)
- "User ID and password failures in VoIP networks with IEMS providing central user authentication and a" (page 60)

File system failures

File system failures may be caused by one of the following:

- a full disk
- configuration errors
- an inability to synchronize the disks
- a back up disk that has a different volume name
- a disk failure

Problem indicators

alarms indicating a disk problem are displaying on the OSS and on Multiservice Data Manager servers. For example,

- 7008 1001
- 7008 1002
- 7008 1005
- 7008 1019
- 7008 1020

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct problems with the file system. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

File system failures

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarms.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Check the status of the file system.	"Displaying information about the file system" "File system restrictions"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*

Task		Use the section...	in...
5.	Determine why the file system is not operational.	"Determining why the file system is not operational"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
6.	Check the disk on the node for a hardware failure.	"Testing a disk" "Interpreting disk test results"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
7.	Check the *adminState, operationalState, usageState,* and *freeSpaceAvailable* attributes under the *FileSystem* component on the control processor disk to determine if the disk is full. Tidy the disk if the disk is reaching capacity.	"Determining why a file cannot be saved"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
		"Disk full conditions"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
		"Correcting a control processor disk full problem" (page 124)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
8.	Verify that the disks are synchronized. If they are not, resynchronize them.	"Displaying information about the file system" "Synchronizing disks"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*

Task		Use the section...	in...
9.	Verify that the volume names are the same for both the active and the standby disks.	"Changing the volume name of a disk"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
10.	Verify that the size of the active and standby disks are the same. If they are not, consider making them the same size, or if you cannot, ensure that the active disk has the lesser capacity.	"Displaying information about the file system" "Different-sized disks" "Formatting a disk"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures* ***Note:*** Step 2 in "Formatting a disk" indicates how to format the size for backward compatibility.

Data collection failures

Data collection failures may be caused by one of the following:

- Nortel Multiservice Data Manager (MDM) server, Management Data Provider (MDP) or the Multiservice Switch / Media Gateway node setup is misconfigured or not in place
- there is no connectivity between the node and the server
- the time-of-day of the node and the server is not synchronized
- data spooling is not turned on
- the queue size threshold has been reached
- the maximum number of queued files has been reached
- a control processor switchover has occurred
- a control processor has experienced a failure

Problem indicators

- BDF files are missing on the Multiservice Data Manager server
- 7003 xxxx alarms indicating a data collection failure are displaying on the OSS and on Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct problems with the data collection system. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Data collection failures

Task		Use the section...	in...
1.	Check the configuration between the server, MDP and the node.	"Summary of Multiservice Data Manager server 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-AAL2/PT-IP*
2.	Check the physical connectivity between the server and the node.	"Information for connecting to Multiservice Data Manager through a Multiservice Switch-only network" "Multiservice Data Manager connectivity overview" "Multiservice Data Manager connectivity using StartUp"	*NN10600-271 Nortel Multiservice Switch 7400/15000/20000 Network Management Connectivity*
3.	Check the network time synchronization between the server and the node.	"Synchronizing manually with a network time server"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
4.	Ensure that FTP access privileges have been activated.	"Activating FTP access privileges"	*NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
5.	On the server, verify that raw data files are being spooled. If they are not being spooled, configure the MDP for the node and verify that data collection is turned on (step 4).	"Verifying that raw data from the node is spooling to the server" (page 123)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Configuring MDP for Multiservice Switch"	*241-6001-309 Nortel Multiservice Data Manager Management Data Provider*
6.	Connect to the network.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
7.	The following types of node data can be spooled: alarms, SCNs, command logs and debug. On the node, verify that data collection spooling is turned on. If it is not, turn it on.	"Verifying that spooling is activated" (page 122)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Turning collector spooling on or off for each data type"	*NN10600-561 Nortel Multiservice Switch 7400/15000/20000 Data Management*

Task		Use the section...	in...
8.	On the server, verify that the files are being converted to BDF format. If they are not, convert the raw data to BDF format.	"Verifying that BDF conversion is taking place" (page 123)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Converting node raw data to BDF"	*241-6001-309 Nortel Multiservice Data Manager Management Data Provider*
9.	On the node, verify that the *agentQueueSize* attribute is not set to zero. If the attribute is set to zero, change the configuration.	"Displaying the agentQueueSize configuration" (page 123)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Agent queue sizes"	*NN10600-561 Nortel Multiservice Switch 7400/15000/20000 Data Management*
10.	Verify that the file system on the control processor is not full.	"Determining why a file cannot be saved"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
		"Add up the disk space requirements" "Calculate the disk partition sizes"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* *241-6001-102 Nortel Multiservice Data Manager Deployment Planning*
11.	Verify that the disk partitions on the server are not full. Delete the files that are not required.	"Calculating the disk partition sizes"	*241-6001-102 Nortel Multiservice Data Manager Deployment Planning*

Task		Use the section...	in...
12.	On the server, verify that the File Prober application is operating properly.	"Controlling MDP processes"	*241-6001-309 Nortel Multiservice Data Manager Management Data Provider*
		"MDP File Prober Manager (MDPFPMGR)" "Error Messages"	*241-6001-310 Nortel Multiservice Data Manager Server Reference*
13.	On the server, confirm that the File Prober has been scheduled to collect data.	"Setting data collection options"	*241-6001-309 Nortel Multiservice Data Manager Management Data Provider*
14.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
15.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarms.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
16.	Check the alarms to see if a control processor switchover occurred or if there was a control processor failure. If this happened, configuration data may have lost.	"Effects of a CP switchover"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
17.	On the node, verify that the data collection configuration is correct by comparing the currently configured values with the customer-defined and default configuration values.	"Displaying data collection configuration" (page 122)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
		"Data collection system configuration"	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
			Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2/PT-IP
18.	Correct any data collection configuration errors. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Configuring MDP for Multiservice Switch" "Managing data collection entries" "Data collection system configuration"	*241-6001-309 Nortel Multiservice Data Manager Management Data Provider* *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/PT-IP*
19.	On the server, open the Alarm Display tool and the Alarm Help.	"Starting Alarm Display" "Starting Alarm Help"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
20.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
21.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

FTP session failures

FTP session failures may be caused by one of the following:

- Multiservice Data Manager server is not configured to communicate with the Multiservice Switch 15000 / Media Gateway 15000 node
- the Multiservice Data Manager server group definitions are incomplete
- the Multiservice Switch / Media Gateway account is configured incorrectly; FTP is not configured by default or the wrong userid and password was used

Problem indicators

- BDF files are missing on the Multiservice Data Manager server

- a 7006 0007 alarm indicating a failed FTP session is displaying on the OSS and on Multiservice Data Manager servers
- alarms indicating illegal login attempts are displaying on the OSS and Multiservice Data Manager servers. For example,
  - 7006 0001
  - 7006 0002
  - 7006 0003

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct problems with FTP session failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

FTP session failures

Task		Use the section...	in...
1.	On the server, verify that all the servers required for network access, surveillance access, and provisioning access have been configured correctly.	"Servers required to support Multiservice Switch network access, surveillance, and provisioning access"	*NN10400-305 Nortel Multiservice Data Manager Administration Fundamentals*
2.	Correct any incorrect server configuration as required. ***Note:*** Consult Nortel GNTS before changing any the server configuration.	"Configuring servers for network access, surveillance access, and provisioning access" "Summary of Multiservice Data Manager server configuration"	*241-6001-303 Nortel Multiservice Data Manager Administration* *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/PT-IP*

Task		Use the section...	in...
3.	On the server, verify that the group definitions allow access to a specific node.	"Host group directory server 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-AAL2/PT-IP*
		"Defining the groups and hosts"	*241-6001-303 Nortel Multiservice Data Manager Administration*
4.	On the server, open the Command Console tool and connect to the network.	"Connecting to the network"	*241-6001-804 Nortel Multiservice Data Manager Utilities*
5.	On the server, open the Network Viewer tool.	"Starting the Network Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
6.	Using the Component Information Viewer tool, examine the node for any alarms indicating a communications problem.	"Starting Component Information Viewer with context"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
7.	On the node, use the Component Information Viewer tool to verify that the *IpAccess*component is configured correctly.	"Displaying diagnostic information in MDM Toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
		"Multiservice Switch user access administration"	*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*
		"Access control configuration"	*NN10225-512 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
			Configuration Attribute Summary PT-AAL1/UA-AAL1/UA-IP/PT-AAL2/PT-IP
8.	Check that the Multiservice Switch / Media Gateway account is configured correctly. This includes checking the user ID, and the access permissions.	"User ID and password failures" (page 58)	this document *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

User ID and password failures

User ID and password failures may be caused by one of the following:

- the interface component is locked
- user ID or password has been changed
- an incorrect scope or impact has been assigned to a userid

Problem indicators

- security logs reporting an attempt to change a user ID, a password, or permissions are displaying on the OSS
- alarms indicating a failed login attempt, or denied permissions are displaying on the OSS and on Multiservice Data Manager servers. For example,
  - 7006 0001
  - 7006 0006

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct problems with userid and password failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Userid and password failures

Task		Use the section...	in...
1.	Open the Command Console tool on the server and connect to the network.	"Connecting to the network"	*241-6001-804 Nortel Multiservice Data Manager Utilities*

Task		Use the section...	in...
2.	On the server, open the Network Viewer tool.	"Starting the Network Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Component Information Viewer tool, examine the node.	"Starting Component Information Viewer with context"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	On the node, use the Sun Admin tool to verify that the user IDs, passwords, and permissions are configured correctly. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Access control 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-AAL2/PT-IP*
		"Configuring general service parameters" "Configuring node basics"	NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures
5.	Correct user ID configuration problems as required. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Access control 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-AAL2/PT-IP*
		"Multiservice Data Manager user access administration" "Multiservice Switch user access administration"	*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*
		"Adding a new userId"	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*

Task		Use the section...	in...
6.	Correct password configuration problems as required. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Multiservice Data Manager user access administration" "Multiservice Switch user access administration" "Setting a password using a secure method"	*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* *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*
7.	If a remote ASCII terminal is being used to manage the network, verify that the Remote Network Communication System (RNCS) user account is configured correctly.	"Creating an RNCS user account"	*241-6001-303 Nortel Multiservice Data Manager Administration*

User ID and password failures in VoIP networks with IEMS providing central user authentication and authorization

Centrally authenticated user ID and password failures may be caused when the RADIUS server on the IEMS:

- fails to respond
- provides a bad value in the authentication request
- receives a non-supported PDU
- receives an incomplete VSA
- receives an unexpected PDU
- receives a bad userid or password

Problem indicators

- the user cannot log on to the MSS/MG15000 switch successfully

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct problems with failures of IEMS central authentication and authorization or userids and passwords. The task table references

procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IEMS centrally authenticated userid and password failures

Task		Use the section...	in...
1.	Verify that the central security server on the IEMS is operating properly. Refer to the IEMS documentation.		
2.	Verify that the userids on the IEMS have the proper access privileges to access the switch.	"Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to IEMS groups"	*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*
3.	Verify that the RADIUS client server on the MSS/MG15000 switch is working properly.	"Verifying the statistics for the MSS/MG15000 RADIUS server" (page 204)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Base software service degradations

Refer to the following section for more information about how to correct Nortel Multiservice Switch 15000 / Media Gateway 15000 base software service degradations:

- "Service degradations due to network synchronization problems" (page 61)
- "Service degradations due to network time server problems" (page 63)

Service degradations due to network synchronization problems

Network synchronization problems resulting in service degradations may be caused by one of the following:

- a remote transmission error
- a degraded signal

Problem indicators

- 7011 5003 alarm against Lp/0 EDS1/0 or Lp/0 EDS1/1 component is displaying on the OSS and on Multiservice Data Manager servers
- 7017 xxxx alarms indicating that the node is in a free run state are displaying on the OSS and on Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct network synchronization problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to network synchronization problems

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	Compare the configured network synchronization values with the recommended values for your solution. Determine how network synchronization is provisioned by issuing the following commands from the Command Console: **`display -prov NetworkSynchronization`** **`display NetworkSynchronization`**	"Network clock synchronization configuration"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
5.	Correct configuration problems as required. If the *clockSource* attribute is not set to *module*, correct the configuration. ***Note:*** Consult Nortel GNTS before changing any provisioning values.	"Configuring the clocking source for the port"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
6.	Monitor the synchronization state of the node.	"Monitoring the network clock synchronization state of the node" (page 130)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
7.	If the node is out-of-synchronization, but the ports are not, contact Nortel GNTS and provide them with the output from the commands performed in this task table.		

Service degradations due to network time server problems

Time server problems resulting in service degradations may be caused by one of the following:

- a loss of connectivity between the Multiservice Switch 15000 / Media Gateway 15000 node and the Multiservice Data Manager server
- a time server that has stopped
- incorrect or obsolete time server provisioning

Problem indicators

- 7015 xxxx time server alarms are displaying on the OSS and on Multiservice Data Manager servers

- time server connectivity alarms are displaying on the OSS
- alarms indicating a time difference between the node, the server and its time server

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct time server problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to network time server problems

Task		Use the section...	in...
1.	On the server, open the Command Console tool and connect to the network.	"Connecting to the network"	*241-6001-804 Nortel Multiservice Data Manager Utilities*
2.	On the server, open the Network Viewer tool.	"Starting the Network Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Component Information Viewer tool, examine the network time server.	"Starting Component Information Viewer with context"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Verify the configuration of the network time server.	"Understanding network time and date configuration" "Synchronizing automatically with a network time server" "Synchronizing manually to a network time server"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
		"Time of day 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-AAL2/PT-IP*

Task		Use the section...	in...
5.	Verify the configuration of node clocking. If the node has lost its clocking configuration, reconfigure and synchronize it with the network time server. If the node and server are out of sync, synchronize the server first, and then the node.	"Configuring the time zone offset" "Synchronizing manually to a network time server" "Verifying the time configuration on the node"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
6.	Verify that the Solaris NTP server is running. Check that the file **`/etc/inet/ntp.conf`** exists, and that the NTP server(s) IP address specified in the file is correct. Using the command **`ps -ef | grep xntpd`**, verify that the file **`/usr/lib/inet/xntpd`** exists. If the server is not running, start it.	"Network TIme Protocol (NTP) support"	*NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*
7.	Verify that the workstation is synchronized with its source. From the UNIX command line, use the command **`ntpq`** to start the NTP query program. At the ntpq> prompt, enter **`rv`** to display the NTP variables, and check that the value for the variable "stratum" is less than sixteen.		SUN documentation
8.	On the Multiservice Data Manager workstation, open the Network Viewer tool and verify that the workstation running the NTP server is connected to the network. If there is connection to the network, go to task 8. If the NTP server is not connected, you may have	"Starting Network Viewer" "Understanding the network display" "Connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservi" (page 76)	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools* this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks*

Task		Use the section...	in...
	OAM connection problems between the server and the node.		*Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
9.	If the problem persists, contact Nortel GNTS and provide them with the following: • the current configuration of the time server • the current software load running on the node • a list of the dates and times when the problem occurred	"Information to collect about a problem" (page 14)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
10.	Check the time server provisioning.	"Synchronizing automatically with a network time server" "Synchronizing manually with a network time server"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*

Software upgrade problems

Refer to the following guide for more information about how to correct Nortel Multiservice Switch 15000 / Media Gateway 15000 software upgrade problems:

- *NN10440-450 Carrier Voice over IP Network Upgrade*

Multiservice Switch 15000 / Media Gateway 15000 management problems

Refer to the following section for more information on the flow of Nortel Multiservice Switch 15000 / Media Gateway 15000 management information in a Carrier Voice over IP solution network:

- "Overview of management information flow in a Carrier Voice over IP solution network" (page 68)

Refer to one of the following sections for more information about how to correct:

- "Alarm flow failures" (page 68)
- "Performance measurement collection failures" (page 71)
- "Connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservi" (page 76)
- "IPSec connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Mult" (page 78)
- "Connection failures between Multiservice Data Manager servers and higher level management system" (page 81)

Refer to the following section for more information about how to correct seasonal time-of-day problems:

- "Seasonal time-of-day not updating" (page 83)

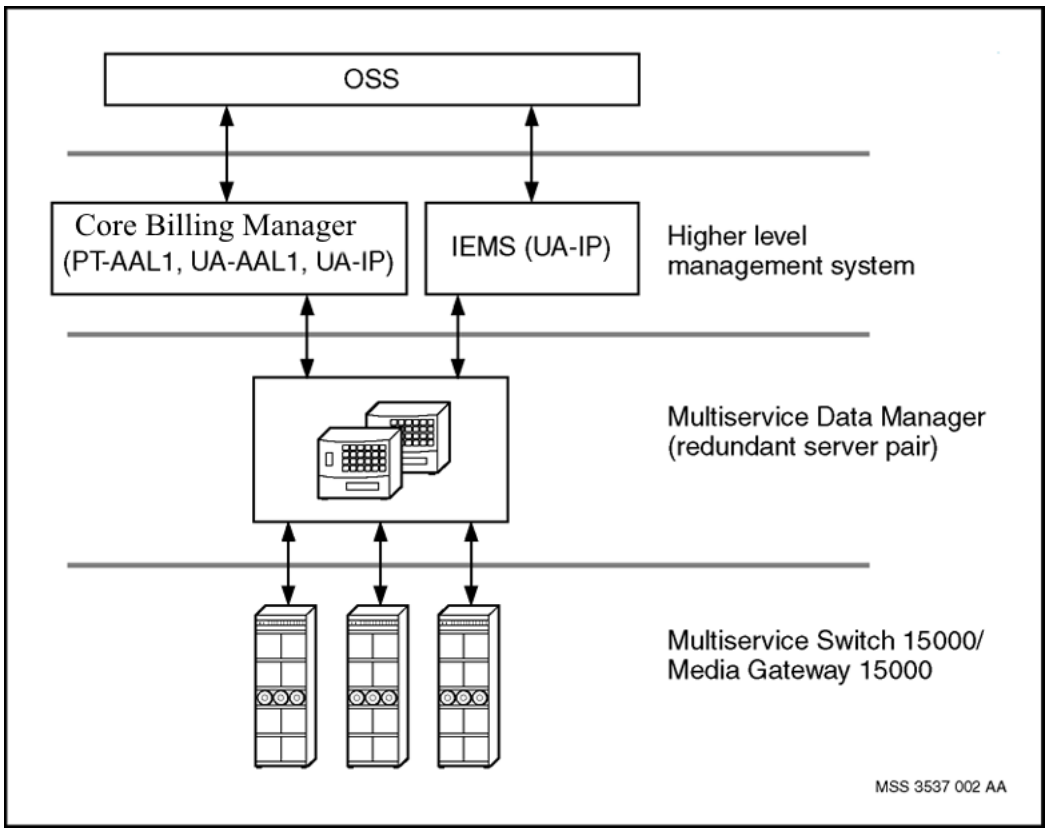
Refer to the following section for more information about troubleshooting central AAA in a VoA solution:

- "Troubleshooting central AAA on the MDM Admin Server in a VoA solution" (page 86)

Overview of management information flow in a Carrier Voice over IP solution network

"Management information flow" (page 68) shows the logical flow of management information in a Carrier Voice over IP solution network. In SN07 PT-AAL1 and UA-AAL1 solution networks, the CS2000 Core Manager provides the interface to the OSS. In SN07 UA-IP/PT-IP solution networks, both the IEMS and the CS2000 Core Manager provide an interface to the OSS.

Management information flow



Corrective Actions for Alarm Flow Failures

Alarm flow failures

Alarm flow failures may be caused by one of the following:

- Multiservice Data Manager server cannot communicate with Multiservice Switch 15000 / Media Gateway 15000 nodes
- in the PT-AAL1 and UA-AAL1 solutions, the Multiservice Data Manager server cannot communicate with the CS2000 Core Manager, or the CS2000 Core Manager cannot communicate with the OSS

- in the UA-IP/PT-IP solution, the Multiservice Data Manager server cannot communicate with the IEMS, or the IEMS cannot communicate with the OSS
- the Multiservice Data Manager pserver application has failed
- the Multiservice Data Manager client set cannot communicate with the server

Problem indicators

- the Multiservice Switch 15000 / Media Gateway 15000 alarms are not displaying on the OSS
- the Multiservice Switch 15000 / Media Gateway 15000 alarms are not displaying on Multiservice Data Manager clients

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct Multiservice Switch 15000 / Media Gateway 15000 alarm flow failures, using the alarm display tool. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Multiservice Switch 15000 alarm flow failures

Task		Use the section...	in...
1.	Visually examine the OSS to determine whether or not Carrier Voice over IP alarms are displaying. Verify that communication has not failed between the OSS and the higher level management system (CS2000 Core Manager or IEMS) Verify that the alarms are reaching the higher level management system. Refer to the appropriate higher level management system documentation or the appropriate third-party OSS customers documentation.		
2.	Verify that there are no connection failures between the nodes and the Multiservice Data Manager server workstations.	"Connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservi" (page 76)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
3.	On the Multiservice Data Manager server workstation, open the Alarm Display tool and verify that node alarms are displaying. If there are alarms, go to task 12.	"Viewing alarms in the Active mode"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	On the server workstation, open the Server Administration tool and the System Log Display tool for use in verifying server operation.	"Starting the Server Administration tool" "Viewing logs associated with a server" "Using the System Log Display tool"	*241-6001-303 Nortel Multiservice Data Manager Administration*
5.	Verify that the Host Group Directory server (HGDS) is running. If the HGDS server is not running, start it. If the HGDS server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
6.	Verify that the MSS Management Data Router server (FMDR) is running. If the FMDR server is not running, start it. If the FMDR server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
7.	Verify that the General Management Data Router server (GMDR) is running. If the GMDR server is not running, start it. If the GMDR server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
8.	Verify that the MSS Management Data Router (FMDR) and General Management Data Router (GMDR) servers are communicating with each other.	"Starting the GMDR Administration tool" "Viewing the states of connections to the surveillance servers"	*241-6001-303 Nortel Multiservice Data Manager Administration*

Task		Use the section...	in...
9.	Verify that the MSS Nodal Provisioning Configuration server (PCSERVER) is running. If the PCSERVER is not running, start it. If the PCSERVER will not start, refer to the exit codes.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
10.	Verify that data is passing on the ports responsible for passing data from the server to the higher level management system. Refer to the hardware specification to determine the port number. If you see data pass, the problem is with the higher level management system.	"Using the snoop commands to check for data transfer" (page 141)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
11.	Verify that the pserver application has been configured to expect data on port 3197.	"Editing the configuration file for a server"	*241-6001-303 Nortel Multiservice Data Manager Administration*
12.	If these tasks do not correct the problem, contact Nortel GNTS and provide them with the following: • a file of recent logs as recorded from the System Log Display tool • the hardware configuration • the load being run	"Information to collect about a problem" (page 14)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Performance measurement collection failures

Performance measurement (PM) collection failures may be caused by one of the following:

- Multiservice Data Manager server cannot communicate with the Multiservice Switch 15000 / Media Gateway 15000 nodes
- Multiservice Data Manager server cannot communicate with the CS2000 Core Manager, or the CS2000 Core Manager cannot communicate with the OSS, or the CS2000 Core Manager has failed
- the Multiservice Data Manager server has failed

- the node is not collecting performance measurements
- the network time between the node and the server is not synchronized
- the node and server time-of-day is not synchronized

Problem indicators

- the 5-minute or 30-minute PMs are not displaying on the OSS

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct performance measurement collection failures with Nortel Multiservice Data Manager (MDM) alarm display tool. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Performance measurement collection failures

Task	Use the section... in...
1.	Visually examine the OSS to determine if Carrier Voice over IP PMs are displaying. Verify that communication has not failed between the OSS and the higher level management system (CS2000 Core Manager). Verify that the PMs are reaching the higher level management system: ***On the*** CS2000 Core Manager: Verify that there are PMs with a timestamp of less than 30-minutes in the 30-minute CSV file. The file is located by default in the following directory: **`/omdata/closedSent/`** ***Note:*** This directory may be user assigned in the UA-AAL1 solution. The file name contains the timestamp. For example: **`PP_30MIN_PM.06_13_2001.1330.PP.THIRTY.CSV`** If the CSV file contains PMs that are older than 30 minutes, the CS2000 Core Manager is not receiving data from the Multiservice Data Manager server. See "Names and locations of SDM files" and "Names and locations of MDM files" in *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* Refer to the appropriate higher level management system documentation or the appropriate third-party OSS customers documentation.

Task		Use the section...	in...
2.	Verify that there are no connection failures between the node and the servers.	"Connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservi" (page 76)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
3.	On the Multiservice Data Manager server workstation, open the Server Administration tool and the System Log Display tool for use in verifying server operation.	"Starting the Server Administration tool" "Viewing logs associated with a server" "Using the System Log Display tool"	*241-6001-303 Nortel Multiservice Data Manager Administration*
4.	Verify that the Host Group Directory server (HGDS) is running. If the HGDS server is not running, start it. If the HGDS server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
5.	Verify that the MSS Management Data Router server (FMDR) is running. If the FMDR server is not running, start it. If the FMDR server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
6.	Verify that the MSS Communications Manager server (FTDM) is running. If the FTDM server is not running, start it. If the FTDM server will not start, refer to the exit codes and error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" "Exit codes" "Error messages"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*

Task		Use the section...	in...
7.	Verify that the Performance Measurement Stream Processor server(s) (PMSP) are running. If a PMSP server is not running, start it. If a PMSP server will not start, refer to the error messages.	"Viewing a server" "Starting a server" "Determining why a server will not start or exit" Error messages	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-310 Nortel Multiservice Data Manager Server Reference*
8.	Verify that the TCP ports of the PMSP server(s) have been properly configured.	"Starting the Nodal Provisioning Administration tool for server administration" "Editing the configuration file for a server"	*241-6001-303 Nortel Multiservice Data Manager Administration*
9.	Verify that the performance data is being sent to the higher level management system: **`ls /opt/MagellanNMS/data/pmsp/backupForSDM`** If there is more than one file for the TCP port of interest, the PMSP server is not sending the performance data to the higher level management system.	"About the PMSP server"	*241-6001-310 Nortel Multiservice Data Manager Server Reference*
10.	Verify that data is passing on the ports responsible for passing data from the server to the higher level management system. If you see data pass, the problem is with the higher level management system.	"Using the snoop commands to check for data transfer" (page 141)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
11.	Ensure that the node is collecting performance measurements. Check that spooling is turned on by issuing the command **`display col/rts sp spooling`**. Make sure that the queue sizes are set to 200. Issue the command *display lp/* eng ds/rts ov agentQueueSize*. Check whether the node is sending the stats anywhere by issuing the command *display col/rts **.* The response should be zero or near zero.	"Turning collector spooling on or off for each data type" "Configuring the agent queue sizes for each LP and each datatype"	*NN10600-561 Nortel Multiservice Switch 7400/15000/20000 Data Management*
12.	Ensure that the node and server are synchronized.	"Updating the time-of-day for seasonal time changes"	*NN10114-511 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL 1/UA-IP/PT-IP/PT-AAL2*
		"Synchronizing manually to a network time server"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
13.	If these tasks do not correct the problem, contact Nortel GNTS and provide them with the following: • a file of recent logs as recorded from the System Log Display tool • the hardware configuration • the load being run	"Information to collect about a problem" (page 14)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservice Data Manager servers

Connection failures between Nortel Multiservice Switch 15000 / Media Gateway 15000 nodes and Nortel Multiservice Data Manager (MDM) servers may be caused by one of the following:

- a faulty connection on the CS LAN
- firewalls or routers between the server and the node
- faulty ATM connectivity
- a faulty Ethernet cable
- a node failure
- Multiservice Data Manager attempted to log in to the wrong account. This could also be an nonexistent account, an account with the wrong user ID and password, or an account without FMIP access.

