>THIS IS **THE WAY**

>THIS IS **NORTEL**™

Nortel Multiservice Switch 7400

Operations: DPN-100 Interworking

NN10600-450

Document status: Standard
Document issue: 7.1S1
Document date: October 2005
Product release: PCR7.1 and up
Job function: Operations
Type: NTP
Language type: U.S. English

Contents

What’s new

There were no new features added to this document.

Attention: To ensure that you are using the most current version of an NTP, check the current NTP list in NN10600-000 *Nortel Multiservice Switch 7400/15000/20000 What’s New*.

DPN-100 interworking configuration

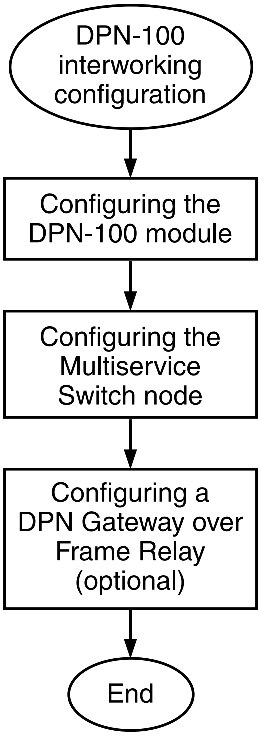
Configure DPN-100 interworking to configure a DPN-100 module, a Multiservice Switch node, and to create a DPN gateway.

For detailed information about Multiservice Switch components mentioned in this chapter, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*.

DPN-100 interworking configuration procedures

This task flow shows you the sequence of procedures you perform to configure interworking between Nortel Multiservice Switch nodes and DPN-100 modules. To link to any procedure, go to DPN-100 interworking configuration procedure navigation (page 8).

DPN-100 interworking configuration procedures


DPN-100 interworking configuration
Configuring the DPN-100 module
Configuring the Multiservice Switch node
Configuring a DPN Gateway over Frame Relay (optional)
End

MSS 3596 001 AA

DPN-100 interworking configuration procedure navigation

- Configuring the DPN-100 module (page 9)
- Configuring the Multiservice Switch node (page 11)
- Configuring a DPN Gateway over Frame Relay (page 14)

Configuring the DPN-100 module

Configure the DPN-100 module for interworking by configuring an RM as a CSRM.

Any RM on a PE386 platform directly connected to the Nortel Multiservice Switch RID subnet can be configured as a CSRM. The following procedure explains how to configure the RM to provide call services to the RID subnet.

For basic information about configuring DPN-100 routing components, see 241-1001-109 *DPN-100 AM and RM Provisioning User Guide*.

Prerequisites

- If X.25/X.75 gateways are deployed on AMs connected to Nortel Multiservice Switch nodes, the DPN nodes are operating at generic G34 (release G3402) or later.
- Wherever DPN Gateway over Frame Relay is deployed, the AMs or MAS connected to Multiservice Switch nodes are running the generic G34 (or later) feature Network Link over Frame Relay.
- Ensure that the RID subnet is in the same RID region as the CSRM, as defined in the CSRM's RID region map.

Procedure steps

Step **Action**

1 Using DPN Architect, upload the software service data bundle from the RM. (For information about DPN Architect, see 241-6001-012 *Nortel Multiservice Data Manager Configuration Management Tools for DPN*.)

2 Add a Call Server Module component.

3 Expand the Call Server Module component to display the subnet RID's subcomponent. Under the subnet RID's component, add a RID subcomponent. The <key value> for this RID component is the RID value of the RID subnet that the CSRM is to support. You can configure more than one RID component for the CSRM.

The new RIDs are added under the RIDs component as RID/<key>, where the <key> is the RID number of the RID subnet. These RIDs are listed in ascending order.

4 Download the bundle.

5 Activate the bundle.

6 After the bundle is activated, confirm it using the confirm activate command.

7 Display the RIDs of the Multiservice Switch subnet(s).

```
CSRsys Query RIDs
```

8 If it is not already connected, connect the CSRM to a Multiservice Switch node of the RID subnet.

9 Ensure the link has staged and the RID routing information has been exchanged by using the list rtg dpn or ping command on the Multiservice Switch node. (For command information, see NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.)

10 Display the RIDs and MIDs of the Multiservice Switch nodes supported by the CSRM.

```
CSRsys Display Interfaces
```

11 On the Multiservice Switch node, ensure that the CSRM's RID is displayed correctly.

```
display rtg dpn
```

--End--

Configuring the Multiservice Switch node

Configure the Nortel Multiservice Switch node to create DPN gateways between Multiservice Switch nodes and DPN-100 modules (AMs, RMs, or CSRMs).

A DPN gateway is a link between a Nortel Multiservice Switch node and a DPN-100 AM, RM, or CSRM provisioned on the Multiservice Switch node.

If the DPN end of a Multiservice Switch-to-DPN connection terminates on a dedicated PE286, the connection is not supported.

Optionally, to run the DPN Gateway over Frame Relay capability, you need to configure Multiservice Switch node-to-node links as DPN Gateways over Frame Relay.

For detailed information about configuring DPRS routing software on Multiservice Switch nodes, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

After you have provisioned a Multiservice Switch node for interworking, you must decide whether you want to use the default setting of closest with regards to CSRM routing. By default, a Multiservice Switch node sends call request packets to the closest CSRM. However, after analyzing your network plan, you may decide to change this setting to shared so that call request packets are evenly distributed between the two CSRMs with the lowest RID values (for source call routing, destination call routing, network user interface, and hunt group services only). This can help minimize congestion. For conceptual information, see Call establishment using CSRMs (page 26). For configuring information, see Configuring the Multiservice Switch node (page 11).

Prerequisites

- To configure DPN-100 modules for connection to Nortel Multiservice Switch nodes, you must ensure that the correct types of trunks or network links are configured. For detailed information on configuring a trunk on an RM or a network link on an AM, see 241-1001-015 *DPN-100 Network Link and Trunk User Guide* and 241-1001-109 *DPN-100 AM and RM Provisioning User Guide*
- Ensure that the modules you want to connect to Multiservice Switch nodes are running the software listed in Configuring the DPN-100 module (page 9).
- Configure the RM with a DPN-100 trunk, specifying *trunk* as the link mode when you define the *Trunk-Network-Link* component.

- Configure the AM with a DPN-100 network link (or UPT network link), specifying *network link* as the link mode when you define the *Trunk-Network-Link* component.

Procedure steps

Step	Action
1	Configure a DPN gateway. Enter configuring mode and define the hardware stack if it does not exist.
2	Add a *DpnGateway* component. **`add dpngate/<n>`** A *UTP* component and a *Framer* component are automatically added to the *DpnGateway* component.
3	Use the set command to change the attribute values. For V.35 and V.11 FPs, ensure that the *flagsBetweenFrames* attribute is set to 3 when the link speed is set to a value greater than 128 kbits/s. This precaution is used to prevent DPN modules from being overrun as indicated by the *Framer* component's *Overrun* attribute. **`set dpngate/<n> utp framer interfaceName <hw>`**
4	Set the *linkType* attribute. For the dial-in link type, see 241-1001-015 *DPN-100 Network Link and Trunk User Guide*, to configure DBNL on the DPN module. **`set dpngate/<n> linkType <linktype>`**
5	To verify that the DPN gateway has staged with the DPN-100, issue the following command to display all the operational attributes of the DPN gateway. The *remoteComponentName* should reflect the PE/PI/PO of the DPN-100 at the remote end of the link. **`d dpngate/<n>`**
6	To optionally minimize congestion, configure CSRM routing as shared versus maintaining the default setting of closest. Set the *csrmRoute* attribute to shared. **`set rtg dpn csrmRoute Shared`**
7	To optionally set the node back to its default (closest), configure the following: **`set rtg dpn csrmRoute Closest`**

--End--

Variable definitions

Variable	Value
<hw>	is the associated LP and port for the *framer* component. For example: Lp/0 X21/1 Lp/2 V35/3 Lp/1 E1/1 Chan/0 Lp/3 DS1/1 Chan/3
<linktype>	is *dedicated* or *dialIn*. The default value is *dedicated*. To support DBNL, enter *dialIn*.
<n>	is the instance number of the *DpnGateway* component.

Configuring a DPN Gateway over Frame Relay

Optionally, configure a DPN Gateway over Frame Relay to create a link between two Multiservice Switch nodes in a RID subnet provisioned on the Nortel Multiservice Switch node.

Prerequisites

- All nodes in the network that are candidates for DPN Gateway over Frame Relay traffic must be running the same version of DPN Gateway over Frame Relay-compatible software.
- For DPN-100 connectivity, the remote must be running DPN-100 G34 feature Network Link over Frame Relay.
- If you configure override speed and round trip delay, these options must match those of the remote.
- This feature does not use the Multiservice Switch standard congestion management capability. This feature can impact the effectiveness of loadspreading. For effective sharing of the load between multiple links (if there are multiple links in a link group), use the loadsharing feature instead of loadspreading.

Procedure steps

Step	Action
1	Create a logical processor. **add sw lpt/<lpt_name>** **set sw lpt/<lpt_name> fl ! frDpnTrunks frameRelayMux**
2	Link the logical processor to the function processor on the shelf and create a physical port on the logical processor. Complete the standard port configuring procedures. (For more information, see NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.)
3	Create an *FrMux* component. This step creates an *FrMux* component and two of its required subcomponents: *Framer* and *Lmi*. **add frMux/<nf>**
4	Link the *Framer* to the logical processor. **set frMux/<nf> framer linkToHardware <hw>**
5	Create a *DataLinkConnectionIdentifier* component. This step creates a *DataLinkConnectionIdentifier* component. The instance value of the *DataLinkConnectionIdentifier* is the DLCI number on which this data link runs. **add frMux/<nf> dataLinkConnectionIdentifier/<dlci>**
6	Create a *DpnGateway* component.

```
add dpnGateway/<ng>
```

You can change gateway parameters now, if necessary.

7 Create an *FrAccess* subcomponent of the gateway.

```
add dpnGateway/<ng> frAccess
```

The *FrMuxSetup* subcomponent and the attributes contained in the *TrafficDescriptor* group are created.

8 Link the *DpnGateway* to *DataLinkConnectionIdentifier*.

This step sets up a one-way link. To make it two-way, you must set the *FrMux* attribute *applicationName* to the component name of *DpnGateway/n*. The gateway component name is communicated to the *DataLinkConnectionIdentifier* as a result of registration that occurs when the provisionable link is set through the *dataLinkName*.

```
set dpnGateway/<ng> frAccess frMuxSetup dataLinkName
dataLinkConnectionIdentifier/<dlci>
```

9 For each separate *DpnGateway*, repeat step 4 through step 8 with a different value of *dlci*.

--End--

Variable definitions

Variable	Value
<dlci>	is the DLCI number on which this data link runs.
<hw>	is the iLP and port on which the software is running (for example, Lp/1 V35/0).
<lpt_name>	is any mnemonic (for example, GTYFR).
<nf>	is the instance number of the *FrMux* component.
<ng>	is the instance number of the *DpnGateway* component.

Maintenance

Use the information in this section to learn about maintaining the interworking network.

For general operations and maintenance procedures, see

- NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*
- 241-2001-351 *DPN-100 Network Control System Operations and Maintenance*, and 241-6001-011 *Nortel Multiservice Data Manager Fault Management Tools*, for DPN-100 modules

For operator command information, see

- NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*
- 241-1001-303 *DPN-100 Operator Commands and Responses*

Navigation

Monitoring the routing system

On a Nortel Multiservice Switch node, you can use the list and display commands to monitor the routing system and network topology. This section contains typical examples of commands and system responses that apply to interworked networks. For more examples of monitoring DPRS, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

Example of listing link information

1 List the node’s gateways.

```
l rtg dpn lg/*
```

A list of internal and external gateways appears. For example:

```
Rtg Dpn lg/R46
Rtg Dpn lg/PARIS3
```

2 Display the attributes of external gateway R46.

```
d rtg dpn lg/R46
```

The attributes of the gateway appear. For example:

```
Rtg Dpn lg/R46
  farEndType = rm
  farEndRid = 46
  farEndMid = 152
  delayMetric = 11
  tputMetric = 47
```

External gateways have a *farEndType* attribute of either AM or RM. In this example, the link is connected to the RM identified by RID 46.

3 Display the attributes of internal gateway PARIS3.

```
d rtg dpn lg/paris3
```

The attributes of the gateway appear. For example:

```
Rtg Dpn lg/PARIS3
  farEndType = em
  farEndRid = 83
  farEndMid = 1122
  delayMetric = 1
  tputMetric = 19
```

Internal gateways have a *farEndType* attribute of EM. In this example, the link is connected to the Multiservice Switch node identified by MID 1122 in RID 83.

To display connected Multiservice Switch nodes from a DPN-100 AM or RM, use the command trunk display.

Example of listing reachable addresses

1 List all reachable nodes, as identified by their MIDs.

```
l rtg dpn mid/*
```

The list of reachable MIDs appears. For example:

```
Rtg Dpn Mid/94
Rtg Dpn Mid/127
Rtg Dpn Mid/128
Rtg Dpn Mid/1122
Rtg Dpn Mid/1377
```

Because RID substitution information must be preserved, an entry for an AM’s MID may remain in the MID forwarding tables even though the MID is no longer accessible. To ensure that a MID is currently reachable, use the command d rtg dpn mid/<mid> delayMetric and d rtg dpn mid/<mid> tputMetric. If a MID is shown in the resulting display with the metric value 2147483647 (to indicate infinity) the MID is not reachable.

2 List all reachable Multiservice Switch subnets, as identified by their RIDs.

```
l rtg dpn rid/*
```

The list of reachable RIDs appears. For example:

```
Rtg Dpn Rid/2
Rtg Dpn Rid/3
Rtg Dpn Rid/13
Rtg Dpn Rid/15
Rtg Dpn Rid/16
```

To display reachable RID subnets from a DPN-100 module, use the command ridrsys display <n>.

3 List all the reachable call servers.

```
l rtg dpn cs/*
```

A list of reachable call servers appears. For example:

```
Rtg Dpn Cs/dcr
Rtg Dpn Cs/scr
Rtg Dpn Cs/npm
Rtg Dpn Cs/grman
Rtg Dpn Cs/gscr
Rtg Dpn Cs/gdcr
```

The instance values indicate

— dcr: destination call router server

— scr: source call router server

— npm: network process monitor system

— grman: gateway call routing manager

— gscr: gateway source call router server

— gdcr: gateway destination call router server

Example of displaying metrics

1 Display the delay and throughput metrics and the next hop link groups to reach RID 18.

```
d rtg dpn rid/18
```

The delay and throughput metrics appear. For example:

```
Rtg Dpn Rid/18
dpnDelayMetric =            5
dpnTputMetric  =           42
delayMetric    = 0:    33574
```

```
                 1:    66000
tputMetric     = 0: 12949664
                 1: 15507360
delayNextHopLinkGroups = 0: Trm Lg/PARIS3
                         1:
tputNextHopLinkGroups  = 0: Trm Lg/LONDON2
                         1:
delayPathTrafficProportions = 0: 100 %
                              1:   0 %
tputPathTrafficProportions  = 0: 100 %
                              1:   0 %
```

The first set of metrics shown in the example (*dpnDelayMetric* and *dpnTputMetric*) is the one that DPRS advertises to other RIDs. The second set of metrics is the one DPRS uses for internal calculations. The traffic proportion attributes show the proportion of VC traffic flows on each path when there is a statistically significant number of VCs.

2 Display delay and throughput metrics for MID 1377.

```
d rtg dpn Mid/1377
```

The delay metric, throughput metric, and next hop link groups appear. For example:

```
Rtg Dpn Mid/1377
delayMetric    = 0:       3174
                 1: 2147483647
tputMetric     = 0:    3905536
                 1: 2147483647
delayNextHopLinkGroups = 0: Trm Lg/PARIS3
                         1:
tputNextHopLinkGroups  = 0: Trm Lg/PARIS3
                         1:
delayPathTrafficProportions = 0: 100 %
                              1:   0 %
tputPathTrafficProportions  = 0: 100 %
                              1:   0 %
substituteRid               = 41
```

In this example, one best-path metric is shown for the delay RCOS and one for throughput. (Variance is turned off, so there is a default value (2147483647) for the next-best path.) The substitute RID in this case is RID 41.

3 Display delay and throughput metrics for the closest DCR.

```
d rtg dpn cs/dcr
```

The delay and throughput metrics appear. For example:

```
Rtg Dpn Cs/dcr
delayMetric    = 0:     660004
                 1: 2147483647
tputMetric     = 0:   15507360
```

```
                 1: 2147483647
delayNextHopLinkGroups = 0: Trm Lg/R65
                         1:
tputNextHopLinkGroups  = 0: Trm Lg/R65
                         1:
delayPathTrafficProportions = 0: 100 %
                              1:   0 %
tputPathTrafficProportions  = 0: 100 %
                              1:   0 %
```

In this example, one best-path metric is shown for the delay RCOS and one for throughput. (Variance is turned off, so a default value is shown for the next-best path.)

Example of displaying routing control statistics

1 Display control statistics on the routing of DPRS traffic to all Multiservice Switch nodes in the RID subnetwork.

```
d rtg dpn
```

A list of operational attributes appears. For example:

```
Rtg Dpn
callServerModuleRids = 65
controlPktTx         = 71
controlPktRx         = 124
controlBytesTx       = 9215
controlBytesRx       = 12472
outOfSequencePkt     = 0
totalPackets         = 6117
throughputPackets    = 6113
delayPackets         = 4
interruptingPackets  = 0
normalReliabilityPackets = 5426
highReliabilityPackets   = 691
discardNoRoute           = 0
discardLpCongested       = 0
```

In this case, the *callServerModuleRids* attribute lists RID 65 as the only CSRM currently supporting the RID subnet.

To display statistics on a DPN-100 module, use the command <pi> <po> display statistics. To display SCR and DCR statistics on a DPN-100 module, use the commands scr display statistics and dcr display statistics.

