NORTEL
NETWORKS

Nortel Networks Multiservice Switch

7400/15000/20000

Operations: Hunt Group Server

NN10600-415

Nortel Networks Multiservice Switch 7400/15000/20000

Operations: Hunt Group Server

Publication: NN10600-415
Document status: Standard
Document version: 6.1S1
Document date: August 2004

Printed in Canada

Publication history

August 2004

August 2004 6.1S1
General availability. Contains information on Nortel Networks Multiservice Switch 7400, 15000, and 20000 for the PCR6.1 release.

Contents

List of figures

List of tables

About this document

This guide describes the hunt group capability for Dynamic Packet Routing System (DPRS) services.

The following topics are discussed in this section:

- “Who should read this document and why” (page 11)
- “What you need to know” (page 12)
- “What’s new in this document” (page 12)
- “Text conventions” (page 12)
- “Related documents” (page 13)
- “How to get more help” (page 14)

Who should read this document and why

This guide is for persons who perform the following tasks for a hunt group:

- planning
- engineering
- installing and configuring
- provisioning
- operating and maintaining
- troubleshooting

What you need to know

This guide assumes that you understand the Nortel Networks Multiservice Switch network architecture. You can learn more about the product by reading NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*.

What's new in this document

There were no new features added to this document.

Other changes made to this document include the following:

- The terms Passport and PVG have been rebranded in conjunction with the new Nortel Networks' brand simplified naming format. Passport is now referred to as the Nortel Networks Multiservice Switch, and PVG is now Media Gateway 7480/15000. For more information on the product rebranding, refer to NN10600-000 *Nortel Networks Multiservice Switch 7400/15000/20000 What's New in PCR6.1*.
- Changes made throughout the document to enhance compliance with Nortel Networks documentation standards (for example, Modular Task Based Information standards).

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- `nonproportional spaced bold type`

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

  Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- `<general_term>`

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE, lowercase

  Nortel Networks Multiservice Switch node commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

Related documents

See NN10600-001 *Nortel Networks Multiservice Switch 7400/15000/20000 Basics: Customer Documentation* for a complete list of documents.

See the following documents for information related to the hunt groups capability:

- NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
- NN10600-900 *Nortel Networks Multiservice Switch 7400/15000/20000 Frame Relay Technology Fundamentals*
- NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/20000 Overview*
- NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server*
- NN10600-060 *Nortel Networks Multiservice Switch 7400/15000/20000 Component Reference*
- NN10600-500 *Nortel Networks Multiservice Switch 6400/7400/15000/20000 Alarms Reference*

How to get more help

For information on training, problem reporting, and technical support, see the “Nortel Networks support services” section in the *product overview document.*

Chapter 1
Hunt group configuration

Configure a hunt group so that a single data network address (DNA) can represent a group of service DNAs.

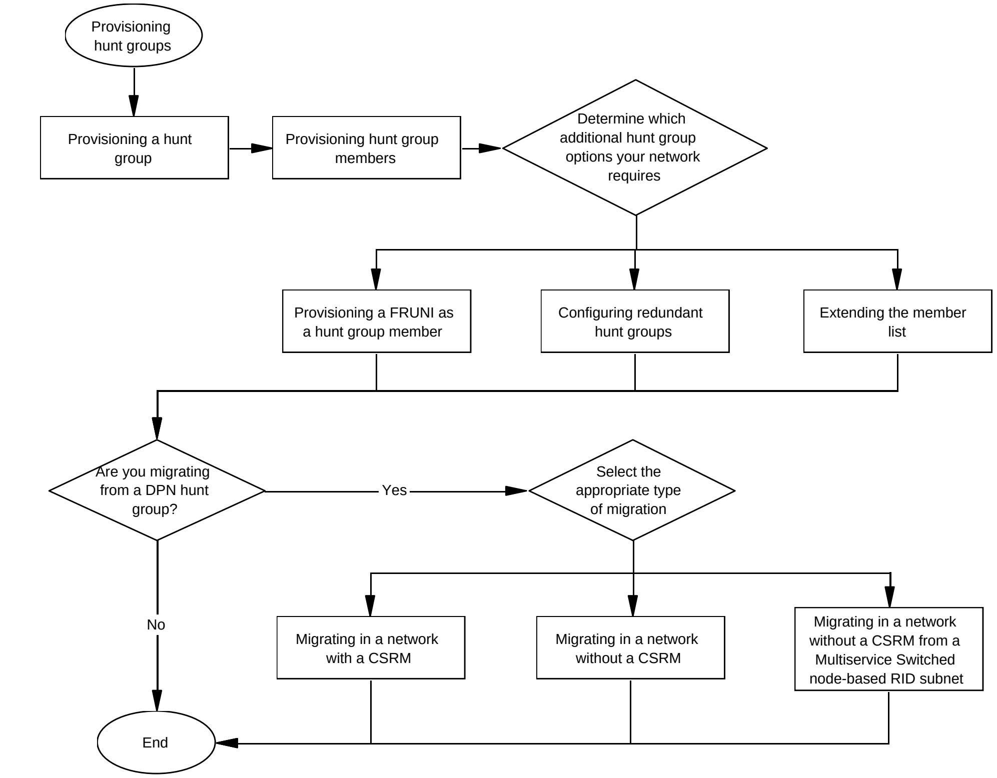
Prerequisites to hunt group configuration

- If you are unfamiliar with the concepts related to creating and using hunt groups, see “Hunt groups” (page 41)
- Before configuring a hunt group, install the base and networking software, and subnetInterface and dpnRouting from the networking software using the procedures in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*.
- Complete the procedure “Configuring call hunting through a hunt group server” in NN10600-755 *Nortel Networks Multiservice Switch 7400 Operations: Voice Networking* before performing this task.

Hunt group configuration procedures

This task flow shows you the sequence of procedures you perform to configure hunt groups. To link to any procedure, go to “Hunt group configuration procedure navigation” (page 17).

Figure 1
Hunt group configuration procedures


Provisioning hunt groups
Provisioning a hunt group
Provisioning hunt group members
Determine which additional hunt group options your network requires
Provisioning a FRUNI as a hunt group member
Configuring redundant hunt groups
Extending the member list
Are you migrating from a DPN hunt group?
Yes
Select the appropriate type of migration
No
Migrating in a network with a CSRM
Migrating in a network without a CSRM
Migrating in a network without a CSRM from a Multiservice Switched node-based RID subnet
End

Hunt group configuration procedure navigation

- “Configuring the HuntGroup component” (page 18)
- “Configuring hunt group members” (page 20)
- “Configuring a FRUNI as a hunt group member” (page 21)
- “Configuring redundant hunt groups” (page 23)
- “Extending the member list” (page 24)
- “Migrating in a network with a CSRM” (page 25)
- “Migrating in a network without a CSRM from an RM-based RID subnet” (page 26)
- “Migrating in a network without a CSRM from a Multiservice Switch node-based RID subnet” (page 27)

Configuring the HuntGroup component

Configure the *HuntGroup* component to which you can assign individual members.

Prerequisites

- The hunt group software named huntGroupSystem must be installed using the procedures in NN10600-270 *Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation*.