Problem indicators

- 0999 0001 proxy alarms indicating that single or multiple Multiservice Switch 15000 / Media Gateway 15000 nodes cannot communicate with the Multiservice Data Manager server are displaying on the OSS

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct failures with the connectivity between the Multiservice Switch 15000 nodes and Multiservice Data Manager servers. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Note: For diagnosis of problems with in-band OAM, refer to the network topology described in the section "OAM connectivity" in *NN10114-511 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Connection failures between the node and Multiservice Data Manager servers

Task		Use the section...	in...
1.	Ping the troubled nodes to verify connectivity.	"Verifying connectivity to a remote host" (page 138)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP*

Task		Use the section...	in...
			Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP
2.	On the server, open the Network Viewer tool and verify that there are no isolated nodes. On the Network Viewer tool, an isolated node will have red links from it to the server.	"Starting Network Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	If a single Multiservice Switch 15000 / Media Gateway 15000 node has failed, use the Network Viewer to identify neighboring nodes and verify if the links between them and the failed node are down. If the links are down, contact your facilities group and report the problem. It may be a problem with the CS LAN, the Ethernet Routing Switch 8600, or a call processing port on the Multiservice Switch 15000 / Media Gateway 15000 node.		
4.	If multiple Multiservice Switch 15000 / Media Gateway 15000 nodes are experiencing connectivity outages, use the Network Viewer to identify node clusters and, if possible, a common node (such as a gateway) that all the failed nodes are using. If the network uses in-band OAM and the problem appears to be with a common piece of equipment (such as a gateway), physically inspect the equipment for problems.		
5.	If using in-band OAM:		
	Verify connectivity from the remote switch to the gateway.	"Verifying connectivity to a remote host" (page 138)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
	On the gateway, verify the PNNI link state to the remote switch.	"Correcting line automatic protection switching problems" (page 126) "Verifying the status of the SONET link layer" (page 142)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
	On the gateway and the remote switch, check for IP packet discards.	"Isolating IP packet discards to an interface" (page 186) "Checking for layer 2 interface-level packet discards" (page 189)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
6.	Check the settings of all the non-Nortel equipment that exists between the failed node and the server. Verify that the configuration settings permit the transfer of data between the node and the server.		third party firewall, router, or other equipment documentation
7.	Verify that the account exists, and that the correct user ID and password is being used. Verify that the account has FMIP access.		

IPSec connection failures between the Multiservice Switch 15000 / Media Gateway 15000 nodes and Multiservice Data Manager servers (VoIP networks only)

Connection failures between Nortel Multiservice Switch 15000 / Media Gateway 15000 switches and Nortel Multiservice Data Manager (MDM) servers or between Nortel Multiservice Data Manager (MDM) servers using IPSec may be caused by one of the following:

- different security keys have been used for the security associations on the MDM server and the MSS/MG15000 switch that were manually configured during the initial configuration of IPSec
- different security keys have been used for the security associations on the two MDM servers
- a service such as FTP data or FMIP selected a security association on the MDM server that is different from the security association selected on the MSS/MG15000 switch
- The *inSPI* and *outSPI* values for the security associations at either end of the connection do not match.
- one end of the connection has IPSec enabled when the other end does not

Problem indicators

- MDM tools such as Command console and service provisioning are not working
- MSS/MG15000 performance and alarm data is not being received by the MDM server
- The IEMS is flooded with alarm messages

Corrective action for an IPSec connection between an MSS/MG15000 switch and an MDM Server

This task table shows you the sequence of tasks you need to perform to isolate and correct failures with the IPSec connectivity between a Multiservice Switch 15000 switch and a Multiservice Data Manager server. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IPSec connection failures between MSS/MG15000 switches and Multiservice Data Manager servers

Task		Use the section...	in...
1.	If the IEMS is flooded with alarms, you can disable the alarms on violation by executing the following command on the MSS/MG15000 switch: **`set Vr/0 Ip Spd/1 alarmonviolation disable`**		
2.	On the MSS/MG15000 switch, examine the statistics for general IPSec operation.	"Viewing IPSec general statistics on the MSS/MG15000" (page 206)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
3.	On the MSS/MG15000 switch, examine the IPSec statistics and security association information for the specific connection.	"Verifying IPSec statistics for a specific connection on the MSS/MG15000" (page 206)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
4.	On the MDM server, examine the IPSec error information.	"Viewing IPSec and SSH error logs on the MDM workstation" (page 207)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
5.	On the MDM server, examine the IPSec security association information for the connection.	"Viewing MDM IPSec information"	*NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*
6.	Compare the security association information for both ends of the connection: • The *inSPI* on one end of the connection must be the same as the *outSPI* on the other end. • The source and destination IP addresses on both ends of the connection must align. • The encryption and authentication algorithms must match. • The encryption and authentication keys must match.		

Corrective action for an IPSec connection between MDM Servers

This task table shows you the sequence of tasks you need to perform to isolate and correct failures with the IPSec connectivity between two Multiservice Data Manager servers. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IPSec connection failures between Multiservice Data Manager servers

Task		Use the section...	in...
1.	On each MDM Server, examine the IPSec error logs.	"Viewing IPSec and SSH error logs on the MDM workstation" (page 207)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
2.	On each MDM Server, examine the IPSec security association information.	"Viewing MDM IPSec information"	*NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*
3.	Compare the security association information for both ends of the connection: • The *inSPI* on one end of the connection must be the same as the *outSPI* on the other end. • The source and destination IP addresses on both ends of the connection must align. • The encryption and authentication algorithms must match. • The encryption and authentication keys must match.		

Connection failures between Multiservice Data Manager servers and higher level management system

Connection failures between Nortel Multiservice Data Manager (MDM) servers and the higher level management system related to Nortel Multiservice Switch / Media Gateway nodes and Multiservice Data Manager may be caused by one of the following:

- a Multiservice Data Manager server has failed
- both Multiservice Data Manager servers have failed
- both Multiservice Data Manager servers have lost connectivity to the higher level management system
- the higher level management system has failed

Problem indicators

- an MDM 3011 0501 alarm is displaying on the OSS
- an SDM325 log is displaying on the OSS
- an IEMS log is displaying on the OSS

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct failures with the connectivity between Multiservice Data Manager servers and the higher level management system that relate to Multiservice Switch and Multiservice Data Manager. The task table

references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Connection failures between Multiservice Data Manager servers and higher level management system

Task		Use the section...	in...
1.	Verify that both servers are running.	"Alarm flow failures" (page 68) "Performance measurement collection failures" (page 71)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AA L1/UA-AAL1/UA-IP/PT-IP*
2.	If the Network Viewer tool shows no activity on either of the Multiservice Data Manager servers, both of the servers may have failed at the same time. Alternatively, one of the servers was not operational for some time and the second server has now failed. Report the problem to • your next level of support • your Multiservice Data Manager administrator • your workstation administrator		
3.	If there is activity on one or both of the servers, use the Network Viewer tool to isolate the problem links between the servers and the higher-level management system. The connectivity failure may be caused by a facilities problem. Report the problem to • your next level of support • your facilities department • your Multiservice Data Manager administrator • your workstation administrator	"Starting Network Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
4.	If the problem is not related to Multiservice Data Manager, check the higher level management system node.	For CS2000 Core Manager For IEMS	*NN10082-911 CS 2000 Core Manager Fault Management* *NN10334-911 IEMS Fault Management*
5.	Verify that IPSec connectivity is established	"Verifying PKI certificate problems"	**NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management**

Time of day for seasonal time changes

Refer to the following section for more information about how to correct seasonal time of day problems:

- "Seasonal time-of-day not updating" (page 83)

Seasonal time-of-day not updating

Provided that at least one Nortel Multiservice Data Manager (MDM) server was up at the time of transition, the seasonal time-of-day is not updating due to the following

- time-of-day script is not running
- the script was running, but the time offset could not be changed

Note: If there was an server reboot, the log file was deleted from /tmp.

Problem indicators

- the time-of-day has not changed to Daylight Savings time, or standard time
- the time offset value is missing or incorrect
- the log file /tmp/tod_output is missing or contains error messages
- the Alarm Display is displaying an alarm relating to time of day

Check the log file timestamp and the last timestamp inside the log file /tmp/tod_output to see if the script was running. If the script was running, and there are error messages, see "Corrective action (time offset)" (page 85). If the script is not running, see "Corrective action (script not running)" (page 84).

Corrective action (script not running)

This task table shows you the sequence of tasks you need to perform to isolate and correct seasonal time-of-day problems when the script has not been running. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Corrective action (script not running)

Task		Use the section...	in...
1.	On the Multiservice Data Manager server, verify that the Solaris NTP server has been configured. Verify that the file **`/etc/inet/ntp.conf`** exists and that the NTP server(s) IP address specified in the file is correct.	"Network Time Protocol (NTP) support"	*NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*
2.	Ensure that the script has executable permissions		
3.	Verify time-of-day provisioning in the crontab file: incorrect date/time to run the script, incorrect script location, missing parameters.	"Updating the time-of-day for seasonal time changes"	*NN10114-511 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL 1/UA-IP/PT-IP/PT-AAL2* 7-24-0991 MDM *15.2 Software Loading and Configuration Including Succession SN08 Installation Method*
4.	Check the crontab activation/provisioning		7-24-0991 MDM *15.2 Software Loading and Configuration Including Succession SN08 Installation Method*

Corrective action (time offset)

This task table shows you the sequence of tasks you need to perform to isolate and correct seasonal time-of-day problems when the script is running, but the time offset has not changed. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Corrective action (time offset)

Task		Use the section...	in...
1.	On the Multiservice Data Manager server, verify that the Solaris NTP server has been configured. Verify that the file **`/etc/inet/ntp.conf`** exists and that the NTP server(s) IP address specified in the file is correct.	"Network TIme Protocol (NTP) support"	*NN10185-461 Upgrading Nortel Multiservice Data Manager in Carrier Voice over IP Networks*
2.	Check for missing or incorrect parameters in crontab provisioning: TOD offset, node access (group name, user ID, password).	"Updating the time-of-day for seasonal time changes"	*NN10114-511 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL 1/UA-IP/PT-IP/PT-AAL2*
		"Configuring the time zone offset"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
		"Setting up a cron job to check for password expiry"	*NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*
			7-24-0991 MDM *15.2 Software Loading and Configuration Including Succession SN08 Installation Method*
3.	Check node group/IP address provisioning.	"Groups of nodes for network access"	*NN10400-305 Nortel Multiservice Data Manager Administration Fundamentals*

Task		Use the section...	in...
4.	Verify theMultiservice Data Manager user account on the node has the right command scope/impact and access permissions (Telnet and FMIP).	"User authentication"	*NN10400-605 Nortel Multiservice Data Manager Network Security Fundamentals*
5.	Check time-of-day synchronization of the node to the server.	"Synchronizing manually to a network time server"	*NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
6.	Check the physical connectivity between the node to the server.	"Information for connecting to Multiservice Data Manager through a Multiservice Switch-only network" "Multiservice Data Manager connectivity overview" "Multiservice Data Manager connectivity using StartUp"	*NN10600-271 Nortel Multiservice Switch 7400/15000/20000 Network Management Connectivity*

Troubleshooting central AAA on the MDM Admin Server in a VoA solution

Most of the troubleshooting for centralized authentication can be done by logging in to User Administration System and searching for errors. Unsuccessful authentications with the RADIUS are usually caused by invalid user IDs or passwords. More information and troubleshooting tips are available in the chapter "Troubleshooting Centralized authentication" under "Unsuccessful authentication attempt on Multiservice Switch nodes" in *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*.

If the Sun ONE Identity server (IS) experiences an uncontrolled shutdown, the DBVERSION files may become corrupted. You must shut down the server according to the procedure given. More information is available in

the chapter "Restore procedures after shutdown" in *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*. (more to come here)

Troubleshooting central AAA on the MDM Admin Server in a VoA solution

Task	See	Reference
For unsuccessful login attempts, use the troubleshooting tips and verify that the correct user IDs and passwords exist, and that the RADIUS server has been correctly configured for central AAA.	• Unsuccessful authentication attempt on Multiservice Switch nodes	Troubleshooting tips in *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*
If the Sun ONE Identity server (IS) experiences an uncontrolled shutdown, DBVERSION files may become corrupt. Shut down and restore the server using the appropriate procedures. ***Note:*** An abnormal system shutdown is strictly unsupported and it is strongly recommended that you use one of the following commands before powering down the system: • "init 0" (which will halt the system) • "init 6" (which will halt and reboot the system) • "shutdown"	• Stopping the NDS processes • Restarting the NDS processes • Recreating the DBVERSION files	Restore procedures after shutdown in *NN10400-606 Nortel Multiservice Data Manager Network Security: User Access Configuration*

PT-AAL1 / UA-AAL1 troubleshooting

This chapter addresses troubleshooting for voice quality and call processing failures and ATM service problems related to Nortel Multiservice Switch equipment, which is unique to the PT-AAL1 and UA-AAL1 Carrier Voice over IP solutions. Refer to one of the following sections for more information about how to correct voice quality, call processing, or ATM service problems:

- "PT-AAL1 / UA-AAL1 call processing problems" (page 89)
- "PT-AAL1 / UA-AAL1 call quality problems" (page 91)
- "ATM service problems" (page 93)

PT-AAL1 / UA-AAL1 call processing problems

Call processing failures due to ATM framework problems

Call processing failures due to ATM framework problems related to Nortel Multiservice Switch equipment and Nortel Multiservice Data Manager (MDM) servers may be caused by one of the following:

- a faulty link or network node
- addressing or routing errors
- resource exhaustion
- protocol errors

Problem indicators

- a TRK113 log is displaying on the OSS
- an XPKT301 log is displaying on the OSS
- CSV stream statistics indicate an non-zero entry. A common non-zero entry is INFAIL or OUTFAIL. For example, INFAIL 3 or OUTFAIL3. For an example of a CSV file, see "Sample CSV file" in *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*.
- a customer reports failed calls

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct ATM framework problems related to Multiservice Switch equipment and Multiservice Data Manager servers that are causing call processing failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Call processing failures due to ATM framework problems

Task		Use the section...	in...
1.	Check for alarms on the CS2000 and isolate the call processing problem.	"Isolating an ATM framework call processing problems" (page 177)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
2.	Check for a faulty link or network component if you see failure cause codes 27, 35, and 36 in a CSV statistics file.	"Correcting ATM framework call processing problems caused by faulty links or network components" (page 179)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
3.	Check for address and routing errors if you see failure cause codes 3, 18, 21, and 28.	"Correcting ATM framework call processing problems caused by addressing or routing errors" (page 180)	this document *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
4.	Check for resource exhaustion if you see failure cause codes 37, 45, 47, and 58.	"Correcting ATM framework call processing problems caused by resource exhaustion" (page 181)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
5.	Check for protocol errors if you see failure cause codes 49, 57, 58, 63, 65, 73, 78, 88, 96, 100, 104, and 111.	"Correcting ATM framework call processing problems caused by protocol errors" (page 182)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

PT-AAL1 / UA-AAL1 call quality problems

Call quality problems due to ATM framework problems

Call processing failures due to ATM framework problems related to Nortel Multiservice Switch equipment and Nortel Multiservice Data Manager (MDM) servers may be caused by one of the following:

- specific route problems
- a specific feature activation
- hardware problems
- insufficient bandwidth
- bad voice quality
- one-way speech path problems

Problem indicators

- a customer reports one-way speech paths or voice quality problems

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct ATM framework problems related to Multiservice Switch equipment and Multiservice Data Manager servers that are causing call

quality failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Call quality problems due to ATM framework problems

Task		Use the section...	in...
1.	Trace the call to see if it has been established. If the connection has been established, check for items in tasks 2 and 3. If the connection has not been established, perform task 4.	"Initiating a connection trace"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
2.	Use the trace outputs (txCellDiscard and rxCellDiscard) to look at the discards along the path.		
3.	Try to isolate the cause by identifying and recording any patterns associated with the problem. Note any of the following: • If the problem occurred after a special feature was activated. • If the problem continues to occur on a specific route. • If the problem continues to occur on specific hardware. • If the problem continues to occur at a specific time of day. Depending on the pattern you observe, collect as much data as possible from logs, alarms, and SCNs. If the problem has occurred several times, do not disconnect the problem call. Call Nortel GNTS using a different line and report the problem.	"Starting the System Log Display tool") "Data viewer window for replay mode"	*241-6001-303 Nortel Multiservice Data Manager Administration* *241-6001-031 Nortel Multiservice Data Manager Performance Management Tools*
4.	Perform a route finder trace to find the address. Check the peer-to-peer connection	"Using the RouteFinder component"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM*

Task	Use the section...	in...
between MG4000s, the ATM addressing table, and the CS2000 table filled with ATM addressing information.		*Fault and Performance Management*

ATM service problems

Refer to the following section for more information about how to correct ATM backbone failures and service degradations:

- "ATM backbone failures due to ATM routing problems" (page 93)
- "Service degradations due to ATM routing problems" (page 98)

ATM backbone failures due to ATM routing problems

ATM backbone failures due to ATM routing problems may be caused by one of the following:

- an incorrect configuration
- CPU utilization on the Nortel Multiservice Switch 15000 node
- resource exhaustion
- ATM interface LRC frame errors
- LP/link SES (severely errored seconds), or UNI signaling problems
- address, PNNI, or UNI misconfiguration
- PNNI or UNI problems

Problem indicators for ATM backbone failures

- 7041 025x, 7041 0401, or 7041 0601 alarms are displaying on the OSS and on Nortel Multiservice Data Manager (MDM) servers
- alarms relating to PNNIs or UNIs configured on the ATM interfaces are displaying on the OSS and on Multiservice Data Manager servers
- alarms relating to the PNNIs and UNIs configured on the ATM interfaces are displaying on the OSS and on Multiservice Data Manager servers
- ATM interface VCC "clear" cause codes are displayed

Problem indicators for ATM backbone service degradations

The following list may indicate ATM backbone service degradations:

- dropped calls
- 0000 300x alarms, 7003 000x threshold crossing alarms, and signalling failure alarms are displaying on the OSS and on Multiservice Data Manager servers

- 5-minute and 30-minute PMs are showing that dropped calls on the ATM interfaces are increasing. For more information, see "Troubleshooting the interval data records in *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*.

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct ATM routing problems that are causing ATM backbone failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

ATM backbone failures due to ATM routing problems

	Task	Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer" Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209)	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools* this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

	Task	Use the section...	in...
		"Summary of cause codes for ATM PNNI version 1.0"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
4.	If the cause codes suggest a problem with the physical layer, or if you see FP alarms, threshold crossing alarms, or ATM link alarms, examine the physical layer for problems. If the cause codes do not suggest a problem or if you do not see these alarms, go to task 5. ***Note:*** Carrier Voice over IP solutions do not support VPCs and VPTs.	"Verifying the status of the link layer" (page 142)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Displaying the OSI state of the ATM interface" "Examining the buffer usage of ATM function processors" "Displaying the overall connection usage of ATM function processors" "Displaying specialized connection usage of ATM function processors" "Identifying troubled connections at the interface level" "Troubleshooting LRC errors at the ATM interface level"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
5.	If the cause codes suggest a problem with the application layer, or if you see related threshold crossing alarms, examine the application layer. ***Note:*** Carrier Voice over IP solutions do not support VPC or VPT multi-service debugging. If the cause codes do not suggest a problem or if you do not see these alarms, go to task 6.	"Determining the OSI state of a virtual connection" "Determining the OSI state of the source and destination SPVCs and SPVPs" "Determining the status of a virtual connection" "Viewing ATM connection statistics" "Viewing CTD calculations"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*

	Task	Use the section...	in...
		"Viewing congestion control activity for connections" "Viewing ATM traffic descriptor parameters"	
6.	If the cause codes suggest a problem with the signalling layer, or if you see signalling-related alarms, examine the signalling layer. ***Note:*** Carrier Voice over IP solutions do not support IISP. If the cause codes do not suggest a problem or if you do not see these alarms, go to task 7.	"Displaying information on the signaling channel" "Displaying information on ILMI PDUs" "Cause code definitions used for call processing troubleshooting" (page 209)	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management* this document. *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
7.	If the cause codes suggest a problem with the routing layer, or if you see alarms related to PNNI connections, examine the routing layer. ***Note:*** Carrier Voice over IP solutions do not support VPT, VPC, or EBR.	"Port ID information" "Displaying information on the number of calls routed" "Displaying a physical link or a virtual path connection" "Monitoring PNNI networking operational measurements" "Displaying SVCC RCC operational attributes" "Displaying logical link relationships in the PNNI networking hierarchy" "Monitoring PNNI path load balancing" "Using the Route Finder component" "Monitoring PNNI route caching"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*

	Task	Use the section...	in...
		"Setting RouteFinder component attributes supporting PNNI load balancing and route caching" "Monitoring the topology data base - Displaying ATM service metrics for a horizontal link" "Cause code definitions used for call processing troubleshooting" (page 209)	this document. *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
8.	If the cause codes suggest a problem with the state of the ATM interface, connection admission, or connection mapping, examine the transport layer.	"Displaying the OSI state of the ATM interface" "Identifying troubled connections" "Examining connection admission" "Displaying ATM interface traffic statistics" "Displaying ATM interface operational attributes" "Displaying the last alarmed peak transmit utilization of an ATM link" "Displaying the ConnectionMapping attributes"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
9.	Do this task for service degradation scenarios only. If you see that calls are incrementing under a specific attribute, look up the description of the attribute for additional information.		*NN10600-060 Nortel Multiservice Switch 7400/15000/20000 Component Reference*, Volumes 2, 5, and 6

	Task	Use the section...	in...
10.	Compare the configured FP values with the recommended values for your solution. Compare the configured link values with the recommended values for your solution. If the configuration values do not match the recommended values, make required configuration changes. ***Note:*** Consult Nortel GNTS before changing your configuration. Provide GNTS with the output of all commands used in this task table.	"Summary of FP configuration" "Summary of link 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-AAL2/PT-IP*
11.	Correct physical layer problems and replace cards as required. ***Note 1:*** If FP resources allow, a faulty port may be reconfigured on a different line pair on the same FP. ***Note 2:*** Consult Nortel GNTS before replacing a card.		
	For OC-3 card replacement:	"Prerequisites for replacing an FP" "Replacing a spared or unspared optical FP"	*NN10254-913 Nortel Networks Multiservice Switch 15000 in Succession Networks Replacing an OC-3/STM-1 FP (PT-AAL1/UA-AAL1)*
	For 4pOC12, 4pDS3, or 12pDS3 card replacement:	"Replacement of a failed FP"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*

Service degradations due to ATM routing problems

ATM routing problems resulting in service degradations may be caused by one of the following:

- memory usage on the Nortel Multiservice Switch 15000 node
- message block usage on the Multiservice Switch 15000 node
- CPU utilization on the Multiservice Switch 15000 node

- signaling channels

Problem indicators

- dropped calls
- a 7039 5000 alarm is displaying on the OSS and on Nortel Multiservice Data Manager (MDM) servers
- threshold crossing alarms are displaying on the OSS and on Multiservice Data Manager servers
- 0000 300x alarms, 7003 000x threshold crossing alarms, and signalling failure alarms are displaying on the OSS and on Multiservice Data Manager servers
- signalling failures for ATM interface VCC failures are showing increased transmit discards or increased receive discards
- 5-minute and 30-minute PMs are showing that dropped calls on the ATM interfaces are increasing. For more information, see "Troubleshooting the interval data records in *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*.