Example Displaying gateways

1 List the provisioned gateway components.

```
l dpngate/*
```

A list of the provisioned gateways appears. For example:

```
DpnGate/50
DpnGate/51
```

2 Display the attributes of gateway 50.

```
d dpngate/50
```

A list of the gateway attributes appears. For example:

```
DpnGate/50
  adminState = unlocked
  operationalState = enabled
  usageState = busy
  availabilityStatus =
  proceduralStatus =
  controlStatus =
  alarmStatus =
  standbyStatus = notSet
  unknownStatus = false
  snmpOperStatus = up
  remoteComponentName = PM/04046 PE/10 PI/10 PO/02
  remoteNamsMnemonic = R46
  linkMode = trunk
  activateReason = dedicated
  measuredSpeedToIf = 64000 bit/s
  measuredRoundTripDelay = 2.0 msec
  maxTxUnit = 2064 bytes
  pktFromIf = 19066
  trunkPktFromIf = 18724
  trunkPktToIf = 18724
  discardUnforward = 0
  discardTrunkPktFromIf = 0
  discardTrunkPktToIf = 0
  stagingAttempts = 1
```

Analyzing network paths

You can view paths from Nortel Multiservice Switch nodes to other Multiservice Switch nodes and DPN-100 modules using the ping command. You can view paths from DPN-100 modules to Multiservice Switch nodes and other DPN-100 modules using the ppath command.

The ping command allows you to send a packet to a specified RID, MID, or both to

- determine the paths to the destination RID, MID, or both, based on the packet's RCOS (delay, throughput, or multimedia), reliability, or priority value
- measure the round trip delay in the network to any RID, MID, or both

For more information on the ping command, see NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

The ppath command is available on all DPN-100 modules. You specify a destination DPN-100 address and RCOS, and the routing system returns the path the packet takes. For more information on the ppath command, see 241-1001-303 *DPN-100 Operator Commands and Responses*.

Alarms

DPRS and DPN routing alarms help in resolving basic configuring errors and operating problems, such as:

- too many links in link group
- communication failure
- staging failures
- excessive procedure errors
- link or protocol errors

For more information about Nortel Multiservice Switch alarms, see NN10600-500 *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*. For more information about DPN-100 alarms, see 241-1001-506 *DPN-100 Alarm Console Indications*.

Overview

This chapter presents an overview of interworking between Nortel Multiservice Switch and DPN-100 networks.

Navigation

What is interworking?

Interworking is the term used to describe routing in a network that contains Nortel Multiservice Switch nodes and DPN-100 nodes. Both networks use a connectionless routing system. The DPN routing system handles packet routing between resource modules (RMs), access modules (AMs), and call server resource modules (CSRMs) in the DPN network. The DPRS routing system controls packet routing between Multiservice Switch nodes. The two routing systems work seamlessly together in an interworking environment.

For information on DPN routing, see 241-1001-110 *DPN Routing System General Description*. For information on DPRS, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

Why use Multiservice Switch and DPN-100 interworking?

Nortel Multiservice Switch nodes complement a DPN-100 network by providing backbone switching services to handle high-throughput data rates. Interworking provides the following benefits in network routing:

- performance—Multiservice Switch node interconnection provides greater network size, flexibility, and performance in DPN-100 networks
- traffic concentration—a Multiservice Switch backbone takes traffic from DPN-100 nodes and their connected devices, and efficiently transports the data across the high-throughput subnet

- scaling ability—interworking allows the creation of extremely large networks, for example, with Multiservice Switch nodes supporting intercity traffic and DPN-100 nodes supporting intracity access traffic
- full integration—both networks are managed by a network management system called Preside Multiservice Data Manager and appear fully integrated to the network operator
- frame relay support—frame relay services interwork seamlessly in a combined network
- service support—DPN-100 services that are not available on Multiservice Switch nodes are carried transparently across the Multiservice Switch sections of a combined network

How does routing work in the combined network?

In a combined network, routing works seamlessly because the DPN and DPRS systems are so similar. However, there are aspects of routing operation that differ from a DPN-only or Nortel Multiservice Switch node-only network. These aspects are described in the following topics:

- Elements of the combined network (page 24)
- Routing in the combined network (page 25)
- Call establishment using CSRMs (page 26)

Elements of the combined network

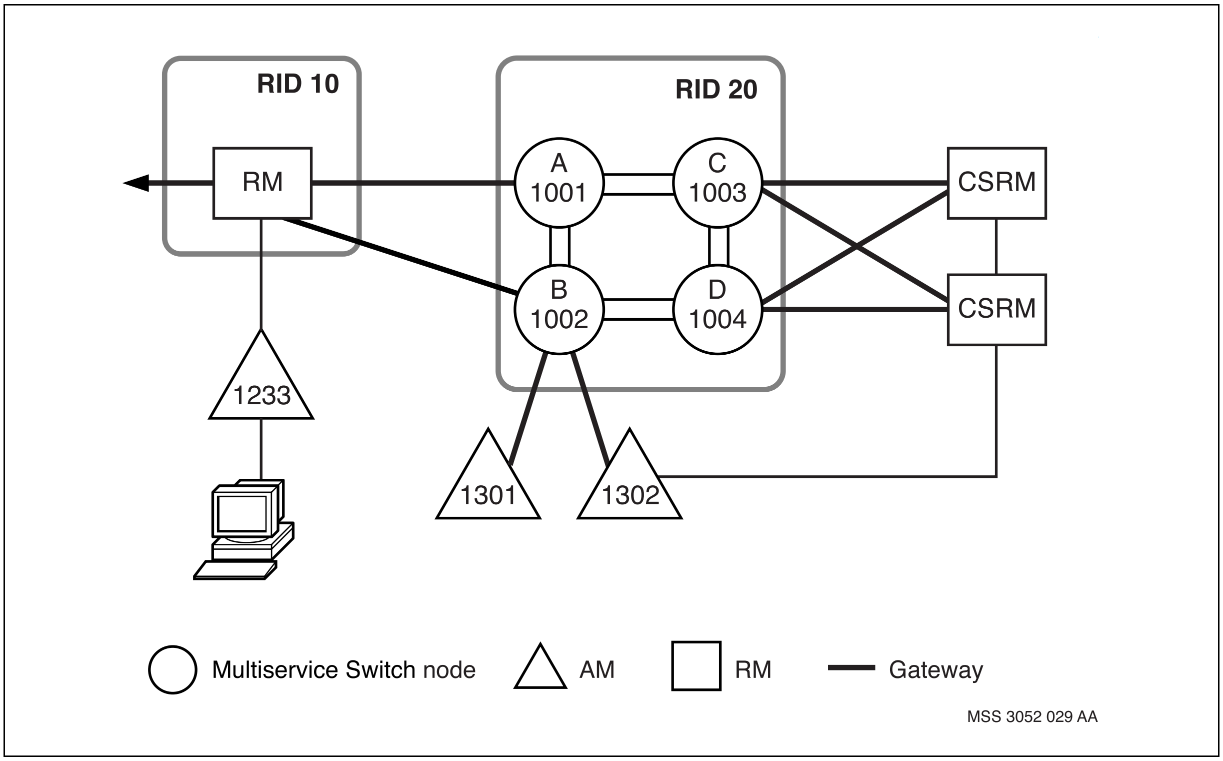
Elements of interworking (page 25) shows part of a small combined network in which a Nortel Multiservice Switch RID subnet is configured as a backbone. In this configuration, RMs and AMs connect to the Multiservice Switch RID subnet, which provides connectivity between them.

Each RM and Multiservice Switch subnet in the network is assigned a routing identifier (RID) value. Each AM and Multiservice Switch node is assigned a module identifier (MID) value.

In a combined network, CSRMs are normally used for call establishment. A CSRM is an RM configured to provide call services for a subnet.

The links between Multiservice Switch nodes and DPN-100 modules are called gateways.

Elements of interworking



Routing in the combined network

A mixed Nortel Multiservice Switch and DPN-100 network uses only one RID/MID address plan. RID addresses identify RID subnets, RMs, and CSRMs. MID addresses identify individual Multiservice Switch nodes in a subnet and AMs.

To allow interworking at the network layer between nodes, Multiservice Switch nodes support DPN-100 routing protocols. The Multiservice Switch DPRS system uses these protocols to exchange the following information with the DPN-100 modules:

- RID information with the DPN-100 RID routing system on an RM
- MID information with the DPN-100 MID routing system on an AM
- logical MID (LMID) information with the call services routing system located on a CSRM

The information exchanged includes:

- the RID, MID, and LMID addressing information for the nodes and services that can be reached through the neighbor node
- the metrics associated with each reachable RID, MID, and LMID address

Using this information, the routing system is able to determine the shortest paths to destination addresses. DPRS places the first link groups leading to these addresses in the forwarding tables.

To distribute the forwarding table information within a RID subnet, DPRS uses its multicast protocol. To distribute information between RID subnets, DPRS uses the DPN RID routing protocol.

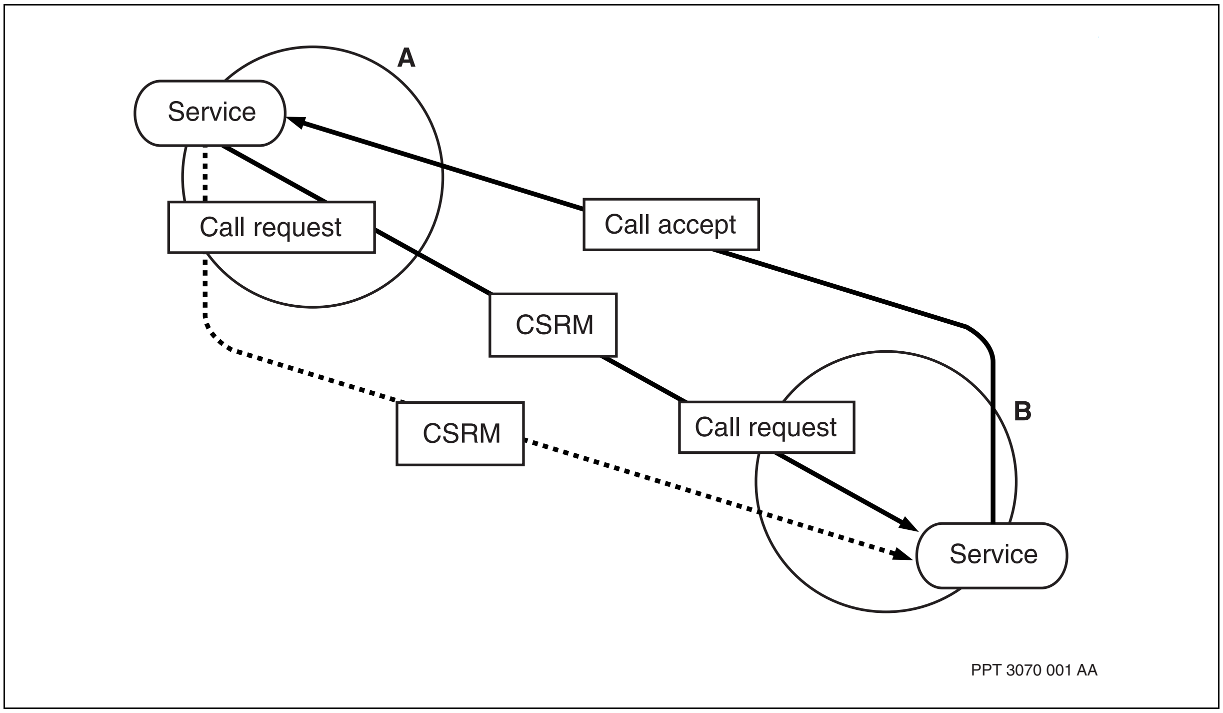
Call establishment using CSRMs

In a combined network, CSRMs provide support for call establishment. The routing system works with the CSRM to set up the virtual circuit (VC) for the call. The figure, Establishing a call (page 27) shows a simplified example of the call establishment process.

By default, the original access service sends a call request packet to the closest CSRM to begin call establishment. The CSRM translates the destination data network address (DNA) provided by the service to determine the MID of the destination. This allows the DPRS forwarding system to deliver the call request packet to the access service at the destination node. The address information is placed in the call accept packet, which is returned to the originating node.

You can configure CSRM routing as shared. This allows the two CSRMs with the lowest RID values to evenly share the call-setup requests (for source call routing, destination call routing, network user identifier, and hunt group services only), thus minimizing congestion. For configuring information, see Configuring the Multiservice Switch node (page 11).

Establishing a call



Routing in a combined network

This chapter describes routing considerations for a combined Nortel Multiservice Switch and DPN-100 network.

Navigation

- Routing process overview (page 28)
- Creating forwarding tables (page 29)
- Establishing the call (page 33)
- Forwarding packets (page 37)

Routing process overview

The figure Routing process overview (page 29) shows an overview of the routing process in a combined network. The first step in the routing process is to obtain the information needed to build the routing tables. The TRM gets the basic information about the links between the nodes in the network.

In a combined network, there are two types of links:

- Nortel Multiservice Switch trunks, which connect Multiservice Switch nodes.
- Gateways, which connect Multiservice Switch nodes to DPN-100 modules.

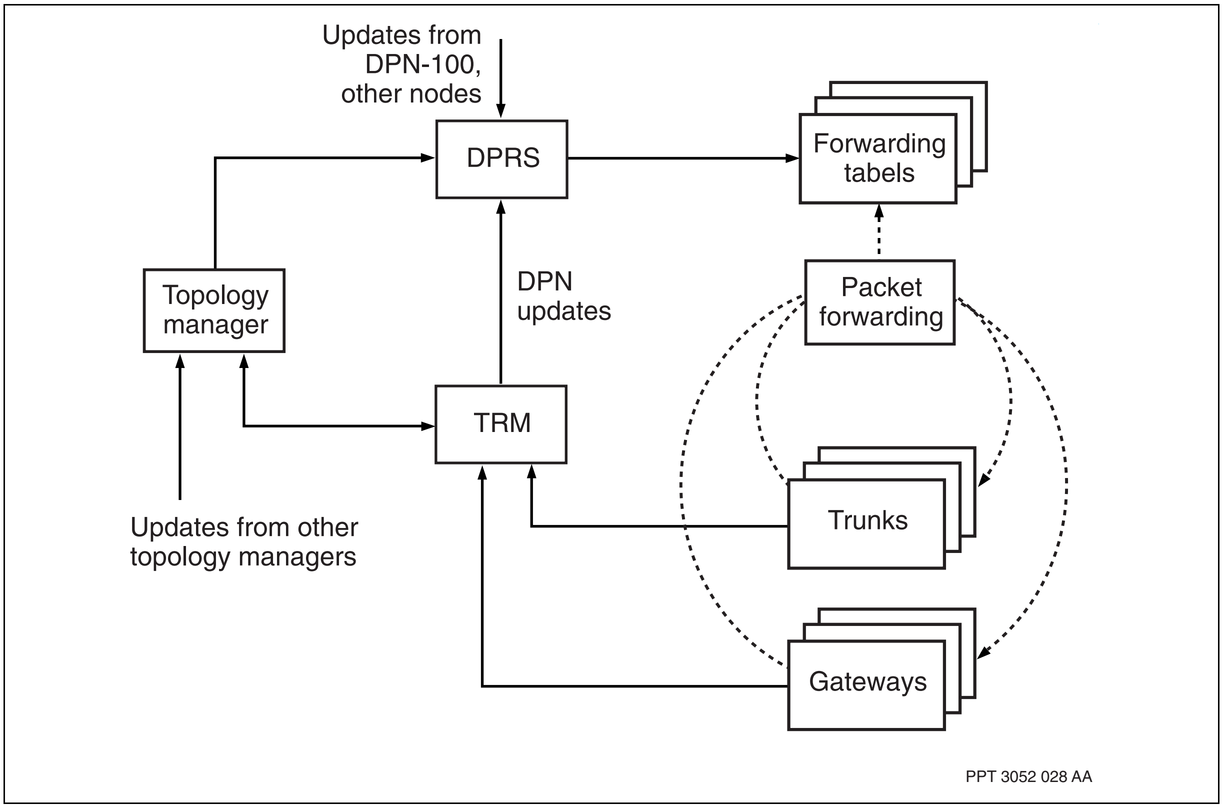
  Gateways include DPN-100 network links, which connect AMs to a RID subnet, and DPN-100 trunks, which connect RMs and CSRMs to a RID subnet.

The TRM sends link information from Multiservice Switch trunks to the topology manager. The topology manager determines the best next-hop throughput and delay link group to use to reach each node in the subnet. The topology manager passes a summary of this information to DPRS.

The TRM sends the DPN link information from the gateways directly to DPRS. DPRS combines this information with the topology information and DPRS updates from other nodes to build and maintain the forwarding tables.

DPRS places the information associated with RMs and other RID subnets in the RID forwarding tables. It places information associated with Multiservice Switch nodes and AMs in the MID routing tables. DPRS uses the forwarding tables to route packets.

Routing process overview



Creating forwarding tables

During the process of creating forwarding tables, DPRS must determine a best path across all the combined network elements of the Nortel Multiservice Switch subnet topology and the DPN topology. To do this, DPRS combines the metric information obtained from DPN-100 modules with that from Multiservice Switch nodes. DPN metrics are calculated differently from Multiservice Switch metrics, therefore the DPRS converts DPN metrics to the Multiservice Switch format.

Calculating DPN RID path metrics

To determine the best path across the entire network, DPRS must calculate a total path metric that allows for the Nortel Multiservice Switch subnet topology and the DPN topology. The calculations are different for throughput and delay metrics.

Nortel Multiservice Switch throughput metrics for a path to a RID from each Multiservice Switch node in a subnet is calculated by summing the

- Multiservice Switch throughput metric from the RID to the Multiservice Switch node supporting the gateway. This metric is converted using the formula
-

  14240 x RidMetric2

- Multiservice Switch throughput metric associated with the best path from the gateway node to the source node. This is the throughput metric obtained from the topology manager. This portion of the sum is zero when considering the path from a gateway node itself through a gateway to the destination RID (the metric from self to self is zero).

The Multiservice Switch delay metric for a path to a RID from each Multiservice Switch node in a subnet is calculated by summing the

- delay metric in DPN format from the RID to the Multiservice Switch node supporting the gateway converted to the Multiservice Switch format with the formula:

  RidMetric x 6000

- delay metric from the gateway node to the source node. This is the delay metric obtained from the topology manager.