Procedure steps

1 Add the *Hg* component.

```
add Hg/<n>
```

2 Link the server to the logical processor.

```
set Hg/<n> lp lp/<m>
```

3 Set the customer identifier for the hunt group.

```
set Hg/<n> cid <id>
```

4 Define the hunt group DNA.

```
set Hg/<n> address <npi>.<addr>
```

5 Set the selection policy for the hunt group.

```
set Hg/<n> policy <policy>
```

6 Set the maximum number of hunt attempts for a call.

```
set Hg/<n> maxHunt <max>
```

7 Set the support for propagation of suffix address digits.

```
set Hg/<n> appendSuffixDigits <setting>
```

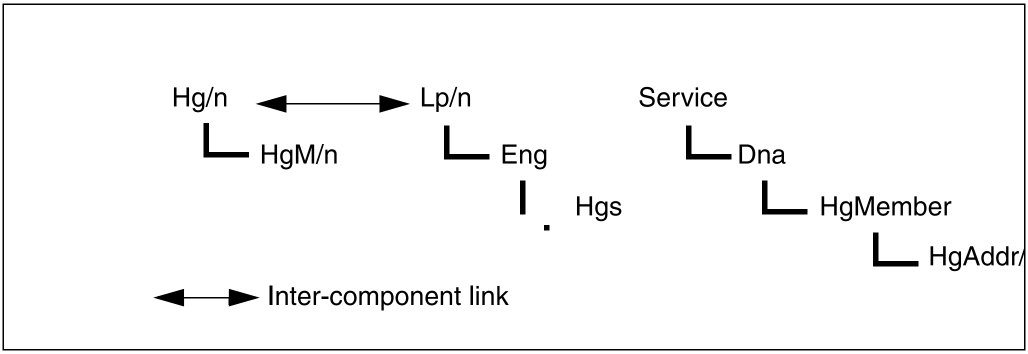
Variable definitions

Variable	Value
<addr>	is the X.121 or E.164 address digits
<id>	is the identifier, in the range of 1 to 8191
<m>	is the number of the LP being provisioned
(Sheet 1 of 2)	

Variable	Value
<max>	is the number in the range of 1 to 63
<n>	is the instance number of the hunt group, in the range of 1 to 65535 (256 for each LP)
<npi>	is the numbering plan indicator, either x for X.121 addresses or e for E.164 addresses
<policy>	is startFromZero, rotary, or mostAvailable
<setting>	is the setting of the support for propagation of suffix address digits. A value of yes causes the server to append suffix address digits. A value of no causes the server not to append suffix address digits.
(Sheet 2 of 2)	

Procedure job aid

Figure 2
Hunt group component hierarchy



Configuring hunt group members

Provision hunt group members by adding the DNA of each member to the group.

Procedure steps

1 Add the *HgM* component.

```
add Hg/<n> Hgm/<m>
```

2 Define the DNA of the hunt group member.

```
set Hg/<n> Hgm/<m> address <npi>.<addr>
```

Variable definitions

Variable	Value
<addr>	is the X.121 or E.164 address digits. A semantic check ensures that a hunt group is not provisioned with duplicate member addresses.
<m>	is the instance number of the hunt group member, in the range of 2 to 63
<n>	is the instance number of the hunt group, in the range of 1 to 65535 (256 for each LP)
<npi>	is the numbering plan indicator, either *x* for X.121 addresses or *e* for E.164 addresses

Configuring a FRUNI as a hunt group member

Configure a FRUNI as a hunt group member. You must define the address of each hunt group to which the FRUNI belongs and add the FRUNI to the list of member DNAs under the Hunt Group Server.

Prerequisites

- A hunt group to which the FRUNI is to be added as a member must have already been provisioned.

Procedure steps

1 Enter provisioning mode.

```
start prov
```

2 Create an instance of the *HuntGroupMember* component under the address component of the interface.

```
add FrUni/<n> Dna HgM
```

3 Specify the maximum permitted change in the available aggregate CIR before the hunt group member sends an availability message packet to the hunt group server, notifying it of the change.

```
set FrUni/<n> Dna HgM aut <threshold>
```

4 Specify the address of the hunt group to which the interface belongs.

```
set FrUni/<n> Dna HgM HgAddr/<x> npi <npi>

set FrUni/<n> Dna HgM HgAddr/<x> dna <dna>
```

5 Optionally, configure a backup hunt group DNA by adding a second *HgAddr* subcomponent under the *HgM* component.

```
add FrUni/<n> Dna HgM HgAddr/<y>
```

6 Specify the backup address for the hunt group.

```
set FrUni/<n> Dna HgM HgAddr/<y> npi <npi>

set FrUni/<n> Dna HgM HgAddr/<y> dna <dna2>
```

7 Add the FRUNI to the list of hunt group addresses under the corresponding hunt group.

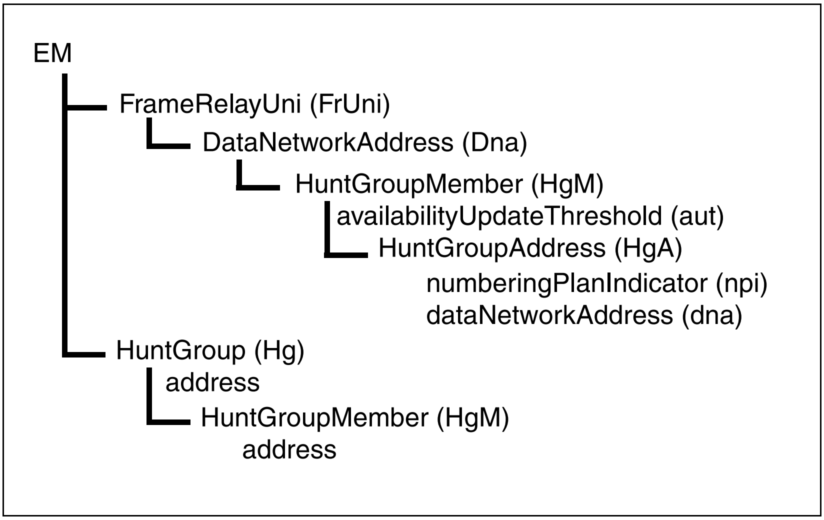
```
add Hg/<g> HgM/<m>

set Hg/<g> HgM/<m> address <npi.dna>
```

Variable definitions

Variable	Value
<dna>	is the data network address of the hunt group
<dna2>	is the backup data network address of the hunt group
<g>	is the instance number of the hunt group
<m>	is the instance number of the hunt group member
<n>	is the instance number of the FRUNI
<npi>	is the numbering plan indicator of the hunt group address
<npi.dna>	is the address of the FRUNI
<threshold>	is the maximum permitted change in CIR in bits/s
<x>	is the instance number of the hunt group address
<y>	is the instance number of the backup hunt group address

Procedure job aid

Figure 3
Configuring a FRUNI as a hunt group member component hierarchy



Configuring redundant hunt groups

Configure redundant hunt groups using the call redirection capability, if you have a critical hunt group that cannot tolerate being out of service. The redundant configuration ensures that the hunt group remains in service if the primary hunt group fails.

Prerequisites

- You must install the call redirection software before you can configure redundant hunt groups. See NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server*.

Procedure steps

1. Provision an alternative hunt group DNA with the identical member list as the primary hunt group.
2. Provision the member services with both the primary and alternative hunt group DNAs so that they can send availability information to both hunt groups.
3. Use the call redirection capability to back up the primary hunt group DNA with the alternative hunt group DNA, making the alternative DNA the first entry in the redirection list for the primary DNA. See NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server* for details.

If there is a failure, the alternative hunt group immediately assumes the call hunting task at the point at which the primary group failed. When the primary group recovers, it resumes the call hunting task on the next new call to the primary DNA. No operator intervention is needed throughout this process.

Extending the member list

Extend the member list using the call redirection capability, if you need a hunt group of more than 63 members. If the primary hunt group is not able to select a member for a call, it sends the call to the call redirection server. The redirection server sends the call to the alternative hunt group for hunting through the alternative member list. You can chain multiple hunt groups together using this process.