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct ATM routing problems that are causing service degradations. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Service degradations due to ATM routing problems

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
		Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Summary of cause codes for ATM PNNI"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
4.	If the cause codes suggest a problem with the physical layer, or if you see FP alarms, threshold crossing alarms, or ATM link alarms, examine the physical layer for problems. If the cause codes do not suggest a problem or if you do not see these alarms, go to task item 5. ***Note:*** Testing a port is service affecting. Contact Nortel GNTS before performing this test.	"Verifying the status of the link layer" (page 142)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*
		"Checking the OSI status of the function processor" "Examining the software status of the function processor" "Examining the buffer usage of ATM function processors"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*

Task		Use the section...	in...
		"Displaying the overall connection usage of ATM function processors" "Displaying specialized connection usage of ATM function processors" "Testing a port" "Interpreting test results"	*NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting*
5.	If the cause codes suggest a problem with the application layer, or if you see related threshold crossing alarms, examine the application layer. ***Note:*** Carrier Voice over IP solutions do not support VPC and VPT. If the cause codes do not suggest a problem or if you do not see these alarms, go to task item 6.	"Determining the OSI state of a virtual connection" "Determining the OSI state of the source and destination SPVCs and SPVPs" "Determining the status of a virtual connection" "Viewing ATM connection statistics" "Viewing CTD calculations" "Viewing congestion control activity for connections" "Viewing ATM traffic descriptor parameters"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
6.	If the cause codes suggest a problem with the signalling layer, or if you see signalling-related alarms, examine the signalling layer. ***Note:*** Carrier Voice over IP solutions do not support IISP. If the cause codes do not suggest a problem or if you do not see these alarms, go to task item 7.	"Displaying information on the signaling channel" "Displaying information on ILMI PDUs" "Handling problems in ATM routing and signaling"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management* *NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*

Task	Use the section...	in...
7. If the cause codes suggest a problem with the routing layer, or if you see alarms related to PNNI connections, examine the routing layer. ***Note:*** Carrier Voice over IP solutions do not support VPT, VPC, or EBR.	"Port ID information" "Displaying information on the number of calls routed" "Displaying a physical link or a virtual path connection" "Monitoring PNNI networking operational measurements" "Monitoring SVCC RCC operational information" "Monitoring logical link relationships in the PNNI networking hierarchy" "Monitoring PNNI path load balancing" "Using the Route Finder component" "Monitoring PNNI route caching" "Setting RouteFinder component attributes supporting PNNI load balancing and route caching" "Monitoring the topology data base - Displaying ATM service metrics for a horizontal link" "Cause code definitions used for call processing troubleshooting" (page 209)	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management* this document. *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/ UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
8.	If the cause codes suggest a problem with the state of the ATM interface, connection admission, or connection mapping, examine the transport layer.	"Displaying the OSI state of the ATM interface" "Identifying troubled connections" "Examining connection admission" "Displaying ATM interface traffic statistics" "Displaying ATM interface operational attributes" "Displaying the last alarmed peak transmit utilization of an ATM link" "Displaying the Connection Mapping attributes"	*NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*
9.	Do this task for service degradation scenarios only. If you see that calls are incrementing under a specific attribute, look up the description of the attribute for additional information.		*NN10600-060 Nortel Multiservice Switch 7400/15000/20000 Component Reference*, Volumes 2, 5, and 6
10.	Compare the configured FP values with the recommended values for your solution. Compare the configured link values with the recommended values for your solution. If the configuration values do not match the recommended values, make configuration changes as necessary. ***Note:*** Consult Nortel GNTS before changing your configuration.	"Summary of FP configuration" "Summary of link 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-AAL2/PT-IP*

Task		Use the section...	in...
11.	Correct physical layer problems as required and replace the FPs as required. ***Note 1:*** If FP resources allow, a faulty port may be reconfigured on a different line pair on the same FP. ***Note 2:*** Consult Nortel GNTS before replacing an FP.		
	For OC-3 card replacement:	"Prerequisites for replacing an FP" "Replacing a spared or unspared optical FP"	*NN10254-913 Nortel Networks Multiservice Switch 15000 in Succession Networks Replacing an OC-3/STM-1 FP (PT-AAL1/UA-AAL1)*
	For 4pOC12, 4pDS3, or 12pDS3 card replacement:	"Replacement of a failed FP"	*NN10600-130 Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade*
12.	Compare the configured link values with the recommended values for your solution.	"Summary of link 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-AAL2/PT-IP*

UA-IP/PT-IP troubleshooting

This chapter addresses troubleshooting for voice call processing problems, voice call quality problems, and IP service problems related to Nortel Multiservice Switch / Media Gateway equipment, which are unique to UA-IP/PT-IP solutions. The focus is on troubleshooting scenarios from a Multiservice Switch 15000 node perspective, with references provided for Media Gateway 15000 troubleshooting. Refer to the following sections for more information about how to correct these problems.

- "UA-IP/PT-IP call processing problems" (page 105)
- "UA-IP/PT-IP call quality problems" (page 110)
- "IP service problems" (page 114)

UA-IP/PT-IP call processing problems

In the UA-IP/PT-IP solution, the Nortel Multiservice Switch 15000 forwards IP packets with H.248 messages in the payload between gateway controllers and media gateways, both Media Gateway 9000 and Media Gateway 15000 (VSP3 and VSP3-o). The failure or degradation of IP packet forwarding is the primary way that Multiservice Switch 15000 nodes can impact voice call processing in the UA-IP/PT-IP solution.

Refer to one of the following sections for more information about how to correct:

- "H.248 packet forwarding problems" (page 105)
- "Media Gateway 15000 call processing problems" (page 108)

H.248 packet forwarding problems

Voice call processing failures due to H.248 packet forwarding problems related to Nortel Multiservice Switch equipment may be caused by one of the following:

- faulty link or network component
- misconfigured addresses
- resource exhaustion

Problem indicators

- non-zero entry for discarded packets in the CSV stream statistics
- threshold is crossed for ICMP packet generation in the CSV stream statistics
- MG9000 H.248 logs are displaying on the OSS
- Media Gateway 15000 H.248 logs are displaying on the OSS

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct H.248 packet forwarding problems related to Multiservice Switch equipment and Nortel Multiservice Data Manager (MDM) servers that are causing call processing problems. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Call processing problems due to H.248 packet forwarding problems

Task		Use the section...	in...
1	Isolate H.248 packet forwarding problems based upon IEMS alarms and/or MG9000 manager alarms. For more information, refer to *NN10408-900 ATM/IP Fault Management*.		
2.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
3.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
5.	If IPSec is configured on the call control connection, verify that the security components have been configured correctly.	"Switched Media Gateway Monitoring" • Verifying IKE phase 1 connection problems • Verifying IKE phase 2 connection problems	*NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management*
6.	Check for link alarms and correct any problems.	"Link failures" (page 26)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
7.	Verify that the node forwarding path between two IP addresses is operational.	"Verifying the forwarding path between two IP addresses" (page 184)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
8.	Check for node-level IP packet discards.	"Checking for node-level IP packet discards" (page 185)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
9.	Isolate IP packet discards to an interface.	"Isolating IP packet discards to an interface" (page 186)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
10.	Check for layer 2 interface-level packet discards.	"Checking for layer 2 interface-level packet discards" (page 189)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
11.	Check for node-level ICMP packet generation.	"Checking for node-level ICMP packet generation/reception" (page 195)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
Note: The CSV stream statistics can be used as an alternate source of the information gathered in steps 7, 8, and 9:			
		"Description of IP physical interface PMs" "Traffic management considerations" "Appendix A Use cases, thresholds, and utilization formulas"	*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*

Media Gateway 15000 call processing problems

Media Gateway 15000 voice call processing problems can be subdivided into two categories:

- problems due to the basic operational state
- specific call processing problems

Problems due to the basic operational state

This task table shows you the sequence of tasks you need to perform to diagnose and correct call processing problems due to the basic operational state of the Media Gateway 15000. The task table references procedures

contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Call processing problems due to Media Gateway 15000 basic operational state

Task		Use the section...	in...
1.	Verify that switched Media Gateway is enabled.	"Verifying that switched Media Gateway is enabled"	*NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management*
2.	Display operational and statistics attributes for switched Media Gateway using IP.	"Displaying operational and statistics attributes for switched Media Gateway using IP"	*NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management*
3.	Display OSI states for switched Media Gateway.	"Displaying OSI states for switched Media Gateway"	*NN10600-782 Nortel Media Gateway 7480/15000 Switched Service Configuration Management*

Specific Media Gateway 15000 call processing problems

This task table shows you the types of problems you need to isolate and correct for specific Media Gateway call processing problems. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

Call processing problems due to specific Media Gateway 15000 call processing problems

Task		Use the section...	in...
1.	Media Gateway service is not operational and no calls are possible.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
2.	Calls are not possible for a connection.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
3.	Modem/fax calls are not working.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
4	Troubleshooting REX	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*

Task		Use the section...	in...
5	Troubleshooting PRI backhaul.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
6.	Troubleshooting SS7 backhaul.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*

UA-IP/PT-IP call quality problems

In the UA-IP/PT-IP solution, the Nortel Multiservice Switch 15000 node forwards IP packets with voice bearer in the payload between media gateways:

- Media Gateway 9000 to Media Gateway 9000
- Media Gateway 15000 (VSP3 and VSP3-o) to Media Gateway 15000 Media Gateway (VSP3 and VSP3-o)
- Media Gateway 9000 to Media Gateway 15000 (VSP3 and VSP3-o)
- Media Gateway 9000 to CS-LAN (UAS, IW-SPM-IP, inter-office, etc.)
- Media Gateway 15000 to CS-LAN (UAS, IW-SPM-IP, inter-office, etc.)

The failure or degradation of IP packet forwarding is the primary way that Multiservice Switch 15000 nodes can impact the quality of voice calls

Refer to the following sections for more information about how to correct problems with the failure or degradation of IP packet forwarding:

- "Bearer packet forwarding problems" (page 110)
- "Media Gateway 15000 call quality problems" (page 113)

Bearer packet forwarding problems

Voice call quality failures due to bearer packet forwarding problems related to Nortel Multiservice Switch equipment may be caused by one of the following:

- faulty link or network component
- misconfigured addresses
- resource exhaustion

Problem indicators

- MG9000 voice quality logs are displaying on the OSS
- Media Gateway 15000 H.248 voice quality logs are displaying on the OSS
- non-zero entry for discarded packets in the CSV stream statistics

- threshold is crossed for ICMP packet generation in the CSV stream statistics

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct bearer packet forwarding problems related to Multiservice Switch equipment and Nortel Multiservice Data Manager (MDM) servers that are causing call quality failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Call quality problems due to bearer packet forwarding problems

Task		Use the section...	in...
1	Isolate bearer forwarding problems based on IEMS alarms and/or MG9000 manager alarms. For more information, refer to *NN10408-900 ATM/IP Fault Management*.		
2.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
3.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
5.	Check for link alarms and correct any problems.	"Link failures" (page 26)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
6.	Verify the node forwarding path between two IP address is operational.	"Verifying the forwarding path between two IP addresses" (page 184)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
7.	Check for node-level IP packet discards.	"Checking for node-level IP packet discards" (page 185)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
8.	Isolate IP packet discards to an interface.	"Isolating IP packet discards to an interface" (page 186)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
9.	Check for layer 2 interface-level packet discards.	"Checking for layer 2 interface-level packet discards" (page 189)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
10.	Check for node-level ICMP packet generation.	"Checking for node-level ICMP packet generation/reception" (page 195)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*

Task	Use the section...	in...
Note: The CSV stream statistics can be used as an alternate source of the information gathered in steps 7, 8, and 9:		
	"Description of IP physical interface PMs" "Traffic management considerations" "Appendix A Use cases, thresholds, and utilization formulas"	*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*

Media Gateway 15000 call quality problems

This table shows you the types of problems you need to diagnose for Media Gateway 15000 voice call quality problems. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

Call quality problems due to Media Gateway voice call quality problems

Task		Use the section...	in...
1.	There is no speech on voice calls.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
2.	There is no speech or data on a call.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
3.	Speech on voice calls is distorted.	"Troubleshooting general Media Gateway problems"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*
4.	Problems with G.729 Annex A and B functionality.	"Troubleshooting G.729 Annex A and B voice compression, silence suppression and DTMF upspeed"	*NN10600-780 Nortel Media Gateway 7480/15000 Technology Fundamentals*

IP service problems

Refer to the following sections for more information about how to correct problems that are specific to the IP service on Nortel Multiservice Switch equipment as deployed in the UA-IP/PT-IP solution:

- "IP addressing problems" (page 114)
- "IP security attack" (page 116)
- "OSPF problems" (page 117)

IP addressing problems

A degradation in packet forwarding caused by IP addressing problems on Nortel Multiservice Switch equipment may be caused by one of the following:

- misconfigured IP addresses
- missing routes

Problem indicators

- packet forwarding works for most but not all source/destination IP address pairs

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct IP addressing problems related to Multiservice Switch equipment and Nortel Multiservice Data Manager (MDM) servers that are causing call quality failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IP service problems due to IP addressing problems

Task		Use the section...	in...
1.	Isolate bearer forwarding problems based on IEMS alarms and/or MG9000 manager alarms. For more information, refer to *NN10408-900 ATM/IP Fault Management*.		
2.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

Task		Use the section...	in...
3.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
5.	Check for link alarms and correct any problems.	"Link failures" (page 26)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
6.	Check the configured IP addresses and correct any problems.	"Verifying the configured IP address" (page 196)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
7.	Check the ARP table and correct any problems.	"Verifying the ARP table" (page 198)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*
8.	Check the forwarding and routing tables and correct any problems.	"Verifying the forwarding and routing tables" (page 198)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP*

IP security attack

An IP security attack may be caused by:

- security hole left open
- compromised userid and password

Problem indicators

- threshold for local destined packets has crossed a threshold in the CSV stream statistics
- high CPU usage on the CP for an extended period of time

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct IP security attack problems related to Nortel Multiservice Switch equipment and Multiservice Data Manager servers that are causing call quality failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Media Gateway, Multiservice Data Manager, or Carrier Voice over IP documents.

IP service problems due to an IP security attack

Task		Use the section...	in...
1.	Isolate bearer forwarding problems based on IEMS alarms and/or MG9000 manager alarms. Refer to *NN10408-900 ATM/IP Fault Management*.		
2.	Connect to Multiservice Data Manager tools.	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
3.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Task		Use the section...	in...
5.	Check for link alarms and correct any problems.	"Link failures" (page 26)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
6.	Verify the statistics for locally destined packets.	"Verifying the statistics for locally destined/generated packets" (page 200)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
7.	Determine which interface(s) are receiving these locally destined packets using CSV stream statistics.	"Description of physical interface PMs"	*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*
8.	If necessary, lock the appropriate interface(s) to block the packets generated by the security attack.	"Locking out packet traffic" (page 203)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*

OSPF problems

OSPF problems may be caused by one of the following:

- configuration errors
- neighboring node is down

Problem indicators

- 7012 10xx, 7021 11xx alarms are displaying on the OSS and on Multiservice Data Manager servers

Corrective action

This task table shows you the sequence of tasks you need to perform to isolate and correct IP security attack problems related to Nortel Multiservice Switch equipment and Multiservice Data Manager servers that are causing call quality failures. The task table references procedures contained in this document or located in other Nortel Multiservice Switch, Multiservice Data Manager, or Carrier Voice over IP documents.

IP service problems due to OSPF problems

Task		Use the section...	in...
1.	Connect to Multiservice Data Manager tools	Appendix "Connecting to Multiservice Data Manager tools" (page 215)	this document, *NN10198-912 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Fault Management Troubleshooting PT-AAL 1/UA-AAL1/UA-IP/PT-IP*
2.	From the Alarm Display tool, launch the Component Information Viewer tool and examine the alarms on the problem node.	"Starting Component Information Viewer with context" "Displaying additional component information in MDM toolset"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
3.	Using the Alarm help and the alarm cause codes, determine the meaning of the alarm.	"Viewing alarm codes from Alarm Display or Component Information Viewer"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Monitor OSPF neighbors and correct any problems.	"Monitoring the OSPF configuration" "Monitoring OSPF neighbors"	*NN10600-801 Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*
5.	Monitor the OSPF link state database and correct any problems.	"Monitoring the OSPF configuration" "Monitoring the OSPF link state database"	*NN10600-801 Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*

Task	Use the section...	in...
6. Monitor the OSPF configuration and correct any problems.	"Monitoring the OSPF configuration"	*NN10600-801 Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*
7. Lock and unlock the OSPF component to re-establish connection with the neighbors: ***Note:*** WARNING: The lock command locks out all the OSPF neighbors that have been configured on a virtual router, not just the one that may be having problems.	"Monitoring the OSPF configuration" "Locking and unlocking the OSPF component"	*NN10600-801 Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*

Corrective action procedures

Use the following corrective action procedures in this chapter for all Carrier Voice over IP solutions as directed by the problem task tables.

Note: These procedures cannot be used as GNTS stand-alone procedures; they must only be used in the context of the task lists found in the remainder of this document.

- "Common corrective action procedures" (page 121)
- "PT-AAL1/UA-AAL1 corrective action procedures" (page 174)
- "UA-IP/PT-IP corrective action procedures" (page 183)

Common corrective action procedures

The following corrective action procedures are common to all Carrier Voice over IP solutions:

- "Correcting data collection problems" (page 122)
- "Correcting file system problems" (page 124)
- "Correcting provisioning view problems" (page 124)
- "Correcting line automatic protection switching problems" (page 126)
- "Correcting network clock synchronization problems" (page 129)
- "Correcting fabric firmware problems" (page 131)
- "Collecting crash data" (page 131)
- "Correcting problems with the Multiservice Switch software and patches" (page 136)
- "Correcting problems with Multiservice Data Manager servers" (page 137)
- "Verifying the status of the link layer" (page 142)
- "Testing Vt1dot5 links" (page 172)

Correcting data collection problems

The following procedures are related to correcting data collection problems:

- "Verifying that spooling is activated" (page 122)
- "Displaying data collection configuration" (page 122)
- "Displaying the agentQueueSize configuration" (page 123)
- "Verifying that raw data from the node is spooling to the server" (page 123)
- "Verifying that BDF conversion is taking place" (page 123)

Verifying that spooling is activated

Step	Action
1	On the node, in operational mode, verify that spooling is activated: `display -p collector/* spooler spooling` If the value of the spooling attribute is "on" for the specific type of data (alarm, scn, log or debug), then spooling is activated.
2	This procedure is complete.

—End—

Displaying data collection configuration

Step	Action
1	On the node, in operational mode, display data collection information for the spooling filename: `display Collector/* Spooler spooling`
2	Display current data collection configuration: `display LogicalProcessor/* Engineering DataStream/*`
3	This procedure is complete.

—End—

Displaying the agentQueueSize configuration

Step	Action
1	On the node, verify that the logical processor agentQueueSize is non-zero: **`display LogicalProcessor/* Engineering DataStream/*`**
2	This procedure is complete.

—End—

Verifying that raw data from the node is spooling to the server

Step	Action
1	On the Multiservice Data Manager server, change to the following directory: **`cd /opt/MagellanMDP/data/mdp/spool`**
2	Verify that the BDF data files are collecting in this directory.
3	This procedure is complete.

—End—

Verifying that BDF conversion is taking place

Step	Action
1	On the Multiservice Data Manager server, access the following directories: `/opt/MagellanMDP/data/mdp/dump/alarms` `/opt/MagellanMDP/data/mdp/dump/log` `/opt/MagellanMDP/data/mdp/dump/scn`
2	Verify that the BDF conversion is taking place by looking for entries in the files. When files are collecting in these directories, it means that the source files are being converted to BDF format.
3	This procedure is complete.

—End—

Correcting file system problems

The following procedures are related to correcting file system problems:

- "Correcting a control processor disk full problem" (page 124)

Correcting a control processor disk full problem

Step	Action
1	On the node, determine the control processor disk usage: `display Filesystem usage` If the value returned for the control processor disk usage is 90% full, remove old provisioning and software files.
2	Remove old provisioning files: `tidy prov` For more information on the tidy prov command, and the time needed to execute it, see *NN10600-050 Nortel Multiservice Switch 7400/15000/20000 Command Reference*.
3	Identify old software files that can be removed: `tidy -query Software`
4	Remove old software files: `tidy Software` For more information on the *tidy sw* command, see *NN10600-050 Nortel Multiservice Switch 7400/15000/20000 Command Reference*. ***Note:*** It takes several hours to run the tidy software command. Ensure that you want to do it, as it uses node resources, and you cannot do anything with the file system while it is running.
5	This procedure is complete.

—End—

Correcting provisioning view problems

The following procedures are related to correcting provisioning problems:

- "Isolating a portable provisioning view problem" (page 125)
- "Reloading a provisioning view" (page 125)

Isolating a portable provisioning view problem

Step	Action
1	On the node, determine the name of the current committed file: `display Provisioning`
2	In operational mode, verify that the provisioning view contains both portable and view files: `ls -p("Provisioning/<committed_view_name>") fs`
3	Check that the provisioning view contains both portable and view files.
4	This procedure is complete.

—End—

Variable values

Variable	Value
<committed_view_name>	The name of the committed view.

Reloading a provisioning view

Step	Action
1	On the node, in operational mode, list all of the provisioning views: `list Provisioning view/*`
2	Change to provisioning mode: `start prov`
3	Use the load command to load the required provisioning view: `load -file(<file_name>) Prov`
4	This procedure is complete.

—End—

Variable values

Variable	Value
<file_name>	The name of the file containing the saved provisioning view.

Correcting line automatic protection switching problems

The following procedures are related to correcting line automatic protection switching (LAPS) problems:

- "Verifying correct functionality of LAPS protected interfaces" (page 126)
- "Determining the active function processor and the active lines" (page 127)
- "Switching from the active function processor to the standby function processor" (page 128)
- "Switching between the active lines and the lines providing equipment protection" (page 128)
- "Identifying line automatic protection switching mode mismatch problems" (page 129)

Verifying correct functionality of LAPS protected interfaces

To test the protection of Nortel Multiservice Switch PNNI/UNI interfaces that use LAPS, a protection switch must be initiated. This consists of locking or physically disconnecting each near end LP SONET port, followed by verification that PNNI/UNI stays up. For example, to test functionality of laps/xy, which was working line lp/x sonet/y and protection line lp/x+1 sonet/y, perform the following procedure.

Step	Action
1	Disconnect the fibers from laps/xy working line (lp/x sonet/y) or enter the following command from the Command Console to disable this SONET port: **DISABLENEXTcmdchk** **lock -force lp/x sonet/y**
2	Confirm that PNNI/UNI signaling stays enabled. Enter one of following commands to confirm that the OSI state is "unlocked, enabled, active" with non-zero "currentConnections": **d -o atmif/xy uni sign** **d -o atmif/xy pnni sign**

3 If PNNI/UNI is disabled, reconnect the fibers or issue the following command to enable the SONET port:

```
unlock lp/x sonet/y
```

4 If PNNI/UNI is disabled by removing/locking lp/x sonet/y, reconnect/unlock lp/x sonet/y, and verify the integrity of end-to-end fiber connectivity of lp/x+1 sonet/y. Also verify that the transport equipment is correctly configured to support 1+1 unidirectional linear APS.

5 Repeat step 1 to step 4 for laps/xy protection line (Lp/x+1 sonet/y).

6 This procedure is complete.

—End—

Determining the active function processor and the active lines

Step	Action

1 On the node, list the function processors (FPs) that are in-service:

```
display Shelf Card/* SparedServices
```

The following shows a sample output using this command:

```
7> display Shelf Card/* SpServ

-------------------------------------------------------------------------------------------
|Card|osiAdmin|osiOper|osiUsage|osiAvail|osiProc |osiCntrl |osiAlarm |osiStby  |osiUnknw
-------------------------------------------------------------------------------------------
|0   |unlck   |ena    |activ   |        |        |         |         |cold     |false
|1   |unlck   |ena    |activ   |        |        |         |         |serv     |false
|2   |unlck|ena|activ|||||hot|false
|3   |unlck|ena|activ|||||serv|false
|8   |unlck|ena|activ|||||serv|false
|9   |unlck   |ena    |activ   |        |        |         |         |hot      |false
```

2 Display and note the line automatic protection switching (LAPS) line configuration:

```
display Laps/* workingline, protectionLine
```

3 This procedure is complete.

—End—

Switching from the active function processor to the standby function processor

Step	Action

1 On the node, change from the in-service function processor (FP) to the standby FP:

```
DISABLENEXTcmdchk

switchover LogicalProcessor/<x>
```

CAUTION
Potential loss of service
Performing a switchover causes minimal traffic loss (<100milliseconds). See "Verifying a switchover between a main FP and its spare" in *NN10600-520 Nortel Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting* for more information.

2 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The name of currently active function processor.

Switching between the active lines and the lines providing equipment protection

Step	Action

1 On the node, in operational mode, switch from the active lines to the lines providing equipment protection:

```
DISABLENEXTcmdchk

switch -force workingToProtection Laps/<xy>
```

2 Switch from the lines providing equipment protection lines to active lines:

```
DISABLENEXTcmdchk

switch -force protectionToWorking Laps/<xy>
```

3 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The card number of the working line.
<y>	The port number of the working line.

Identifying line automatic protection switching mode mismatch problems

Step	Action
1	On the node, in operational mode, clear any alarms raised on the line automatic protection switching (LAPS) component: **clear Laps/<xy>**
2	Display the *modeMismatchAlarm* attribute and confirm that the alarm is turned off: **display Laps/<xy> modeMismatchAlarm**
3	Confirm that the mode (uni or bidirectional) is the same at both ends of the connection: **display -prov Laps/<xy> mode**
4	If the mode is not the same at both ends, reconfigure the connection.
5	This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The card number of the working line.
<y>	The port number of the working line.

Correcting network clock synchronization problems

The following procedures are related to correcting synchronization problems:

- "Monitoring the network clock synchronization state of the node" (page 130)

Monitoring the network clock synchronization state of the node

Step	Action

1 On the node, while in operational mode, review the network clock synchronization configuration:

```
display -p NetworkSynchronization
```

2 In operational mode, review the network clock synchronization configuration:

```
display NetworkSynchronization
```

The following shows a sample output using this command:

```
13> display NetworkSynchronization

adminState = unlocked
operationalState = enabled
usageState       = busy
clockSyncState   = synchronized
activeReference  = Lp/0 EDS1/0
standbyReference =

ok              2001-08-21 12:42:42.85
```

The *clockSyncState* attribute should be synchronized.

3 In operational mode, examine each port for alarms:

```
display LogicalProcessor/0 eds1/0
display LogicalProcessor/0 eds1/1
```

The following shows a sample output using this command:

```
13> display LogicalProcessor/0 eds1/0

Lp/0 EDS1/0
snmpOperStatus = up
adminState     = unlocked
operationalState = enabled
usageState       = active
availabilityStatus =
proceduralStatus   =
controlStatus      =
alarmStatus        =
standbyStatus      = notSet
unknownStatus      = false
losAlarm           = off
lofAlarm           = off
rxAisAlarm = off

ok              2001-08-21 12:42:42.85
```

The *losAlarm*, *lofAlarm*, and *rxAisAlarm* attributes should be *off*. If they are *on*, investigate these alarms.