Calculating AM metrics

AM metrics consist of simple hop counts. DPRS converts the hop counts into delay and throughput metrics. Because the delay and throughput characteristics of the links are not available, DPRS weights the hop count conversion in favor of the RID subnet paths over the AM paths. When the AM hop counts are converted to Nortel Multiservice Switch metrics, they are converted to large Nortel Multiservice Switch metrics. This process weights the high-speed Multiservice Switch backbone over the lower-speed AM links to limit traffic to the Multiservice Switch subnet as much as possible.

The throughput metric for a path to an AM or Multiservice Switch MID is calculated by summing

- The throughput metric from the AM MID to the Multiservice Switch node supporting the gateway. This value is the DPN-100 hop count from the

MID routing table update (MRTU) converted to the Multiservice Switch throughput metric with the following formula:

50283333 x ((hopCount x 2) + R)

where
R = 1 if the path from the Multiservice Switch node to AM is entirely through AMs
R = 0 if the path to the AM traverses an RM
(R is almost always 1, even in the case of a direct connection to an AM)

This part of the sum is always zero when considering the metric to the MID of a Multiservice Switch node.

- The throughput metric from the gateway node to the source node. This is the throughput metric obtained from the topology manager.

The delay metric for a path to an AM MID from each Multiservice Switch node is calculated by summing

- The delay metric from the MID to the Multiservice Switch node supporting the gateway. This value is the DPN-100 hop count from the MRTU converted to the Multiservice Switch delay metric with the following formula

  233333 x ((hopCount x 2) + R)

  where
  R = 1 if the path from the Multiservice Switch node to AM is entirely through AMs
  R = 0 if the path to the AM traverses an RM
  (R is almost always 1, even in the case of a direct connection to an AM)

  This part of the sum is always zero when considering the metric to the MID of a Multiservice Switch node.

- The delay metric from the gateway node to the source node. This is the delay metric obtained from the topology manager.

LMID routing

CSRMs distribute a list of the servers they support (such as source call router and destination call router) to the adjacent Nortel Multiservice Switch nodes. DPRS on these nodes then distributes this list to all other Multiservice Switch nodes in the subnet so that they can make optimal path selections (in the same way that RID paths are selected). The cost of traversing the subnet to reach a gateway to a CSRM is accounted for in the path selection process. DPRS selects up to two next-hop link groups for each RCOS and stores them in the LMID forwarding tables.

When there are two CSRMs in use to support the RID subnet, DPRS on each Multiservice Switch node selects the minimum metric paths to the closest CSRM. If a server on one of the CSRMs is not available or if the CSRM fails, DPRS calculates paths to the server functions on the other CSRM and places them in the forwarding table.

An LMID forwarding table is used for Multiservice Switch nodes that have CSRM routing provisioned as closest by default. If you configure CSRM routing as shared, a RID forwarding table is used. For more information on call establishment, see Call establishment using CSRMs (page 26).

Selecting paths

When the metric calculation process produces more than two equal minimum-metric paths for a route, DPRS uses routing determinism algorithms to determine which paths to put in the forwarding tables. There are routing determinism rules for RM, AMs, and CSRMs.

Preferred-path routing cannot be provisioned between DPN-100 modules and Nortel Multiservice Switch nodes. However, you can configure trunk overrides to achieve a similar effect. For more information on trunk overrides, see NN10600-420 *Nortel Multiservice Switch 7400/15000/20000 Operations: Trunking*.

Selecting paths from RMs

The routing determinism algorithm for routes with equal metric paths between RMs and RID subnets (or beyond) depends on the RCOS. For the delay RCOS, DPRS selects

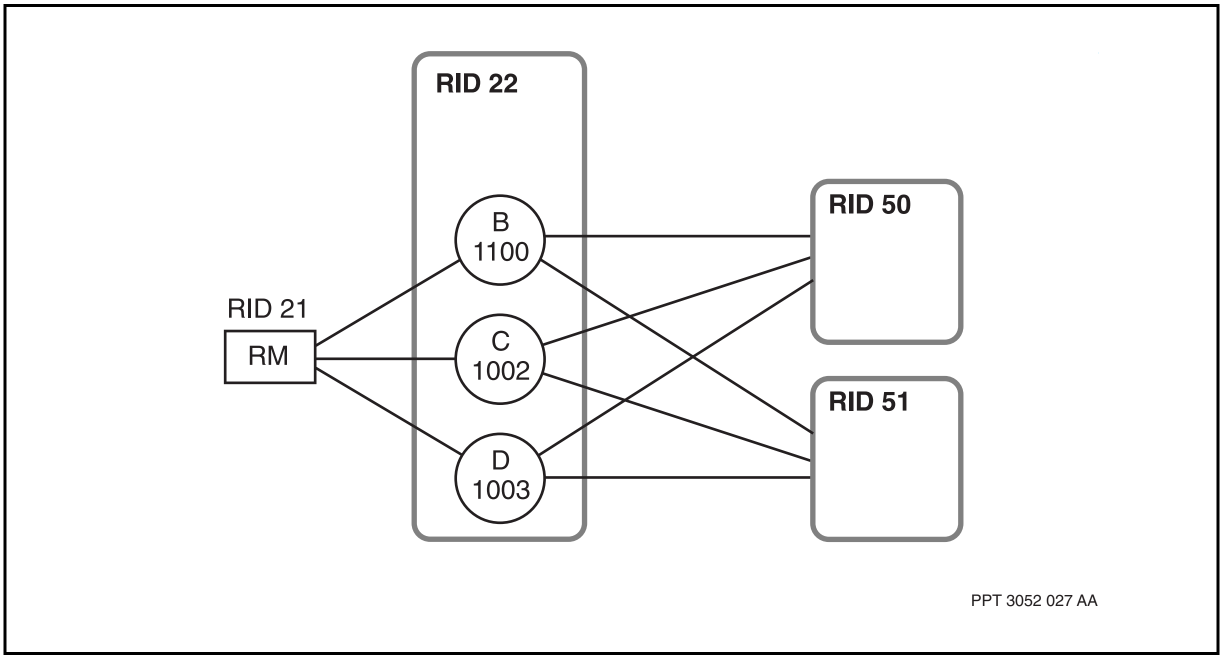
- the Multiservice Switch node with the highest MID value if the destination RID value is odd
- the Multiservice Switch node with the lowest MID value if the destination RID value is even

For the throughput RCOS, DPRS selects

- the Multiservice Switch node with the lowest MID value if the destination RID value is odd
- the Multiservice Switch node with the highest MID value if the destination RID value is even

For example, in the figure Selecting paths from RMs (page 33), DPRS selects node B to reach RID 51 for the delay RCOS. To reach RID 50, DPRS picks node C.

Selecting paths from RMs



Selecting paths from AMs

If an AM is connected to two Multiservice Switch nodes in the same RID subnet through equal metric paths, DPRS sends traffic directly to the appropriate node if it is destined for that MID. Otherwise, DPRS loadshares the traffic between the two Multiservice Switch nodes.

Establishing the call

The process of establishing the call differs slightly depending on whether the call destination is within the single RID subnet, or in another RID subnet.

For details on call routing in a DPN-100 network, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description*.

Call establishment inside a RID subnet

When the source and destination nodes are in the same RID subnet, one CSRM handles both source and destination call routing functions. The figure Call routing in the subnet (page 35) shows the process of establishing a call in a single RID subnet. The diagram shows the three phases in the process:

In the following example, the DNIC has been omitted.

1 Creating the call request packet

The VC process of the access service creates the call request packet. The packet contains: the DNA (1021001), RID (51), MID (1001), and MPID (x) of the source access service; the DNA (1030101) of the destination access service; and the LMID (8B40) of the source call router (SCR) in the closest CSRM.

The VC process sends the call request packet to DPRS packet forwarding, which recognizes the RID of 0 as indicating the current subnet. Packet forwarding determines that the LMID is an SCR address. It looks up the LMID in the LMID forwarding table, and sends the call request packet to the closest SCR function available on a CSRM.

2 Translating the prefix-DNA

The SCR translates the prefix of the DNA in the call request packet to the destination RID using the prefix-DNA mapping tables. These tables contain the provisioned values of prefix-DNAs and their corresponding MIDs and RIDs. The SCR then puts the destination RID value (51) in the call request packet and sends it to the destination call router (DCR).

Using the DCR mapping tables, the DCR maps the next portion of the prefix-DNA (10301) and obtains the destination MID (1004).

The DCR puts the destination MID value (1004) in the call request packet with the address (1) of the Nortel Multiservice Switch final destination call router (FDCR) that handles DNAs supported on the destination node. The DCR then invokes DPRS packet forwarding again to send the packet to the destination node.

3 Finding the access service

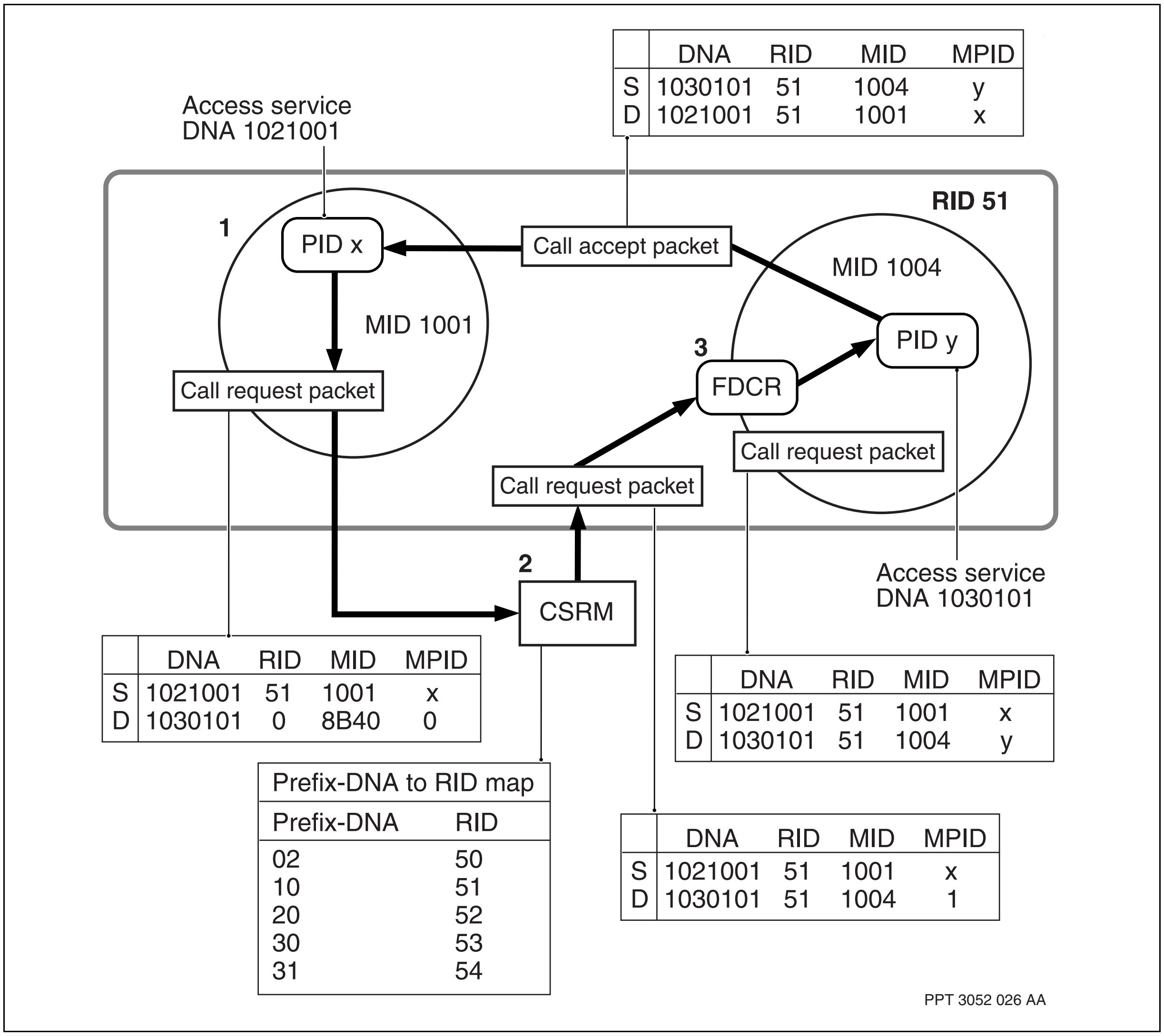
At the destination node, the Multiservice Switch node’s FDCR translates the rest of the DNA to determine the MPID (y) of the destination access service. The FDCR sends the call request to the destination access service, which creates the destination VC.

4 Returning the call accept packet

The VC process exchanges the source and destination fields in the call request packet to create the call accept packet. The packet contains: the DNA (1030101), RID (51), MID (1004), and MPID (y) of the source access service, as the packet’s address; and the DNA (1021001), RID (51), MID (1001), and MPID (x) of the destination access service.

Packet forwarding returns this packet to the source access service by the most direct route.

Call routing in the subnet



	DNA	RID	MID	MPID
S	1030101	51	1004	y
D	1021001	51	1001	x

	DNA	RID	MID	MPID
S	1021001	51	1001	x
D	1030101	0	8B40	0

Prefix-DNA to RID map	
Prefix-DNA	RID
02	50
10	51
20	52
30	53
31	54

	DNA	RID	MID	MPID
S	1021001	51	1001	x
D	1030101	51	1004	y

	DNA	RID	MID	MPID
S	1021001	51	1001	x
D	1030101	51	1004	1

Call establishment outside the RID subnet

In the figure, Call routing outside the subnet (page 37) shows the process of establishing a call between multiple RID subnets. The diagram shows the four phases in the process:

1 Creating the call request packet

This phase of the process operates identically to the single-RID subnet process. The call request packet contains the DNA (2062201) of the access service, and the LMID (8B40) of the SCR in the nearest CSRM.

2 Translating the RID

In this case, the SCR maps the prefix-DNA (20) to RID 52, so the call request packet is updated with this RID value. The SCR sets the MID field to the LMID (8080) of the DCR. DPRS packet forwarding sends the packet to the RID subnet 52. The packet then continues to the DCR server in the closest CSRM. In this example, it is the DCR at LMID 8080.

3 Translating the MID

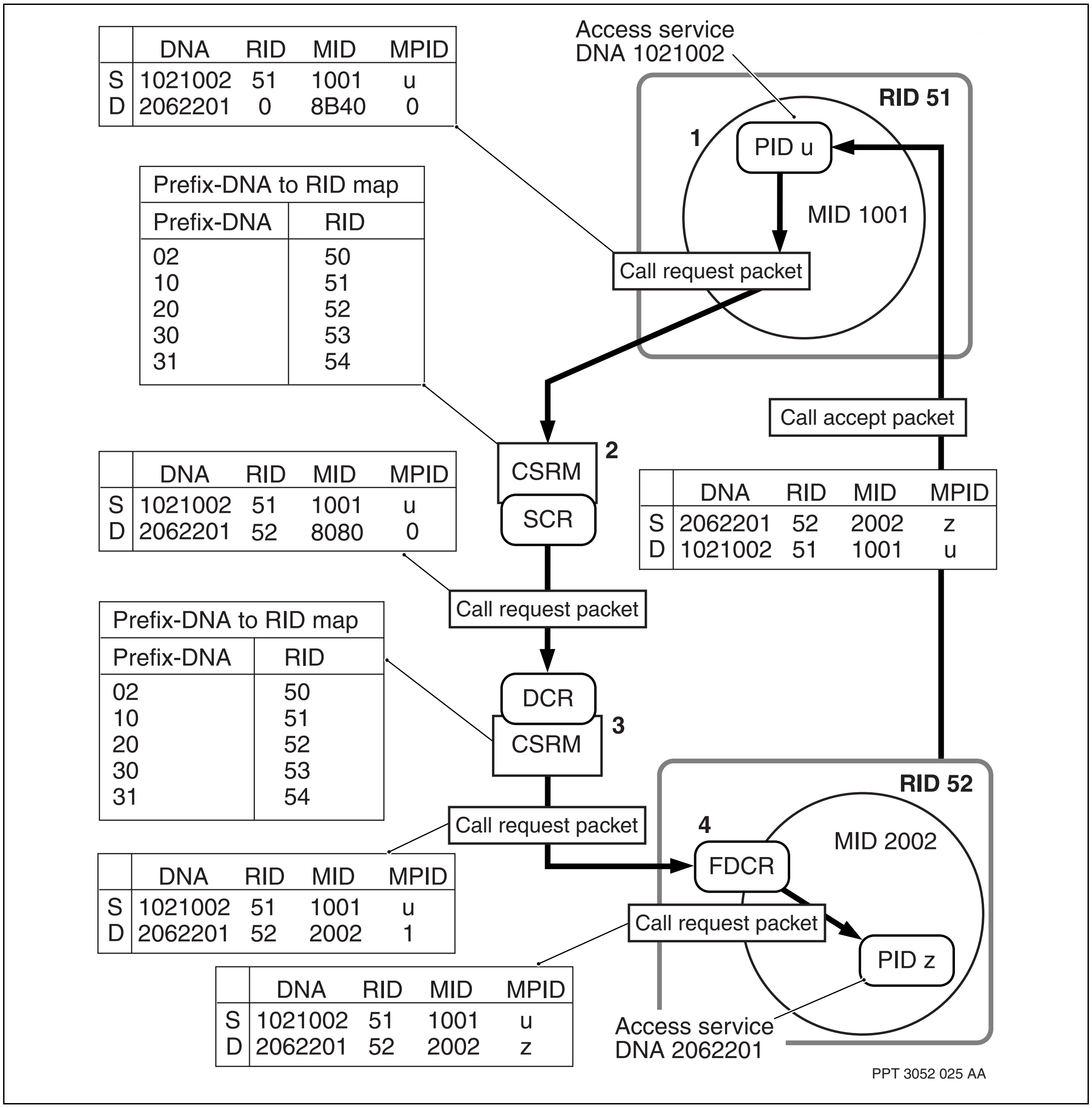
This phase of the process is identical to the translation of the prefix-DNA in the case of the single-RID subnet. The DCR maps the prefix-DNA (20622) to MID 2002, and the packet is sent to the FDCR at LMPID 1.

4 Finding the access service

This phase of the process operates identically to the case of the single-RID subnet.