Prerequisites

- You must install the call redirection software before you can extended member lists. See NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server*.

Procedure steps

1. Provision an alternative hunt group with a different hunt group DNA and a different member list from the primary hunt group.
2. Provision the member services with the alternative hunt group DNA.
3. Use the call redirection capability to back up the primary hunt group DNA with the alternative hunt group DNA. See NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server* for more details.

Migrating in a network with a CSRM

Migrate a DPN hunt to the Nortel Networks Multiservice Switch node hunt group service by changing the location of the hunt group server from the DPN node to the Multiservice Switch node. When there is a CSRM in the network, the CSRM does all source and destination call routing functions in the network.

> ***Note:*** In the process of migrating to the Multiservice Switch node capability, the original hunt group DNA remains the same.

The information in this section applies to Nortel Networks Multiservice Switch 7400 series nodes only.

Procedure steps

1. Provision the Multiservice Switch node hunt group with the same hunt group DNA and member list as the DPN hunt group that it will replace.
2. Activate the provisioning data. The CSRM destination call routing entry is dynamically overwritten to map to the Multiservice Switch node.
3. Take the DPN hunt group out of service.

Migrating in a network without a CSRM from an RM-based RID subnet

When there is no CSRM in the network, source and destination call routing functions are distributed among the Nortel Networks Multiservice Switch nodes in the network. To migrate from DPN hunt groups within RM-based RID subnets to Multiservice Switch node hunt groups, you must use the DPN source call router (SCR) retry capability.

> ***Note:*** In the process of migrating to the Multiservice Switch node capability, the original hunt group DNA remains the same.

The information in this section applies to Nortel Networks Multiservice Switch 7400 series nodes only.

Procedure steps

1. Provision the Multiservice Switch node hunt group with the same hunt group DNA and member list as the DPN hunt group that it will replace.
2. Activate the provisioning data.
3. On the RM supporting the DPN hunt group, provision a SCR entry for the hunt group DNA to the Multiservice Switch node RID on which the hunt group is located.
4. On the RM supporting the DPN hunt group, provision SCR retry for the destination call router (DCR).
5. On the Multiservice Switch node(s) which are directly connected to the RM supporting the DPN hunt group, provision a DPRS call router (CR) entry to map the hunt group DNA to the Multiservice Switch node.
6. Take the DPN hunt group out of service. Calls to the hunt group DNA are now routed to the Multiservice Switch hunt group by the DPN SCR retry capability.
7. Provision a DPRS CR entry to map the hunt group DNA to the Multiservice Switch node. Make this change on all DPRS call routers in the network.
8. Delete the SCR retry for the DCR.

Migrating in a network without a CSRM from a Multiservice Switch node-based RID subnet

When there is no CSRM in the network, source and destination call routing functions are distributed among the Nortel Networks Multiservice Switch nodes in the network. To migrate from DPN hunt groups within Multiservice Switch node-based RID subnets to Multiservice Switch node hunt groups, you must use the Multiservice Switch node's call redirection server in a RID/MID redirection configuration.

> ***Note:*** In the process of migrating to the Multiservice Switch node capability, the original hunt group DNA remains the same.

The information in this section applies to Nortel Networks Multiservice Switch 7400 series nodes only.

Procedure steps

1. Provision the Multiservice Switch node hunt group with the same hunt group DNA and member list as the DPN hunt group that it will replace.
2. Activate the provisioning data.
3. Provision the Multiservice Switch node's call redirection (CRS) entry for the hunt group DNA to the Multiservice Switch node on which the hunt group is located. This process is called RID/MID redirection.
4. Take the DPN hunt group out of service. Calls to the hunt group DNA are now redirected to the Multiservice Switch node hunt group.
5. Provision a DPRS CR entry to map the hunt group DNA to the Multiservice Switch node. Make this change on all DPRS call routers in the network.
6. Delete the call redirection entry for the hunt group DNA.

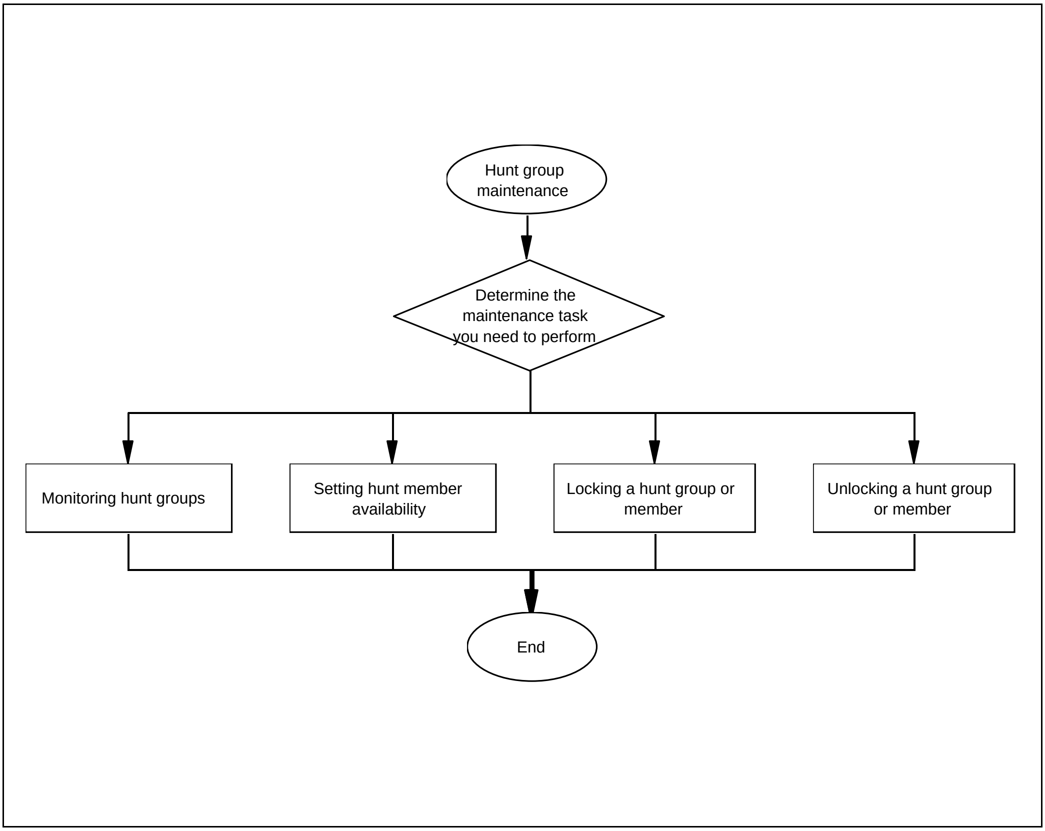
Chapter 2
Hunt group maintenance

Maintain hunt groups and solve problems that occur after installation.

Hunt group maintenance procedures

This task flow shows you the sequence of procedures you perform to maintain hunt groups. To link to any procedure, go to “Hunt group maintenance procedure navigation” (page 30).

Figure 4
Hunt group maintenance procedures


Hunt group maintenance
Determine the maintenance task you need to perform
Monitoring hunt groups
Setting hunt member availability
Locking a hunt group or member
Unlocking a hunt group or member
End

Hunt group maintenance procedure navigation

- “Monitoring hunt groups” (page 31)
- “Setting hunt group availability” (page 32)
- “Locking a hunt group member” (page 33)
- “Unlocking a hunt group member” (page 34)
- For additional information on hunt group maintenance. refer to “Additional information on hunt group maintenance” (page 35).

Monitoring hunt groups

Monitor hunt groups to determine its status and associated members.