4 While in operational mode, display the clocking source for each port:

```
display LogicalProcessor/* Sonet/* clock
```

5 Verify that the clocking source is set to *module*.

For more information on setting the clocking source to *module*, see "Configuring network clock synchronization for a DS3 or E3 FP" in *NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.

6 This procedure is complete.

—End—

Correcting fabric firmware problems

The following procedures are related to correcting fabric firmware problems:

- "Identifying the firmware that is installed on the fabric card" (page 131)

Identifying the firmware that is installed on the fabric card

Step	Action
1	On the Nortel Multiservice Switch 15000 / Media Gateway 15000 node, verify the fabric card firmware version in use: `display Shelf FabricCard/<n> banks`
2	Verify the version of fabric card firmware that is recommended: `display Shelf FabricCard/<n> recommended VersionToInstall`
3	If the versions do not match, install the new version of firmware.
4	This procedure is complete.

—End—

Variable values

Variable	Value
<n>	The fabric card identifier.

Collecting crash data

The following procedures are related to collecting data following the crash of a node:

- "Isolating the problem that causes a crash" (page 132)

Isolating the problem that causes a crash

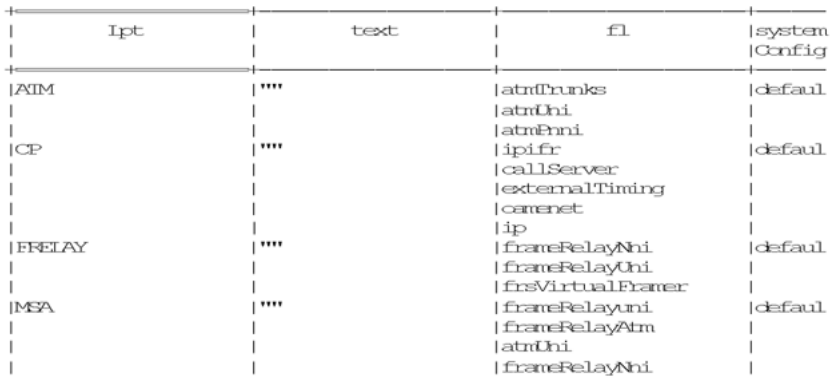
Step	Action
1	Collect alarm and SCN entries for the hour preceding the crash for the affected node using the BDF Viewer tool.
2	Collect security log information on the most recent provisioning or service changes made to the node. Note any operator activities that occurred on the node during or just prior to the crash. Use the BDF Viewer tool.
3	Collect information on any service disruption/degradation observed on the card either before or after the crash.
4	If this is not the first time a crash has occurred, collect information about previous crashes, including frequency and the time of day at which they occurred.
5	Capture data logged on the node during the crash. From the node command line enter the following commands: **display -notab Shelf Card/* diagnostics recoverableError line/*** The following is sample output using this command: `1 1|Recoverable Software error at line 856 in file pqc6CqmMgr.cc` `| 2|--- Reason ---` `| 3|Something wrong with ingress FFL length: 7000 7001` `| 4|` `| 5|CPU utilization: 100 percent busy CPU: powerPC Model number : 8` `| | (769-revision)` **display -notab Shelf Card/* diagnostics trapData line/*** The following is sample output using this command: `10|*** An exception has occurred at task level ***` `| 11|*** An exception has occurred at task level ***` `| 12|*** An exception has occurred at task level ***` `| 14|Unrecoverable Software error at line 16421 in file tadmIf.cc during` `| | interrupt 172 (0x000000ac), currenttask "PevTmrSrvc" (0x f6c36d0)`
6	At the node command line, capture card-specific data, such as CPU utilization, memory usage, and software features: **display -notab -prov LogicalProcessor/***

The following is sample output using this command:

```
Lp/0
mainCard = Shelf Card/0
spareCard = Shelf Card/1
logicalProcessorType = Sw Lpt/CP
linkToApplications =
customerIdentifier = 0
Lp/2
mainCard = Shelf Card/2
spareCard =
logicalProcessorType = Sw Lpt/ATM
linkToApplications =
customerIdentifier  = 0
```

display -prov Software LogicalProcessorType/*

The following is sample output using this command:



lpt	text	fl	systemConfig
ATM	""	atmTrunks	default
		atmUni	
		atmPnni	
CP	""	ipifr	default
		callServer	
		externalTiming	
		camenet	
		ip	
FRELAY	""	frameRelayNni	default
		frameRelayUni	
		frsVirtualFramer	
MSA	""	frameRelayuni	default
		frameRelayAtm	
		atmUni	
		frameRelayNni	

display -notab -oper LogicalProcessor/*

The following is sample output using this command:

```
Lp/0
adminState = unlocked
operationalState = enabled
usageState   = active
availabilityStatus=
proceduralStatus =
controlStatus  =
alarmStatus   =
standbyStatus  = providingService
unknownStatus        = false
activeCard = Shelf Card/0 mainCardStatus    = active
spareCardStatus = available
restartOnCpSwitch  = false
```

display -notab -oper Shelf Card/*

The following is sample output using this command:

```
Shelf Card/0
adminState = unlocked
operationalState = enabled
usageState = active
availabilityStatus =
proceduralStatus =
controlStatus =
alarmStatus =
standbyStatus = providingService
unknownStatus = false
currentLP = Lp/0
failureCause = none
selfTestFault = none
sparingConnectionStatus = notApplicable
hardwareAlarm = none
insertedCardType = CPeD
productCode = NTHW06CA-05
pmRevisionCode = NTHW17AA-05
imRevisionCode = N/A
serialNumber = NNTM03503U82
activeFirmwareVersion = CE0128A
inactiveFirmwareVersion = CD02S1A
memoryCapacity = fastRam : 0 kbyte
normalRam : 262144 kbyte
sharedRam : 0 kbyte
sharedMsgBlockCapacity = 2048 kbyte
localMsgBlockCapacity = 768 kbyte
timeInterval = 4 minutes
cpuUtil = 1 %
cpuUtilAvg = 1 %
cpuUtilAvgMin = 1 %
cpuUtilAvgMax = 1 %
memoryUsage = fastRam : 0 kbyte
normalRam : 61657 kbyte
sharedRam : 0 kbyte
memoryUsageAvg = fastRam : 0 kbyte
normalRam : 61657 kbyte
sharedRam : 0 kbyte
memoryUsageAvgMin = fastRam : 0 kbyte
normalRam : 61657 kbyte
sharedRam : 0 kbyte
memoryUsageAvgMax = fastRam : 0 kbyte
normalRam : 61657 kbyte
sharedRam : 0 kbyte
sharedMsgBlockUsage = 0 kbyte
```

7 At the node command line, capture shelf-specific data, such as current software and patch level, time since last outage, current committed file, list of function processors currently inserted, and CP disk status:

`display -current Software avList`

The following is sample output using this command:

```
avList = base_C00S1C

trunks_CC00S1C,
networking_CC00S1C,
ip_CC00S1C,
atmNetworking_CC00S1C,
frameRelay_CC00S1C,
fabric_CC00S1C
```

display -current Software patch

display -current -oper prov

The following is sample output using this command:

```
Prov
adminState = unlocked
operationalState = enabled
usageState    = idle
provisioningActivity = none
activityProgress   = n/a
standbyCpActivity = none
standbyCpActivityProgress = n/a
  committedFileName       =
OCALFLDBBB1_01252002.full.001
   currentViewFileName     =
OCALFLDBBB1_01252002.full.001
lastUsedFileName          =
OCALFLDBBB1_01252002.full.001
provisioningSession    =
provisioningUser       =none
checkRequired          =no
confirmRequired          =no
  editViewName                =
OCALFLDBBB1_01252002.full.002
editViewAddedComponents = 0
editViewDeletedComponents = 0
editViewChangedComponents = 0
ok
```

display -current -oper fs

The following is sample output using this command:

```
Fs
adminState = unlocked
operationalState = enabled
usageState    = active
volumeName    = OCALFLDBBB1
activeDisk = Fs Disk/0
syncStatus = synchronized
syncProgress = 100%
capacity   = 811122688 bytes
freeSpace   = 359333888 bytes
usage           = 55
```

8 This procedure is complete.

—End—

Correcting problems with the Multiservice Switch software and patches

The following procedures are related to correcting problems with Nortel Multiservice Switch / Media Gateway software and patches:

- "Isolating check prov problems" (page 136)

Note: For more information about auto-patching and the problems encountered, refer to "Auto-patching for MSS/MG15000 nodes from the MDM" in *NN10114-511 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier Voice over IP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP/PT-IP/PT-AAL2*.

Isolating check prov problems

Step	Action
1	On the node, determine which versions of software are available: **`list Software ApplicationVersion/*`** ***Note:*** To view the versions of the software, go to www.nortel.com. Click the Software link for the specified product documentation.
2	Determine which version of the software is currently active by displaying the application version list: **`display Software AvList`** The release is indicated by the version number after the underscore. If the system displays applications with versions of *CD02xx* or higher, the node has already been upgraded. ***Note:*** Your node may have a different list of software application versions. The following shows a sample output using this command: `PROV 2> d Sw Avl` `Sw` `avList = base_CD02A, ip_CD02A,` `networking_CD02A, atmNetworking_CD02A,` `ok 2001-08-10 10:21:06.75`
3	Determine what patches to application versions are currently available:

```
list Software ApplicationVersion/* Patch/*
```

4 Determine which patches are currently active by displaying the patch list:

```
display Software PatchList
```

Note: To view the current patch list, go to www.nortel.com Click the Software link for the specified product documentation.

5 Determine which features and logical processors have been configured for each logical processor type (LPT):

```
display Software LogicalProcessorType/*
featureList,logicalProcessors
```

6 Ensure that the features that are configured for each logical processor are supported in the solution.

7 This procedure is complete.

—End—

Correcting problems with Multiservice Data Manager servers

The following procedures are related to correcting problems with Nortel Multiservice Data Manager servers:

- "Verifying connectivity using the PING command" (page 137)
- "Verifying connectivity to a remote host" (page 138)
- "Adding and starting the pserver process" (page 139)
- "Verifying that the pserver process is running" (page 140)
- "Using the snoop commands to check for data transfer" (page 141)

Verifying connectivity using the PING command

The PING command can be used to test connectivity between Nortel Multiservice Data Manager (MDM) servers and the higher-level management systems, between the higher-level management systems and the OSS, and between Nortel Multiservice Switch / Media Gateway equipment and Multiservice Data Manager servers.

The PING command is used to test IP connectivity to a destination IP address. This is done by sending an ICMP query packet to the destination address. If the destination host can be reached, the packet is returned.

Step	Action
1	On the server, start a session in Solaris.
2	Ping a remote host: `ping <-RDdfnqrvL> <-c count> <-i wait> <-l preload><-I a.b.c.d> <-T ttl> <-p pattern> <-s packetsize> host <data size> <npackets>` For example: • To ping a remote host use: `ping 47.73.7.67`
3	The following example command is displayed when the PING command is successful: `47.73.7.67 is alive.` ***Note:*** If the command replies with a "network or host unreachable message", go to and complete procedure, "Verifying connectivity to a remote host" (page 138). Otherwise, go to complete procedure, "Adding and starting the pserver process" (page 139).
4	To stop the PING command: `CTRL-C`
5	This procedure is complete.

—End—

Verifying connectivity to a remote host

The TRACEROUTE command can be used to test connectivity between the node and the higher-level management system, and between the higher-level management system and Nortel Multiservice Data Manager servers.

Perform this procedure if the procedure "Verifying connectivity using the PING command" (page 137) failed or the host was unreachable.

Step	Action
1	On the server, start a session in Solaris.
2	Traceroute a remote host: `traceroute [ -adFIlnSvx ] [ -A addr_family ] [ -c traffic_class ] [ -f first_hop ] [ -g gateway ]`

```
[ -i iface ] [ -L flow_label ] [ -m max_hop  ]
[ -P pause_sec ] [ -p port ] [ -Q max_timeout]
[-q nqueries] [ -s src_addr] [ -t tos ] [-w
wait_time] host [packetlen]
```

For example:

- To traceroute a remote host use:

  ```
  traceroute 47.73.7.67
  ```

3 Traceroute stops automatically when it either reaches the destination IP address, times out trying to reach this address, or the maximum number of hops is reached. To interrupt the execution of this command type

```
CTRL-C
```

4 This procedure is complete.

—End—

Adding and starting the pserver process

Step	Action

1 On the server, in the Server Administration window, select *Authorize* from the Edit menu.

The Server Administration dialog for new servers opens.

2 If required, enter the password and click OK.

3 In the Server Administration window, select *New Server* from the Edit menu.

4 In the New Server Selection window, click *Other->Empty server template*.

5 In the Descriptive name field, enter a unique name containing the text string **`pserver`**. Include **`pserver`** in the name to be able to verify that the server is running under this name.
The server name can be up to 22 characters long and cannot already be listed in the Server Name list in the Server Administration window.

6 In the Startup command field, enter the following:

```
/opt/MagellanNMS/bin/pserver -m -e 3197
/opt/MagellanNMS/bin/gmdrapi -h localhost
```

The command line option *-m* tells the pserver to manage any spawned processes. The command line option *-e* tells the pserver to spawn all processes with an execvp instead of through a shell. Specifying both of these commands ensures that all spawned processes are shut down when the pserver shuts down or is stopped for any reason.

The *3197* value represents the default pserver port number. If you use the default port number, you will minimize the downtime needed to establish the interface between the pserver and the node's fault handling application on the higher level management system.

If you need to use a port number other than the default, you must choose a value in the range of 1025 to 4999 inclusively. As well, the port number you enter here must be identical to the port number selected when the node's fault handling application was configured.

7 Select the *Automatic startup at reboot time* option.

8 Leave the default settings for the remaining options in the dialog.

9 Click *Save and Start* to close the dialog.

10 Verify that you configured the pserver process correctly. See "Adding and starting the pserver process" (page 139).

11 Verify that the server is running. See "Correcting problems with Multiservice Data Manager servers" (page 137).

12 Verify that the CS2000 Core Manager is receiving node information from the server. See the CS2000 Core Manager documentation suite for more information.

13 This procedure is complete.

—End—

Verifying that the pserver process is running

Step	Action

1 On the server, in the xterm window, verify that the pserver process is running:

```
ps -ef | grep pserver
```

An example of the information returned by the system is as follows:

```
root 3064 222 0 11:03:06 pts/0 0:00 grep pserver
root 2937 271 0 11:02:00 ?  0:00 pserver 3197
/opt/MagellanNMS/bin/gmdrapi
```

```
-h localhost
```

2 Open the Multiservice Data Manager window:

```
/opt/MagellanNMS/bin/nmstool &
```

The copyright dialog and the Multiservice Data Manager window opens.

3 Click *OK* to close the copyright dialog.

4 From the window, choose System > Administration > Server Administration.

The Server Administration window opens.

5 In the Server Administration window, select *Refresh server list* from the File menu.

The status of the servers updates.

6 In the server list, click on the pserver.

The information for the server becomes highlighted to indicate that the server is selected.

7 From the Edit menu, select *View*.

The Server Administration dialog to view servers opens. In this dialog, the Server name indicates the descriptive name assigned to the server. State indicates the state of the server.

8 Verify that the pserver is in a *Running* state.

9 This procedure is complete.

—End—

Using the snoop commands to check for data transfer

Step	Action

1 On the server, start a session in Solaris.

2 Enter the following command:

```
snoop -h
```

3 Enter the following command:

```
snoop <port#>
```

If data is passing on the port, the passing data is shown as output in real time.

4 This procedure is complete.

—End—

Variable values

Variable	Value
<port#>	The number of the port that you are checking for data transfer.

Verifying the status of the link layer

The following procedures are used to verify the status of the appropriate link layer:

- "Verifying the status of the SONET link layer" (page 142)
- "Verifying the status of the Vt1dot5 link layer" (page 150)
- "Verifying the status of the DS3 link layer" (page 153)
- "Verifying the status of the IMA link layer" (page 158)
- "Verifying the status of the Gigabit Ethernet link layer" (page 165)
- "Verifying the status of the Link Aggregation (LAG) layer" (page 168)
- "Verifying the status of the OAM Ethernet link layer" (page 171)

Verifying the status of the SONET link layer

There are two types of configured SONET links:

- LAPS (line automatic protection switching) protected
- PBG (port bridge group) protected (UA-AAL1 only)

LAPS protected SONET links

Step	Action
1	Verify the provisioned state of the LAPS protected SONET links: `display -prov Laps/<xy> workingline,protectionline` The following shows a sample output using this command for <x> = 2 and <y> = 01:

```
> display -prov Laps/201 workingline,protectionline
Laps/201
   workingLine = Lp/2 Sonet/1
   protectionLine = Lp/3 Sonet/1
```

2 Verify the OSI state of LAPS. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Laps/<xy> osistate

The following shows a sample output using this command for <x> = 2 and <y> = 01:

```
> display Laps/201 osistate
Laps/201
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the OSI state of the SONET path layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Laps/<xy> Sts/0 osistate

The following shows a sample output using this command for <x> = 2 and <y> = 01:

```
> display Laps/201 Sts/0 osistate
Laps/201 Sts/0
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

4 Verify the operational state of the SONET path layer. The fields "lopAlarm", "rxAisAlarm", "rxRfiAlarm", "signalLabelMismatch",

"txAis", and "txRdi" should have the value "off" under normal operation.

display Laps/<xy> Sts/0 operational

The following shows a sample output using this command for <x> = 2 and <y> = 01:

```
> display Laps/201 Sts/0 operational
Laps/201 Sts/0
   lopAlarm = off
   rxAisAlarm = off
   rxRfiAlarm = off
   signalLabelMismatch = off
   txAis               = off
   txRdi               = off
```

5 Execute the following command twice to verify that the SONET path statistics are incrementing normally. The only fields that should be incrementing under normal operation are "pathErrorFreeSec" and "farEndPathErrorFreeSec".

display Laps/<xy> Sts/0 statistics

The following shows a sample output using this command for <x> = 2 and <y> = 01:

```
> display Laps/201 Sts/0 statistics
Laps/201 Sts/0
   pathErrorFreeSec = 6693
   pathCodeViolations = 0
   pathErroredSec     = 0
   pathSevErroredSec  = 0
   pathAisLopSec      = 0
   pathUnavailSec     = 0
   pathFailures       = 0
   farEndPathErrorFreeSec = 6693
   farEndPathCodeViolations = 0
   farEndPathErroredSec     = 0
   farEndPathSevErroredSec  = 0
   farEndPathAisLopSec      = 0
   farEndPathUnavailSec     = 0
   farEndPathFailures       = 1
```

6 Verify the operation of the SONET line and section layer for a single interface/port. Repeat the commands for the mate port <x+1>.

Use the following command to verify the OSI state of the SONET link layer. The key fields "adminState", "operationalState", and "alarmStatus should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> Sonet/<y> osistate

The following shows a sample output using this command for <x> = 2 and <y> = 1:

```
> display Lp/2 Sonet/1 osistate
Lp/2 Sonet/1
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

Use the following command to verify the operational state of the SONET link layer. The key fields "losAlarm", "lofAlarm", "rxAisAlarm", "rxRfiAlarm", "unusableTxClockRefAlarm", "txAis", and "txRdi" should have the value "off" under normal operation.

display Lp/<x> Sonet/<y> operational

The following shows a sample output using this command for <x> = 2 and <y> = 1:

```
> display Lp/2 Sonet/1 operational
Lp/2 Sonet/1
   losAlarm = off
   lofAlarm = off
   rxAisAlarm = off
   rxRfiAlarm = off
   unusableTxClockRefAlarm = off
   txAis                   = off
   txRdi                   = off
   s1Rx                    = 0
```

Execute the following command twice to verify that the SONET section and line statistics are incrementing normally. The only fields that should be incrementing under normal operation are "runningTime", "errorFreeSec", and "farEndLineErrorFreeSec".

display Lp/<x> Sonet/<y> statistics

The following shows a sample output using this command for <x> = 2 and <y> = 1:

```
> display Lp/2 Sonet/1 statistics
Lp/2 Sonet/1
   runningTime = 5121
   errorFreeSec = 5121
   sectCodeViolations = 0
   sectErroredSec     = 0
   sectSevErroredSec  = 0
   sectLosSec         = 0
   sectSevErroredFrmSec = 0
   sectFailures         = 0
   lineCodeViolations   = 0
   lineErroredSec       = 0
   lineSevErroredSec    = 0
   lineAisSec           = 0
   lineUnavailSec       = 0
   lineFailures         = 0
   farEndLineErrorFreeSec = 5121 seconds
   farEndLineCodeViolations = 0
   farEndLineErroredSec     = 0
   farEndLineSevErroredSec  = 0
   farEndLineAisSec         = 0
   farEndLineUnavailSec     = 0
   farEndLineFailures       = 0
```

If any abnormal operation is found, return to the step "Verify the operation of the physical layer." in "SONET link failures" (page 26).

7 This procedure is complete.

—End—

PBG protected SONET links (UA-AAL1 solutions only)

Step	Action

1 Verify the provisioned state of the PBG protected SONET links:

`display -prov Pbg/<xy>`

The following shows a sample output using this command for <x> = 14 and <y> = 06:

```
> display -prov Pbg/1406
Pbg/1406
   customerIdentifier = 0
   workingLine        = Lp/14 Sonet/6
   bridgeLine         = Lp/15 Bso/6
```

2 Verify the OSI state of the PBG. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Pbg/<xy> osistate

The following shows a sample output using this command for <x> = 14 and <y> = 06:

```
> display Pbg/1406 osistate
Pbg/1406
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the OSI state of the PBG path layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Pbg/<xy> Sts/0 osistate

The following shows a sample output using this command for <x> = 14 and <y> = 06:

```
> display Pbg/1406 Sts/0 osistate
Pbg/1406 Sts/0
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

4 Verify the operational state of the PBG path layer. The fields "lopAlarm", "rxAisAlarm", "rxRfiAlarm", "signalLabelMismatch", "txAis", and "txRdi" should have the value "off" under normal operation.

display Pbg/<xy> Sts/0 operational

The following shows a sample output using this command for <x> = 14 and <y> = 06:

```
> display pbg/1406 Sts/0 operational
Pbg/1406 Sts/0
   lopAlarm = off
   rxAisAlarm = off
   rxRfiAlarm = off
   signalLabelMismatch = off
   txAis               = off
   txRdi               = off
```

5 Execute the following command twice to verify that the PBG path statistics are incrementing normally. The only fields that should be incrementing under normal operation are "pathErrorFreeSec" and "farEndPathErrorFreeSec".

display Pbg/<xy> Sts/0 statistics

The following shows a sample output using this command for <x> = 14 and <y> = 06:

```
> display Pbg/1406 Sts/0 statistics
Pbg/1406 Sts/0
   pathErrorFreeSec = 524587
   pathCodeViolations = 149
   pathErroredSec     = 21
   pathSevErroredSec  = 18
   pathAisLopSec      = 17
   pathUnavailSec     = 0
   pathFailures       = 2
   farEndPathErrorFreeSec = 524587
   farEndPathCodeViolations = 9
   farEndPathErroredSec     = 4
   farEndPathSevErroredSec  = 0
   farEndPathAisLopSec      = 0
   farEndPathUnavailSec     = 0
   farEndPathFailures       = 0
```

6 Verify the OSI state of the bridged SONET link layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> Bso/<y> osistate

The following shows a sample output using this command for <x> = 15 and <y> = 6:

```
> display Lp/15 Bso/6 osistate
Lp/15 Bso/6
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

7 Execute the following command twice to verify that the SONET section and line statistics are incrementing normally. The only fields that should be incrementing under normal operation are "runningTime", "errorFreeSec", and "farEndLineErrorFreeSec".

display Lp/<x> Sonet/<y> statistics

The following shows a sample output using this command for <x> = 14 and <y> = 6:

```
> display Lp/14 Sonet/6 statistics
Lp/14 Sonet/6
   runningTime = 5121
   errorFreeSec = 5121
   sectCodeViolations = 0
   sectErroredSec     = 0
   sectSevErroredSec  = 0
   sectLosSec         = 0
   sectSevErroredFrmSec = 0
   sectFailures         = 0
   lineCodeViolations   = 0
   lineErroredSec       = 0
   lineSevErroredSec    = 0
   lineAisSec           = 0
   lineUnavailSec       = 0
   lineFailures         = 0
   farEndLineErrorFreeSec = 5121 seconds
   farEndLineCodeViolations = 0
   farEndLineErroredSec     = 0
   farEndLineSevErroredSec  = 0
   farEndLineAisSec         = 0
   farEndLineUnavailSec     = 0
   farEndLineFailures       = 0
```

If any abnormal operation is found, return to the step "Verify the operation of the physical layer." in "SONET link failures" (page 26).

8 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of the configured port, starting from 0.