When the call path setup is off-network, the SCR on the closest CSRM forwards the call setup request to the gateway SCR (GSCR). The GSCR sends the call to the gateway DCR (GDCR) on the destination RID. The GDCR then sends the call to the selected destination gateway. For more information on gateway call routing, see Network planning and engineering (page 59).

Call routing outside the subnet



	DNA	RID	MID	MPID
S	1021002	51	1001	u
D	2062201	0	8B40	0

Prefix-DNA to RID map

Prefix-DNA	RID
02	50
10	51
20	52
30	53
31	54

	DNA	RID	MID	MPID
S	1021002	51	1001	u
D	2062201	52	8080	0

	DNA	RID	MID	MPID
S	2062201	52	2002	z
D	1021002	51	1001	u

Prefix-DNA to RID map

Prefix-DNA	RID
02	50
10	51
20	52
30	53
31	54

	DNA	RID	MID	MPID
S	1021002	51	1001	u
D	2062201	52	2002	1

	DNA	RID	MID	MPID
S	1021002	51	1001	u
D	2062201	52	2002	z

Forwarding packets

The DPN-100 routing system uses a round-robin scheme in selecting the next hop link group. Because this scheme increases packet disordering, the Nortel Multiservice Switch network uses a loadspreading algorithm to handle this aspect of packet forwarding. For information about packet forwarding algorithms, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

Traffic management

This chapter describes traffic management considerations for a combined Nortel Multiservice Switch node and DPN-100 node network.

Navigation

Backup RCOS routing

In a DPN-100 network, the routing system has an alternative RCOS scheme. In this scheme, DPN routing uses the delay RCOS path as an alternative for throughput RCOS traffic when a throughput path is not available for a destination. The reverse situation also applies. If there is no delay path available, delay RCOS traffic is sent over throughput paths.

In a Nortel Multiservice Switch network, DPRS can use a throughput path as an alternative for delay traffic, but does not use a delay path as an alternative for throughput traffic.

Congestion management

In a combined network, congestion control considerations include:

- reliability
- discard priority

Reliability

The normal reliability (NR) bit in the subnet header controls the forwarding behavior for a packet under congestion conditions. In a combined network, the NR bit has the following effect:

- If the NR bit is set (normal reliability), packet forwarding tries all the other links in the group when a link is unavailable. Packet forwarding does not try the other link group under these conditions.
- When the NR bit is not set (high reliability), packet forwarding tries to find a link in the alternative link group if it cannot find one in the first group.

The same effects apply to congested links between RMs and RID subnets. If an RM has more than one equal-metric link group to a RID subnet, the alternative link group is selected from the set of link groups remaining after the primary link group is selected. If the RM has a single link group to the subnet, an alternative link group to another RID is selected.

If DPRS sends a packet on a congested link, packet forwarding sets the forward congestion indication (FCI) in the packet's common header.

Discard priority

In Nortel Multiservice Switch networks, a packet's effective discard priority is derived from a combination of the discard priority (DP) bit in the packet's common header and the priority bit in the DPRS header. This discard status is compared to the link's congestion level indicated in the link table to determine whether to discard the packet.

In DPN-100 routing systems, the priority bit is used to select queues. In DPRS, the priority bit is used to help determine discard priority. If the priority bit is set, the DP value from the common header is increased by one level to make the packet less likely to be discarded.

Multiservice Switch discard priority system has four levels of priority. Normally, the lowest discard priority (discarded first) is assigned to packets that are in excess of their reported bandwidth. For example, this priority level could include frame relay packets that exceed their committed information rate (CIR). The highest discard priority (never discarded) is reserved for network control traffic.

Multiservice Switch-to-DPN discard priority mappings (page 40) shows the mapping of DPN traffic packet type to Multiservice Switch discard priority.

Multiservice Switch-to-DPN discard priority mappings

Multiservice Switch discard priority	DPN discard priority
3	Discard eligible data (DE bit=1 packets, call, call accept)
2	All data and data acknowledgment packets, priority call, priority call accept, accept, idle probe, reset, nfc recov and recov confirm
1	Priority data and priority data acknowledgment packets, priority accept, all call disconnect packets, abort
0	Routing table updates and all network control traffic

Overflow routing

In DPN-100 networks, overflow routing allows high-reliability traffic to be routed over an alternative equal-cost path when the primary path is congested. In Nortel Multiservice Switch networks, overflow routing also occurs on non-equal alternative paths when variance is in effect. For information about variance, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

In a combined network, normal-reliability traffic can overflow to an uncongested link in the first choice link group. High-reliability traffic can overflow to an uncongested link in the other link group (if there is one).

RID substitution

In DPN-100 networks, RID substitution is a routing feature that dynamically enables traffic to be rerouted through an AM's other cluster RID when the network link to one of its supporting RIDs fails. RID substitution is supported in a combined network between Nortel Multiservice Switch RID subnets and RMs, and between interconnected RID subnets.

Multiservice Switch nodes in a RID subnet learn the substitute RID for an AM when it connects to the subnet. DPRS saves this information and propagates it to all the nodes in the RID subnet. When an AM disconnects from the RID subnet, the RID substitution information for the AM's MID is preserved. An entry for the MID remains in the MID routing tables, even though the MID is not accessible through any link group. This entry contains only the RID substitution information for the MID.

The substitute RID information remains in the forwarding tables until:

- The AM connects to the RID subnet again and reports a new substitute RID.
- The AM reconnects to its gateway nodes but no longer reports a substitute value (no longer has a connection to another cluster RID). In this case, the

nodes with gateways to the AM cluster no longer report a substitute RID value for the AM. The other Multiservice Switch nodes in the RID subnet still contain the original substitute RID for the AM in their forwarding tables until they reboot.

RID splitting

You can configure RID splitting in the DPN-100 DCR. RID splitting is used during AM migration as a temporary mechanism to route the AM's calls to the AM's new home RID. After the network-wide SCR preix DNA mapping tables are updated, the mechanism is no longer needed.

RID splitting is supported between Nortel Multiservice Switch nodes and DPN-100 modules, as well as between Multiservice Switch RID subnets. For more information about RID splitting, see Splitting a RID subnet (page 87).

RID redirection

In DPN-100 networks, RID redirection (or RID backup) provides a similar functionality to RID splitting on a more permanent basis. You can use RID redirection to back up an AM's cluster RID with another RID. Under failure conditions, the backup RID takes over calls from the original cluster RID. For more information on RID redirection, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description*.

You can also back up a Nortel Multiservice Switch subnet RID with another Multiservice Switch subnet RID using this method. However, the preferred method of back up in the Multiservice Switch network is to use the call redirection server. For more information on call redirection, see NN10600-410 *Nortel Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server*.

Dial-in gateway

DPN gateways support dial-in links between a DPN module and a Nortel Multiservice Switch network. For dial-in links in a DPN network, see 241-1001-015 *DPN-100 Network Link and Trunk User Guide*.

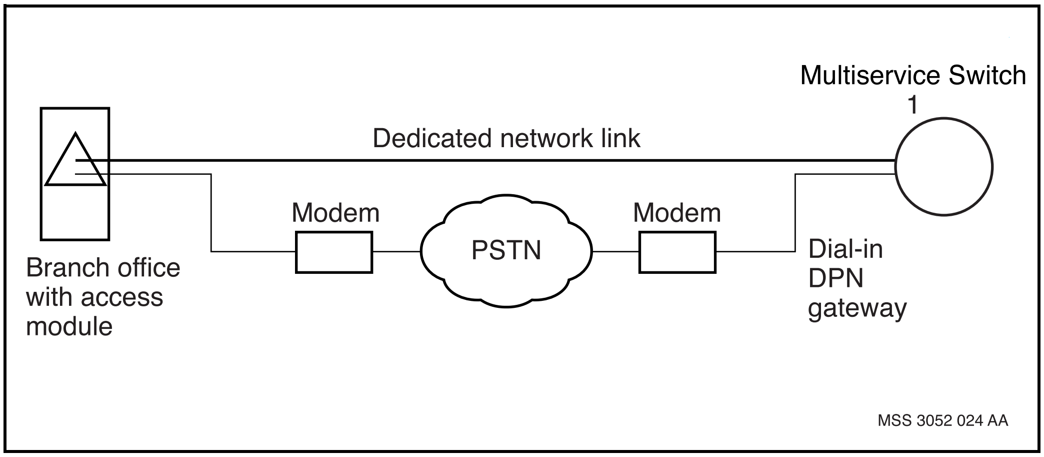
DPN gateway over frame relay does not support dial-in functionality.

Dial-in DPN gateway link types

You can configure the *DpnGateway linkType* attribute as dedicated (the default) or dialIn. Dial-in DPN gateways are dial backup network links (DBNL). A DBNL link provides connectivity between a remote DPN module and a Nortel Multiservice Switch network when a dedicated DPN gateway connection breaks. This capability allows continued service, minimizes data loss, and eliminates node isolation.

The remote module configured with a DBNL makes a modem call through a public switched telephone network to a dial-in port in the Multiservice Switch network. When the local modem completes the connection on the Multiservice Switch side, the dial-in link stages as a normal network link. See the figure Dial-in DPN gateways functionality (page 42) for an illustration of the dial-in functionality.

Dial-in DPN gateways functionality



Dial-in DPN gateways and DPN dial-up network links

The dial-in DPN gateway capabilities include the following points:

- DBNLs connected to a Nortel Multiservice Switch node instead of a DPN module, reduce DPN hardware requirements in a Multiservice Switch network.
- DBNLs connected to a Multiservice Switch node instead of a DPN module, increase bandwidth effectiveness and reduce delays. Calls do not have to transit through a DPN module to reach the Multiservice Switch network.
- Multiservice Switch nodes do not support the password security feature available on DPN dial backup links. DPN modules must not run this feature on backup links for Multiservice Switch nodes.
- Auto-enable and auto-disable scripts on DPN modules function on backup links for Multiservice Switch nodes when the software on both systems includes this feature.
- Dial-in DPN gateways in ISDN networks require an ISDN modem. The ISDN modem allows calling line ID validation.
- Multiservice Switch nodes do not support backup from stub AMs since the parent AM MID is not available on Multiservice Switch nodes.

Activation

A manual operator command or an automatic activation script activates a dial-in link as follows:

- the operator or script manually enters the dial command on DPN
- a DBNL automatically activates to avoid module isolation

When the dial-in link is active, the operational parameters in Nortel Multiservice Switch node indicate the remote link type as DBNL.

Disabling

A manual operator command or an automatic disable script, disables a dial-in link. When the link is disabled, both the Nortel Multiservice Switch nodes and DPN modules display a dial-in link out-of-service alarm. The DBNL automatic disabling script functions as it does on a DPN module, whether the local end is a DPN module or a Multiservice Switch node.

Tandem suppression

Both DPRS and DPN-100 routing systems have a tandem suppression capability. When Nortel Multiservice Switch tandem suppression is enabled on a node, intra-subnet tandem traffic is blocked. The only DPN traffic routed to the node is traffic destined for the node itself or any connected AMs or neighboring RIDs (subnets or RMs). For more information, see NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

For information about the DPN-100 tandem suppress capability, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description*.

Trunk group factor

On RMs and CSRMs, you can configure a trunk group factor (TGF). This factor indicates whether adding a link to a link group will alter the metric of the link group in the throughput RCOS. Although you can still configure a TGF on an RM connected to a RID subnet, you cannot configure a TGF on a Nortel Multiservice Switch node. Instead, the Multiservice Switch node receives the TGF for each link group from the neighbor RM and follow its example, ensuring equal metrics in both directions. For more information on TGFs, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description*.

Variance

Variance improves traffic spreading across the Nortel Multiservice Switch backbone by providing more balanced link usage across the network through the safe use of unequal-metric paths. In addition to the better spreading of traffic, which helps avoid congestion situations, variance provides more possible paths for high-reliability traffic overflow when congestion does occur.

If you configure variance on a node, it affects any RID or MID destination you can reach from that node, including RMs and AMs. It also affects any path Multiservice Switch nodes' can compute, including gateway paths. See NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System* for more information on variance.

Delay and throughput cutoff

The ability to configure the delay and throughput cutoff values can be a useful mechanism for fine tuning routing within a DPN-100 network. These values are used by the RID routing system to determine at which point a switch can be considered unreachable. If the metric value to reach the switch exceeds the cutoff for that COS, then the switch is considered unreachable for that COS.

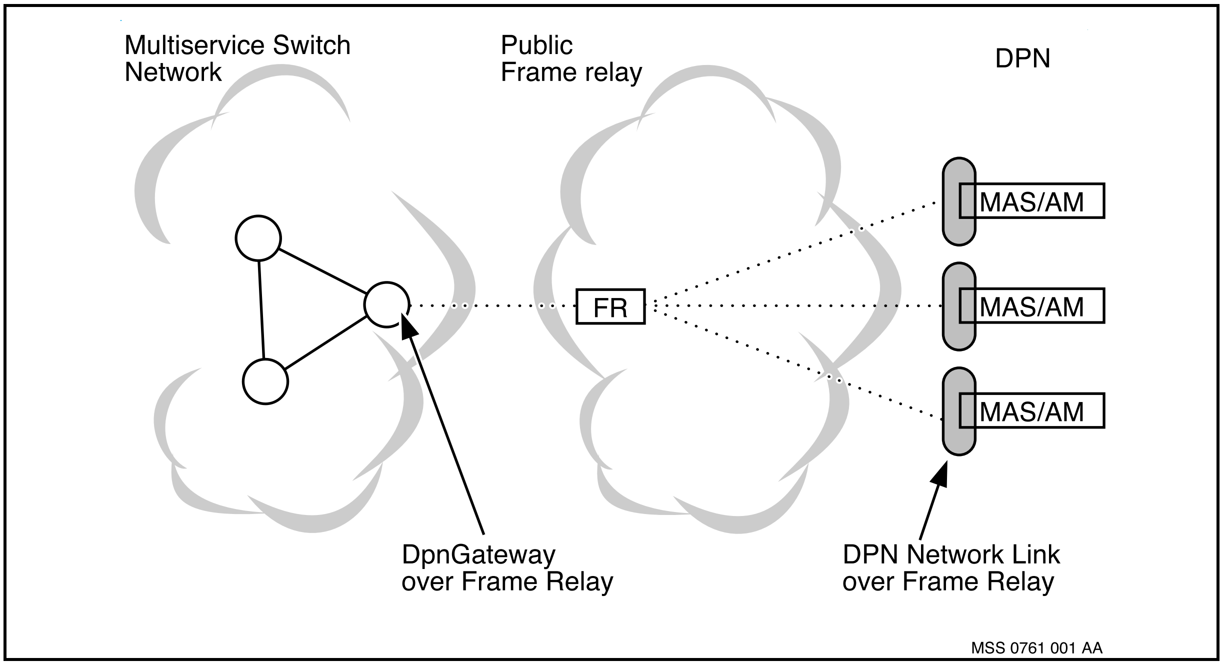
With the interconnecting RID subnets feature, Nortel Multiservice Switch modules engage in the RID routing protocol with other Multiservice Switch nodes in different RID subnets. Neither side has any knowledge of the cutoff values of other nodes. Multiservice Switch nodes have two provisionable cutoff attributes for the *Rtg Dpn* component. A default value is provided for these attributes. The same DPN-100 default cutoff value of 245 is used for the throughput cutoff. However, a value of 128 is used for the delay cutoff default.

Reasonable values to set for each are approximately double the largest RID delay and throughput metric values expected anywhere in the network. To ensure routing behavior consistency, you must configure all Multiservice Switch nodes in the network to have the same cutoff values. See NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System* for more information on metric cutoff.

DPN Gateway over Frame Relay

DPN Gateway over Frame Relay is a capability that allows you to connect DPN AMs and Multi-service Access Switches (MAS) to Nortel Multiservice Switch nodes through a public frame relay network. See the figure DPN Gateway over Frame Relay (page 45) for a sample network scenario.

DPN Gateway over Frame Relay



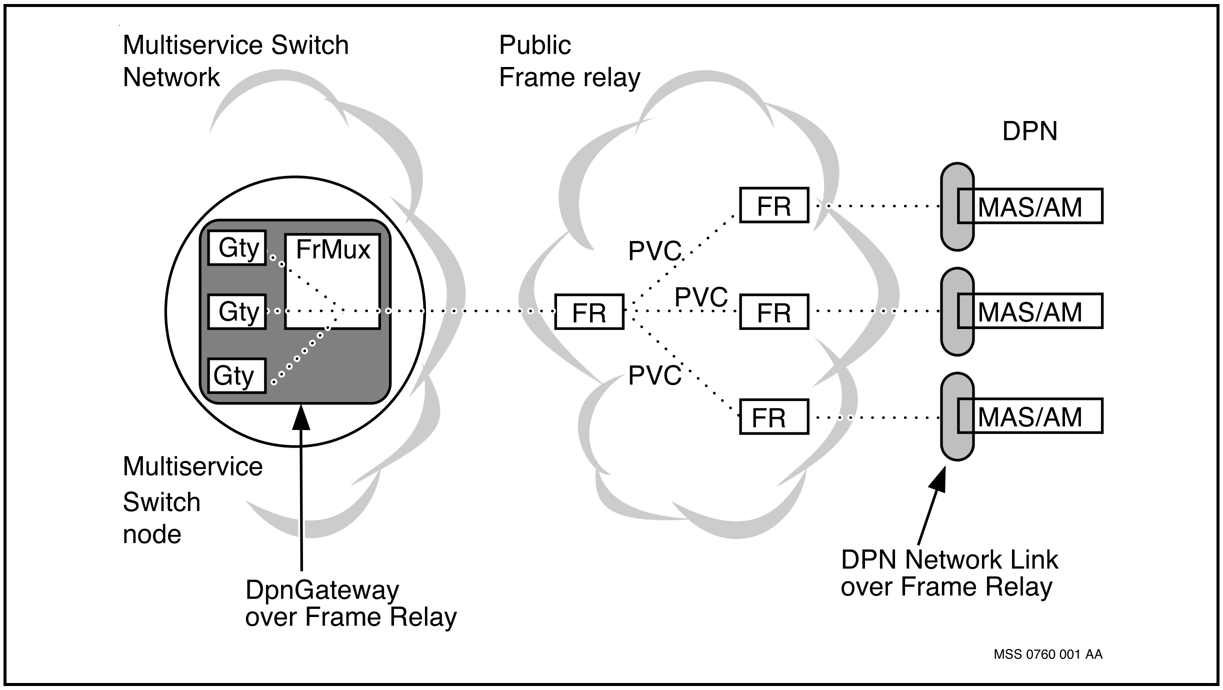
DPN Gateway over Frame Relay cannot connect an RM to a Multiservice Switch node.