Procedure steps

1 Determine what instances of hunt groups have been defined.

```
list hg/*
```

2 Display the status of a specific hunt group.

```
display hg/<n>
```

3 Display all the members of a specific hunt group.

```
display hg/<n> hgm/*
```

4 Display a specific member of a hunt group.

```
display hg/<n> hgm/<m>
```

5 Determine how many hunt groups are on a specific LP.

```
list lp/<x> eng hgs
```

6 Display the engineering statistics for all hunt groups on a specific LP.

```
display lp/<x> eng hgs
```

Variable definitions

Variable	Value
<m>	is the instance number of the hunt group member
<n>	is the instance number of the hunt group
<x>	is the instance number of the logical processor

Setting hunt group availability

Set hunt group availability using the set command to manually change a group member's availability value. The server accepts this value as if it were reported in a member service's availability update message.

Procedure steps

1 Set the availability value for a hunt group member.

```
set hg/<n> hgm/<m> availability <avail>
```

Variable definitions

Variable	Value
<avail>	is the availability
<m>	is the instance number of the hunt group member
<n>	is the instance number of the hunt group

Example of locking a hunt group member

1 Set the availability value for hunt group member 2 in hunt group 7 to 500.

```
set hg/7 hgm/2 availability 500
```

Locking a hunt group member

Lock a hunt group member to prevent the server from selecting that member during a hunt. You can use the lock and unlock commands to lock and unlock the hunt group at the component level. When you lock a hunt group, all calls are sent for call redirection.

> ***Note:*** While a hunt group or hunt group member is locked, the server still processes availability updates from hunt group members.

Procedure steps

1 Lock a hunt group member.

```
lock hg/<n> hgm/<m>
```

2 Optionally, you can lock the entire hunt group.

```
lock hg/<n>
```

Variable definitions

Variable	Value
<m>	is the instance number of the hunt group member
<n>	is the instance number of the hunt group

Example of locking a hunt group member

1 Lock hunt group member 2 in hunt group 5.

```
lock hg/5 hgm/2
```

Unlocking a hunt group member

Unlock a hunt group member to allow the server to select that member during a hunt. You can use the unlock command to unlock the hunt group at the component level.

Procedure steps

1 Unlock a hunt group member.

```
unlock hg/<n> hgm/<m>
```

2 Optionally, you can unlock the entire hunt group.

```
unlock hg/<n>
```

Variable definitions

Variable	Value
<m>	is the instance number of the hunt group member
<n>	is the instance number of the hunt group

Example of unlocking a hunt group member

1 Unlock hunt group member 2 in hunt group 5.

```
unlock hg/5 hgm/2
```

Additional information on hunt group maintenance

This section provides additional information on hunt group maintenance, including the following sections:

- “OSI states” (page 35)
- “Alarms” (page 36)
- “Common problems and corrective actions” (page 36)

OSI states

See the following tables for information on OSI states:

- “Hg component state combinations” (page 35) shows the valid OSI states for the *Hg* component.
- “HgM component state combinations” (page 36) shows the valid OSI states for the *HgM* component.

Table 1
Hg component state combinations

Combination (administrative, operational, usage)	Details
Unlocked, disabled, idle	This transient state is valid when the hunt group is activating.
Unlocked, enabled, idle	This transient state is valid when the hunt group changes its operational state from disabled to enabled.
Unlocked, enabled, active	This state is valid when the hunt group is fully operational. This is the normal state for a hunt group.
Locked, enabled, idle	This state is valid when the hunt group is administratively prohibited from hunting call requests.

Table 2
HgM component state combinations

Combination (administrative, operational, usage)	Details
Unlocked, disabled, idle	This state is valid while the hunt group member is activating, or if the *Hg* component is administratively prohibited from hunting call requests.
Unlocked, enabled, idle	This transient state is valid when the hunt group member changes its operational state from disabled to enabled.
Unlocked, enabled, active	This state is valid when the hunt group member is available to receive calls. This is the normal state for a hunt group member.
Locked, enabled, idle	This state is valid when the hunt group member is administratively prohibited from receiving a call.
Locked, disabled, idle	This state is valid when the hunt group member is administratively prohibited from receiving a call while the *Hg* component is administratively prohibited from hunting call requests.

Alarms

The alarm associated with hunt groups is the unknown member alarm (7058 0001). This alarm occurs if a DNA that is not listed as a hunt group member reports availability to the hunt group server.

For more information on individual alarms, see NN10600-500 *Nortel Networks Multiservice Switch 6400/7400/15000/20000 Alarms Reference*.

Common problems and corrective actions

The table “Common problems and corrective actions summary” (page 37) provides guidelines on how to respond to problems that can occur when you are using hunt groups. The table lists the problem, the probable cause (if applicable), and the corrective action to take.

Table 3
Common problems and corrective actions summary

Problem	Probable cause	Corrective action
The call does not connect.	The hunt group is down.	Review the outstanding alarms to make sure that the hunt group activated correctly. Make sure that the hunt group is unlocked.
	There is no route to the hunt group.	First, determine that calls are not reaching the hunt group by displaying the *Hg/n* operational attributes. If there is no increment of the *huntAttempts* or *failedCalls* attributes, the hunt group did not receive the call. Make sure that the call correctly signals the hunt group address. Make sure that the hunt group address prefix is correctly provisioned on either the CSRM or all Nortel Networks Multiservice Switch node CRs in the network. Verify connectivity to the hunt group node using the Ping Rtg Dpn command.
	There are no available members.	Display the *Hg/n HgM/n* operational attributes to make sure that at least one member is unlocked with an *availability* attribute value greater than zero. If all members report zero availability, increase the size of the hunt group by adding more members.
(Sheet 1 of 3)		

Table 3 (continued)
Common problems and corrective actions summary

Problem	Probable cause	Corrective action
The call does not connect.	There is no route to the hunt group member services.	Determine if calls are reaching the member service Make sure that the member service address is correctly provisioned in the *Hg/n HgM/n* component. Make sure that the member service address prefix is correctly provisioned on either the CSRM or all Multiservice Switch node CRs in the network. Verify connectivity to the member service node using the Ping Rtg Dpn command.
	The member service clears the call.	Use the call clear cause and the appropriate service guide to determine the reason for the clear. Make sure that the member service is compatible with the information being signalled in the call. If possible, attempt a call directly to the member service, without using the hunt group, to see if it connects. If suffix digits are signalled on the call, make sure that the member service can accept them.
The call needs many hunts to connect.	The member list is incorrect.	Make sure that all *Hg/n HgM/n* components are correctly provisioned with the member service address.
	The selection policy is inefficient.	Make sure that the hunt group member services are provisioned to report their availability if the *mostAvailable* selection policy is used.
(Sheet 2 of 3)		

Table 3 (continued)
Common problems and corrective actions summary

Problem	Probable cause	Corrective action
The call needs many hunts to connect.	The hunt group is over-engineered.	Increase the size of the hunt group by adding more members.
The CP of the hunt group node consistently displays high CPU utilization.	The SDCR and FDCR are over-engineered.	Make sure that the Multiservice Switch node is not configured with many hunt groups in addition to the call redirection server. Distribute some hunt groups to other nodes in the network.
(Sheet 3 of 3)		

Chapter 3
Hunt groups

See the following sections for an overview of Nortel Networks Multiservice Switch node hunt group capability for DPRS services:

What is a hunt group?

A hunt group is a single data network address (DNA) that represents a group of service DNAs. The hunt group server resides on a Nortel Networks Multiservice Switch node and has a unique DNA. The network operator configures a group of DNAs to belong to the hunt group. When users call the DNA assigned to the hunt group, the server forwards the call to one of the hunt group members.