Verifying the status of the Vt1dot5 link layer

There are two aspects that need to be verified:

- Vt1dot5 link layer
- the DS1 underlying the Vt1dot5 layer

For the Vt1dot5 layer:

Step	Action
1	Verify the OSI state of the Vt1dot5 layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation. **display Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> osistate** The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3: `display Laps/1200 Sts/2 Vt1dot5/6,3 osistate` `Laps/1200 Sts/2 Vt1dot5/6,3` `  adminState = unlocked` `  operationalState = enabled` `  usageState = busy` `  availabilityStatus =` `  proceduralStatus =` `  controlStatus =` `  alarmStatus =` `  standbyStatus = notSet` `  unknownStatus = false`
2	Verify the operational state of the Vt1dot5 layer. The fields "rxAisAlarm", "rxRdiAlarm", "rxRfiAlarm", "unequippedAlarm", "traceIdMismatchAlarm", "lopAlarm", "txAis", and "txRdi" should have the value "off" under normal operation. **display Laps/<xy> sts/<n> Vt1dot5/<l>,<m> operational** The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 operational
Laps/1200 Sts/2 Vt1dot5/6,3
   rxAisAlarm = off
   rxRdiAlarm = off
   rxRfiAlarm = off
   unequippedAlarm = off
   traceIdMismatchAlarm = off
   lopAlarm             = off
   txAis                = off
   txRdi                = off
```

3 Execute the following command twice to verify that the Vt1dot5 statistics are incrementing normally. The only fields that should be incrementing under normal operation are "pathErrorFreeSec" and "farEndPathErrorFreeSec".

display Laps/<xy> sts/<n> Vt1dot5/<l>,<m> statistics

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 statistics
Laps/1200 Sts/2 Vt1dot5/6,3
   pathErrorFreeSec = 38933
   pathCodeViolations = 0
   pathErroredSec     = 0
   pathSevErroredSec  = 0
   pathAisLopSec      = 0
   pathUnavailSec     = 0
   pathFailures       = 0
   farEndPathErrorFreeSec = 38933
   farEndPathCodeViolations = 0
   farEndPathErroredSec     = 0
   farEndPathSevErroredSec  = 0
   farEndPathAisLopSec      = 0
   farEndPathUnavailSec     = 0
   farEndPathFailures       = 0
```

4 This procedure is complete.

—End—

For the DS1 underlying the Vt1dot5 layer:

Step	Action
1	Verify the OSI state of the DS1. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1 osistate

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 DS1 osistate
Laps/1200 Sts/2 Vt1dot5/6,3 DS1
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

2 Verify the operational state of the DS1 layer. The fields "rxAisAlarm", "lofAlarm", "rxRaiAlarm", "txAisAlarm", and "txRaiAlarm" should have the value "off" under normal operation.

display Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1 operational

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 DS1 operational
Laps/1200 Sts/2 Vt1dot5/6,3 DS1
   rxAisAlarm = off
   lofAlarm   = off
   rxRaiAlarm = off
   txAisAlarm = off
   txRaiAlarm = off
```

3 Execute the following command twice to verify that the DS1 statistics are incrementing normally. The only fields that should be incrementing under normal operation are "runningTime" and "errorFreeSec".

display Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1 statistics

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 ds1 statistics
Laps/1200 Sts/2 Vt1dot5/6,3 DS1
   runningTime = 39494
   errorFreeSec = 39494
   erroredSec    = 0
   sevErroredSec = 0
   sevErroredFrmSec = 0
   unavailSec       = 0
   crcErrors        = 0
   frmErrors        = 0
   slipErrors       = 0
```

If any abnormal operation is found in these corrective action procedures, return to the step "Verify the operation of the physical layer" in "Vt1dot5 link failures" (page 28).

4 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of the configured port, starting from 0.
<n>	The number (0,1, or 2) of the synchronous transport signal (STS) for the channelized OC3 TDM port.
<l>	The number of the virtual tributary group (VTG) in the STS. The range is 1 to 7.
<m>	The number of the virtual tributary equivalent to a DS1 (VT1.5) in the VTG. The range is 1 to 4.

Verifying the status of the DS3 link layer

Step	Action

1 On the node, check the state of card sparing for the 12pDS3Atm electrical FPs.

Determine the sparing configuration for the card:

display -prov Lp/<x>

The following shows a sample output using this command for <x> = 10:

```
> display -prov Lp/10
Lp/10
   mainCard = Shelf Card/10
   spareCard = Shelf Card/11
   logicalProcessorType = Sw Lpt/ATM10
   linkToApplications   =
   oneForNSparingBehavior = delayedSwitchOver
   customerIdentifier     = 0
```

Determine the state of the main card:

display shelf card/<x> sparedservices

The field "standbyStatus" should have the value "providingService" which means the electrical ports on the card are currently actively transmitting and receiving data.

The following shows a sample output using this command for <x> = 10:

```
> display shelf card/10 sparedservices
Shelf Card/10 SpServ
   adminState = unlocked
   operationalState = enabled
   usageState       = active
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = providingService
   unknownStatus      = false
```

Determine the state of the spared card:

display shelf card/<x+1> sparedservices

If the "availabilityStatus" of the "hotStandby" card is "degraded", then refer to "Sparing panel failures" (page 35) to correct problems with the sparing panel.

The following shows a sample output using this command for <x> = 10 and <y> = 0:

```
> display shelf card/11 sparedservices
Shelf Card/11 SpServ
   adminState = unlocked
   operationalState = enabled
   usageState       = active
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = hotStandby
   unknownStatus      = false
```

2 Verify the OSI state of the DS3 link layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> DS3/<y> osistate

The following shows a sample output using this command for <x> = 10 and <y> =0:

```
> display Lp/10 DS3/0 osistate
Lp/10 DS3/0
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the operational state of the DS3 link layer. The fields "losAlarm", "lofAlarm", "rxAisAlarm", "rxRaiAlarm", "rxIdle", "txAis", "txRai", and "txIdle" should have the value "off" under normal operation.

display Lp/<x> DS3/<y> operational

The following shows a sample output using this command for <x> = 10 and <y> =0:

```
> display Lp/10 DS3/0 operational
Lp/10 DS3/0
   losAlarm = off
   lofAlarm = off
   rxAisAlarm = off
   rxRaiAlarm = off
   rxIdle     = off
   txAis      = off
   txRai      = off
   txIdle     = off
```

4 Execute the following command twice to verify that the DS3 line and path statistics are incrementing normally. The only fields that should be incrementing under normal operation are "runningTime" and "errorFreeSec".

display Lp/<x> DS3/<y> statistics

The following shows a sample output using this command for <x> = 10 and <y> = 0:

```
> display Lp/10 DS3/0 statistics
Lp/10 DS3/0
   runningTime = 363055 seconds
   errorFreeSec = 363055
   lineCodeViolations = 0
   lineErroredSec     = 0
   lineSevErroredSec  = 0
   lineLosSec         = 0
   lineFailures       = 0
   pathCodeViolations = 0
   pathErroredSec     = 0
   pathSevErroredSec  = 0
   pathSefAisSec      = 0
   pathUnavailSec     = 0
   pathFailures       = 0
```

5 Verify the operational state of the DS3 Cbit framing. The field "farEndAlarm" should be "none" and the fields "loopbackAtFarEndRequested" and "loopedbackTofarEnd" should be blank under normal operation.

display Lp/<x> DS3/<y> CBit operational

The following shows a sample output using this command for <x> = 10 and <y> = 0:

```
> display Lp/10 DS3/0 Cbit operational
Lp/10 DS3/0 CBit
   farEndAlarm = none
   loopbackAtFarEndRequested =
   loopedbackToFarEnd        =
```

6 Execute the following command twice to verify that the DS3 Cbit path statistics are incrementing normally. The only fields that should be incrementing under normal operation are "cbitErrorFreeSec" and "farEndErrorFreeSec".

```
display Lp/<x> DS3/<y> CBit statistics
```

The following shows a sample output using this command for <x> = 10 and <y> =0:

```
> display Lp/10 DS3/0 CBit statistics
Lp/10 DS3/0 CBit
   cbitErrorFreeSec = 363382
   cbitCodeViolations = 0
   cbitErroredSec     = 0
   cbitSevErroredSec  = 0
   cbitUnavailSec     = 0
   farEndErrorFreeSec = 363382
   farEndCodeViolations = 0
   farEndErroredSec     = 0
   farEndSevErroredSec  = 0
   farEndSefAisSec      = 0
   farEndUnavailSec     = 0
   farEndFailures       = 1
```

If any abnormal operation is found in this corrective action procedure, return to the step "Verify the operation of the physical layer." in "DS3 link failures" (page 29).

7 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of the configured port, starting from 0.

Verifying the status of the IMA link layer

Step	Action
1	On the node, check the state of card sparing for the 4pDS3ChAtm electrical FPs. Determine the sparing configuration for the card: **display -prov Lp/<x>** The following shows a sample output using this command for <x> = 14: ``` > display -prov Lp/14 Lp/14 mainCard = Shelf Card/14 spareCard = Shelf Card/15 logicalProcessorType = Sw Lpt/ATM14 linkToApplications = oneForNSparingBehavior = delayedSwitchOver customerIdentifier = 0 ``` Determine the state of the main card. The field "standbyStatus" should have the value "providingService" which means the electrical ports on the card are currently actively transmitting and receiving data. **display shelf card/<x> sparedservices** The following shows a sample output using this command for <x> = 14: ``` > display shelf card/14 sps Shelf Card/14 SpServ adminState = unlocked operationalState = enabled usageState = active availabilityStatus = proceduralStatus = controlStatus = alarmStatus = standbyStatus = providingService unknownStatus = false ``` Determine the state of the spared card: **display shelf card/<x+1> sparedservices** If the "availabilityStatus" of the "hotStandby" card is "degraded", then refer to "Sparing panel failures" (page 35) to correct problems with the sparing panel.

The following shows a sample output using this command for <x> = 14:

```
> display shelf card/15 sps
Shelf Card/15 SpServ
   adminState = unlocked
   operationalState = enabled
   usageState       = active
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = hotStandby
   unknownStatus      = false
```

2 Verify the OSI state of the IMA link layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> DS3/<y> IMA/<z> osistate

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display Lp/14 DS3/1 IMA/2 osistate
Lp/14 DS3/1 Ima/2
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the operational state of the IMA link layer. The key fields "failureCause" and "remoteDefect" have values of "noFailure" and "noDefect" respectively under normal operation. In addition, the field "remoteLidsActive" should be the same as the field "remoteLidsConfig"; otherwise a configured T1 has been lost.

display Lp/<x> DS3/<y> IMA/<z> operational

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display Lp/14 DS3/1 IMA/2 operational
Lp/14 DS3/1 Ima/2
   failureCause = noFailure
   remoteDefect = noDefect
   remoteLidsConfig = 1 2 3 4 5 6 7 8
   remoteLidsActive = 1 2 3 4 5 6 7 8
   cellCapacity     = 28740 cell/s
   remoteGid        = 3
   clockingModeMismatch = no
   activeProtocol       = atmForum10
```

4 Execute the following command twice to verify that the IMA statistics are incrementing normally. The only field that should be incrementing under normal operation is "runningTime".

display Lp/<x> DS3/<y> IMA/<z> statistics

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display Lp/14 DS3/1 IMA/2 statistics
Lp/14 DS3/1 Ima/2
   runningTime = 369178 seconds
   unavailSec  = 38
   failures    = 1
   receiveCellUtilization = 48 %
   transmitCellUtilization = 10 %
```

5 Verify the OSI state of the links under the IMA layer. The key fields "adminState" (osiAdmin), "operationalState" (osiOper), and "alarmStatus" (osiAlarm) should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> DS3/<y> IMA/<z> Lk/* osistate

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display Lp/14 DS3/1 IMA/2 Lk/* osistate

Lp/14 DS3/1 Ima/2 Lk/*
+==+------+----+-----+--------+--------+-------+--------+-----+---
|Lk|osiAd |osiO|osiUs |osiAvai|osiProc |osiCntr|osiAlar | osiS|osiUn
|  | min  |per | age |     l |        |     l |     m  | tby | knw
+==+------+----+-----+--------+--------+-------+--------+-----+---
| 1 |unlck | ena | busy |       |        |       |        | nSet | false
| 2 |unlck | ena | busy |       |        |       |        | nSet | false
| 3 |unlck | ena | busy |       |        |       |        | nSet | false
| 4 |unlck | ena | busy |       |        |       |        | nSet | false
| 5 |unlck | ena | busy |       |        |       |        | nSet | false
| 6 |unlck | ena | busy |       |        |       |        | nSet | false
| 7 |unlck | ena | busy |       |        |       |        | nSet | false
| 8 |unlck | ena | busy |       |        |       |        | nSet | false
```

6 Verify the operational state of the links under the IMA link layer. The key fields "failureCause" (cause) and "remoteDefect" (remDef) have values of "noFailure" and "noDefect" respectively under normal operation.

display Lp/<x> DS3/<y> IMA/<z> Lk/* operational

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display Lp/14 DS3/1 IMA/2 Lk/* operational

Lp/14 DS3/1 Ima/2 Lk/*
+====+--------+--------+----+----+--------+--------
|Lk  | cause  |remDef  |rem |    rel        | oif
|    |        |        |Lid |          msec|
+====+--------+--------+----+--------------+--------
| 1  | noFail | noDefe |  1 |            1 | noOif
| 2  | noFail | noDefe |  2 |            0 | noOif
| 3  | noFail | noDefe |  3 |            0 | noOif
| 4  | noFail | noDefe |  4 |            0 | noOif
| 5  | noFail | noDefe |  5 |            0 | noOif
| 6  | noFail | noDefe |  6 |            0 | noOif
| 7  | noFail | noDefe |  7 |            1 | noOif
| 8  | noFail | noDefe |  8 |            1 | noOif
```

7 Execute the following command twice to verify that the IMA link statistics are incrementing normally. The only field that should be incrementing under normal operation is "runningTime" (running seconds).

display Lp/<x> DS3/<y> IMA/<z> Lk/* statistics

The shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2:

```
> display lp/14 ds3/1 ima/2 lk/* statistics

Lp/14 DS3/1 Ima/2 Lk/*
  Use -noTabular to see hidden attributes: idle, rxStuff,
txStuff, iv, feUnavail and feSes.
+===+---------+-------+-------+---------+-------+-----
|Lk | running | uus   | ses   | unavail |  fail |  feUus
|   | seconds |       |       |         |       |
+===+---------+-------+-------+---------+-------+-----
| 1 |  369859 |    35 |     4 |       0 |     1 |    35
| 2 |  369859 |    35 |     4 |       0 |     1 |    35
| 3 |  369859 |    35 |     4 |       0 |     1 |    35
| 4 |  369859 |    35 |     4 |       0 |     1 |    35
| 5 |  369859 |    35 |     4 |       0 |     1 |    35
| 6 |  369859 |    35 |     3 |       0 |     1 |    34
| 7 |  369859 |    35 |     3 |       0 |     1 |    34
| 8 |  369859 |    35 |     3 |       0 |     1 |    34
```

8 This procedure is complete.

—End—

If a problem is detected with a particular link in an IMA group, check the underlying DS1 layer for problems.

Step	Action

1 Determine which DS1s have been provisioned to belong to the IMA group that is being investigated:

`display -prov Lp/<x> DS3/<y> IMA/<z> Lk/*`

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 2. In this example, the IMA group has eight DS1s (17 to 24) configured.

```
> display -prov Lp/14 DS3/1 IMA/2 lk/*

Lp/14 DS3/1 Ima/2 Lk/*
+====+--------------------+-------------------------
|Lk  |   interfaceName    | Response
+====+--------------------+-------------------------
|  1 | Lp/14 DS3/1 DS1/17 |
|    |  Chan/0            |
|  2 | Lp/14 DS3/1 DS1/18 |
|    |  Chan/0            |
|  3 | Lp/14 DS3/1 DS1/19 |
|    |  Chan/0            |
|  4 | Lp/14 DS3/1 DS1/20 |
|    |  Chan/0            |
|  5 | Lp/14 DS3/1 DS1/21 |
|    |  Chan/0            |
|  6 | Lp/14 DS3/1 DS1/22 |
|    |  Chan/0            |
|  7 | Lp/14 DS3/1 DS1/23 |
|    |  Chan/0            |
|  8 | Lp/14 DS3/1 DS1/24 |
|    |  Chan/0            |
```

2 Verify the OSI state of a DS1. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> DS3/<y> DS1/<z> osistate

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 19:

```
> display Lp/14 DS3/1 DS1/19 osistate
Lp/14 DS3/1 DS1/19
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the operational state of the DS1 layer. The fields "rxAisAlarm", "lofAlarm", "rxRaiAlarm", "txAisAlarm", and "txRaiAlarm" should have the value "off" under normal operation.

display Lp/<x> DS3/<y> DS1/<z> operational

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 19:

```
> display Lp/14 DS3/1 DS1/19 operational
Lp/14 DS3/1 DS1/19
   rxAisAlarm = off
   lofAlarm   = off
   rxRaiAlarm = off
   txAisAlarm = off
   txRaiAlarm = off
```

4 Execute the following command twice to verify that the DS1 statistics are incrementing normally. The only fields that should be incrementing under normal operation are "runningTime" and "errorFreeSec".

display Lp/<x> DS3/<y> DS1/<z> statistics

The following shows a sample output using this command for <x> = 14, <y> = 1, and <z> = 19:

```
> display Lp/14 DS3/1 DS1/19 statistics
Lp/14 DS3/1 DS1/19
   runningTime = 558
   errorFreeSec = 558
   erroredSec   = 0
   sevErroredSec = 0
   sevErroredFrmSec = 0
   unavailSec       = 0
   crcErrors        = 0
   frmErrors        = 0
   slipErrors       = 0
```

If any abnormal operation is found in this corrective action procedure, return to the step "Resolve IMA specific problems." in "IMA link failures" (page 31).

5 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).

Variable	Value
<y>	The number of the configured port, starting from 0.
<z>	The number of the IMA group, typically 0,1 or 2.

Verifying the status of the Gigabit Ethernet link layer

Step	Action

1 On the node, check the state of the 4pGE electrical FPs.

Determine the number of provisioned 4PGE FPs:

display -prov Lpgroup/* Lp/*

The following shows a sample output using this command to determine the provisioned Gigabit Ethernet cards:

```
> display -prov Lpgroup/* Lp/*

LpG/* Lp/*
+======+====+--------+--------------------------------
| LpG  | Lp |  mig   | Response
+======+====+--------+--------------------------------
|    7 | 14 | stayIn |
|    7 | 15 | moveTo |
```

Determine the provisioning of the FPs. Execute the following command for each FP identified:

display -prov Lp/<x>

The following shows a sample output using this command for <x> = 14:

```
> display -prov Lp/14
Lp/14
   mainCard = Shelf Card/14
   spareCard =
   logicalProcessorType = Sw Lpt/GE14
   linkToApplications   =
   oneForNSparingBehavior = delayedSwitchOver
   customerIdentifier     = 0
ok             2004-06-21 21:23:35.35
```

Verify the OSI state for the FPs. Execute the following command for each FP identified:

display Lp/<x> osistate

The following shows a sample output using this command for <x> = 14:

```
> display Lp/14 osistate
Lp/14
   adminState = unlocked
   operationalState = enabled
   usageState       = active
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = providingService
   unknownStatus      = false
```

2 Verify the OSI state of the Gigabit Ethernet link layer. The key fields "adminState", "operationalState", and "alarmStatus" should be "unlocked", "enabled", and blank respectively under normal operation.

display Lp/<x> Eth/<y> osistate

The following shows a sample output using this command for <x> = 14 and <y> = 1:

```
> display Lp/14 Eth/1 osistate
Lp/14 Eth/1
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

3 Verify the operational state of the Gigabit Ethernet link layer.

display Lp/<x> Eth/<y> operational

The following shows a sample output using this command for <x> = 14 and <y> =1:

```
> display Lp/14 Eth/1 operational
Lp/14 Eth/1
   failureCause = noFailure
   autoNegStatus = succeeded
   actualLineSpeed = 1000 Mbit/s
   actualDuplexMode = full
```

4 Execute the following command twice to verify that the Gigabit Ethernet link statistics are incrementing normally. Only the fields "framesTransmittedOk", "framesReceivedOk", "octetsTranmittedOk", and "octetsReceivedOk" should be incrementing under normal operation.

display Lp/<x> Eth/<y> statistics

The following shows a sample output using this command for <x> = 14 and <y> = 1:

```
> display Lp/14 Eth/1 statistics
Lp/14 Eth/1
   framesTransmittedOk = 37154892
   framesReceivedOk    = 28805447
   octetsTransmittedOk = 5127669040
   octetsReceivedOk    = 3974909196
   undersizeFrames     = 0
   fragments           = 0
   framesTooLong       = 0
   jabbers             = 0
   fcsErrors           = 0
   symbolErrors        = 0
   pauseFramesReceived = 0
   alignmentErrors     = 0
   singleCollisionFrames = 0
   multipleCollisionFrames = 0
   deferredTransmissions   = 0
   lateCollisions          = 0
   excessiveCollisions     = 0
   macTransmitErrors       = 0
   carrierSenseErrors      = 0
   macReceiveErrors        = 0
```

If any abnormal operation is found in this corrective action procedure, return to the step "Verify the operation of the physical layer." in "Gigabit Ethernet link failures" (page 33).

5 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of the configured port, starting from 0.

Verifying the status of the Link Aggregation (LAG) layer

Step	Action

1 If LAG is provisioned to aggregate and distribute traffic amongst two or more Gigabit Ethernet links, execute the following command to verify the OSI state of the group. The key fields "adminState", "operationalState", and "usageState" should be "unlocked", "enabled", and "busy" respectively under normal operation.

display Lp/<x> Lag/<y> osistate

The following shows a sample output using this command for <x> = 2 and <y> = 0:

```
> display Lp/2 Lag/0 osistate
Lp/2 Lag/0
    adminState = unlocked
    operationalState = enabled
    usageState       = busy
    availabilityStatus =
    proceduralStatus   =
    controlStatus      =
    alarmStatus        =
    standbyStatus      = notSet
    unknownStatus      = false
```

2 Verify the operational state of the LAG layer. Under normal operation, the field "failureCause" should be "noFailure". Since a Carrier Voice over IP network operates in passive mode, the fields "actor" and "partnerOperSystemId" should both be blank under normal operation.

display Lp/<x> Lag/<y> operational

The following shows a sample output using this command for <x> = 2 and <y> = 0:

```
> display Lp/2 Lag/0 operational
Lp/2 Lag/0
   failureCause = noFailure
   actorSystemId = ""
   partnerOperSystemId = ""
```

3 Execute the following command twice to verify that the LAG layer statistics are incrementing normally. Only the fields "runningTime", "rxFrameOctects", "txFrameOctects", "rxFramePackets", and "txFramePackets" should be incrementing under normal operation.

display Lp/<x> Lag/<y> statistics

The following shows a sample output using this command for <x> = 2 and <y> = 0:

```
> display Lp/2 Lag/0 statistics
Lp/2 Lag/0
   runningTime = 22822 seconds
   unavailSecs = 9
   failures    = 0
   rxFrameOctets = 8510363260
   txFrameOctets = 41832684653
   rxFramePackets = 61604301
   txFramePackets = 129718188
   rxFrameDiscards = 0
   txFrameDiscards = 80
   rxFrameErrors   = 0
   txFrameErrors   = 0
```

4 Verify the OSI state of the individual links in the LAG layer. The key fields "adminState", "operationalState", and "usageState" should be "unlocked", "enabled", and "busy" respectively under normal operation.

display Lp/<x> Lag/<y> Lk/<z> osistate

The following shows a sample output using this command for <x> = 2, <y> = 0, and <z> = 1:

```
> display Lp/2 Lag/0 lk/1 osistate
Lp/2 Lag/0 Lk/1
   adminState = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
```

5 Verify the operational state of the individual links in the LAG layer. Under normal operation, the field "failureCause" should be "noFailure". Since a Carrier Voice over IP network operates in passive mode, the field "partnerOperPortNumber" should be zero under normal operation.

display Lp/<x> Lag/<y> Lk/<z> operational

The following shows a sample output using this command for <x> = 2, <y> = 0, and <z> = 1:

```
> display Lp/2 Lag/0 Lk/1 operational
Lp/2 Lag/0 Lk/1
   partnerOperPortNumber = 0
   failureCause          = noFailure
```

6 Execute the following command twice to verify that the individual link statistics are incrementing normally. Only the field "runningTime" should be incrementing under normal operation. Since a Carrier Voice over IP network operates in passive mode, the fields "rxLacp", "txLacp", "rxMarker", and "txMarker" should have the value zero under normal operation.

display Lp/<x> Lag/<y> Lk/<z> statistics

The following shows a sample output using this command for <x> = 2, <y> = 0, and <z> = 1:

```
> display Lp/2 Lag/0 Lk/1 statistics
Lp/2 Lag/0 Lk/1
   runningTime = 22882 seconds
   unavailSecs = 8
   failures    = 0
   rxLacp      = 0
   txLacp      = 0
   rxInvalidLacp = 0
   rxMarker      = 0
   txMarker      = 0
   rxInvalidMarker = 0
```

7 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of link aggregate group (LAG), starting from 0.
<z>	The number of the link in the LAG, starting from 0.

Verifying the status of the OAM Ethernet link layer

Step	Action
1	Verify the OSI state of the OAM Ethernet link layer. The key fields "adminState" and "operationalState" should be "unlocked" and "enabled" respectively under normal operation. **display Lp/<x> OamEnet/<y> osistate** The following shows a sample output using this command for <x> = 0 and <y> = 0: `> display Lp/0 OamEnet/0 osistate` `Lp/0 OamEnet/0` `  adminState = unlocked` `  operationalState = enabled` `  usageState = busy`
2	Verify the operational state of the OAM Ethernet link layer. The key fields "activeStatus" and "standbyStatus" should be set to "available". **display Lp/<x> OamEnet/<y> operational** The following shows a sample output using this command for <x> = 0 and <y> = 0: `> display Lp/0 OamEnet/0 operational` `Lp/0 OamEnet/0` `  macAddress = 00-02-5F-5A-E8-00` `  activeStatus = available` `  standbyStatus = available` `  actualLineSpeed = 100 Mbit/s` `  actualDuplexMode = full`

3 Execute the following command to verify that the OAM Ethernet link statistics are normal. All fields should be zero under normal operation.