Establishing this connection through a public frame relay network, rather than leased line, has the following advantages:

- The user has the benefit of lower frame relay tariffs, compared to leased line costs.
- The amount of interconnecting equipment is reduced because the frame relay service acts like a logical multiplexor.

The figure, Detailed look at DPN Gateway over Frame Relay (page 46) illustrates the multiplexing aspect of the feature and the logical nature of the connection. The Multiservice Switch side of the connection is DPN Gateway over Frame Relay. The DPN side of the connection is the DPN feature Network Link over Frame Relay. Many connections can be established on a single physical interface and are extended to their destinations by permanent virtual circuits (PVCs) in the public frame relay network.

Detailed look at DPN Gateway over Frame Relay



The traffic types handled by this service are the same as DpnGateway running on its own link. DPN Gateway over Frame Relay runs in network link mode only.

DPN Gateway over Frame Relay features

The following sections describe features of DPN Gateway over Frame Relay, including:

- Function processor support (page 47)
- Traffic management (page 47)
- Classes of service (page 48)
- Bandwidth management (page 48)
- Queueing architecture (page 49)
- Software component architecture (page 50)

- Trunking protocol architecture (page 51)
- Protocol stack (page 52)

Function processor support

The table, Function processor support (page 47) lists the maximum number of DpnGateways that are supported on the FPs that run DPN Gateway over Frame Relay.

Function processor support

Function processor	Maximum number of DpnGateways supported
DS1	40
E1	
DS1-8P	
V.11	
V.35	
DS1C	100
E1C	

Traffic management

DPN Gateway over Frame Relay links take part in node traffic management by monitoring the queue length against CIR-based thresholds. The forward congestion indication (FCI) is set on frames that are transmitted on congested DPN Gateway over Frame Relay links.

The posted congestion level is the maximum of the combined levels for the high and normal emission priority queues. When the normal emission priority queue reaches its provisioned discard level, no new packets of lower discard priority are accepted in either the high or normal emission priority queues. The normal emission priority queue is serviced after the high emission priority queue is empty.

When more than one DPN Gateway over Frame Relay link is provisioned between two modules, load sharing is the traffic balancing method used. This mechanism places consecutive packets of a call on any links in a link group, with the aim of achieving equitable load on all links. If a link to which the packet is directed is congested, then the packet is discarded. This works identically whether the link is registered with the shelf congestion management (discard by forwarding), or not (discard by the service).

Load spreading is not fully supported for this feature. The link does not provide congestion feedback information, consequently, all packets from a particular call are always directed to the first-choice link. If this link becomes congested, the packets are discarded, instead of being forwarded to another link.

Classes of service

DPN Gateway over Frame Relay supports only connectionless data traffic with the following classes of service:

- high emission priority
- normal emission priority

Emission priorities are implemented by maintaining two queues for each DpnGateway, one for high emission priority and one for normal emission priority. The high emission priority queue is always serviced first. The normal emission priority queue is serviced when there are no frames in the high emission priority queue.

Bandwidth management

DpnGateway traffic is transmitted on a frame relay link through a single logical channel identified by its data link connection identifier (DLCI). The link’s total transmit bandwidth is the sum of the bandwidths allocated to each logical channel on the link. The transmit bandwidth is managed on each DLCI by a traffic shaping mechanism that ensures that transmitted egress traffic conforms to subscribed traffic parameters. If a connection is offered traffic in excess of the peak cell rate, the excess frames are buffered.

Traffic shaping is applicable to egress traffic only. No bandwidth management is done on ingress traffic.

Traffic shaping is based on a CIR. Traffic shaping sends out frames at approximately constant maximum speed, corresponding to the provisioned CIR. The output traffic can only exhibit small bursts, corresponding to 10 ms of transmission at the CIR speed. This is done as follows:

- When a frame is accepted for transmission, the frame size is added to the credit account of the logical channel.
- The credit account is decremented every 10 ms by the amount that corresponds to 10 ms of transmission at the CIR speed.
- New frames are accepted only when the credit account is zero (0) and the maximum number of frames accepted equals 10 ms of transmission.

  It is strongly recommended that the aggregate of all CIRs does not exceed the frame relay link speed.

If the aggregate of configured CIRs does not exceed the frame relay link speed, the bandwidth for every logical channel is guaranteed. If the aggregate of configured CIRs does exceed the frame relay link speed, there is no guarantee that the bandwidth for every logical channel will be available. In this case, the user must weigh the advantages of higher link usage against the disadvantages of potentially increased delays, data loss due to discards, and decreased throughput.

DPN Gateway over Frame Relay does not have the frame relay service’s excess information rate (EIR) capabilities and does not use the committed burst (Bc) parameter.

Queueing architecture

The queueing architecture of DPN Gateway over Frame Relay is shown in the figure Queueing architecture (page 50).

Traffic coming from the bus is handled first by the traffic management function, as described on Traffic management (page 47).

The output of the high and normal emission queues is controlled by the following mechanisms:

- emission priorities

  Emission priorities are applied to each DpnGateway in a multi-DpnGateway environment.

- traffic shaping

  A frame is dequeued only when traffic shaping allows it to go. Otherwise the frame stays in the queue without unnecessary retrieval.

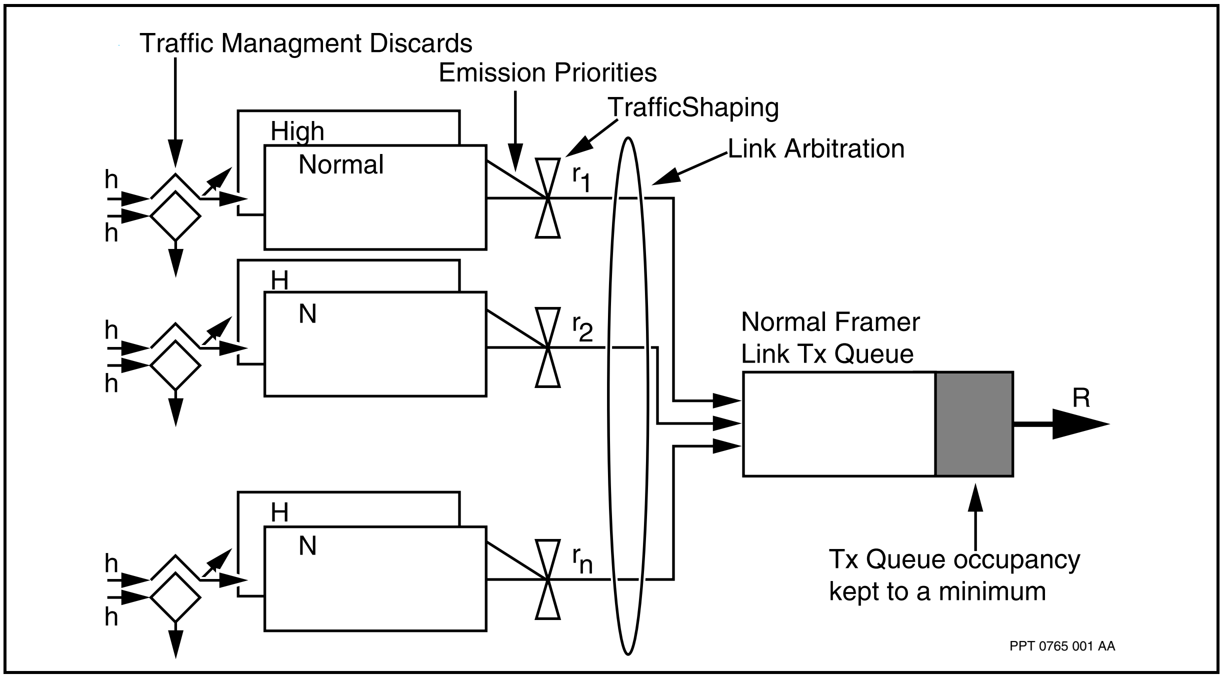
- link arbitration

  Link arbitration is based on a round-robin loop. On each visit to a DpnGateway, its two queues are dealt with according to the emission priority mechanism.

- interaction with the framer output queue

  Only the normal framer link transmission queue is used. Multiple DpnGateway software queues handle the buffering requirements. The framer output queue is fed at a rate that does not leave idle time on the link.

Queueing architecture



Software component architecture

The figure, DPN Gateway over Frame Relay components (page 51) illustrates the software components of DPN Gateway over Frame Relay. DpnGateways and the supporting FrMux must be on the same FP.

The *FrAccess* component contains all of the attributes related to the link layer protocol (LTP, described in Protocol stack (page 52)).

The *FrMuxSetup* subcomponent of FrAccess contains all of the traffic parameters (CIR and maximum frame size) for the frame relay DLCI, and the component name of the DLCI on which the Gateway runs.

The *FrMux* component provides a frame relay interface and supports the following:

- the user side procedure of the user network interface (UNI-USP)
- the reception of the asynchronous status message (ASM) for the ANSI and CCITT LMI protocols

The *DataLinkConnectionIdentifier* subcomponent of *FrMux* represents a single logical channel of the *FrMux*, over which the traffic of one DpnGateway is transmitted.

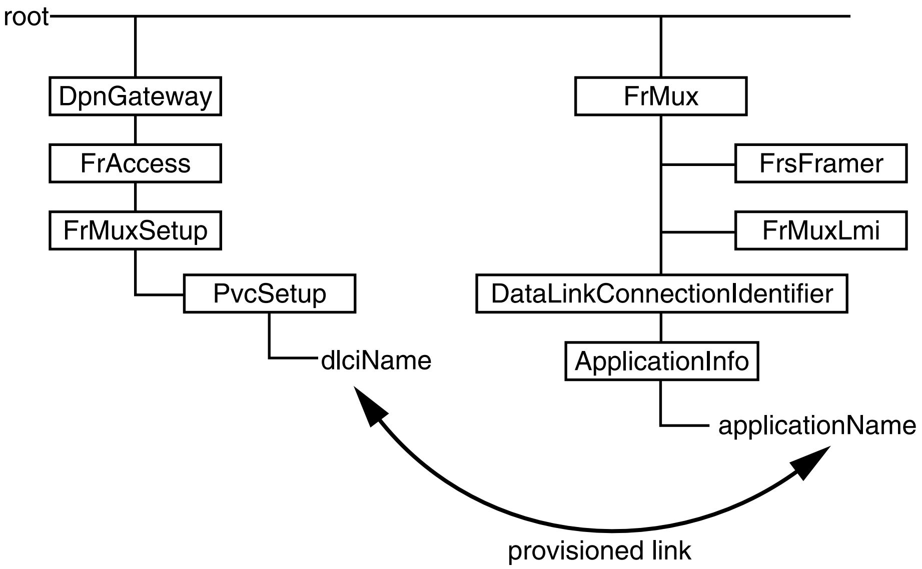
Trunking protocol architecture

DPN Gateway over Frame Relay is divided into the following two subsystems:

- a frame relay interface
- the DpnGateway and FrAccess applications

The location of DpnGateway and FrAccess within the Nortel Multiservice Switch trunking protocol architecture is shown in the figure Multiservice Switch trunking protocol architecture (page 51).

DPN Gateway over Frame Relay components



PPT 0762 001 AA

Multiservice Switch trunking protocol architecture

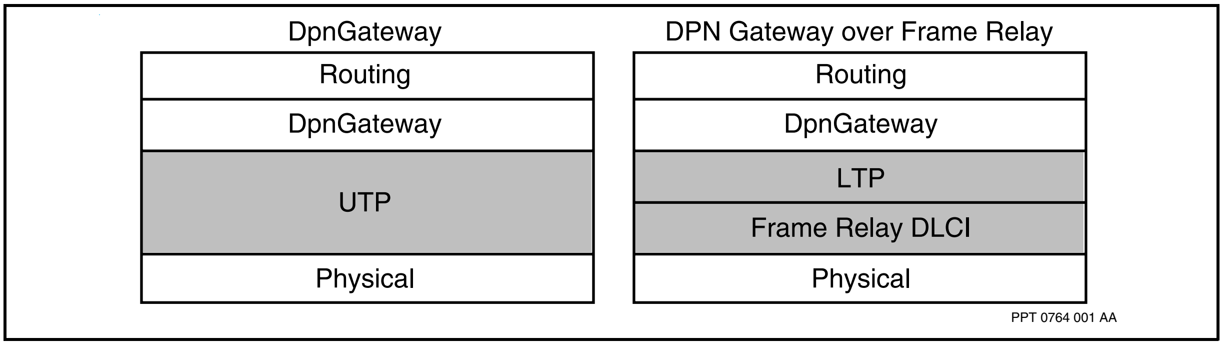
<table>
<tr><td colspan="3">Trunk</td><td colspan="2"><b>DpnGateway</b></td></tr>
<tr><td>Trunk</td><td>AtmAccess</td><td colspan="2">UTP</td><td><b>FrAccess</b></td></tr>
<tr><td></td><td>ATM</td><td colspan="2"></td><td><b>FR</b></td></tr>
<tr><td colspan="5">Physical</td></tr>
</table>

PPT 0763 001 AA

Protocol stack

The protocol stack of the DPN Gateway over Frame Relay feature is compared to the protocol stack of the existing DpnGateway service in the figure Comparison of protocol stacks (page 52).

Comparison of protocol stacks



The universal trunking protocol (UTP) layer of the DpnGateway service is replaced with the light-weight trunk protocol (LTP) and frame relay. From the routing system's point of view, DpnGateway running on FrAccess is indistinguishable from a DpnGateway running on UTP.

See FrAccess link protocol considerations (page 53) for a description of how LTP differs from UTP.

The frame relay DLCI layer conforms to all existing standards for a PVC-based frame relay access. See Standards and DPN Gateway over Frame Relay (page 55) for more information.

Interaction with the routing system

While choosing the link, the routing system enforces all of the applicable class of service parameters, with the exception of transmit priorities. Exercising the transmit priority is a joint activity. Routing uses priority in link selection, and DpnGateway keeps high and normal priority transmit data separately, exercising the transmission choices on an individual link.

Traffic shaping limits the transmission speed to the configured CIR. This speed is set once, during initialization. Alternatively, the speed can be provisioned with the *overrideTransmitSpeed* attribute. This attribute takes precedence over the measured speed if the attribute is non-zero.

In frame relay, round trip delay (RTD) is measured by DPN Gateway protocol. Measured RTD may be overridden by configuring the attribute *overrideRoundTripDelay* to a non-zero value.

Losses in a third party frame relay network

The frame relay connection over an external network is potentially more lossy than the leased line used for normal DpnGateway. Relative to a DpnGateway, DPN Gateway over Frame Relay is more vulnerable to the following adverse conditions in a public network:

- variable delays
- traffic congestion, possibly severe enough to cause data loss

Nortel Multiservice Switch virtual circuit (VC) or Multiservice Switch service applications (at a level above the DpnGateway) account for and safeguard against these adverse conditions, where possible.

However, critical applications using DPN Gateway over Frame Relay must be capable of recovering from variable delays and data loss themselves. For the network provider using DPN Gateway over Frame Relay, it is important to know how heavy the losses are on the public frame relay network connection.

Operational attribute *lostFrames* (in group *Statistics* of FrAccess) keeps a count of lost frames. Link quality monitoring is also based on this count.

Another concern in a loss-prone public network is that MRTU broadcasts may be lost. For example, since the MRTUs are treated as data frames in UTP, losing the last one of a series may adversely impact the network. As a safety measure against this possibility, the LTP protocol implements an LTP level acknowledgment mechanism with a one-packet MRTU-wait-for-acknowledgment queue, and timer based retransmissions.

FrAccess link protocol considerations

To increase throughput, the FrAccess link protocol (LTP) has the following simplifications relative to UTP:

- acknowledgments and retransmissions are left to higher levels
- window-based flow control is removed, reducing the number of control frames required
- the frame numbers are a fixed size, reducing processing requirements
- the CIR is used as the link speed, eliminating link speed measurements

As a result, the LTP provides increased throughput on stable links but may be lossy. Recovery from losses in the public frame relay network is accomplished by the application level (above the routing level shown in the figure Comparison of protocol stacks (page 52)). For acknowledged protocols, losses are handled by the VC mechanism within the Nortel Multiservice Switch and DPN network. For unacknowledged protocols, losses must be handled by a high-level application external to the Multiservice Switch and DPN network.

DpnGateway protocol considerations

When the DpnGateway receives an enable indication from FrAccess, it initiates a neighbor discovery protocol, followed by a testing protocol. After successful completion of these, DpnGateway considers itself on-line. The DpnGateway then registers with the routing system and starts carrying user data.

Loop/Neighbor check protocol

After a DpnGateway link is operational, it employs a neighbor checking protocol. The identity of a module, FP, or port is communicated to its neighbor to ensure the following:

- The link is still in service.
- There is no accidental looping.
- The neighbor is still the same.

The Nortel Multiservice Switchside of the link periodically sends a control packet, called a neighborcheck packet. The DPN side responds to this packet according to the neighbor checking protocol. The DPN side periodically sends a level 2 control frame (referred to as a loopcheck frame) to which the Multiservice Switch side responds. If a break of the continuity is detected by either side, the link is taken down and alarms are generated at both ends.

Support of the quality of service

DPN Gateway over Frame Relay maintains service through quality of service indicators described in the table Quality of service indicators (page 55). In addition, mechanisms exist for DpnGateway to:

- receive a packet from the Nortel Multiservice Switch subnet
- calculate the longitudinal redundancy checks (LRCs) for the packet
- compare the calculated LRC with the LRC in the packet

Packets with mismatched LRCs are discarded instead of being sent into the public frame relay network.