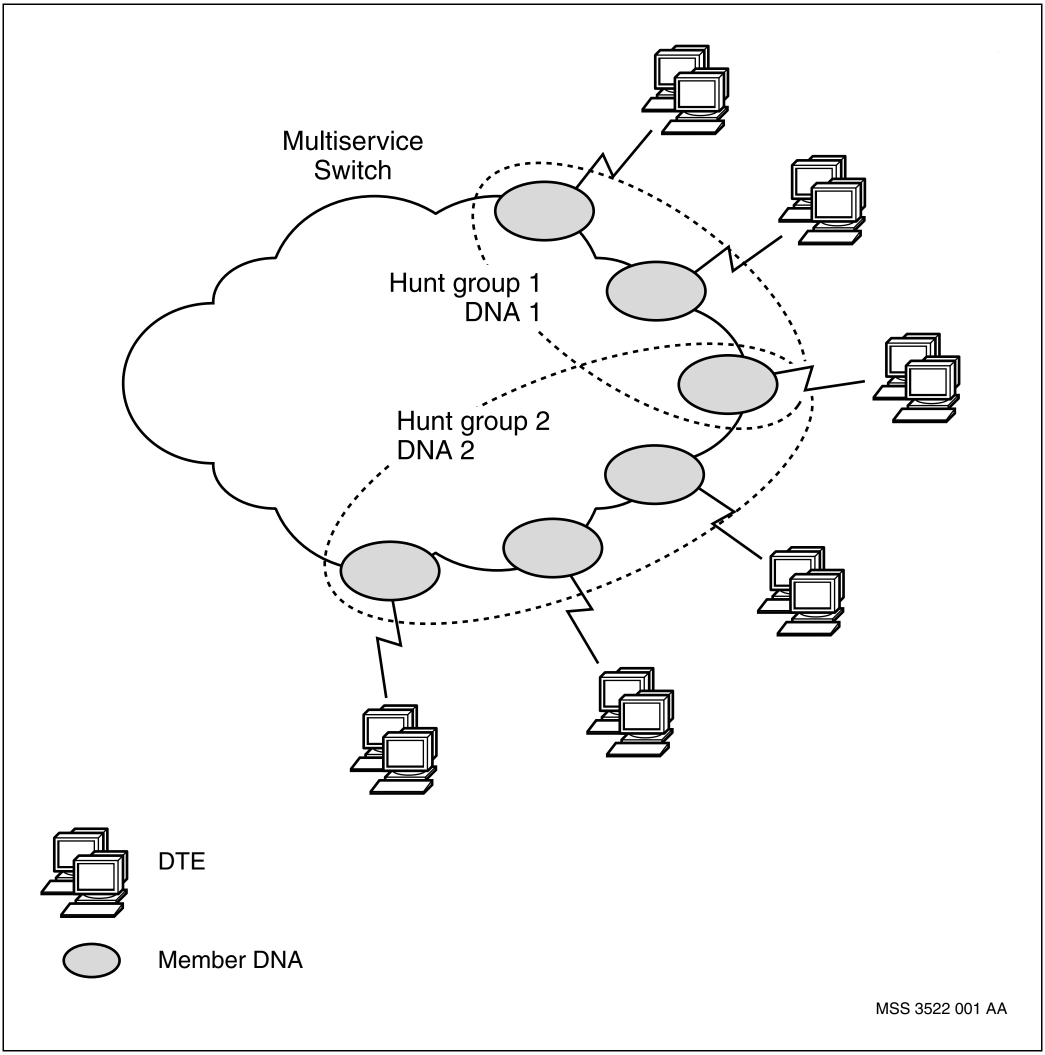
The figure “Hunt groups and members” (page 43) shows two hunt groups in a Multiservice Switch network. Each group contains member DNAs connected to data terminal equipment (DTE). One DNA is a member of both hunt groups.

A hunt group member is any single-service DNA that can accept a hunted call. Hunt group members can receive calls using their own DNAs, as well as through the hunt group server. A call made directly to a hunt group member is treated as a normal call, which the member accepts or rejects independently of the hunt group.

Nested hunt groups are not supported. This means that a hunt group member cannot be a hunt group server itself.

You can define and manage a hunt group individually, without any effect on hunt group members or other hunt groups.

Figure 5
Hunt groups and members



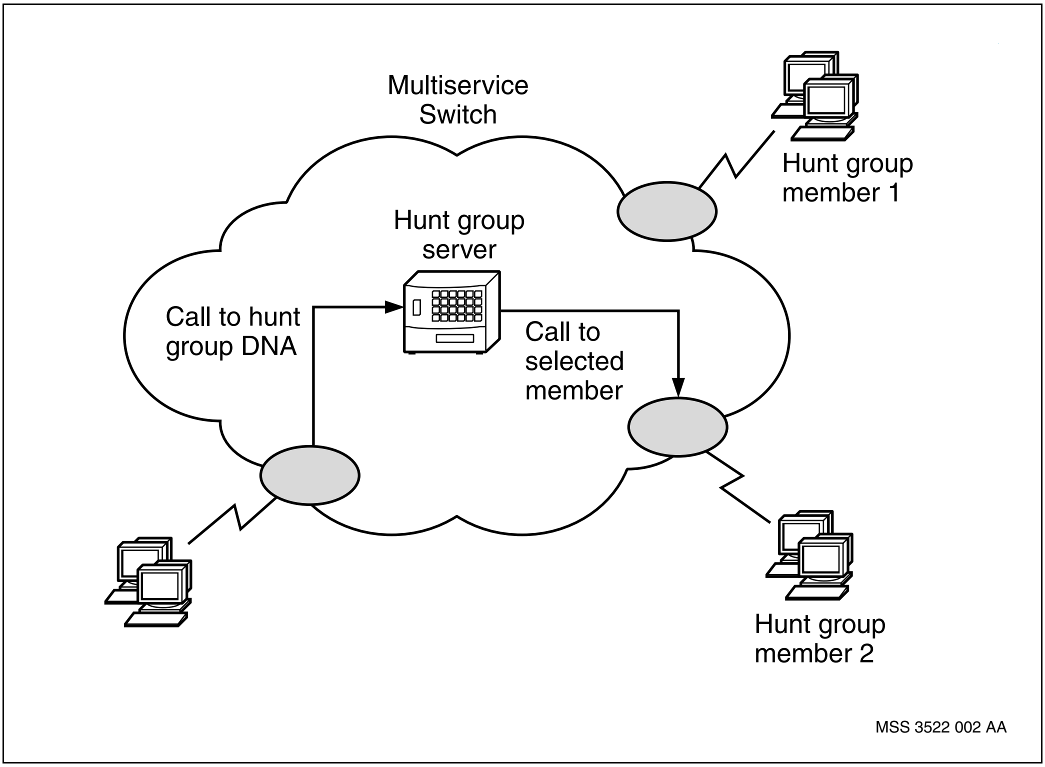
Why use a hunt group?

A hunt group provides the network with the benefits of higher capacity and higher availability. There is higher capacity because the calls are spread across several lines. There is higher availability because the failure of some member lines does not prevent access to other members belonging to the same hunt group.

What is call hunting?

The figure “Call hunting” (page 45) shows the hunt group server and two hunt group members. When a call for the hunt group DNA arrives, the network forwards it to the hunt group server. The server selects an eligible DNA from its list of hunt group members, and sends the call to that member. If that member does not accept the call, the server selects the next member on the list. This process continues until the call connects or the server has tried all the members.