```
display Lp/<x> OamEnet/<y>
oamenetstatistics,statistics
```

The following shows a sample output using this command for <x> = 0 and <y> = 0:

```
> display Lp/0 OamEnet/0 oamenetstatistics,statistics
Lp/0 OamEnet/0
   clearToSendSignalLoss = 0
   frameTooShort         = 0
   numberOfRxCollisions  = 0
   lackOfResourcesDiscards = 0
   overrunErrors           = 0
   alignmentErrors         = 0
   fcsErrors               = 0
   singleCollisionFrames   = 0
   multipleCollisionFrames = 0
   deferredTransmissions   = 0
   lateCollisions          = 0
   excessiveCollisions     = 0
   carrierSenseErrors      = 0
```

If any abnormal operation is found in this corrective action procedure, return to the step "Verify the operation of the physical layer." in "OAM Ethernet link failures" (page 34).

4 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The card number of the OAM Ethernet line.
<y>	The port number of the OAM Ethernet line.

Testing Vt1dot5 links

Step	Action

1 On the node, lock the Vt1dot5 link:

```
DISABLENEXTcmdchk
lock Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1
```

CAUTION
Service affecting
Locking a DS1 will cause a loss of service.

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> lock Laps/1200 Sts/2 Vt1dot5/6,3 DS1
Laps/1200 Sts/2 Vt1dot5/6,3 DS1
```

2 Run the test:

`start Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1 Test`

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> start laps/1200 sts/2 Vt1dot5/6,3 DS1 Test
Laps/1200 Sts/2 Vt1dot5/6,3 DS1 Test
   Test started.
```

3 When the test is finished, view the test results:

`display Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1 Test Results`

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> display Laps/1200 Sts/2 Vt1dot5/6,3 DS1 Test Results
Laps/1200 Sts/2 Vt1dot5/6,3 DS1 Test
   elapsedTime = 1.00 minutes
   timeRemaining = 0.00 minutes
   causeOfTermination = testTimeExpired
   bitsTx              = 3776000
   bytesTx             = 472000
   frmTx               = 0
   bitsRx              = 3776000
   bytesRx             = 472000
   frmRx               = 0
   erroredFrmRx        = 0
   bitErrorRate        = 0e+00
```

Note: This test may take several minutes to complete. If the command to review the test results is run before the test is complete, the interim data will be displayed and the "causeOfTermination" field will display "testRunning".

4 Unlock the port to return it to service:

```
unlock Laps/<xy> Sts/<n> Vt1dot5/<l>,<m> DS1
```

The following shows a sample output using this command for <x> = 12, <y> = 00, <n> = 2, <l> = 6, and <m> = 3:

```
> unlock Laps/1200 Sts/2 Vt1dot5/6,3 DS1
Laps/1200 Sts/2 Vt1dot5/6,3 DS1
```

5 This procedure is complete.

—End—

Variable values

Variable	Value
<x>	The number of the logical processor. By convention, this should be the even number of the slot in an adjacent FP slot pair (2,4,6,8,10,12 or 14).
<y>	The number of the configured port, starting from 0.
<n>	The number (0,1, or 2) of the synchronous transport signal (STS) for the channelized OC3 TDM port.
<l>	The number of the virtual tributary group (VTG) in the STS. The range is 1 to 7.
<m>	The number of the virtual tributary equivalent to a DS1 (VT1.5) in the VTG. The range is 1 to 4.

PT-AAL1/UA-AAL1 corrective action procedures

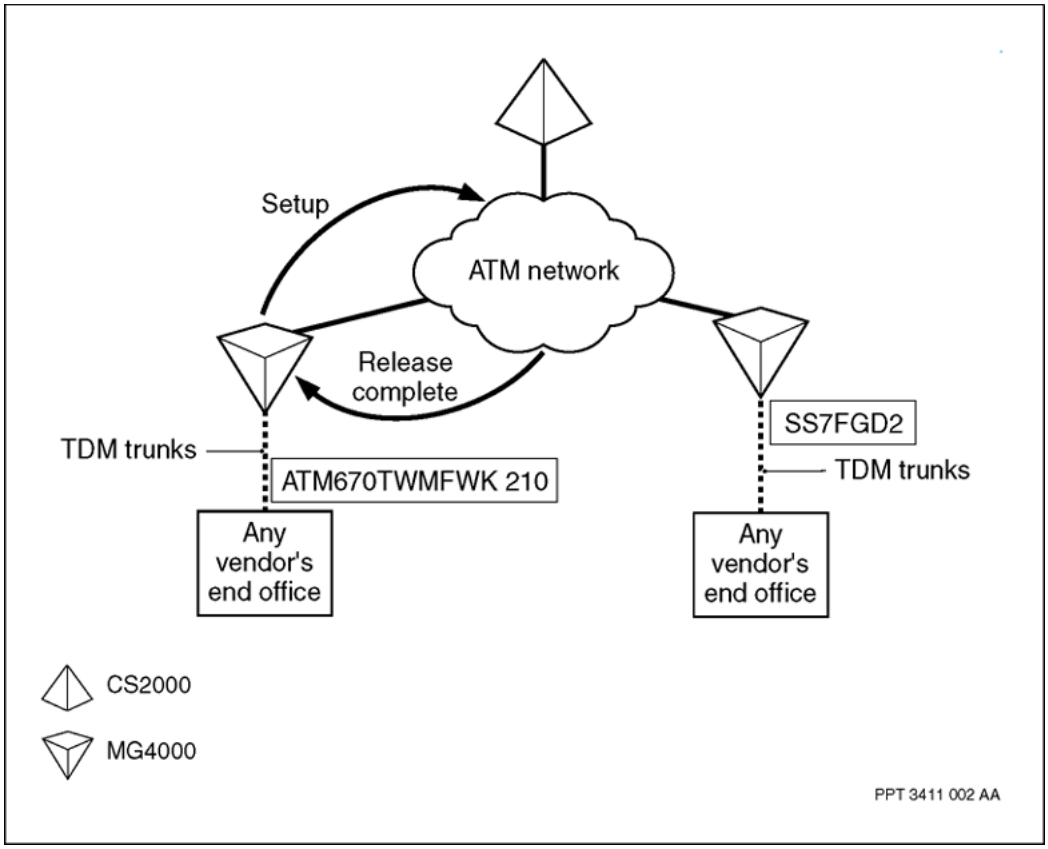
The following corrective action procedures apply to PT-AAL1/UA-AAL1 solutions:

- "Correcting call processing problems" (page 174)

Correcting call processing problems

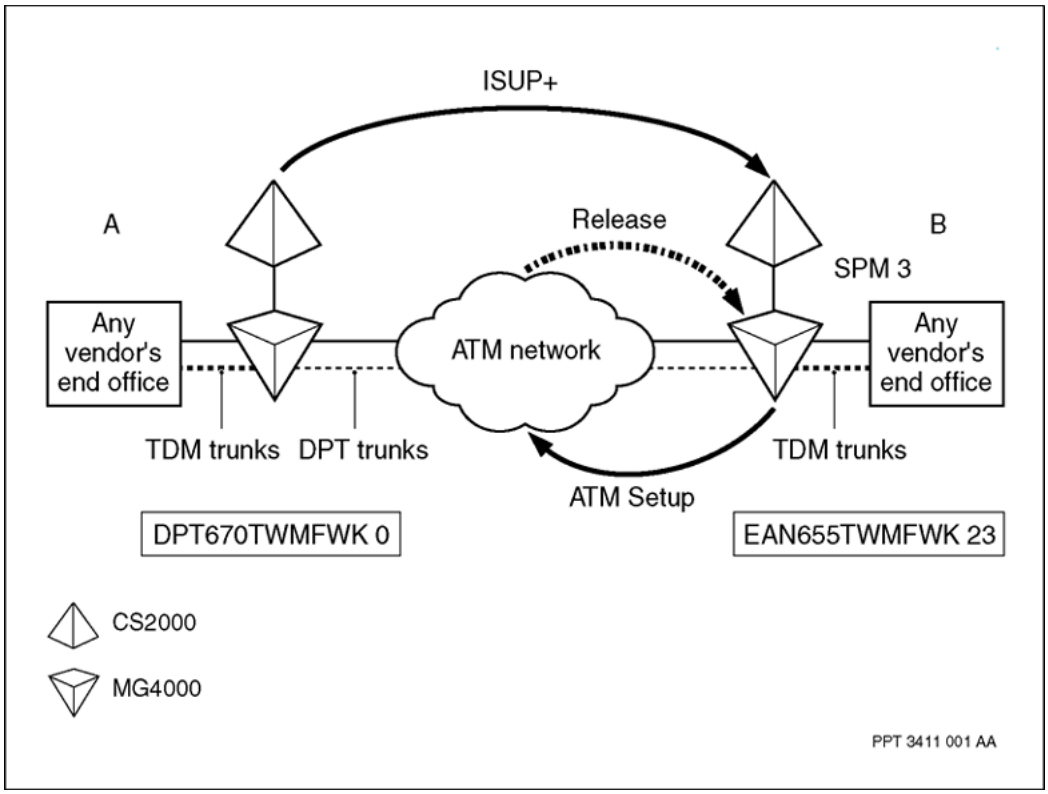
When a call processing failure occurs in a network with only one call processor, the CS2000 generates a TRK113 log and pegs an INFAIL operational measurement in the TRK OM group. The figure "Intra-switch ATM fault scenario" (page 175) shows an example of an ATM fault scenario and identifies the components involved in call processing.

Intra-switch ATM fault scenario



When a call processing failure occurs in a network with more than one call processor, the CS2000 generates an XPKT301 log and pegs an INFAIL operational measurement in the TRK OM group. The figure "Inter-switch DPT fault scenario" (page 176) shows an example of a Dynamic Packet Trunk (DPT) fault scenario in an ATM network with more than one call processor.

Inter-switch DPT fault scenario



- "Isolating an ATM framework call processing problems" (page 177)
- "Correcting ATM framework call processing problems caused by faulty links or network components" (page 179)
- "Correcting ATM framework call processing problems caused by addressing or routing errors" (page 180)
- "Identifying the address of a Multiservice Switch component" (page 181)
- "Correcting ATM framework call processing problems caused by resource exhaustion" (page 181)
- "Correcting ATM framework call processing problems caused by protocol errors" (page 182)
- "Isolating one-way speech path problems" (page 183)

The following procedures are related to correcting call processing problems:

Isolating an ATM framework call processing problems

Step	Action
1	Use the alarm reporting function to locate either a TRK113 log or an XPKT301 log.
2	Examine the TRK113 log for problem details. The following TRK113 log sample shows a problem caused by lost integrity: `LSCS03BH TRK113 OCT18 01:09:27 7603` `FLT TRUNK TRBL TRBCODE= INTEGRITY_LOST` `TRBLINFO= NIL REPORTED BY CKT ATM670TWMFWK 210` `ORIG CKT ATM670TWMFWK 210 TERM CKT SS7FGD2 531` `CALLID= 11141287`
3	Perform an I.610 loopback test on the specified MG4000 peer-to-peer connection. See the procedure, "Performing a Peer Connection I.610 Loopback Test" in *NN10076-911 MG 4000 Fault Management*.
4	Examine the XPKT301 log for problem details. The following XPKT301 log sample shows a problem caused by resource exhaustion: `MSH10_I06BE XPKT301 JUN07 18:44:12 9710 INFO UNI` `Connection Failure` `LOCATION: SPM 14` `Orig Agent: CKT SMG5251MFIT1I 108` `Orig Node: SPM 14` `Term Agent:SMG14ABS7IT1O 462` `Term Node: MG9K 12` `Called Number: 4042340014` `CallID: 10944678` `Cause=41 TEMP_FAILURE` `DEBUG: <NIL>`
5	Look up the failure cause code to find out what the problem is. See Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).
6	On the PMultiservice Data Manager server, open the System Log Display tool. For more information, see the section "Starting the System Log Display tool" in *241-6001-303 Nortel Multiservice Data Manager Administration*.

7 Monitor the NTM statistics for each ATM interface using the System Log Display tool. To view NTM statistics through Multiservice Data Manager, the -savefile option is defined by the Performance Measurement Stream Processor (PMSP) server. The NTM statistics are located in /opt/MagellanNMS/data/pmsp/<group>/closedNotSent/<file>.

a. Check that the SYSUTIL statistic is not greater than 60%.

   This statistic together with the node message block exhaustion alarms 7013 0021 and 7013 0022 indicate machine congestion.

b. Check that link capacity and ingress and egress CLP0+1 count statistics have not exceeded the pre-determined thresholds.

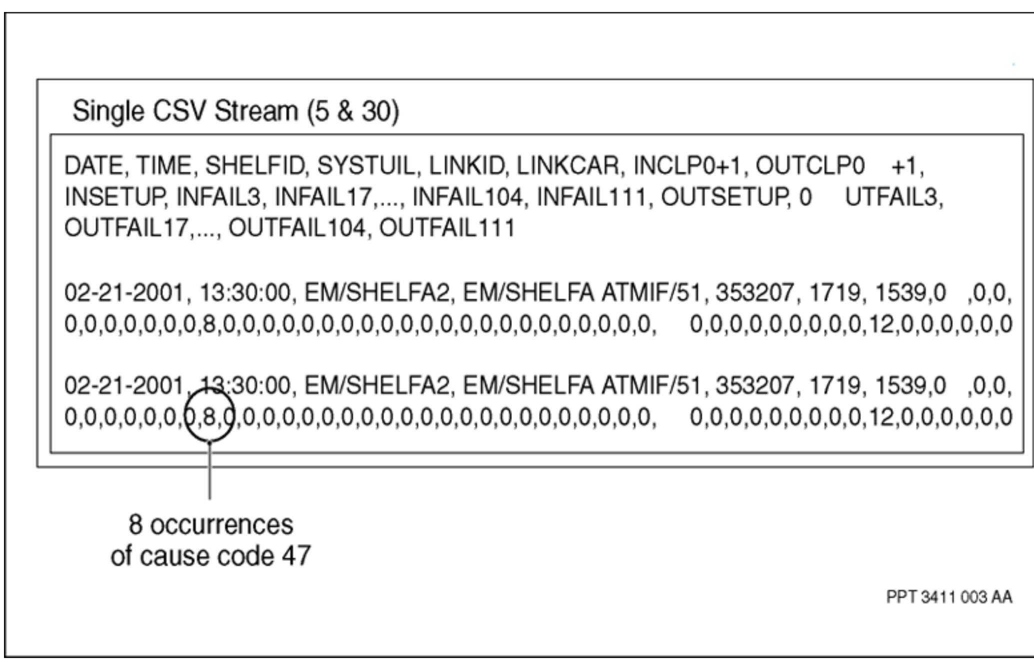
c. Check that the sum of all the INSETUP and OUTSETUP statistics for each function processor pair do not exceed capacity, especially during peak hours.

d. Verify that incoming and outgoing SETUP failure cause codes map to a CS log.

For more information, see the section "Description of setup PDU failure messages" in *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*.

Note: A non-zero entry in the statistic must be treated as a fault.

The following CSV stream statistic sample shows a non-zero entry:



8 This procedure is complete.

—End—

Correcting ATM framework call processing problems caused by faulty links or network components

Step	Action

1 On the server, open the System Log Display tool.

For more information, see "Starting the System Log Display tool" in *241-6001-303 Nortel Multiservice Data Manager Administration*.

2 Examine the 5-minute NTM statistics for non-zero entries.

Note: To view NTM statistics through Multiservice Data Manager, the -savefile option is defined by the Performance Measurement Stream Processor (PMSP). The NTM statistics are located in /opt/MagellanNMS/data/pmsp/<group>/closedNotSent/<file>.

3 Identify any faulty links and any alarms in the ATM network.

4 If the failure code is *Destination out of order*, contact your network engineers and give them the following information:

- NTM statistics
- failure logs
- Multiservice Switch software load
- node configuration

For a description of routing cause codes, see Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).

5 If the problem is a VPI/VCI problem with failure codes 35 or 36, contact Nortel GNTS and give them the following information:

- NTM statistics
- failure logs
- Multiservice Switch load
- node configuration

For a description of routing cause codes, see Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).

6 This procedure is complete.

—End—

Correcting ATM framework call processing problems caused by addressing or routing errors

Step	Action
1	Check the ATM End Station Address (AESA) on the CS2000 and record the value. See "Datafilling the MNATMIF table" in *NN10099-511 IW SPM ATM Configuration Management Overview*.
2	Check the AESA on the node and record the value. For more information, see "Identifying the address of a Multiservice Switch component" (page 181).
3	Verify that the AESA values on the CS2000 and the node are the same.
4	From the first node to the MG 4000, perform a packet trace. See "Initiating a connection trace" in *NN10600-715 Nortel Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management*.
5	If the problem is not resolved, and the values are the same, contact Nortel GNTS and give them the following information: • ATM AESA • NTM statistics • failure logs • Multiservice Switch load • node configuration If the values are not the same, contact Nortel GNTS and request assistance with changing an incorrect AESA index entry. For a description of routing cause codes, see Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).
6	This procedure is complete.

—End—

Identifying the address of a Multiservice Switch component

Step	Action
1	On the server, open the Command Console. For more information, see "Starting the Command Console" in *241-6001-804 Nortel Multiservice Data Manager Utilities*.
2	Log in to the node that is experiencing problems. For more information, see "Managing network connections" in *241-6001-804 Nortel Multiservice Data Manager Utilities*.
3	Check the AESA of the component on the node: **`list atmif/<atmif identifier> uni address/*`** The address index for the ATM interface is listed. The following is a sample address index: `atmif/200 uni Address/39123455430000000000000000000000000000`
4	Record the value.
5	This procedure is complete.

—End—

Correcting ATM framework call processing problems caused by resource exhaustion

Step	Action
1	On the server, open the System Log Display tool. For more information, see "Starting the System Log Display tool" in *241-6001-303 Nortel Multiservice Data Manager Administration*.
2	Examine the 5-minute NTM statistics for non-zero entries. ***Note:*** To view NTM statistics through Multiservice Data Manager, the -savefile option is defined by the Performance Measurement Stream Processor (PMSP). The NTM statistics are located in /opt/MagellanNMS/data/pmsp/<group>/closedNotSent/<file>.
3	Identify any links in the ATM network with capacity problems. Cause codes: 37, 45, 47, and 58 indicate capacity problems. For a description of these cause codes, see Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).

4 Contact your network planner to find out how to add a new interface or a new shelf to your existing ATM Network.

5 This procedure is complete.

—End—

Correcting ATM framework call processing problems caused by protocol errors

Step	Action

1 On the server, open the System Log Display tool.

For more information, see "Starting the System Log Display tool" in *241-6001-303 Nortel Multiservice Data Manager Administration*.

2 Examine the 5-minute NTM statistics for non-zero entries.

Note: To view NTM statistics through Multiservice Data Manager, the -savefile option is defined by the Performance Measurement Stream Processor (PMSP). The NTM statistics are located in /opt/MagellanNMS/data/pmsp/<group>/closedNotSent/<file>.

For more information, see "NTM statistics file management" in *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 cause codes indicate protocol error problems. For a description of these cause codes, see Appendix "Cause code reference for PT-AAL1 / UA-AAL1 call processing" (page 209).

- 49 : QoS unavailable
- 57 : Bearer capability not authorized
- 58 : Bearer capability not presently available
- 63 : Service or option not available, unspecified
- 65 : Bearer capability not implemented
- 73 : Unsupported combination of traffic parameters
- 78 : AAL parameters cannot be supported
- 88 : Incompatible destination
- 96 : Mandatory information element missing
- 99 : Information element non-existent or not implemented
- 100: Invalid information element contents

- 104: Incorrect message length
- 111: Protocol error, unspecified

3 Contact Nortel GNTS and give them the following information:

- NTM statistics
- failure logs
- Multiservice Switch load
- node configuration

4 This procedure is complete.

—End—

Isolating one-way speech path problems

Step	Action
1	Isolate the cause by identifying any patterns associated with the problem.
2	Record the pattern you observe.
3	Depending on the pattern you observe, collect as much data from logs, alarms, and SCNs as possible using the BDF Viewer tool.
4	If the problem has occurred several times, do not disconnect the call. Contact Nortel GNTS using a different line and report the problem.
5	This procedure is complete.

—End—

UA-IP/PT-IP corrective action procedures

The following corrective action procedures apply to UA-IP/PT-IP solutions:

- "Verifying the forwarding path between two IP addresses" (page 184)
- "Checking for node-level IP packet discards" (page 185)
- "Isolating IP packet discards to an interface" (page 186)
- "Checking for layer 2 interface-level packet discards" (page 189)
- "Checking for node-level ICMP packet generation/reception" (page 195)
- "Verifying the configured IP address" (page 196)

- "Verifying the ARP table" (page 198)
- "Verifying the forwarding and routing tables" (page 198)
- "Verifying the statistics for locally destined/generated packets" (page 200)
- "Locking out packet traffic" (page 203)
- "Verifying the statistics for the MSS/MG15000 RADIUS server" (page 204)
- "Viewing IPSec general statistics on the MSS/MG15000" (page 206)
- "Verifying IPSec statistics for a specific connection on the MSS/MG15000" (page 206)
- "Viewing IPSec and SSH error logs on the MDM workstation" (page 207)

Verifying the forwarding path between two IP addresses

Step	Action
1	Execute the following command to trace a route to an IP address reachable from a Multiservice Switch 15000 node: **`ping -src(<addr1>) -tr -ip(<addr2>) Vr/VOIP Ip Icmp`** The following shows a sample output using this command for <addr1> of 10.16.16.161 and <addr2> of 10.15.16.1: `> ping -src(10.16.16.161) -tr -ip(10.15.16.1) Vr/VOIP Ip Icmp` `Vr/VOIP Ip Icmp` `IP Trace Route for 10.15.16.1:` `Path taken:` `Hop 1: 10.48.0.1 (time = 2ms)` `Hop 2: 10.15.16.1 (time = 0ms)`
2	This procedure is complete.

—End—

Variable	Value
<addr1>	The address of the node requesting the route trace. This command option is not mandatory, but helps to ensure that the ping reply will be routed back to the correct source.
<addr2>	The destination address of the route to be traced.

Checking for node-level IP packet discards

Step	Action
1	Execute the following command twice to verify how the IP statistics are incrementing over time: **display Vr/VOIP Ip statistics** The following shows a sample output using this command:

```
> display Vr/VOIP Ip statistics
Vr/VOIP Ip
   inReceives = 480623708
   inHdrErrors = 0
   inAddrErrors = 0
   forwDatagrams = 473961927
   inUnknownProtos = 0
   inSrcRouteDiscards = 0
   inDiscards          = 0
   inDelivers          = 0
   outRequests         = 6646657
   outDiscards         = 0
   outNoRoutes         = 6647085
   reasmTimeOut        = 5 seconds
   reasmReqds          = 0
   reasmOks            = 0
   reasmFails          = 0
   fragOks             = 0
   fragFails           = 0
   fragCreates         = 0
   routingDiscards     = 0
```

2	Examine changes in the statistics relating to normal operation: Under normal operation, the fields "inReceives" and "forwDatagrams" should be incrementing, while the fields "inDelivers" and "outRequests" may be incrementing slowly because of dynamic routing protocol messages such as OSPF.
3	Examine changes in the fields relating to IP packet discards: "inDiscards", "outDiscards", "outNoRoutes", and "routingDiscards" If "outNoRoutes" is increasing, then the node is generating ICMP unreachable messages back to the host/router that sent a packet that cannot be forwarded. The node uses one of its own IPv4 source addresses (the address owned by the interface that is sending the ICMP packet) in the IP header and the IPv4 destination address is the address of the original host/router.

If "routingDiscards" is increasing, then the node is discarding packets that cannot be forwarded by sending them to a default discard route that has been configured on the node.

4 To determine if a default discard route has been configured, execute the following command:

```
display Vr/VOIP Ip Static Discard/*
```

The following shows a sample output using this command when no default discard route has been configured:

```
> display Vr/VOIP Ip Static Discard/*
Vr/VOIP Ip Static
Component has no provisioned or operational subcomponents
of the requested type.
```

The following shows a sample output using this command when a default discard route has been configured:

```
> display Vr/VOIP Ip Static Discard/*
Vr/VOIP Ip Static Discard/*,*
+========+==========+---------------------------------
| addr   | destMask |Response
+========+==========+---------------------------------
|0.0.0.0 |0.0.0.0   |Component has no operational data.
```

5 This procedure is complete.

—End—

Isolating IP packet discards to an interface

Step	Action

1 Execute the following command twice to collect IP packet transmit and receive statistics across the various media of the virtual router:

```
display Vr/VOIP IfTableEntry/*
componentName,ifInUcastPkts,ifOutUcastPkts
```

Examine the statistics for the "IfTableEntry" instances to see if IP packets are being received and transmitted as expected across the various media of the virtual router. If packets are not being transmitted or received at the expected rates, you are finished with this procedure.

Note: Keep track of the "IfTableEntry" instance and the associated "componentName (compName)" for use with the remaining commands in this procedure. The "IfTableEntry" instance is the key unique identifier for each media type that is configured for the virtual router.

The following shows a sample output using this command:

```
> display Vr/VOIP IfTableEntry/*
componentName,ifInUcastPkts,ifOutUcastPkts

Vr/VOIP IfTableEntry/*
+=============+--------------------+----------+--------
|IfTableEntry|      compName       | inUcast  | outUcast
+=============+--------------------+----------+--------
|           6|La/141               |     57101| 233405047
|           9|La/151               |  94545255|         2
|          14|Vm/3 If/0            |   2091967|   1998085
|          15|AtmMpe/1420          |  34173222|  30657244
|          18|AtmMpe/1520          |  2955033 |   2335157
|          25|AtmMpe/1500          |  74256463|  70652772
|          48|AtmMpe/1000          |   2955045|   2331918
|          49|AtmMpe/1100          |  39370402|  34412854
|          50|AtmMpe/1001          |   2955056|   2330485
|          51|AtmMpe/1101          |  34173284|  30445209
|          52|AtmMpe/1400          |   2955068|   2326298
|          54|AtmMpe/800           |  54917087|  48261789
|          55|AtmMpe/810           |        19|        26
|          63|AtmMpe/1401          |  34173222|  30657244
|          65|AtmMpe/1501          |   2955033|   2335157
|          69|AtmMpe/1402          |  74256463|  70652772
|          70|AtmMpe/1502          |   2955045|   2331918
|          75|AtmMpe/1421          |  39370402|  34412854
|          76|AtmMpe/1521          |   2955056|   2330485
|          81|AtmMpe/1422          |  54917087|  48261789
|          82|AtmMpe/1522          | 217961761| 101343620
```

2 If the IP packets for the media of interest are being transmitted and received as expected, execute the following command twice to view the packet discard statistics for those media:

`display Vr/VOIP IfTableEntry/* ifInDiscards,ifOutDiscards,ifInErrors,IfOutErrors`

If the packet discards statistics are remaining constant, then you are finished with this procedure.