Quality of service indicators

Items being monitored	Indicator name/details	Statistic name/function
Frame relay congestion statistics	**Forward Explicit Congestion Notification (FECN)** Derived from packets travelling in the public frame relay network to DpnGateway direction.	**fecnFrmFromIf** • Tally of FECNs received **fecnFrmToIf** • Tally of FECNs transmitted • Zero. Not set by this service
	Backward Explicit Congestion Notification (BECN) Derived from packets travelling in the DpnGateway to public frame relay network direction.	**becnFrmFromIf** • Tally of BECNs received **becnFrmToIf** • Tally of BECNs transmitted • Zero. Not set by this service
Discard Eligible frames and bytes	**Discard Eligible (DE)** The DPN feature Network Link over Frame Relay always sends packets into the public frame relay network with the DE bit reset.	**deFrmFromIf** • Tally of packets received with the DE bit set **deBytesFromIf** • Tally of bytes received with the DE bit set
Lost packet statistics	The DPN feature Network Link over Frame Relay attaches a sequence number to each packet it transmits. DpnGateway monitors for breaks in sequence numbers to detect lost frames.	**lostFramesFromIf** • Tally of packets lost in the public frame relay network
Discarded packet statistics	When the frames waiting for transmission in the DpnGateway queues exceed the highest congestion threshold, any new arrivals are discarded.	**discardExcessToIf** • Tally of packets discarded in the DpnGateway to interface direction as a result of congestion on the transmit buffers

Standards and DPN Gateway over Frame Relay

This feature’s local management interface (LMI) of FrMux can be configured to function as one of the following:

- User Network Interface, User side (Vendor Forum)
- User Network Interface, User side (ANSI T1.617, Annex D)

- User Network Interface, User side (CCITT Q.933, Annex A)

The following tables describe DPN Gateway over Frame Relay compliance with standards. The terms used in the tables are:

- Noted. This is used where the specification provides clarification, non-specific information or details that do not relate directly to the DPN Gateway over Frame Relay service.
- Fully complies with. The DPN Gateway over Frame Relay functionality fully complies with the text for this section.
- Compliant with these exceptions. The DPN Gateway over Frame Relay service does not completely comply with the text. Exceptions are indicated below.
- Not supported. The DPN Gateway over Frame Relay service does not support the functionality described in the text.

Compliance with Vendor Forum Specification

DPN Gateway over Frame Relay complies with “Frame Relay Specification with Extensions”, Issue I of Joint Specification, Revision 1.0, September 1990, Document # 001-208966. This specification was produced jointly by Nortel Networks, StrataCom Inc., Digital Equipment Corporation, and Cisco.

Frame Relay compliance with joint specification

Section	Section title	Compliance
Section 1	Introduction	Noted
Section 2	References	Noted
Section 3	Overview	Noted
Section 4	Physical Interfaces	Fully complies with
Section 5	Frame Relay Data Link Interface	Noted
Section 5.1	Specifications	Fully complies with The value of dN1 is 2100
Section 5.2	Procedures	Fully complies with
Section 5.3.1	Standard Addressing Convention	Fully complies with
Section 5.3.2	Configurable Parameters	The value of dN1 is configurable from 1 to 2100 bytes
Section 6	Local Management Interface - Common Extensions	Fully complies with
Section 7	Local Management Interface - Optional Extensions	Not supported

Compliance with Annex D of T1.617

DPN Gateway over Frame Relay complies with American National Standard for Telecommunications (ANSI) Annex D of T1.617.

Frame Relay compliance to Annex D of T1.617 ANSI (June 1991)

Section	Section title	Compliance
Section D.1	Messages Used for PVC Status	Fully complies with
Section D.1.1	Status	fully complies with. Asynchronous PVC status report reception also supported
Section D.1.2	Status Enquiry	Fully complies with
Section D.2.1	Protocol Discriminator	Fully complies with
Section D.2.2	Call Reference	Fully complies with
Section D.2.3	Message Type	Compliant with exceptions Only Status and Status Enquiry messages are supported
Section D.3.1	Report Type	Fully complies with
Section D.3.2	Link Integrity Verification	Fully complies with
Section D.3.3	PVC Status	Compliant with exceptions Only two-octet DLCIs supported
Section D.4	Procedures	Noted
Section D.4.1	Periodic Polling	Fully complies with
Section D.4.2	Link Integrity Verification	Fully complies with
Section D.4.3	Reporting New PVCs	Fully complies with
Section D.4.4	Reporting the availability of a PVC	Fully complies with
Section D.5	Error Conditions	Noted
Section D.5.1	Network Operation Errors	Not applicable to UNI-USP
Section D.5.2	User Equipment Operation Errors	Fully complies with
Section D.6	Optional Network procedures	Not applicable to UNI-USP
Section D.7	System Parameters	Compliant with exceptions Possible values of T391 and T392 range from 5 to 30 seconds in increments of 5 seconds.

Compliance with Annex A of ITU-T Q.933

This feature complies with ITU-T (formerly CCITT) standards Annex A of Q.933.

Frame Relay compliance to Annex A of ITU-T Q.933 (1992)

Section	**Section title**	**Compliance**
Section A.1	Messages Used for PVC Status	Fully complies with
Section A.1.1	Status	Fully complies with, Asynchronous PVC status report also supplied
Section A.1.2	Status Enquiry	Fully complies with
Section A.2.1	Protocol Discriminator	Fully complies with
Section A.2.2	Call Reference	Fully complies with
Section A.2.3	Message Type	Compliant with exceptions Only Status and Status Enquiry messages are supported
Section A.3.1	Report Type	Fully complies with
Section A.3.2	Link Integrity Verification	Fully complies with
Section A.3.3	PVC Status	Fully complies with Only two-octet DLCIs supported
Section A.4	Procedures	Noted
Section A.4.1	Periodic Polling	Fully complies with
Section A.4.2	Link Integrity Verification	Fully complies with
Section A.4.3	Reporting New PVCs	Fully complies with
Section A.4.4	Reporting the Availability of a PVC	Fully complies with
Section A.5	Error Conditions	Noted
Section A.5.1	Network Operation Errors	Not applicable to UNI-USP
Section A.5.2	User Equipment Operation Errors	Fully complies with
Section A.6	Optional bi-directional Network Procedures	Not applicable to UNI-USP
Section A.7	System Parameters	Possible values of T391 and T392 range from 5 to 30 seconds in increments of 5 seconds.

Network planning and engineering

This chapter describes network planning and engineering considerations for a combined network.

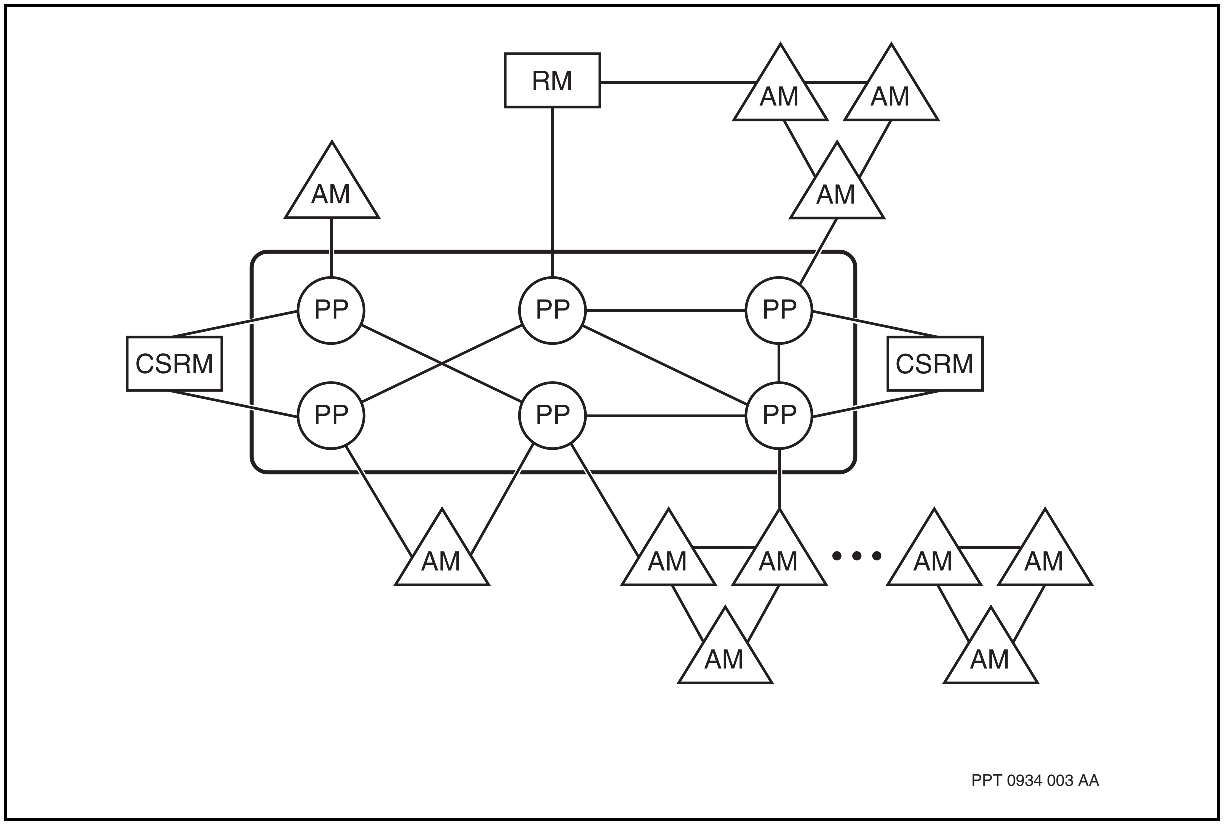
Navigation

Planning the network

An interworked network can provide various scenarios, as shown in the figure Elements of Interworking (page 60). Some of the possible interworking topologies include:

- Nortel Multiservice Switch RID subnet as part of a RID backbone
- Multiservice Switch RID subnet as part of a RID/MID backbone
- Multiservice Switch RID subnet supporting AMs
- Stand-alone Multiservice Switch RID subnet.

Elements of Interworking



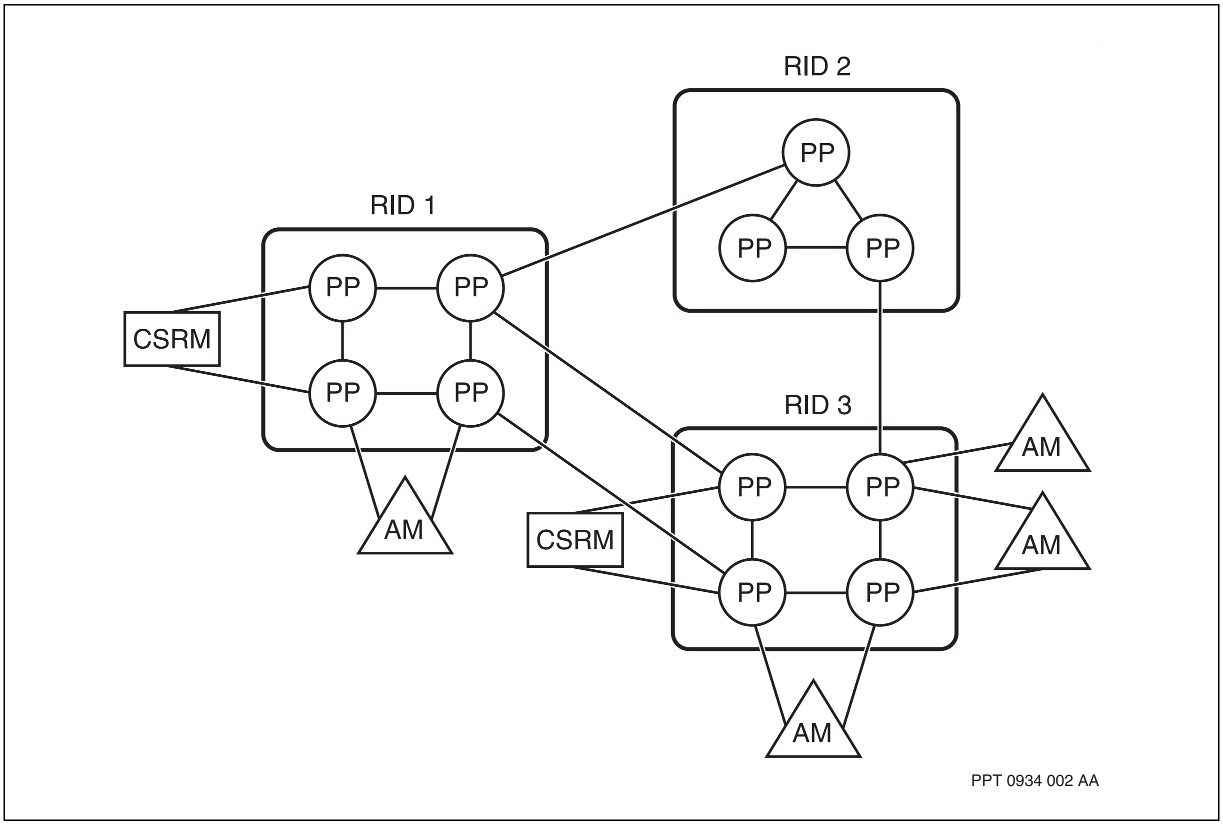
In a combined network, CSRMs are normally used for call establishment. Each CSRM is assigned a RID and should have a dual connection to the RID subnet to protect against a connection failure between the CSRM and the RID subnet. The two CSRMs should be connected to two different Multiservice Switch nodes in the subnet. For additional redundancy, it is recommended that two CSRMs be configured for each RID subnet. Each CSRM must be able to support the entire subnet on failure of the other CSRM.

The figure, Elements of Interworking (page 60) shows RMs and AM clusters connected to a RID subnet. An AM can connect to RMs and RID subnets in the following configurations:

- AM cluster to two RMs
- AM cluster to one RM and one Multiservice Switch node
- AM cluster to two Multiservice Switch nodes in one RID subnet
- AM cluster to two Multiservice Switch nodes each in separate RID subnets

All the AMs in this topology can reach each other and interwork with all the RMs and the RID subnet.

Multiservice Switch subnets



The figure, Multiservice Switch subnets (page 61) shows a topology in which three RID subnets are interconnected. The two subnets with connected AMs have redundantly- connected CSRMs. Call routing in the Multiservice Switch node-only subnet is handled by Multiservice Switch call routers.

Engineering considerations

Engineering considerations are described in the following topics:

- Engineering guidelines (page 61)
- RMs in a combined network (page 65)
- AMs in a combined network (page 69)
- CSRMs in a combined network (page 77)

Engineering guidelines

This section provides guidelines on how to interconnect Nortel Multiservice Switch RID subnets, RMs, AMs, and CSRMs.

RID subnet guidelines

When setting up a RID subnet, follow these requirements and guidelines:

- RID values range from 1 to 126. The maximum number of RIDs (RMs, CSRMs, and RID subnets) in a network is 126.
- MID values range from 1 to 1909. A RID subnet supports an engineering maximum of 500 Multiservice Switch nodes in a Multiservice Switch node-only network. In a combined Multiservice Switch and DPN-100 network, a RID subnet can support an engineering maximum of 300 Multiservice Switch nodes and 1600 AMs.
- Multiservice Switch clusters do not contribute to the node-count for a RID subnet, but they do use a MID value. Within a RID subnet then, Multiservice Switch clusters would use some of the 1909 MID values available. The total number of MIDs in a RID subnet, including all Multiservice Switch backbone nodes, all Multiservice Switch cluster nodes, and all AMs cannot exceed 1909, the maximum number of MIDs allowed in a RID subnet.
- A minimum of one CSRM must be directly connected to each RID subnet if the RID subnet is supporting DPN-100 AMs or Magellan Access Switches (MAS).

  Each CSRM should have two connections to the RID subnet, preferably to two separate Multiservice Switch nodes for increased redundancy. A CSRM can connect to a Multiservice Switch cluster node, however the network will not benefit from the CSRM loadsharing feature.
- A RID subnet can be part of only one RID region, or local access transport area (LATA).
- Each Multiservice Switch node, or Multiservice Switch cluster node (if deployed), in a RID subnet must have a unique MID provisioned under the Multiservice Switch RID.
- For redundancy purposes, each Multiservice Switch cluster node should have two connections to one or more nodes in the backbone. Multiservice Switch cluster nodes connect only to backbone nodes.
- Each Multiservice Switch node should have two connections to one or more nodes in the subnet, ideally using separate function processors for each trunk.
- Individual RID subnets must be designed with sufficient resiliency to prevent a subnet from being severed.

RM guidelines

The RM provides routing, trunking, and management functions for DPN-100. When setting up an RM, follow these requirements and guidelines:

- An RM supports up to 32 link groups to other nodes (RMs or Multiservice Switch nodes). A link group connected to a RID subnet can support up to 4 links between the RM and one Multiservice Switch node.
- Each RM must be operating the software listed in DPN-100 interworking configuration (page 7).
- Preferred-path service data cannot be used to select a particular path when an RM is connected by equal-metric link groups to two or more Multiservice Switch nodes in a RID subnet. This is because, the network management system, Preside Multiservice Data Manager, views a RID subnet as a single node. If you want to force traffic from an RM to take a particular route into the RID subnet, you can configure override on the trunks in a way to achieve the routing behavior. (See NN10600-420 *Nortel Multiservice Switch 7400/15000/20000 Operations: Trunking*).

AM guidelines

AMs provide user access termination, concentration, and local data switching. When setting up an AM, follow these requirements and guidelines:

- An AM cluster should connect to a maximum of two nodes at the network level. These nodes can be two Multiservice Switch nodes in the same RID subnet, two Multiservice Switch nodes in different RID subnets, or one Multiservice Switch node and one RM.
- RID subnets support AM clusters with up to 28 AMs in a cluster. Up to three levels of AMs can be configured with cross-links.
- Each set of links from an AM to a Multiservice Switch node is treated as a separate link group by the AM. Each link group can contain up to four links.
- Each AM in a cluster attached to a RID subnet must be operating the software listed in DPN-100 interworking configuration (page 7).
- AM intra-cluster traffic is not routed through the RID subnet. This traffic should be considered when engineering the use of links in a cluster. If traffic between two AMs in a RID subnet must be routed through the RID subnet, the AMs should be in separate clusters.
- AMs connect to RID subnets using network links, as they do in connection to RMs.
- A DPN-100 AM cluster can be connected to a Multiservice Switch cluster node. Simply follow the same requirements as those for connecting an AM cluster to a regular Multiservice Switch network.