Figure 6
Call hunting



Role of hunt groups

Nortel Networks Multiservice Switch node hunt groups provide a hunt group capability for switched calls (calls that use switched virtual circuits). The Multiservice Switch hunt group capability supports DPRS-based services, such as frame relay. Any Multiservice Switchnode service that uses the DPN hunt group feature can migrate to a Multiservice Switch node hunt group.

Hunt group features

Hunt groups provide the following features:

- Nortel Networks Multiservice Switch node function processors (FP) support up to 256 hunt groups, and each hunt group can contain up to 63 members (subject to engineering limitations).

- A hunt group can be located on any Multiservice Switch node in the network.
- Multiservice Switch node hunt groups can coexist with DPN hunt groups in a mixed network topology.
- The hunt group feature provides flexible network administration. You can add or delete members from the group without affecting the hunt group DNA.
- You can assign the hunt group DNA and member DNAs in either E.164 or X.121 format.

  Note: You cannot provision hunt group members on Passport 4400-series nodes.

A hunt group can be provisioned on a spared LP as a warm standby feature on Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 nodes. A warm standby application or feature can operate together with a hot standby application or feature on the same FP without affecting the ability of the hot standby application or feature to provide hitless services.

See NN10600-550 *Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures* for a description of hitless services and hot, warm and cold standby applications and features.

Call hunting

The hunt group registers its DNA with the final destination call router (FDCR) of the DPRS routing system. This practice ensures that all calls to the hunt group DNA arrive at the hunt group through DPRS call routing mechanisms.

The call hunting process includes the following topics:

- “Initial hunt” (page 47)
- “Subsequent hunts” (page 49)
- “Unsuccessful hunts” (page 50)

Initial hunt

When a new call arrives at the hunt group, the server selects a group member using the provisioned selection policy. The server then takes the following actions:

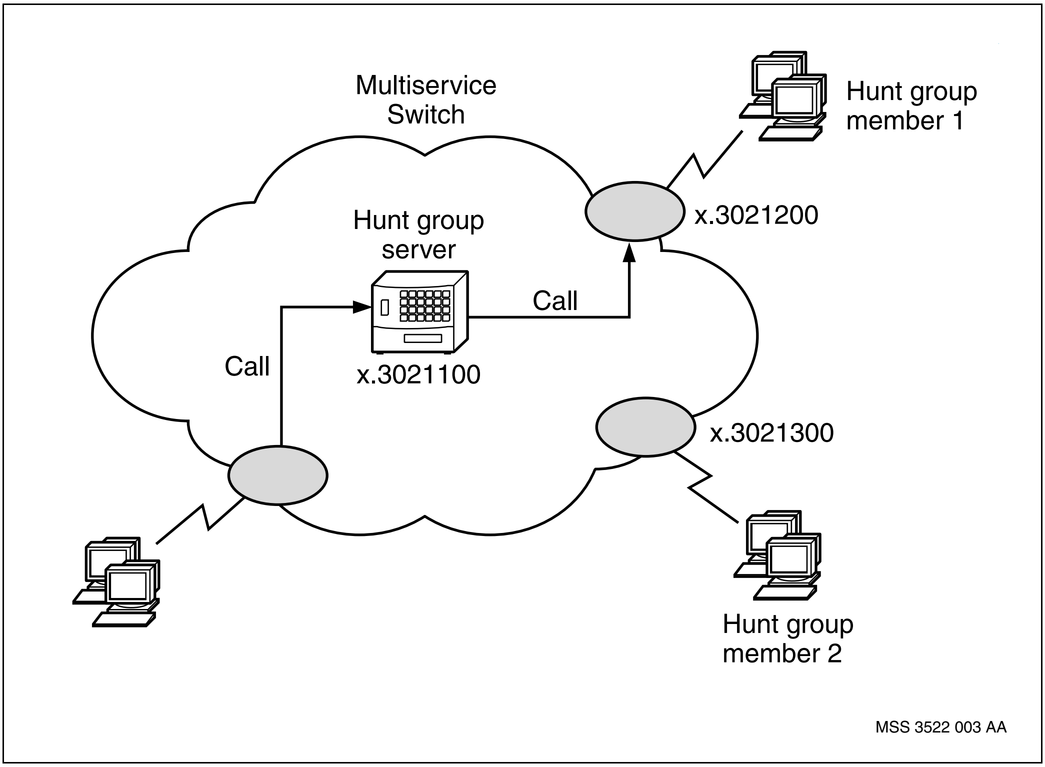
- saves the destination address
- replaces the destination address with the DNA of the selected member
- identifies the call as hunted

The DPRS routing system forwards the call to the selected member.

Figure 7, “Initial hunt,” (page 48) shows an example of the initial hunt. In the example, the hunt group server receives a call on its DNA, x.30211000 (the x indicates an X.121 address). The server selects hunt group member 1, and forwards the call to destination x.30212000.

If the hunt group member accepts the call, the hunt is considered successful, and there is no further interaction between the server and the member.

Figure 7
Initial hunt



Subsequent hunts

If the hunt group member does not accept the call in the initial hunt, the DPRS routing system

- restores the original destination address
- forwards the call to the hunt group, as the destination address of the call is now the hunt group DNA

When the hunt group receives a hunted call, it is an indication of a failed hunt attempt. The server continues hunting at the next member, and takes the following actions:

- selects the next hunt group member
- replaces the destination address with the DNA of the selected member

DPRS then forwards the modified call to the new hunt group member.

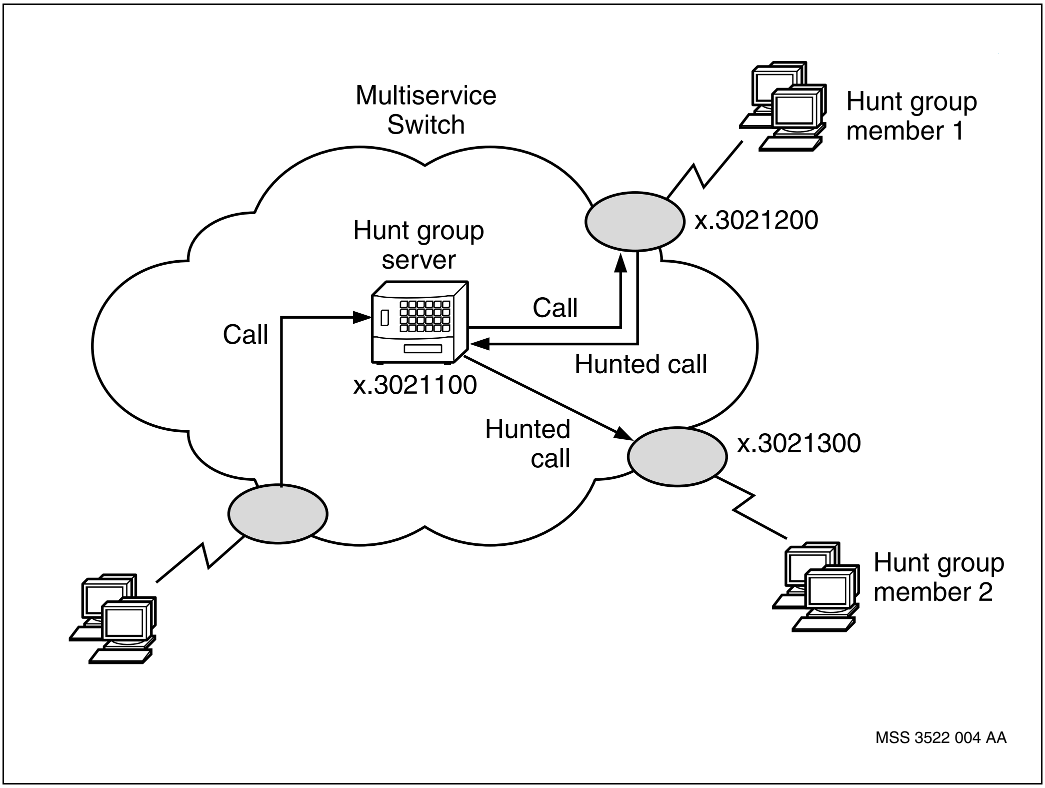
Figure 8, “Subsequent hunt attempt,” (page 50) shows an example of a subsequent hunt attempt. When the call to hunt group member 1 fails, it is returned to the server at DNA x.30211000. The server selects member 2, modifies the call, and forwards it to destination x.30213000.