The following shows a sample output using this command:

```
> display Vr/VOIP IfTableEntry/*
ifInDiscards,ifOutDiscards,ifInErrors,IfOutErrors

Vr/VOIP IfTableEntry/*
+=============+==========+==========+==========+=======
|IfTableEntry|inDiscard |outDiscard|  inErr   |  outErr
+=============+==========+==========+==========+=======
|          15|         0|       139|         0|         0
|          18|         0|         3|         0|         0
|          25|         0|         0|         0|         0
|          48|         0|         2|         0|         0
|          49|         0|         1|         0|         0
|          50|         0|       133|         0|         0
|          51|         0|         0|         0|         0
|          52|         0|         6|         0|         0
|          54|     23922|         5|         0|         0
|          55|      3101|         3|         0|         0
|          63|         0|         5|         0|         0
|          65|         0|         0|         0|         0
|          69|         0|         4|         0|         0
|          70|         0|         0|         0|         0
|          75|         0|         3|         0|         0
|          76|         0|        64|         0|         0
|          81|         0|        66|         0|         0
|          82|         0|         2|         0|         0
```

3 If the packet discard statistics over the media of interest are incrementing, check the layer 3 discard statistics.

For ATM media:

Execute the following command twice to check the layer 3 discard statistics over the ATM medium of interest:

`display -notab <componentName> Ac/* statistics`

The following shows a sample output using this command for <componentName> = AtmMpe/1401:

```
> display -notab AtmMpe/1401 Ac/* statistics
AtmMpe/1401 Ac/1
   outPackets = 384377
   outOctets  = 47734364
   outDiscards = 5
   inPackets   = 364261
   inOctets    = 17484528
   inUnknownProtos = 0
   inErrors        = 0
```

For Gigabit Ethernet (LAN) media:

Execute the following command twice to check the layer 3 discard statistics over the Ethernet medium of interest:

display <componentName> Framer statistics

The following shows a sample output using this command for <componentName> = La/151:

```
> display La/151 Framer statistics
La/151 Framer
   rxFrames = 47443943
   rxBytes  = 6539143786
   txFrames = 64495394
   txBytes  = 8916204195
   rxDiscard = 0
   txDiscard = 0
   rxFrameError = 0
   lrcErrors    = 0
```

4 This procedure is complete.

—End—

Variable	Value
<componentName>	The combination of the component type and instance number associated with a particular IfTableEntry value. The format of the componentName is: component type / instance number. Examples of component names are: AtmMpe/<n> where <n> is the instance number La/<xy> where <x> is the logical processor number and <y> is the number of the configured port.

Checking for layer 2 interface-level packet discards ATM interface

Step	Action

1 Execute the following two commands to collect layer 2 information for the ATM medium of interest:

display Vr/VOIP IfTableEntry/<i> componentname

display -prov <componentName> Ac/*

The key layer 2 information is the AtmIf instance number and VCC instance number.

The following shows a sample output using these commands for <i> = 18 and <componentName> = AtmMpe/1520:

```
> display Vr/VOIP IfTableEntry/18 componentName
Vr/VOIP IfTableEntry/18
   componentName = AtmMpe/1520

> display -prov AtmMpe/1520 Ac/*

AtmMpe/1520 Ac/*
+===+--------------------+---+----+------+------------
|Ac |        link        |ipC|ipDs|mplsSi|        ipIf
|   |                    |os | cp |  g   |
+===+--------------------+---+----+------+------------
|  1|AtmIf/803 Vcc/0.43  |  0|  na|shared|!
|   | Nep                |   |    |      |
```

2 To verify if ATM cells are being transmitted and if transmitted cells are being discarded at an ATM interface level, execute the following command twice:

display AtmIf/* txCell,txCellDiscard

The following shows a sample output using this command:

```
> display AtmIf/* txCell,txCellDiscard

AtmIf/*
+=====+--------------------+--------------------
|AtmIf|       txCell       |   txCellDiscard
+=====+--------------------+--------------------
|  800|           607123854|                   0
|  802|           640559100|                   2
|  803|           900594228|                   0
| 1000|            38345481|                   0
| 1001|            35149877|                   0
| 1400|            18143520|                   0
| 1401|            18143454|                   0
| 1402|            18143395|                   0
| 1420|            18130920|                   0
| 1421|            18143445|                   0
| 1422|            18143473|                   0
```

3 To verify if ATM cells are being received and whether received cells or frames are being discarded at an ATM interface level, execute the following command twice:

display AtmIf/*
rxCell,rxCellDiscard,aal5RxErrors,lrcFrameErrors

The following shows a sample output using this command:

```
> display AtmIf/*
rxCell,rxCellDiscard,aal5RxErrors,lrcFrameErrors

AtmIf/*
+=====+-------------+---------------+----------+------
|AtmIf|      rxCell | rxCellDiscard |aal5Errors| lrcErrs
+=====+-------------+---------------+----------+------
|  800|    907179372|              0|         0|       0
|  802|    907987688|              0|         0|       0
|  803|    644861171|              0|   1032879|       0
| 1000|     44236193|            276|         0|       0
| 1001|     28671496|            151|         0|       0
| 1400|     15829487|        8440004|         0|       0
| 1401      15829503|        8440021|         0|       0
| 1402|     15829518|        8440013|         0|       0
| 1420|     15828822|        8439652|         0|       0
| 1421|     15828826|        8439682|         0|       0
| 1422|     15828810|        8439656|         0|       0
```

4 If transmit discards are occurring, determine the VCC connection(s) in which the ATM cells or frames are being discarded.

Execute the following command twice to verify if ATM cells are being transmitted, and if any cells or frames are being discarded at a VCC level:

```
display <componentName> Vcc/*
txCell,txCellDiscard,txFrameDiscard
```

The following shows a sample output using this command for <componentName> = AtmIf/803:

```
> display AtmIf/803 Vcc/*
txCell,txCellDiscard,txFrameDiscard

AtmIf/803 Vcc/*
+==========+----------------+-------------+-----------
|   Vcc    |  txCell        |      txcd   |   txfd
+==========+----------------+-------------+-----------
|0.32      |       115795189|            0|          0
|0.33      |         3503444|            0|          0
|0.34      |       103301041|            0|          0
|0.35      |         3503446|            0|          0
|0.36      |        56572004|            0|          0
|0.37      |         3503449|            0|          0
|0.38      |        56572026|            0|          0
|0.39      |         3503448|            0|          0
|0.40      |        56572027|            0|          0
|0.41      |         3503450|            0|          0
|0.42      |        56572034|            0|          0
|0.43      |         3503454|            0|          0
|0.44      |        56572047|            0|          0
|0.45      |         3503021|            0|          0
|0.46      |        56572053|            0|          0
|0.47      |         3498716|            0|          0
```

5 If receive discards are occurring, determine the virtual channel connection(s) (VCCs) in which the ATM cells or frames are being discarded.

Execute the following command twice to verify if ATM cells are being received, and if any cells or frames are being discarded at a VCC level:

`display <componentName> Vcc/*`
`rxCell,rxCellDiscard,rxFrameDiscard`

The following shows a sample output using this command for <componentName> = AtmIf/803:

```
> display AtmIf/803 Vcc/*
rxCell,rxCellDiscard,rxFrameDiscard

AtmIf/803 Vcc/*
+==========+==============+===========+==========
|   Vcc    |    rxCell    |    rxcd   |    rxfd
+==========+==============+===========+==========
|0.32      |     125507460|          0|         0
|0.33      |       7806506|          0|     55037
|0.34      |      64398122|          0|         0
|0.35      |       7806503|          0|     67017
|0.36      |      32235710|          0|         0
|0.37      |       5038986|          0|    102437
|0.38      |      32235722|          0|         0
|0.39      |       5038986|          0|     91862
|0.40      |      32235716|          0|         0
|0.41      |       5038984|          0|     90116
|0.42      |      32235720|          0|         0
|0.43      |       5038987|          0|    105429
|0.44      |      32235720|          0|         0
|0.45      |       5038986|          0|     92395
|0.46      |      32235722|          0|         0
|0.47      |       5038984|          0|     57626
```

6 Execute the following command twice to more closely to examine the discard statistics on the VCC where the cells or frames are being discarded:

`display <componentName> Vcc/<n> statistics`

The following shows a sample output using this command for <componentName> = AtmIf/803 and <n> = 0.39:

```
> display AtmIf/803 Vcc/0.39 statistics
AtmIf/803 Vcc/0.39
   txCell = 3706619
   txCellDiscard = 0
   txFrameDiscard = 0
   txFrameDiscardClp = 0
   rxCell            = 5097692
   rxCellDiscard     = 0
   rxCellDiscardClp  = 0
   rxFrameDiscard    = 93899
   rxFrameDiscardClp = 0
   rxAal5FrameError  = 93899
   rxAal5FrameAbort  = 83610
```

7 This procedure is complete.

—End—

Variable	Value
<i>	The IfTableEntry instance number.
<componentName>	The combination of the component type and instance number associated with a particular IfTableEntry value. The format of the componentName is: component type / instance number. Examples of component names are: AtmMpe/<n> where <n> is the instance number La/<xy> where <x> is the logical processor number and <y> is the number of the configured port.
<n>	The instance number of the virtual channel connection.

Gigabit Ethernet interface

Step	Action
1	Execute the following command to collect layer 2 information for the Gigabit Ethernet medium of interest: **display -prov <componentName> Framer** The following shows a sample output using these commands for <componentName> = La/141: `> display -prov La/141 framer` `La/141 Framer` `  interfaceName = Lp/14 Eth/1`
2	Execute the following command twice to verify that the Gigabit Ethernet link statistics are incrementing correctly. **display Lp/<x> Eth/<y> statistics** Under normal operation, only the fields "frameTransmittedOk", "framesReceivedOk", "octetsTransmittedOk" and "OctetsReceive-dOk" should increment in value. The following shows a sample output using this command for <x> = 14 and <y> = 1:

```
> display Lp/14 Eth/1 statistics
Lp/14 Eth/1
   framesTransmittedOk = 81259
   framesReceivedOk    = 96576
   octetsTransmittedOk = 7126394
   octetsReceivedOk    = 7962970
   undersizeFrames     = 0
   fragments           = 0
   framesTooLong       = 0
   jabbers             = 0
   fcsErrors           = 0
   symbolErrors        = 0
   pauseFramesReceived = 0
   alignmentErrors     = 0
   singleCollisionFrames = 0
   multipleCollisionFrames = 0
   deferredTransmissions   = 0
   lateCollisions          = 0
   excessiveCollisions     = 0
   macTransmitErrors       = 0
   carrierSenseErrors      = 0
   macReceiveErrors        = 0
```

3 This procedure is complete.

—End—

Variable	Value
<x>	The number of the logical processor. By convention, it is the number of the 4pGigE FP and ranges in value from 2 to 15. The slot pairs are 2/3, 4/5, ... 14/15.
<y>	The number of the configured port, starting from 0.

Checking for node-level ICMP packet generation/reception

Step	Action

1 Execute the following command twice to verify whether ICMP packets are being generated by a node. Under normal operation, none of these statistics are expected to be increasing in value. The key field is "OutDestUnreachs".

display Vr/VOIP Ip Icmp statistics

The following shows a sample output using this command:

```
> display Vr/VOIP Ip Icmp statistics
Vr/VOIP Ip Icmp
   inMsgs = 0
   inErrors = 0
   inDestUnreachs = 0
   inTimeExcds    = 0
   inParmProbs    = 0
   inSrcQuenchs   = 0
   inRedirects    = 0
   inEchos        = 0
   inEchoReps     = 0
   inTimestamps   = 0
   inTimestampReps = 0
   inAddrMasks     = 0
   inAddrMaskReps  = 0
   inRtrAdvs       = 0
   inRtrSolicits   = 0
   outMsgs         = 6873986
   outErrors       = 0
   outDestUnreachs = 6873986
   outTimeExcds    = 0
   outParmProbs    = 0
   outSrcQuenchs   = 0
   outRedirects    = 0
   outEchos        = 0
   outEchoReps     = 0
   outTimestamps   = 0
   outTimestampReps = 0
   outAddrMasks     = 0
   outAddrMaskReps  = 0
   outRtrAdvs       = 0
   outRtrSolicits   = 0
```

2 This procedure is complete.

—End—

Verifying the configured IP address

Step	Action

1 To verify the IP addresses and subnets that have been configured on a virtual router of a Multiservice Switch 15000 node, execute the following command:

`display Vr/VOIP Ip IpInterfaceEntry/*`

Check the mask, current status, protocol port name and associated media type for each address.

The following shows a sample output using this command:

```
> display Vr/VOIP Ip IpInterfaceEntry/*

Vr/VOIP Ip If/*
   Use -noTabular to see hidden attributes: ncHardwareAddress,
   broadcastAddress, mtu and hardwareAddress.
+=============+===============+======+==================+======
|     addr    |     mask      |status|      pPName      | type
+=============+===============+======+==================+======
|10.48.0.98   |255.255.255.252 |up    |Pp/8600_1B        |ethern
|10.48.0.162  |255.255.255.252 |down  |Pp/8600_1C        |atmMpe
|10.48.0.130  |255.255.255.252 |down  |Pp/8600_2B        |ethern
|10.0.0.33    |255.255.255.224 |up    |Pp/9K_1_CC        |atmMpe
|10.16.0.33   |255.255.255.248 |up    |Pp/9K_1_OAM       |atmMpe
|10.0.0.65    |255.255.255.224 |up    |Pp/9K_2_CC        |atmMpe
|10.16.0.65   |255.255.255.248 |up    |Pp/9K_2_OAM       |atmMpe
|10.0.0.97    |255.255.255.224 |up    |Pp/9K_3_CC        |atmMpe
|10.16.0.97   |255.255.255.248 |up    |Pp/9K_3_OAM       |atmMpe
|10.0.0.129   |255.255.255.224 |up    |Pp/9K_4_CC        |atmMpe
|10.16.0.129  |255.255.255.248 |up    |Pp/9K_4_OAM       |atmMpe
|10.0.0.9     |255.255.255.252 |up    |Pp/NSTA12_IPMCONN |virtua
|10.0.0.1     |255.255.255.252 |up    |Pp/NSTA12_MG      |virtua
|10.0.0.5     |255.255.255.252 |up    |Pp/NSTA12_SG      |virtua
|10.48.0.1    |255.255.255.252 |up    |Pp/PP_D6_1000_CC  |atmMpe
|10.48.0.5    |255.255.255.252 |up    |Pp/PP_D6_1001_CC  |atmMpe
|10.48.0.9    |255.255.255.252 |down  |Pp/PP_D7_800_CC   |atmMpe
```

2 To verify the static routes that have been manually configured on a virtual router of a Multiservice Switch 15000 node and the states of the next hops, execute the following command:

`display Vr/VOIP Ip Static RouteEntry/* Nexthop/*`

The following shows a sample output using this command:

```
> display Vr/VOIP Ip Static RouteEntry/* Nexthop/*

Vr/VOIP Ip Static Route/*,*,* Nh/*
+============+===============+===+=============+=====+====+=====+====
|   addr     |     mask      |tos| Nh          |osiAd|osiO|osiUs| hbS
|            |               |   |             | min |per | age |
+============+===============+===+=============+=====+====+=====+====
|0.0.0.0     |0.0.0.0        |  0|10.48.0.97   |unlck|ena |activ|undete
|0.0.0.0     |0.0.0.0        |  0|10.48.0.129  |unlck|dis |idle |undete
|10.0.16.0   |255.255.240.0  |  0|10.48.0.2    |unlck|ena |activ|undete
|10.0.32.0   |255.255.240.0  |  0|10.48.0.10   |unlck|dis |idle |undete
|10.16.16.0  |255.255.240.0  |  0|10.48.0.2    |unlck|ena |activ|undete
|10.16.32.0  |255.255.240.0  |  0|10.48.0.10   |unlck|dis |idle |undete
```

3 This procedure is complete.

—End—

Verifying the ARP table

Step	Action
1	To check the ARP table for a virtual router on a Nortel Multiservice Switch node, execute the following command: **display Vr/VOIP Ip Arp *** Each ARP entry that has a type of "static" was configured manually while each ARP entry that has a type of "dynamic" was automatically resolved by the node. The following shows a sample output using this command:
2	This procedure is complete.

```
> display Vr/VOIP Ip Arp *

Vr/VOIP Ip Arp DynHost/*,*
   Use -noTabular to see hidden attributes: tda and ncPhysAddress.
+===========+===+==================+=====+======+====+=====+====
|    addr   |cos|    physAddress   | mtu |encap |pvcN|ifInd| type
|           |   |                  |     |      | o  | ex  |
+===========+===+==================+=====+======+====+=====+====
|10.0.0.2   |na |""                |18936|notApp|   0|   14|static
|10.0.0.6   |na |"                 |18936|notApp|   0|   65|static
|10.0.0.10  |na |""                |18936|notApp|   0|   43|static
|10.0.0.34  |0  |""                | 9180|notApp|   1|   20|static
|10.0.0.35  |0  |""                | 9180|notApp|   1|   20|static
|10.16.0.34 |0  |""                | 9180|notApp|   1|   24|static
|10.16.0.35 |0  |""                | 9180|notApp|   1|   24|static
|10.48.0.2  |1  |""                | 9180|notApp|   3|   48|dynami
|10.48.0.2  |2  |""                | 9180|notApp|   2|   48|dynami
|10.48.0.2  |3  |""                | 9180|notApp|   1|   48|dynami
|10.48.0.6  |1  |""                | 9180|notApp|   3|   49|dynami
|10.48.0.6  |2  |""                | 9180|notApp|   2|   49|dynami
|10.48.0.6  |3  |""                | 9180|notApp|   1|   49|dynami
|10.48.0.97 |na |00-0C-F8-A2-22-03  | 1500|ethern|   0|    6|dynami
```

—End—

Verifying the forwarding and routing tables

Step	Action
1	To check the forwarding table of a virtual router on a Multiservice Switch 15000 node, execute the following command: **display Vr/VOIP Ip Fwd/*** The following shows a sample output using this command:

```
> display Vr/VOIP Ip Fwd/*

Vr/VOIP Ip Fwd/*,*,*,*
   Use -noTabular to see hidden attributes: metric, nextHopAs,
interfaceName,
   pPName and age.
+===============+=================+===+===========+=====+======+====
|      addr     |       mask      |tos|  gateway  |ifInd|type|protocol
|               |                 |   |           | ex  |      |
+===============+=================+===+===========+=====+======+====
|0.0.0.0        |0.0.0.0          |  0|10.48.0.97 |    6|remote|netmgm
|10.0.0.0       |255.255.255.252  |  0|10.0.0.1   |   14|localI|local
|10.0.0.1       |255.255.255.255  |  0|10.0.0.1   |   14|localI|local
|10.0.0.32      |255.255.255.224  |  0|10.0.0.33  |   20|localI|local
|10.0.0.33      |255.255.255.255  |  0|10.0.0.33  |   20|localI|local
|10.0.16.0      |255.255.240.0    |  0|10.48.0.2  |   48|remote|netmgm
|10.2.1.32      |255.255.255.224  |  0|10.48.0.97 |    6|remote|ospf
|10.2.1.64      |255.255.255.224  |  0|10.48.0.97 |    6|remote|ospf
|10.2.1.96      |255.255.255.224  |  0|10.48.0.97 |    6|remote|ospf
|10.2.1.128     |255.255.255.224  |  0|10.48.0.97 |    6|remote|ospf
|10.2.16.0      |255.255.255.0    |  0|10.48.0.97 |    6|remote|ospf
|10.2.17.0      |255.255.255.0    |  0|10.48.0.97 |    6|remote|ospf
|10.2.32.0      |255.255.255.0    |  0|10.48.0.97 |    6|remote|ospf
|10.15.0.0      |255.255.0.0      |  0|10.48.0.97 |    6|remote|ospf
|10.16.0.32     |255.255.255.248  |  0|10.16.0.33 |   24|localI|local
|10.16.16.0     |255.255.240.0    |  0|10.48.0.2  |   48|remote|netmgm
|10.255.255.255 |255.255.255.255  |  0|0.0.0.0    |    0|notDef|netmgm
|127.0.0.0      |255.0.0.0        |  0|0.0.0.0    |    0|notDef|netmgm
|224.0.0.0      |255.0.0.0        |  0|0.0.0.0    |    0|notDef|netmgm
```

2 To check the routing table of a virtual router on a Multiservice Switch 15000 node, execute the following command:

`display Vr/VOIP Ip Rdb/*`

The following shows a sample output using this command:

```
> display Vr/VOIP Ip Rdb/*

Vr/VOIP Ip Rdb/*,*,*,*
+===============+================+=======+==========+======+====+====
|     addr      |      mask      | proto|  gateway  |metric|pref|age
+===============+================+=======+==========+======+====+====
|0.0.0.0        |0.0.0.0         |remote |10.48.0.97|     1| 253|  7003
|10.0.0.0       |255.255.255.252 |local  |10.0.0.0  |     0|   0|  7068
|10.0.0.1       |255.255.255.255 |local  |10.0.0.1  |     0|   0|  7068
|10.0.0.32      |255.255.255.224 |local  |10.0.0.32 |     0|   0|  7053
|10.0.0.33      |255.255.255.255 |local  |10.0.0.33 |     0|   0|  7053
|10.0.16.0      |255.255.240.0   |remote |10.48.0.2 |     1|  72|  7010
|10.2.1.32      |255.255.255.224 |ospfEx |10.48.0.97|    12|  80|  5157
|10.15.0.0      |255.255.0.0     |ospf   |10.48.0.97|    21|  30|  5157
|10.16.0.32     |255.255.255.248 |local  |10.16.0.32|     0|   0|  7052
|10.16.16.0     |255.255.240.0   |remote |10.48.0.2 |     1|  72|  7010
|10.255.255.255 |255.255.255.255 |specia |0.0.0.0   |     0|   0|  7068
|127.0.0.0      |255.0.0.0       |specia |0.0.0.0   |     0|   0|  7069
|224.0.0.0      |255.0.0.0       |specia |0.0.0.0   |     0|   0|  7069
```

3 This procedure is complete.

—End—

Verifying the statistics for locally destined/generated packets

Step	Action
1	To check for locally destined and generated ICMP packets, execute the following command twice: **display Vr/VOIP Ip Icmp statistics** Under normal operation, none of these statistics are expected to be increasing in value. The key fields to examine for the rate of change are "inMsgs", "inErrors", "inDestUnreachs", "inTimeExcds", "inEchos", "inEchoReps", "outMsgs", "outErrors", "outDestUnreachs", "outTimeExcds", "outEchos", and "outEchoReps". The following shows a sample output using this command:

```
> display Vr/VOIP Ip Icmp statistics
Vr/VOIP Ip Icmp
   inMsgs = 0
   inErrors = 0
   inDestUnreachs = 0
   inTimeExcds    = 0
   inParmProbs    = 0
   inSrcQuenchs   = 0
   inRedirects    = 0
   inEchos        = 0
   inEchoReps     = 0
   inTimestamps   = 0
   inTimestampReps = 0
   inAddrMasks     = 0
   inAddrMaskReps  = 0
   inRtrAdvs       = 0
   inRtrSolicits   = 0
   outMsgs         = 6873986
   outErrors       = 0
   outDestUnreachs = 6873986
   outTimeExcds    = 0
   outParmProbs    = 0
   outSrcQuenchs   = 0
   outRedirects    = 0
   outEchos        = 0
   outEchoReps     = 0
   outTimestamps   = 0
   outTimestampReps = 0
   outAddrMasks     = 0
   outAddrMaskReps  = 0
   outRtrAdvs       = 0
   outRtrSolicits   = 0
```

2 To check locally destined and generated TCP packets, execute each of the following commands twice:

display Vr/VOIP Ip Tcp statistics

Check for incrementing statistics. Under normal operation, none of the fields should be incrementing. In particular, the fields "inSegs", "inErrs", and "outRsts" should not increment under normal operation. Any values for the "inSegs" field could indicate possible security attacks.

The following shows a sample output using this command:

```
> display Vr/VOIP Ip Tcp statistics
Vr/VOIP Ip Tcp
   rToAlgorithm = other
   rToMin       = 2000 msec
   rToMax       = 128000 msec
   maxConn      = -1
   activeOpens  = 0
   passiveOpens = 0
   attemptFails = 0
   estabResets  = 0
   currEstab    = 0
   inSegs       = 0
   outSegs      = 0
   retransSegs  = 0
   inErrs       = 0
   outRsts      = 0
```

display Vr/0 Ip Tcp

Check for incrementing statistics. Under normal operation, only the fields "inSegs" and "outSegs" are incrementing in the order of less than twenty packets per second (except in the case of software download). In particular, the fields "inErrs" and "outRsts" should not increment under normal operation.

The following shows a sample output using this command:

```
> display Vr/0 Ip Tcp
Vr/0 Ip Tcp
   rToAlgorithm = other
   rToMin = 2000 msec
   rToMax = 128000 msec
   maxConn = -1
   activeOpens = 128
   passiveOpens = 637
   attemptFails = 15
   estabResets = 10
   currEstab = 8
   inSegs = 403303
   outSegs = 329919
   retransSegs = 1
   inErrs = 0
   outRsts = 24
```

3 To check locally destined and generated UDP packets, execute each of the following commands twice:

display Vr/VOIP Ip Udp statistics

Check for incrementing statistics. Under normal operation, none of the fields should be incrementing. In particular, the fields "inDatagrams", "noPorts", and "inErrors" should not increment under normal operation.

The following shows a sample output using this command:

```
> display Vr/VOIP Ip Udp statistics
Vr/VOIP Ip Udp
   inDatagrams = 0
   noPorts     = 0
   inErrors    = 0
   outDatagrams = 0
```

display Vr/0 Ip Udp

Check for incrementing statistics. Under normal operation, only "inDatagrams" and "outDatagrams" are incrementing at the rate of approximately one packet per minute. In particular, the fields "inErrors", and "noPorts" should not increment under normal operation.