CSRM guidelines

When setting up a CSRM (a full-function RM with call services), follow these requirements and guidelines:

- CSRM minimum configuration:
  - 16-bit common memory
  - RM office processing element (PE) for call server on PE386 or greater
  - source call router (SCR) on PE386 or greater
  - destination call router (DCR) on PE386 or greater
  - gateway source call router (GSCR) on PE386 or greater if X.25/X.75 gateways are supported anywhere in the network
  - gateway destination call router (GDCR) on PE386 or greater if the RID subnet supports X.25/X.75 gateways
  - UTP trunk PE (RID/MID gateway) on PE386 or greater
- Each CSRM must be operating the software listed in DPN-100 interworking configuration (page 7).
- All CSRMs must be directly connected to the RID subnet they support and must be configured with the same call services.
- DPN-100 CSRMs associated with a RID subnet are allowed to be connected to the backbone portion of the subnet only. Connections to a Multiservice Switch cluster node are disallowed; in order to prevent these connections, links to these modules are disabled automatically on a cluster node. This results in the raising of an alarm if a link between a cluster node to a CSRM is attempted.
- A CSRM must have sufficient memory to handle the total number of DNAs supported by the RID subnets.

  For additional information, refer to 241-1001-153 *DPN-100 System Engineering Guidelines* and 241-1001-156 *DPN-100 Access/Resource Module Engineering*.
- A CSRM must be in the same RID region (LATA) as a RID subnet for which it is providing call services.
- The CSRM must have a unique RID not shared by any RID subnet or RM in the network.
- An RM may be connected to the RID subnet before or after it is configured as a CSRM.
- A CSRM can support up to eight RID subnets (subject to engineering limitations).

- Two CSRMs should be directly connected to each RID subnet. Each CSRM must be capable of supporting the entire RID subnet in terms of throughput and SCR/DCR memory capacity.
- If more than two CSRMs are configured to support a RID subnet, the two CSRMs with the lowest RID values are brought into service. The routing system generates a minor alarm that indicates which CSRMs are not in use.
- If a single Multiservice Switch node is connected to more than one CSRM, the links to each CSRM should be of equal metrics to ensure load spreading from the Multiservice Switch node to the CSRMs. If the CSRMs are not connected with equal metrics, the call services on the CSRM connected at the higher metric are used only under failure conditions.
- When CSRM traffic is routed from within the subnet to a CSRM, the traffic is routed to the CSRM closest to the traffic's point of origin. For large and geographically dispersed RID subnets supported by two CSRMs, ensure that the CSRMs are also geographically dispersed to loadshare the traffic.
- By default, CSRM routing on Nortel Multiservice Switch 7400 nodes is set to closest. You can configure CSRM routing as shared so that each subsequent call request packet alternates between two CSRMs. For more information, see Call establishment using CSRMs (page 26).

For more detailed information on CSRM requirements, see Deployment strategies (page 80).

Network management guidelines

The network traffic engineering (NTE) application of Preside Multiservice Data Manager views a RID subnet as a single RID. For this reason, the preferred path routing, preferred secondary path routing, and tandem suppress features are not supported within a RID subnet. However, deterministic routing rules between the DPN-100 modules and Multiservice Switch nodes allow full determination of the route traffic takes through the RID subnet. For additional information, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description* and NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System*.

RMs in a combined network

This section provides topology examples of interworking with RMs.

Low-connectivity RID subnets

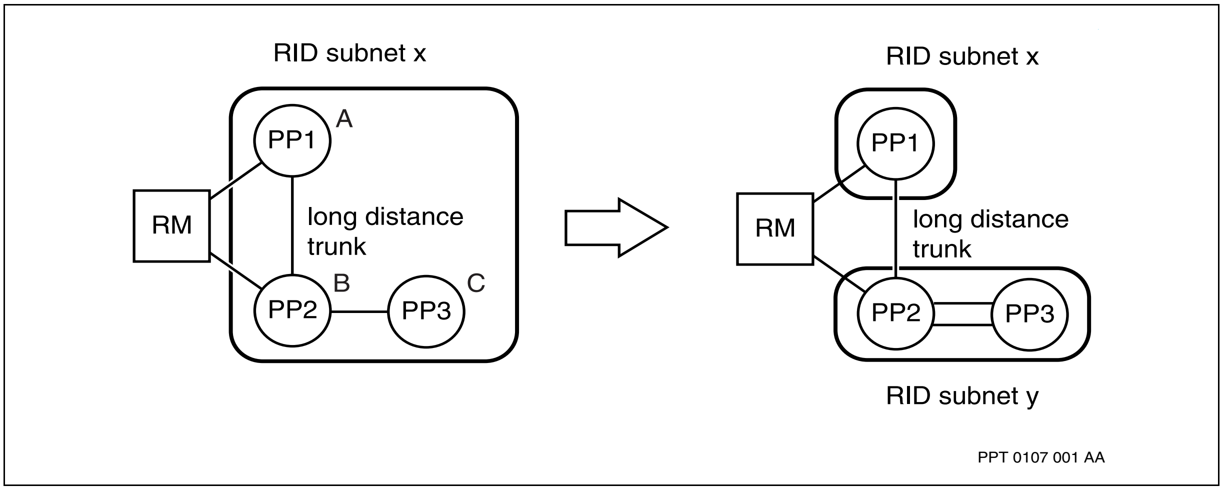
Nortel Multiservice Switch engineering rules require that adequate connectivity (a minimum of two links) exist in a Multiservice Switch RID subnet so that it does not partition into separate subnets under failure conditions. This rule protects the network from the case in which a severed RID subnet results in two separated modules each reporting the same two RIDs to the network.

(This scenario is identical to two RMs in a DPN-100 network with identical RIDs.) In this situation, RID routing cannot function correctly as it cannot distinguish between the two instances of the RID entities.

In certain cases, it is not possible to install adequate connectivity in a RID subnet to meet this engineering rule. An example of this is shown in the figure RID subnets with low connectivity (page 66) in which two parts of a RID subnet are widely separated. Additional connectivity between node PP1 and node PP3 is prohibited due to cost. In this example, if the link PP1-PP2 goes down, there is no routing between node PP1 and node PP2 even though a path exists through the RM. This is because the RM still views PP1 and PP2 as being the same RID.

In this situation, the two widely-separated portions of the network can be configured into separate RID subnets, as shown in the figure RID subnets with low connectivity (page 66). Now, if the PP1-PP2 link fails, routing from node PP1 to node PP2 can still occur since traffic is rerouted through the RM. If this is not a good solution, as in the case of high-speed frame relay traffic between the Multiservice Switch nodes, it is necessary to engineer the network accordingly. (See Tandem through RM (page 67)).

RID subnets with low connectivity

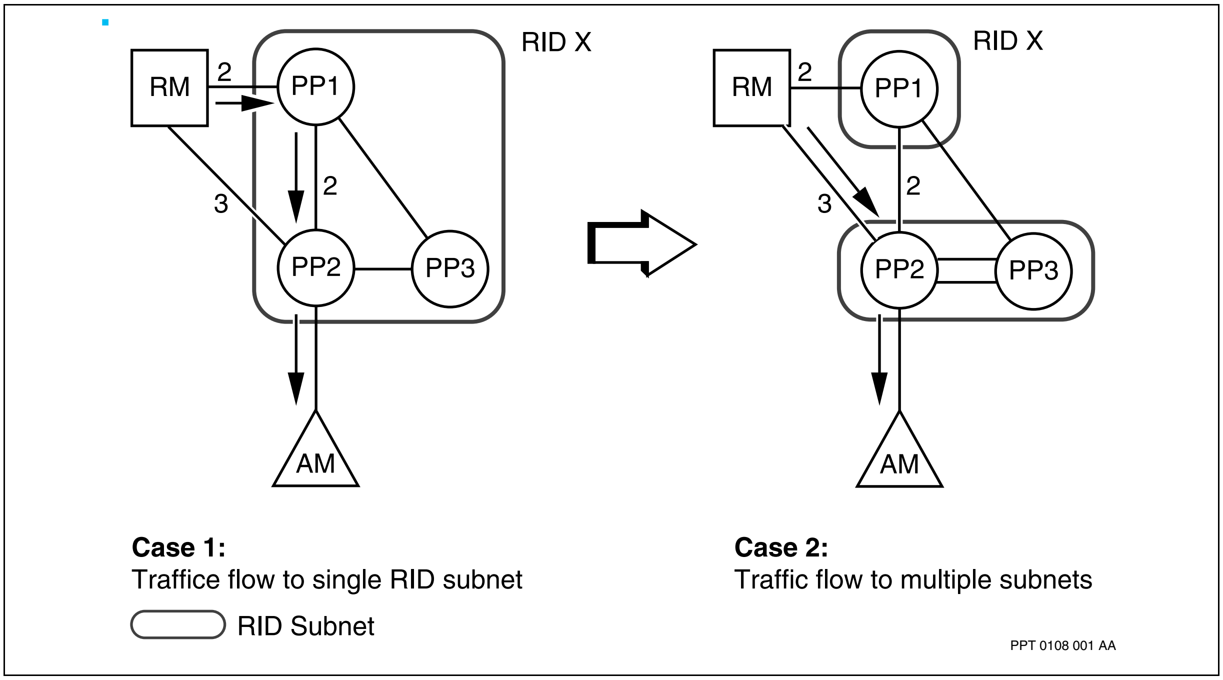


Routing from an RM into a RID subnet

The topology shown in the figure Routing from RM to RID subnet (page 67) displays a 3-node Nortel Multiservice Switch subnet interconnected to some DPN-100 modules. Traffic from an RM to a Multiservice Switch RID subnet always takes the best-cost path into the RID subnet. If paths to the subnet RID are equal, then RM determinism takes effect. (See Selecting paths (page 32)).

In the topology in the figure Routing from RM to RID subnet (page 67), sample costs are assigned to each of the links along the possible paths to node PP2 from the RM. Traffic from the RM destined to the subnet RID always takes the path RM-PP1 if this is the best cost path. The implication of this configuration is that traffic destined for node PP2 or its connected AM always takes the path RM-PP1-PP2. The impact of this routing scheme may differ amongst network configurations. In some cases, the extra hop between node PP1 and node PP2 may be insignificant. If this extra routing hop has a severe impact, you can deploy interconnecting RID subnets to solve the problem. If node PP1 and node PP2 are each in their own RID subnet, traffic from the RM to node PP2, and its connected modules, is routed at the RID level to node PP2, taking the direct path.

Routing from RM to RID subnet



Case 1:
Traffice flow to single RID subnet

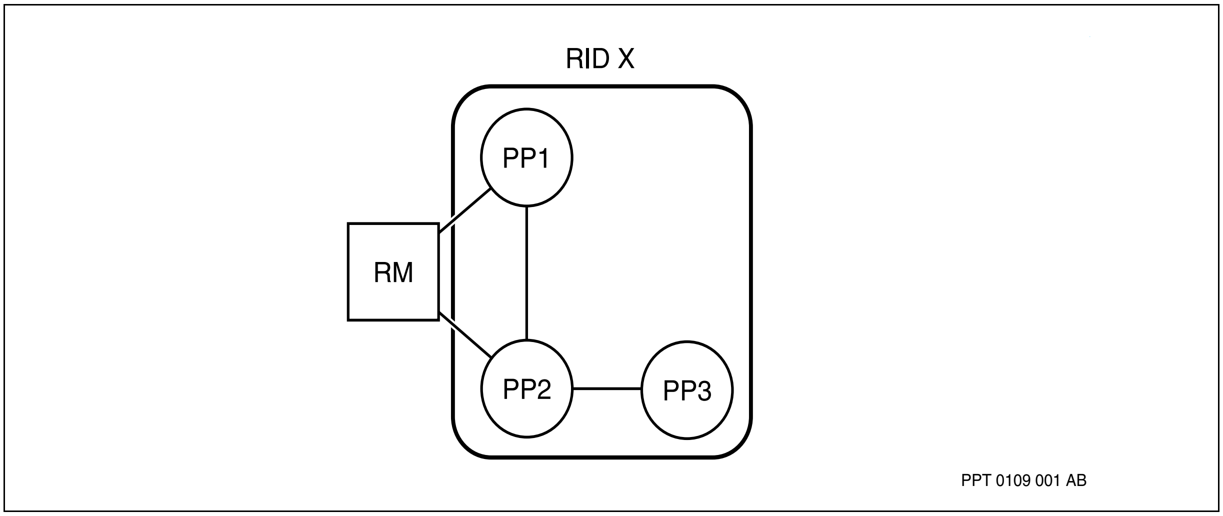
Case 2:
Traffic flow to multiple subnets

Tandem through RM

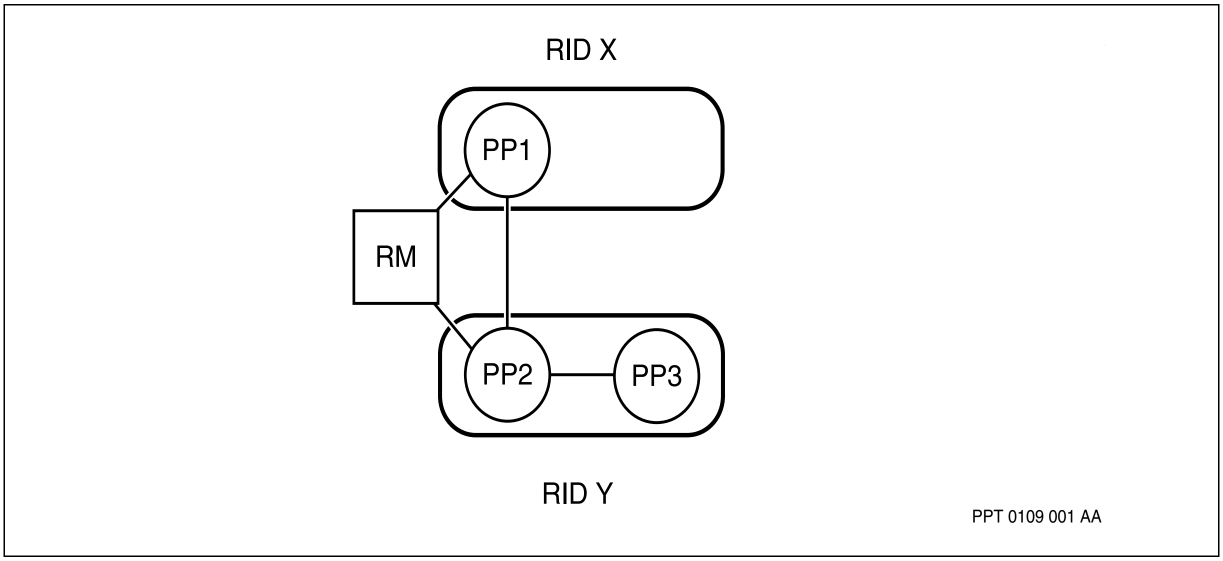
The figures, Tandem through RM (one RID subnet) (page 68) and Tandem through RM (two RID subnets) (page 68) display a scenario of interconnecting RID subnets that allows for routing backup through an RM when the trunk between two Nortel Multiservice Switch nodes is severed. The impact of this rerouting through the RM must be considered when engineering the network. If a high-speed application is run between the two nodes, the RM may not be able to support the tandeming of this traffic if the Multiservice Switch trunk fails. For this reason, the RM should not be connected between the nodes as illustrated in Tandem through RM (one RID subnet) (page 68) without considering the engineering implications.

To avoid the RM tandem scenario, the network manager can either avoid connecting an RM between two RID subnets, or the RM can be tandem-suppressed through DPN-100 configuring. If the RM is tandem-suppressed, only traffic destined for the RM and its connected AMs is sent from the Multiservice Switch nodes to the RM. No traffic is routed to any RIDs beyond the suppressed RM. See the figure, RM tandem suppress (page 69). If tandem backup is needed, you can replace the RM with another Multiservice Switch node in its own RID subnet.