Subsequent hunt attempts continue until a member accepts the call.

A hunt group member can become unreachable because the Nortel Networks Multiservice Switch node is isolated (all Multiservice Switch trunks to the node are down). In this case, subsequent hunting cannot occur unless the network supports call redirection or a call server resource module (CSRM) with a remote server interface.

CSRMs are supported on Nortel Networks Multiservice Switch 7400 series nodes.

Figure 8
Subsequent hunt attempt



Unsuccessful hunts

The hunt group server may fail to connect the call under the following circumstances:

- The server has exhausted the list of hunt group members.
- The hunt group is locked.
- The call has been hunted for the provisioned number of maximum hunt attempts.

When a hunt is unsuccessful, the server attempts to send the call for redirection. (For information on call redirection, see NN10600-410 *Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server*.)

Member availability

Before a hunt group member can receive a call, the server must recognize the member as available. Each member reports to the hunt group server whether or not it is available to receive calls. See the following sections for an explanation of availability:

- “Availability representation” (page 51)
- “Reporting availability” (page 51)

Availability representation

A member’s availability is represented by a decimal value in the range zero to 4095. The hunt group server recognizes availability reports as follows:

- The higher the value, the more available the member is.
- A value of zero indicates that the member is not available to receive calls.

During initialization, the hunt group assumes that all of its members are equally available, and sets their availability to the maximum. Similarly, the server sets the availability value of a new member to the maximum. This practice ensures that the server tries sending a call to a member that has not reported its availability. The hunt attempt triggers the member to report its true availability. If a member never reports, its availability remains at the maximum value.

Reporting availability

Services that use the hunt group capability have different methods of determining their availability. Some services base their availability on unused logical channels, others on bandwidth or memory capacity. Each service calculates its own availability, and sends the information to the hunt group server in a DPRS availability packet called the availability message packet (AMP).

The hunt group server does not poll its members for availability information. It is the responsibility of the member service to provide accurate information that reflects its current availability without overloading the hunt group. For more information on availability calculation and reporting, see the appropriate service guide.

If a member's availability remains at zero for 2.5 hours, the hunt group server resets it to the maximum value. This practice ensures that lost availability information does not prevent a member from returning to service.

You can manually change a group member's availability value. The server accepts a value entered with the set command as if it were received from a member in an availability update. You typically use this capability to recover from a suspected lost update.

Member selection

You can provision a policy for the hunt group server to use in selecting members. See the following sections for descriptions of the three possible selection policies:

- "Start from zero" (page 52)
- "Rotary" (page 53)
- "Most available" (page 54)

Start from zero

You typically use the start-from-zero policy when you want the first member to receive the majority of the calls and subsequent members to receive only overflow calls.

On an initial hunt, the server selects the first available member (the member with the lowest provisioned instance number). Subsequent hunts for the call select the first available member starting with the next lowest-numbered member. The server sorts the list of members in ascending order by the provisioned instance of the *HuntGroupMember* component.

Figure 9, "Start-from-zero selection," (page 53) shows a sample hunt group. Using the start-from-zero selection policy in this example, the server always selects the HuntGroupMember/1 (HgM/1) component for all initial hunts. For subsequent hunts in the same call, the server selects HgM/2, HgM/3, and HgM/4, in that order. Table 4, "Start-from-zero hunt," (page 53) summarizes the hunt selection for the members illustrated in Figure 9, "Start-from-zero selection," (page 53).

Figure 9
Start-from-zero selection

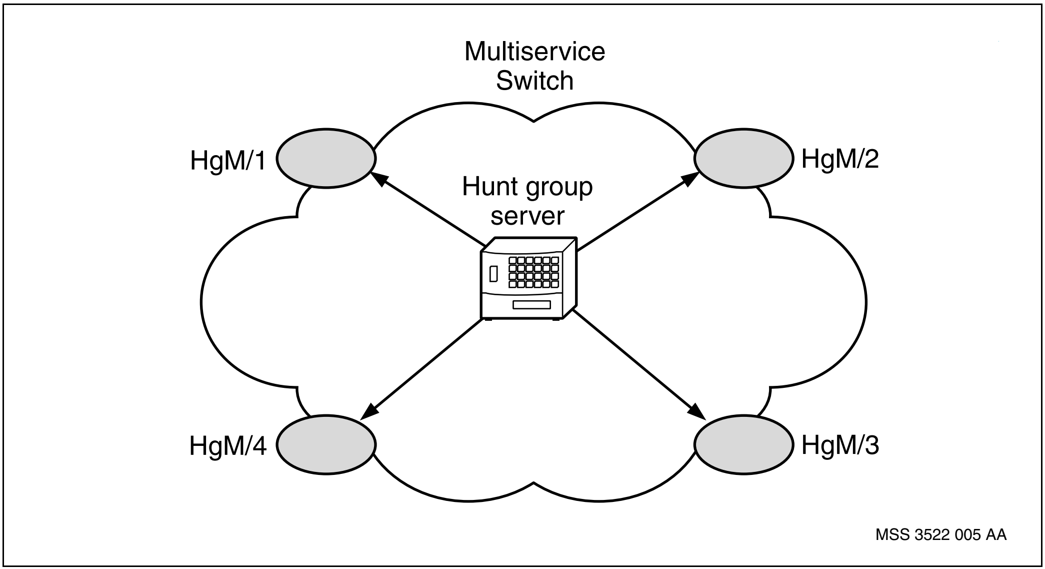


Table 4
Start-from-zero hunt

Hunt	Selection for call 1	Selection for call 2
Initial hunt	HgM/1	HgM/1
Subsequent hunt	HgM/2	HgM/2
Subsequent hunt	HgM/3	HgM/3
Subsequent hunt	HgM/4	HgM/4

Rotary

You typically use the rotary policy to spread the calls equally across the members of the hunt group.

On an initial hunt, the server selects the first available member starting from the member selected for the initial hunt of the previous call. Subsequent hunts for the call select the next available member starting from the member chosen for the initial hunt. As in the start-from-zero policy, the server sorts the list in ascending order by the *HuntGroupMember* component instance.

Using the rotary selection policy for the example in Figure 9, “Start-from-zero selection,” (page 53), the server cycles through HgM/1, HgM/2, HgM/3, and HgM/4, in that order, for initial hunts. For subsequent hunts in the same call, the server continues cycling through the members, beginning at the next member on the list after the one selected in the initial hunt. Table 5, “Rotary hunt,” (page 54) summarizes the rotary hunt selection for the members illustrated in Figure 9, “Start-from-zero selection,” (page 53).

Table 5
Rotary hunt

Hunt	Selection for call 1	Selection for call 2
Initial hunt	HgM/1	HgM/2
Subsequent hunt	HgM/2	HgM/3
Subsequent hunt	HgM/3	HgM/4
Subsequent hunt	HgM/4	HgM/1

Most available

You typically use the most-available policy when you want to send each call to the member with the highest probability of connecting it.