The following shows a sample output using this command:

```
> display Vr/0 Ip Udp
Vr/0 Ip Udp
inDatagrams = 257
noPorts = 3
inErrors = 0
outDatagrams = 8094
```

4 This procedure is complete.

—End—

Variable	Value
Vr/0	The management virtual router. This Vr is used for handling OAM traffic to the nodes. This includes TCP sessions such as FMIP, telnet, or FTP, and UDP traffic such as NTP time synchronization with the Multiservice Data Manager workstations.
Vr/VOIP	Virtual routers used for routing traffic only. These virtual routers never provide termination for TCP or UDP streams.

Locking out packet traffic

CAUTION
Service affecting
All of the following commands are service affecting. The only variation is the degree to which service is affected.

Step	Action

1 Enter the high impact command confirmation:

```
DISABLENEXTcmdchk
```

CAUTION
Service affecting
Locking an interface will cause a loss of service.

2 The following commands can be used to lock out traffic on different types of interfaces:

For ATM interfaces:

The following command locks out the traffic of all ATM connections configured under an ATM MPE component:

```
lock AtmMpe/<n>
```

For Ethernet interfaces:

The following command locks out all traffic on an Ethernet interface:

```
lock La/<y>
```

For a single protocol port:

The following command locks out all the traffic being sent to a single protocol port from its associated media (linkToMedia):

```
lock Vr/VOIP Pp/<protocolport>
```

3 If the problem interface can not be isolated, then the following command can be executed:

```
DISABLENEXTcmdchk
```

```
lock Vr/VoIP IP
```

Note: **All traffic** that passes through this virtual router is locked out.

4 This procedure is complete.

—End—

Variable	Value
<n>	The instance number of the ATM MPE component.
<y>	The number of the configured port starting from 0.
<protocolport>	The character string for the protocol port name.

Verifying the statistics for the MSS/MG15000 RADIUS server

Step	Action

1 To display the operating statistics for the RADIUS server, execute the following commands:

```
display Ac Radius Server/<x>
```

```
display Ac Radius
```

The following shows sample output for <x> = 0:

```
> display Ac Radius Server/0
Ac Radius Server/0
    adminstate          = unlocked
    opstate             = enabled
    usagestate          = active
    accessrequest       = 21
    accessaccepts       = 21
    accessrejects       = 0
    packetsdropped      = 0
    accessretransmissions  = 0
    timeouts            = 0
    badauthentications  = 0
    pendingrequests     = 0
    unknowntypes        = 0
    malformedaccessresponses = 1
    roundtriptime       = 1 second
> display Ac Radius
Ac Radius
    badserveraddresspdus = 0
```

Check the statistics for the following fields:

- "adminstate" - if the value for both Servers is locked, then you have closed access
- "opstate" - if the value for both Servers is disabled, then you have closed access
- "accessrequest" - increments when a login authentication is requested
- "accessaccepts" - increments when a login authentication request is accepted
- "accessrejects" - increments when an access request is rejected due to a bad userid/password combination or an invalid PDU type
- "packetsdropped" - increments when an unexpected RADIUS PDU was received from the RADIUS server
- "timeouts" - increments when a response from the RADIUS server was not within the response window
- "badauthentications" - increments when a bad value is found in the authentication request field
- "unknowntypes" - increments when a non-access accept or reject PDU is received from the RADIUS server
- "malformedaccessresponses" - increments when an incomplete VSA is received from the RADIUS server
- "roundtriptime" - a high value indicates network or RADIUS server delays

- "badserveraddresspdus" - increments when a response is received from a RADIUS server other than the one to which the request was sent

2 This procedure is complete.

—End—

Variable	Value
<x>	The number of the RADIUS server.

Viewing IPSec general statistics on the MSS/MG15000

Step	Action
1	Verify the general statistics for the security policy database by executing the following command: `display Vr/0 Ip Spd/1` Verify the values for the fields "outDiscards", "inSaLookupFailures", "inDiscards" and "inMismatch".
2	This procedure is complete.

—End—

Verifying IPSec statistics for a specific connection on the MSS/MG15000

If a specific service such as FTP, Telnet, FMIP or NTP is not working, use this procedure to display the IPSec statistics for the service.

Step	Action
1	Using the procedure "Viewing MSS/MG15000 IPSec information" located in *NN10180-612 Nortel Multiservice Switch 15000, Media Gateway 15000 and Multiservice Data Manager in Carrier VoIP Networks Security and Administration - Securing Network Elements*, display the IPSec configuration information for the switch.
2	Identify the policy index, security association IP address and SPI for the service of interest.
3	Display the statistics for the policy and security association associated with the service of interest by executing the following command:

```
display Vr/0 Ip Spd/1 Policy/<x> Sa/<a.b.c.d>,esp,<y>
```

Verify the values for the fields "inTraffic", outTraffic", "inPackets", "decryptErrors", "authErrors", "policyErrors" and "otherErrors".

If the field "authErrors" is non-zero, then verify the authentication parameters.

If the field "decryptErrors" is increasing, then verify the key used for encryption.

If the field "policyErrors" is increasing, then verify the security association parameters for the SPIs.

4 This procedure is complete.

—End—

Variable	Value
`Vr/0`	The management virtual router. This Vr is used for handling OAM traffic to the nodes. This includes TCP sessions such as FMIP, telnet, or FTP, and UDP traffic such as NTP time synchronization with the Multiservice Data Manager workstations.
`<x>`	The instance value of the policy for inbound or outbound traffic.
`<y>`	The security parameter index (SPI) for the security association.
`<a.b.c.d>`	The IP address for the security association.

Viewing IPSec and SSH error logs on the MDM workstation

This procedure is used to set the level of the log information that is required to capture IPSec and SSH error logs for viewing.

Step	Action
1	Ensure that logging has been set at the debug level by editing the file */etc/syslog.conf*: `vi /etc/syslog.conf`
2	Add the following line: `*.debug /var/adm/messages` Save and close the file.

Note: Do not stay at this level for any length of time due to the high level of disk usage.

3 Execute the following command to view the violations that are being generated:

```
tail -f /var/adm/messages
```

4 This procedure is complete.

—End—

Appendix A
Cause code reference for PT-AAL1 / UA-AAL1 call processing

There are five groups of cause codes used to troubleshoot problems with call processing:

- cause code definitions used for call processing troubleshooting
- resource unavailable class definitions
- service or option not implemented class definitions
- invalid message (parameter out of range) class definitions
- protocol error (unknown message) class definitions

Cause code definitions used for call processing troubleshooting

Cause Number 1: unallocated (unassigned) number indicates that the called party cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).

Cause Number 2: no route to specified transit network indicates that the equipment sending this cause has received a request to route the call through a particular network which it does not recognize. The equipment sending this cause does not recognize the transit network because either the transit network does not exist or because the transit network, while it does exist, does not serve the equipment that is sending this cause. This cause is supported on a network-dependent basis.

Cause Number 3: no route to destination indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination required. This cause is supported on a network-dependent basis.

Cause Number 10: VPCI/VCI unacceptable indicates that the virtual channel most recently identified is not acceptable to the sending entity for use in this call.

Cause Number 16: normal call clearing indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations. the source of this cause is not the network.

Cause Number 17: user busy This cause is used to indicate that the called party is unable to accept another call because the user busy condition has been encountered. This cause value may be generated by the called user or by the network.

Cause Number 18: no user responding is used when a called party does not respond to a call establishment message with a connect indication within the prescribed period of time allocated.

Cause Number 19: no answer from user (user alerted) is used when a called party does not respond to a call establishment message with a connect indication within the prescribed period of time.

Cause Number 21: call rejected indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

Cause Number 22: number changed is returned to a calling party when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this capability, cause number #1, "unassigned (unallocated) number", is used.

Cause Number 23: user rejects all calls with calling line identification restriction (CLIR) is returned by the called party when the call is offered without calling party number information and the called party requires this information.

Cause Number 27: destination out of order indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. This means that a signalling message was unable to be delivered to the remote user due possible to a physical layer or SAAL failure at the remote user end, or because the user equipment is off-line.

Cause Number 28: invalid number format (address incomplete) indicates that the called user cannot be reached because the called party number is not in a valid format or is not complete.

Cause Number 30: response to STATUS ENQUIRY is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message. This cause is used to report a normal event only when no other cause in the normal class applies.

Cause Number 31: normal, unspecified reports a normal event only when no other cause in the normal class applies.

Cause Number 32: too many pending add party requests is not provided.

Cause Number 34: requested called party soft PVPC or PVCC unavailable indicates that there is no appropriate circuit/channel presently available to handle the call.

Resource unavailable class definitions

Cause Number 35: requested VPCI/VCI not available indicates that the requested VPCI/VCI is not available.

Cause Number 36: VPC/VCI assignment failure is not provided.

Cause Number 37: user cell rate not available is not provided.

Cause Number 38: network out of order indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time. Immediately re-attempting the call is unlikely to be successful.

Cause Number 41: temporary failure indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time. The user may wish to try another call attempt immediately.

Cause Number 42: switching equipment congestion is not provided.

Cause Number 43: access information discarded indicates that the network could not deliver access information to the remote user as requested, for example, ATM adaptation layer parameters, broadband low layer information, broadband high layer information, or sub-address as indicated in the diagnostic.

Cause Number 45: no VPCI/VCI available indicates that there is no appropriate VPCI/VCI presently available to handle the call.

Cause Number 47: resource unavailable, unspecified is used to report a resource unavailable event only when no other cause in the resource unavailable class applies. Service or option not available class definitions

Cause Number 49: Quality of Service unavailable is used to report that the requested Quality of Service cannot be provided.

Cause Number 50: requested facility not subscribed is not provided.

Cause Number 51: user cell rate not available is used to report that the requested ATM Traffic Descriptor cannot be obtained.

Cause Number 53: call cleared due to change in PGL b;outgoing calls barred within CUG c indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.

Cause Number 57: bearer capability not authorized indicates that the user has requested a bearer capability that is implemented by the equipment which generated this cause, but the user is not authorized to use.

Cause Number 58: bearer capability not currently available indicates that the user requested a bearer capability that is implemented by the equipment which generated the cause but which is not available at this time.

Cause Number 63: Service or option not available, unspecified is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Service or option not implemented class definitions

Cause Number 65: bearer capability not implemented indicates that the equipment sending this cause does not support the bearer capability requested.

Cause Number 73: unsupported combination of traffic parameters indicates that the combination of traffic parameters contained in the ATM traffic descriptor information element is not supported.

Cause Number 78: AAL parameters cannot be supported is not provided.

Cause Number 79: service or option not implemented, unspecified is not provided.

Invalid message (parameter out of range) class definitions

Cause Number 81: invalid call reference value indicates that the equipment sending this cause has received a message with a call reference that is not currently in use on the user-network interface.

Cause Number 82: identified channel does not exist indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call.

Cause Number 88: incompatible destination indicates that the equipment sending this cause has received a request to establish a call that has broadband low layer information, broadband high layer information, or other compatibility attributes that cannot be accommodated.

Cause Number 89: invalid endpoint reference value indicates that the equipment sending this cause has received a message with an endpoint reference that is currently not in use on the user-network interface.

Cause Number 91: invalid transit network selection indicates that a transit network identification was received that is of an incorrect format.

Cause Number 92: too many pending add party requests indicates a temporary condition when the calling party sends an add party message but the network is unable to accept another add party message because its queues are full.

Cause Number 93: AAL parameters cannot be supported indicates that the equipment sending this cause has received a request to establish a call that has ATM adaptation layer parameters and which cannot be accommodated.

Protocol Error (unknown message) class definitions

Cause Number 96: mandatory information element is missing indicates that the equipment sending this cause has received a message that is missing an information element and which must be present in the message before the message can be processed.

Cause Number 97: message type non-existent or not implemented indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined, or defined, but not implemented by the equipment sending this cause.

Cause Number 99: information element non-existent or not implemented indicates that the equipment sending this cause has received a message that includes information element(s) not recognized because the information element identifier(s) are not defined, or are defined, but not implemented by the equipment sending the cause. This cause indicates that the information element(s) were discarded. However, the information element is not required to be present in the message for the equipment sending this cause to process the message.

Cause Number 100: invalid information element contents indicates that the equipment sending this cause has received an information element that it has implemented; however, one or more of the fields in the information element are coded in such a way that it cannot be implemented by the equipment ending this cause.

Cause Number 101: message not compatible with call state indicates that a message has been received that is incompatible with the call state.

Cause Number 102: recovery on timer expiry indicates that a procedure has been initiated by the expiry of a timer in association with error handling procedures.

Cause Number 104: incorrect message length is not provided.

Cause Number 111: protocol error, unspecified is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause Number 127: internetworking, unspecified is not provided.

Cause Number 128: next node unreachable is not provided.

Cause Number 129: release received from outside the global rerouting domain is not provided.

Cause Number 130: global rerouting operation complete is not provided.

Cause Number 160: DTL Transit not my node ID is not provided.

Appendix B Connecting to Multiservice Data Manager tools

Refer to the following section for more information about how to connect to Nortel Multiservice Data Manager (MDM) tools. If access to the MDM Toolset tools has been restricted, ensure that your userid is assigned to a user group with appropriate authorization. Use these procedures where indicated in the specific chapter.

Connecting to Multiservice Data Manager tools

	Task	Use the section...	in...
1.	Using the MDM Toolset on the Multiservice Data Manager server, open the Command Console tool and connect to the network.	"Connecting to the network"	*241-6001-804 Nortel Multiservice Data Manager Utilities*
2.	On the server, log the command output to a file.	"Logging command output to a file"	*241-6001-804 Nortel Multiservice Data Manager Utilities*
3.	On the server, open the Network Viewer tool, the Alarm Display tool, and the Alarm Help.	"Starting Network Viewer" "Starting Alarm Display" "Starting Alarm Help"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*
4.	Using the Network Viewer tool, determine if there is a Multiservice Switch node that is experiencing problems.	"Understanding the network display"	*241-6001-011 Nortel Multiservice Data Manager Fault Management Tools*

Appendix C
Using the PVG DS0 visibility tool

DS0 Visibility Tool is an on-switch safe tool that allows the user to display aspects of a DS0 endpoint that are not a direct consequence of provisioning messages, but rather a result of processing Media Gateway Controller (MGC) commands, and state changes induced by the traffic stream.

The DS0 Visiblity Tool is available for VSP2, VSP3, VSP3-0, and 2pVSP4e FP cards on the MG 15000 in switched configurations.

The DS0 Visibility tool is a stand-alone tool that is available during the lifetime of the card and does not require loading/deloading.

Current available attributes displayed using the DS0 visibility tool are:

- DS0 connection ID: terminatation ID, context ID, ephemeral ID
- RTAG and LCID
- DS0 connection mode: inactive, looparound, sendOnly, recvOnly, sendRecv
- DS0 call state: idle, inCall, oos, oosGwc
- Current connectivity information:
  - Call controller IP address and UDP port
  - remote and local IP/UDP port
  - ATM address/VCCI/CID
  - connection duration
- Current value of Type of Call: voice, VBD, CCD, T38
- Negotiated capabilities:
  - DTMF relay: On/Off and Dynamic Payload Type
  - Autonomous Fax relay: Enable/Disable, Remote T.38 UDP port, effective redundancy depth, packet threshold size, T.38 maximum bit rate

  - VBD upspeed: On/Off and LogLaw

- DS0 codec:
  - Type: NA, EVRC, SMV, Q13, CSD, AMR, G711u, G711a, G729, G726-40, G726-32, G726-24, EVRC0
  - Profile: NA, P1, P2, P3, P7, Custom 100, Custom 200
  - Packetization time: 0ms/ 5ms/10ms/20ms
  - Dynamic payload: NA, G711u, G711a, CN, G729-8k, Microsoft-Rta, Evrc, Evrc0, CCD, G726-16-IETF, G726-24-IETF, G726-32-IETF, G726-40-IETF, G726-16-ITU, G726-24-ITU, G726-32-ITU, G726-40-ITU, Wildcard
- DS0 ecan setting: On/Off
- DS0 silence suppression setting: On/Off
- TrFO: active/inactive/NA
- Digit Collection in progress: Y/N
- Tones Playing: Tone ID
- Per call stats:PS, PR, TPL, BU, BO, PD, IR, duration, jitter, latency, and Call Type

Appendix D
Using safe shell debug commands

Safe shell commands provide additional tools for use in the debug shell mode to monitor and display debug data without impacting services on the card. Generally, these commands exist on all MSS 15K VSP cards except where otherwise noted.

Command	Description	VSP FP Exceptions
dMa	SPM - print the state of the Memory Allocator	
showOvldCounters	SPM - shows the OVLD counters	
printBufferCounts	SPM - print out counts of bufferRep + objectBroker counts	
dAll	SPM - display various information such as CRCS, MDCS, NTRQ, DLCX, Resets, etc...	
OMshow	SPM - OM related info including the error history	
printPEDBstat	SPM - display the Protocol Engine database status	
PrintCurrentTransaction	SPM - display the current transactions	
displaySoRestoreErrors	SPM - display if there was a restore failure and the SO that failed to be restored and the reason it failed	
displaySoPopulateErrors	SPM - checks if there was a populate failure and prints out the SO that failed to be populated and the reason it failed	
jaPrint	SPM - print data held by the Journalling Agent	
printJTransCounts	SPM - messages sent, nacks sent, acks received, nacks retransmitted etc	
getAllDsvcStats	SPM - display the dsvc statistics for the system	
printBufferUse	SPM - display how many buffers are owned by each task for each buffer size	
memShow	SPM - display the memory usage	

Command	Description	VSP FP Exceptions
getCpuUtilization	SPM - display the CPU utilization	
gt	SPM - output all current TDM trunk data	
gs	SPM - get provisioned trunk id details	
gg	SPM - displays CmGatewayConfig and PacketProfileConfig	
gi	SPM - get all provisioned IP access trunks	
ga	SPM - get all provisioned AAL2 trunks	
showPEProv	SPM - show the Protocol Engine Provisioning	
showQMgrs	SPM - display stats on msgs sent/received for all queue managers	VSP2, VSP3
showQMgr	SPM - display stats on msgs sent/received for specified queue managers	VSP2, VSP3
dbShow	SPM - Displays all information for that connection	
iepRoot	SPM - Displays all information for Root	
iepIP	SPM - Displays all information for that IP ephemeral endpoint	
iepATM	SPM - Displays all information for that ATM ephemeral endpoint	
iepH248Term	SPM - Displays all information for that termination	
cpb	SPM - Displays a list of all endpoints in state CPB	
getProtType	SPM - Displays current protocol name and version	
printProtList	SPM - Displays available protocol versions	
PrintIncTransList	SPM - Print the incoming transaction list.	
PrintAgedOutTransList	SPM - Print the age out transaction list	
PrintOutTransList	SPM - Print the outgoing transaction list.	
PrintQuaTransList	SPM - Print the quarantine transaction list	
PrintToProcessTransList	SPM - Print the Transaction to be process for an H.248 message.	
PrintAckRequestTransList	SPM - Print the immediate ack list	
PrintCurrentDatagram	SPM - Print the current datagram	
PrintConnComp	SPM - Print the connection object	
PrintMaintComp	SPM - Print the maintenance object	

Command	Description	VSP FP Exceptions
PrintTransComp	SPM - Print the transaction object.	
PrintNotifComp	SPM - Print the notification object	
PrintTrunksMainState	SPM - Print the current SSM Trunks Maintainance state	
printAuditOfContextDB	SPM - Display audit of contexts	
printContext DB	SPM - Display all information about all active contexts	
printPackageDB	SPM - Display the content of the package database	
printMessageQueueState	SPM - Display the Input Message Queue Stats	
printLoggedInfo	SPM - Displays logged information	
getDsvcComponent	SPM - Display state of DSVC component	
getDsvcPrecreation	SPM - Display precreation state	
peov	SPM - Display the overload status of the PE	
printAuditTaskResults	SPM - Display the Context Ids cleared by the post-journal audit of PE-CM databases	
checkVpmTimer	SPM - prints the status of vpmTimer	
printVpmList	SPM - Prints the Outstanding vpmList	
getMdcxRetryInfo	SPM - Dump MDCX retry data	
printDsvcList	SPM - Prints information about the DSVCs lists	
class_counts	SPM - displays values of all Class counters	
vpmTip	SPM - Local Tip Count	
feTip	SPM - Far End Tip Count	
feUSC	SPM - Far End USC Count	
nCasProv	SPM - Show CAS Trunk Prov Msg Counts	
nCli	SPM - Cell Loss Integration Count	
peReq	SPM - PE Request Count (Valid/Invalid)	
nAal2	SPM - No of messages sent by CM to Aal2Type3Task	
dcenabled	SPM - Query Digit Collection capability	
ssmpending	SPM - Display info on pending request to SSM	
ssmactive	SPM - Display active request on SSM	
nCrcx	SPM - Valid CRCX Count	

Command	Description	VSP FP Exceptions
nMdcx	SPM - Valid MDCX Count	
nNtrq	SPM - Valid NTRQ Count	
nDlcx	SPM - Valid DLCX Count	
nAudit	SPM - Valid Audit Count	
nTrunksMain	SPM - Valid TrunksMain Count	
nReset	SPM - Valid Reset Count	
nSrvChng	SPM - Valid SrvChng Count	
ipCap	SPM - Ip Capability Set Tx/Rx	
newCap	SPM - New Capability Set Tx/Rx	
callStat	SPM - Call Statistics Tx/Rx	
dFax	SPM - Display fax tone setting	
sModem	SPM - Modem tone setting	
dSilSup	SPM - Display Silence Suppression settings	
sCodec	SPM - Codec settings	
dCodec	SPM - Display possible codec settings	
sEcan	SPM - Echo Cancellor settings	
dEcan	SPM - Echo Cancellor possible settings	
sEpType	SPM - Descriptor Protocol settings	
sCodecIndex	SPM - Codec Index settings	
sPll	SPM - Packet Log Law settings	
dRNA	SPM - Remote Nsap Address settings	
opState	SPM - Displays message counters for SSM/VPM operational state	
dispAnnCapability	SPM - Query Announcements capability	
getSSMRtag	SPM - Display the current SSM Rtag	
printE1ToSTM1	SPM - Converts an E1 to it s internal STM1 value	
cmOMshow	SPM - Displays the OM statistics for commands and ACKS/ NACKS and verb	
showUSCstats	SPM - Itu mode USC statistics	
showSSMStats	SPM - Print requests, acks and notifications for the ssm	
printAesaTable	SPM - Prints the full AESA/NSAP table	
getDsvcState	SPM - get state of given trunk ID	

Command	Description	VSP FP Exceptions
getDsvcStats	SPM - get stats of the NSAP address associated with the given trunk	
getDsvcTimerState	SPM - get short/long cache timer state of given trunk ID	
getNsapState	SPM - get state of NSAP associated with the given trunk ID	
getPersistenceTimer	SPM - get length of persistence timer in ms	
getTimeoutTimer	SPM - get length of creation timeout in ms	
listDsvcs	SPM - list DSVCs in the system	
mdisp	SPM - Display rtags being monitored	VSP3-o, 2pVSP4e
printVcacFlag	SPM - Print the state of the VCAC flag	
vcacIp	SPM - get VCAC stats associated with the IP trunk	
vcacProv	SPM - get VCAC provisioned values	
vcacVcci	SPM - get VCAC stats associated with the given VCC	
vcctr	SPM - get the VCCs already attempted for this CRCX	
printCMPEInfo	SPM - Dumps all the entries in the CMPE buffer	
printTerminalInfo	SSM - output terminal data for channel rtag,lcid	VSP2
displayAllIuaData	SSM - display All Iua Data	
mtpDumpQ703	SSM - Dump the state information of the entire Q703 application	VSP2, VSP3
m2uaPrint	SSM - dumps the entire M2ua	VSP2, VSP3
v5DisplayData	SSM - display the data for v5	
associationShowAll	SSM - display the digServer status	

Appendix E
SVC Failure Alarms

These PVG ATM alarms indicate existing PDC SVC failure conditions. All the alarms display file and line which allows you to locate the failure condition and fix it if required. In some cases different alarms reuse the same text message because it is the same type of failure. However, the file and line are different due to different code location and the reason for the failure is different.

The following table lists the probable cause of alarms in index group 7056, subindex 0007 (Voice Server Processor (VSP)/Narrowband Service Trunk over ATM (Nsta)).

Note: The relevant fields in these alarms are:

- status: message
- probable cause: processor problem
- severity: major

Alarm
SVC creation failure: incompatible destination - cause 88
SVC failure - no matching connection (code 18)
SVC failure - no matching connection (code 18)
SVC failure - no matching connection (code 18)
SVC failure: free SVC pool exhausted (code 18)
The SVC creation failed - no user responding (code 18)
The SVC creation failed - no user responding (code 18)
SVC create failure: incoming setup pdu IE problem
SVC setup failure: napCauseResourceUnavail (47)
SVC create failure: could not send setup pdu

The alarms are displayed as shown below:

```
PROV 169>
        Nsta/14 Vgs; 2005-09-11 08:28:25.91
MSG major processing processorProblem
70560007
        ADMIN: unlocked OPER: enabled USAGE: active
        AVAIL: PROC: CNTRL:
        ALARM: STBY: notSet UNKNW: false
        Id: 0F000004 Rel:
        Com: SVC failure - no matching connection (code 18)
        Int: 0/0/0/0; pvgCfsNetworkInterfaceMgr.cc; 2423; CG02Aha

Card 15 ->
        Nsta/14 Vgs Aal2Svc TConn/561; 2005-09-12 06:21:20.95
MSG major processing processorProblem 70560007
        ADMIN: unlocked OPER: enabled USAGE: active
        AVAIL: PROC: CNTRL:
        ALARM: STBY: notSet UNKNW: false
        Id: 0F000004 Rel:
        Com: SVC create failure: incoming setup pdu ie problem
        Int: 0/0/0/0; pvgCfsReceivingConnection.cc; 762; CG02Ahi
```

Carrier VoIP

MSS15K, MG15K, and MDM in Succession Networks Fault Management Troubleshooting PT-AAL1/UA-AAL1/UA-IP/PT-IP

Publication: NN10198-912
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.