On an initial hunt, the server selects the most available member based on the availability information reported by the members. Subsequent hunts for the call select the next most available member starting from the member chosen for the initial hunt. The server sorts the list of members in descending order by the *availability* attribute of the *HuntGroupMember* component. As availability information appears from the members, the server updates the list accordingly.

Figure 10, “Most-available selection,” (page 55) shows the most-available selection policy. In this example, the server selects HgM/3 for all initial hunts because it is the first member in the list with the highest availability value. For subsequent hunts of the same call, the server selects HgM/4, HgM/2, and HgM/1, in that order. Table 6, “Most-available hunt,” (page 56) summarizes the hunt selection for the members illustrated in Figure 10, “Most-available selection,” (page 55).

When you use the most-available selection policy, the member services must be provisioned to send their availability information to the hunt group. If a service does not report this information, its availability remains at the maximum value set during initialization.

Figure 10
Most-available selection

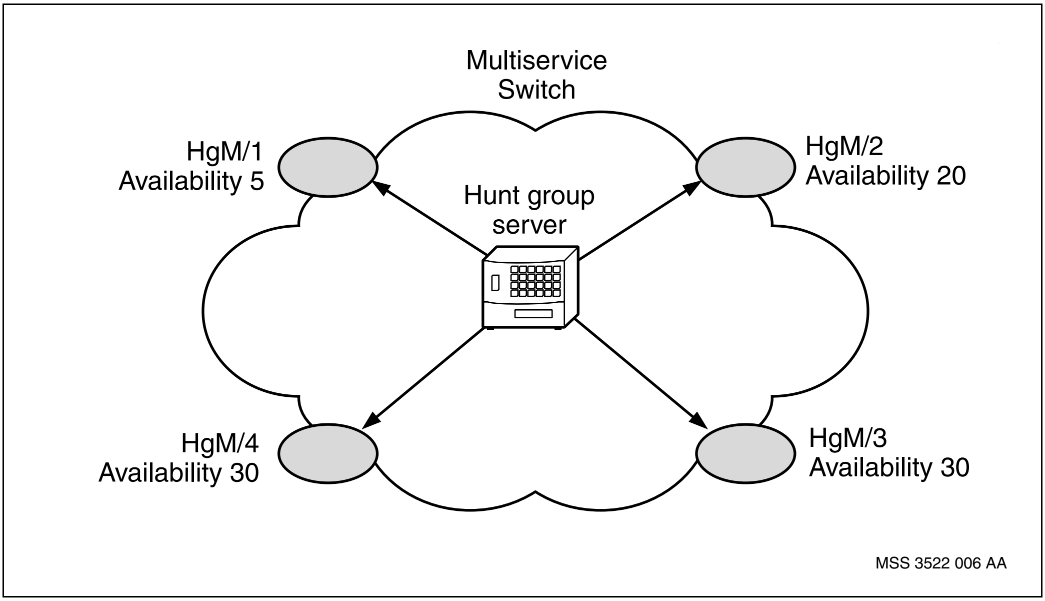


Table 6
Most-available hunt

Hunt	Selection for call 1	Selection for call 2
Initial hunt	HgM/3	HgM/3
Subsequent hunt	HgM/4	HgM/4
Subsequent hunt	HgM/2	HgM/2
Subsequent hunt	HgM/1	HgM/1

Addressing for hunt groups

Hunt groups support both X.121 and E.164 addressing plans for hunt group and member DNAs.

Hunt groups also support suffix address digits for the hunt group DNA. Suffix address digits are any trailing digits signalled in a call beyond the provisioned hunt group DNA. You can provision the hunt group to preserve the suffix digits for hunted calls. The server then appends them to the member DNA before forwarding the call to the member (as long as the member DNA length does not exceed 15 digits with suffix digits).

If you are using hunt groups to provide a gateway call routing functionality across frame relay networks, you must provision a separate hunt group for each external network that you want to reach. The DNA of each hunt group instance must correspond to the network identifier (DNIC) of its associated external network. You must also provision the FR NNI that connects to the external network as a member of the hunt group.

For more information about configuring the FR NNI service, see NN10600-901 *Nortel Networks Multiservice Switch 7400/15000/20000 Frame Relay Configuration Management*.

Use the following guidelines when defining hunt group addresses:

- You must assign the hunt group a DNA that is unique in the network. The format of the hunt group DNA is subject to the DPRS routing hierarchy. (See NN10600-030 *Nortel Networks Multiservice Switch 7400/15000/ 20000 Overview*.)

- If the hunt group is migrating from a DPN hunt group, plan to re-use the DPN hunt group DNA.
- If you provision the *appendSuffixDigits* attribute, the hunt group server preserves suffix digits for hunted calls, regardless of the numbering plan in use. If you need suffix addressing, make sure that the member DNA length does not exceed 15 digits with the suffix digits appended.
- If the hunt group connects to an external network, the hunt group DNA must correspond to the network identifier (DNIC) of its associated external network.

Note 1: If suffix digits cause a member DNA to exceed the maximum address length of 15 digits, the server does not select that member. The server increments the *maxAddrLenExceeded* attribute.

Note 2: Some applications cannot connect a call with a 15-digit address. In some cases these applications clear the call without sending it back to the hunt group server. In these cases, hunting stops.

Spared hunt groups

A hunt group can be provisioned on a spared LP as a warm standby feature on Nortel Networks Multiservice Switch 15000 and Multiservice Switch 20000 nodes. In this configuration, two instances of the hunt group exist: an active instance on the active card and a standby instance on the standby card. The routing system cannot see the standby hunt group instance. The standby hunt group instance does not receive any calls to hunt or any availability updates from the hunt group members. Only the active hunt group instance performs these activities.

After an equipment protection or software migration switchover, the standby hunt group instance becomes active and registers with the routing system to receive calls and availability updates.

Member availability information is not preserved between the active and standby hunt group instances. After the switchover, the newly active hunt group instance assumes that all of the hunt group members are completely available.

Hunt group location

Consider the following objectives when choosing the location of the hunt group server in the network:

- avoid overloading of network resources
- minimize network congestion
- maintain the reliability of subscriber services

There are two strategies you can use to deploy hunt groups: distributed and centralized.

In the distributed strategy, hunt groups can be deployed near the member services. The advantages of this strategy are:

- Calls that need hunting are near the hunt group members, reducing the time to connect the call.
- The network resources used to support hunt groups are distributed throughout the network.
- The potential for loss of member availability messages is reduced.

  Note: Do not deploy a hunt group server on the same FP as a member service, unless the complete member list is also located on that FP. Otherwise, a single FP failure can make the entire hunt group inaccessible.

In the centralized strategy, hunt groups are deployed in a central location in the network. The advantages of this strategy are:

- You can use a common format for hunt group DNAs.
- Hunt group management can be centralized.
- Engineering of network resources for hunt groups can be centralized.

Centralized hunt groups can generate a considerable load on Nortel Networks Multiservice Switch node’s routing system, particularly the call router (CR) and final destination call router (FDCR). If you are planning a centralized system of hunt groups, you need to consider the engineering recommendations for the CR and FDCR systems. The call redirection server (CRS) also generates a significant load on the CR, so do not deploy many centralized hunt groups on a node that supports a CRS.

Nortel Networks Multiservice Switch 7400/15000/20000

Operations: Hunt Group Server

Release Release 6.1

Publication: NN10600-415
Document status: Standard
Document version: 6.1S1
Document date: August 2004
Printed in Canada

NORTEL
NETWORKS