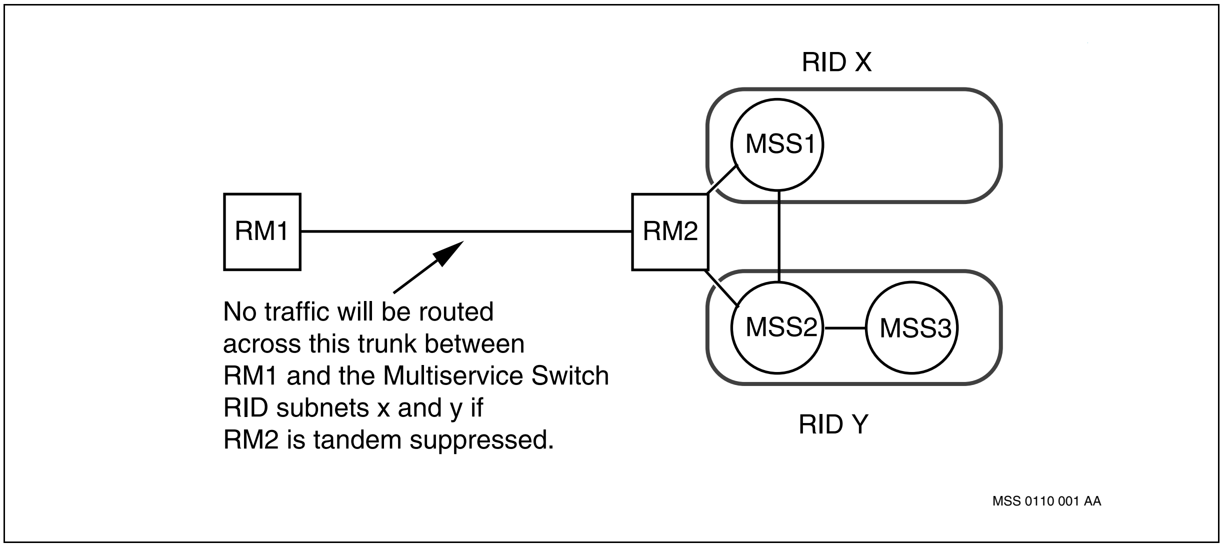
Tandem through RM (one RID subnet)



Tandem through RM (two RID subnets)



RM tandem suppress


RID X
MSS1
RM1
RM2
No traffic will be routed across this trunk between RM1 and the Multiservice Switch RID subnets x and y if RM2 is tandem suppressed.
MSS2
MSS3
RID Y
MSS 0110 001 AA

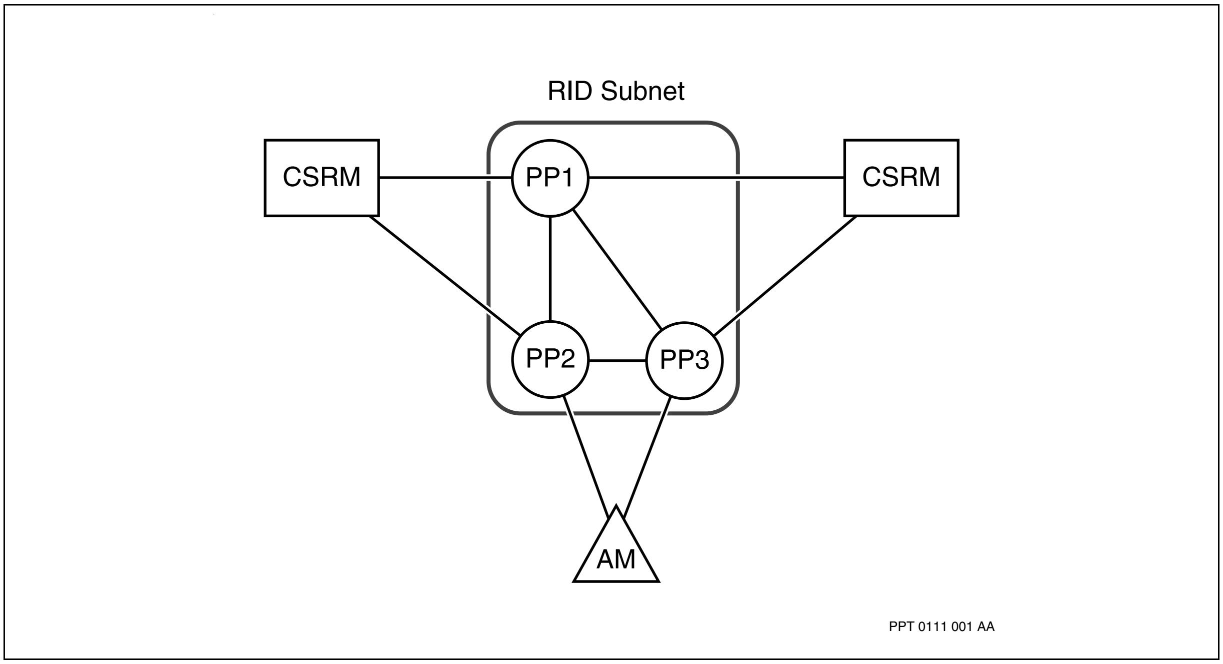
AMs in a combined network

This section provides some examples for interworking with AMs.

Connecting AM Clusters to RID Subnets

The figure, AM connected to RID subnet (page 69) shows a topology with an AM connected to a RID subnet. An AM views a Nortel Multiservice Switch RID subnet as a single-cluster RID.

AM connected to RID subnet

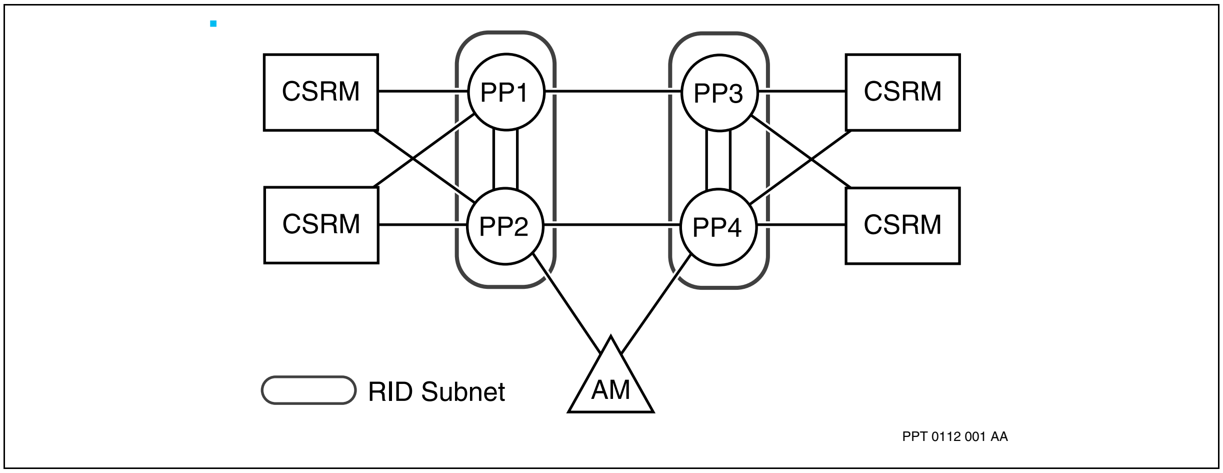


If an AM is connected by equal-cost paths to the subnet RID, the AM loadshares its inbound traffic across both paths, unless the traffic is specifically destined for either node PP2 or node PP3. In this example, the AM is appropriately engineered with two paths up to the network level (in this case, to two Multiservice Switch nodes in the same RID subnet).

Connecting an AM cluster to a Multiservice Switch RID subnet reduces the number of AMs allowed in the AM cluster to 28 from 30.

AMs can connect to two separate RID subnets as long as each RID subnet is not engineered to be a separate routing zone. The figure AM connected to multiple RID subnets (page 70) shows an AM topology connected to two interconnecting RID subnets. In this case, the same engineering recommendations are valid as in the case of AM connectivity to a single RID subnet. An AM cluster should connect to a maximum of two nodes at the network level. So if an AM cluster is connected to two RID subnets, the cluster should connect to only one Multiservice Switch node in each subnet. In this topology, the AM loadshares traffic to both RID subnets unless one of the subnets is the traffic's destination. As in the case of the single RID subnet, the number of AMs allowed in the AM cluster is 28. Although AMs can connect to two separate RID subnets, a recommended engineering guideline is to maintain AM connectivity within the same RID subnet. Connecting AMs to two Multiservice Switch nodes in the same RID subnet simplifies the network design as well as the backup scenarios if connectivity from the AM to one of the Multiservice Switch nodes fails.

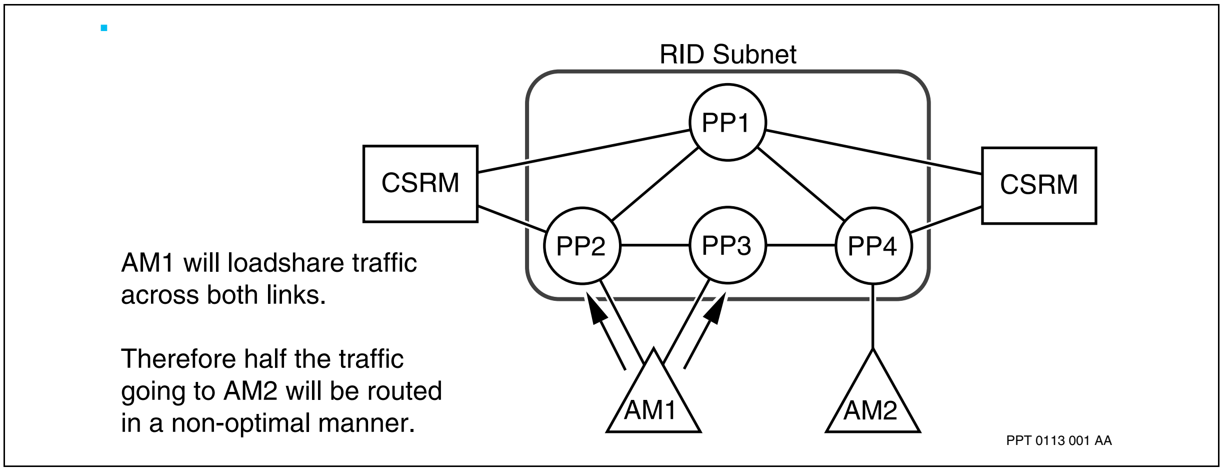
AM connected to multiple RID subnets



Routing from AMs into a RID subnet

The figure, AM-to-RID subnet routing (page 71) shows another example of AMs connected to a RID subnet. AMs loadshare inbound traffic over equal-cost paths. So, in this topology, traffic from AM1 to the network level, including the subnet RID, is loadshared across the links to node PP2 and node PP3, unless the traffic is destined for either node. In the latter case, the direct link is used to reach the node.

AM-to-RID subnet routing


RID Subnet
PP1
CSRM
CSRM
PP2
PP3
PP4
AM1 will loadshare traffic across both links.
Therefore half the traffic going to AM2 will be routed in a non-optimal manner.
AM1
AM2
PPT 0113 001 AA

AM topologies

The deployment of AMs across interconnecting RID subnets must take into account the same considerations as in the case of AMs connected across two RMs. If an AM is connected to two different RID subnets, these subnets should be directly connected by a trunk to handle the impact if one of the AM links up to the network fails.

Large AM topologies

One of the advantages of deploying Nortel Multiservice Switch nodes in a network is the capability of supporting more AMs with fewer backbone modules. A Multiservice Switch backbone needs fewer modules than an RM backbone for the same number of AMs. Multiservice Switch nodes also directly support more AMs than an RM.

Although RID subnets can physically connect more than 1909 modules (AMs and Multiservice Switch nodes), the maximum of 1909 modules per RID subnet still applies. This maximum results from the available addressing space for MIDs. But this value is not limiting, since the DPN addressing hierarchy determines address uniqueness based on RID and MID. This allows for the reuse of MIDs, as long as the RID is different. If you need more than 1909 modules, you can configure more than one Multiservice Switch RID subnet in the network.

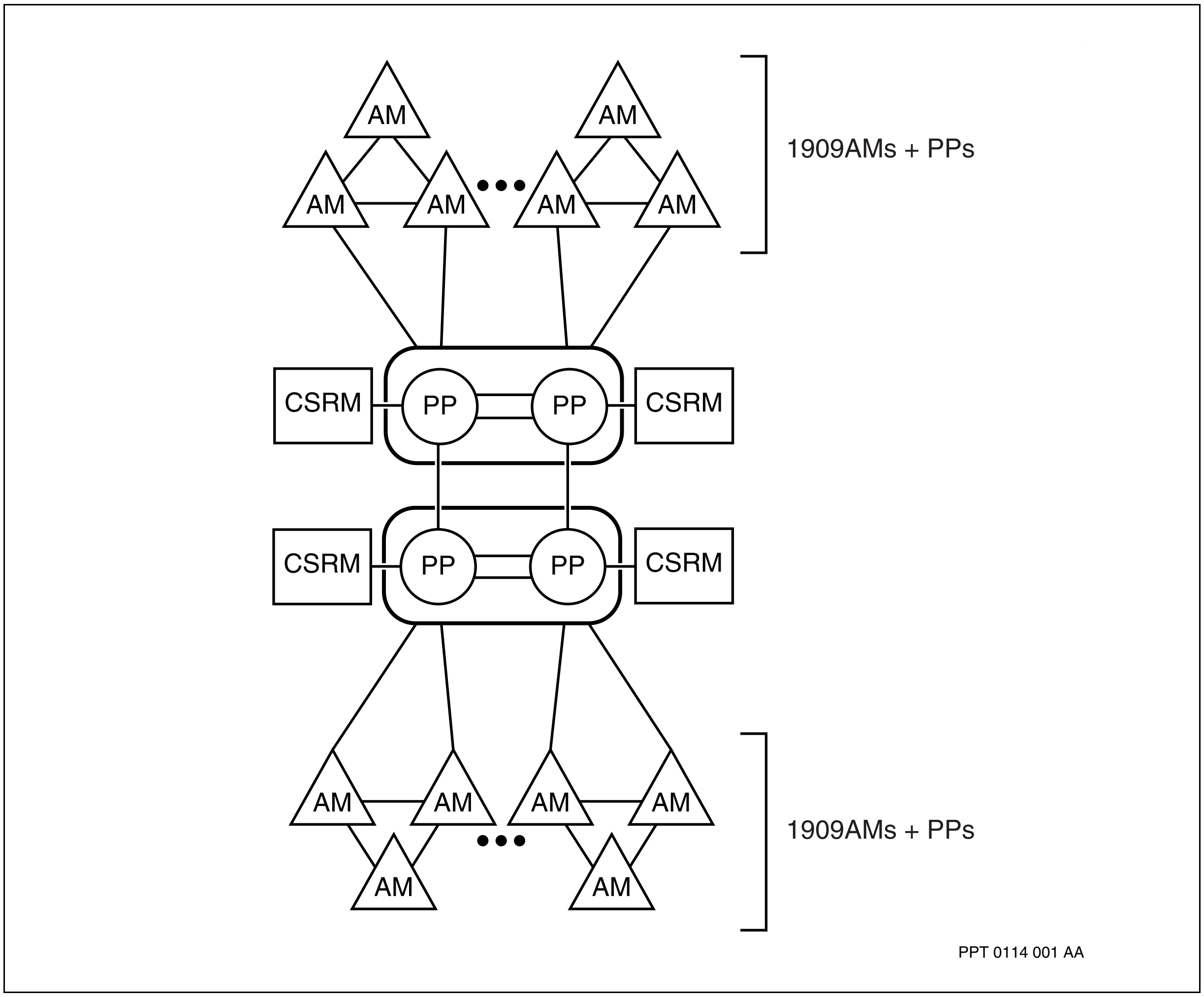
To reuse MIDs in a network, you must control the reassignment of the MIDs through the use of routing zones. The figure, Large AM topologies (page 73) illustrates how large numbers of AMs can be supported using this feature.

A Multiservice Switch RID subnet can support up to 1909 modules, constituting a routing zone. However, it is not necessary to consider each Multiservice Switch RID subnet a routing zone. This practice limits the AM topologies when small Multiservice Switch RID subnets (one to two nodes) are used, since AMs should not be connected across routing zones. For this reason, a routing zone is not a provisioned entity. It is administered by the network manager as MID reuse is needed in the network. When you reuse MIDs, ensure that a MID can not be connected to two routing zones. If a Multiservice Switch RID subnet must be its own separate routing zone, ensure that no AMs are connected to another RID subnet or to an RM outside the AM’s zone.

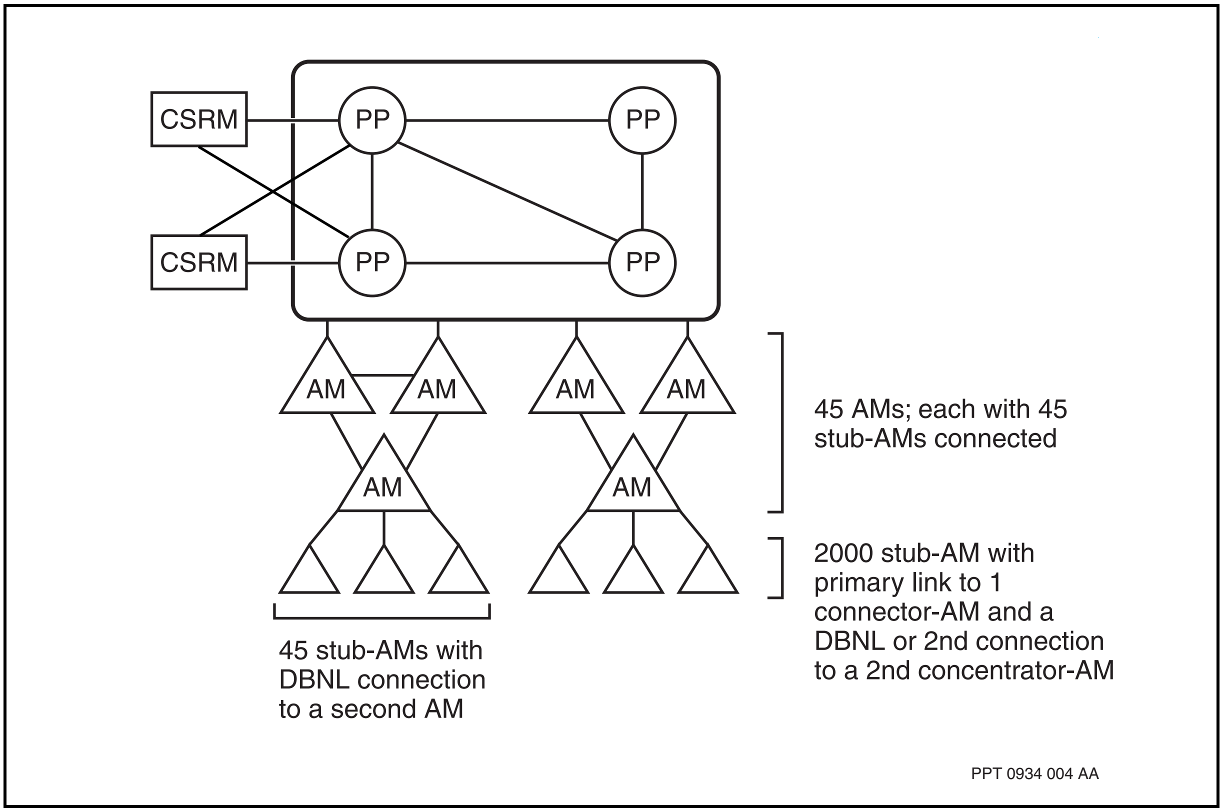
Alternatively, large numbers of AMs can be supported using stub-AMs as described in 241-1001-111 *DPN-100 Routing & Call Establishment General Description*. This method allows a RID subnet to support in excess of forty thousand modules, since stub-AMs do not impact MID routing limits (such as the number of MIDs in a routing zone or AMs in an AM cluster). The stub-AM method has the additional advantage of reducing the amount of MID routing traffic in the network. The figure Using stub-AMs (page 74) illustrates how stub-AMs can be used to support large numbers of modules using a single RID.

As with RMs, other factors must be considered when deploying such large numbers of AMs. The routing limits alone are insufficient to guarantee that the network is properly engineered. You should consider additional factors, such as traffic volumes on the AMs, gateway speeds, call setup demands, redundancy requirements, and end-to-end delays.

Large AM topologies



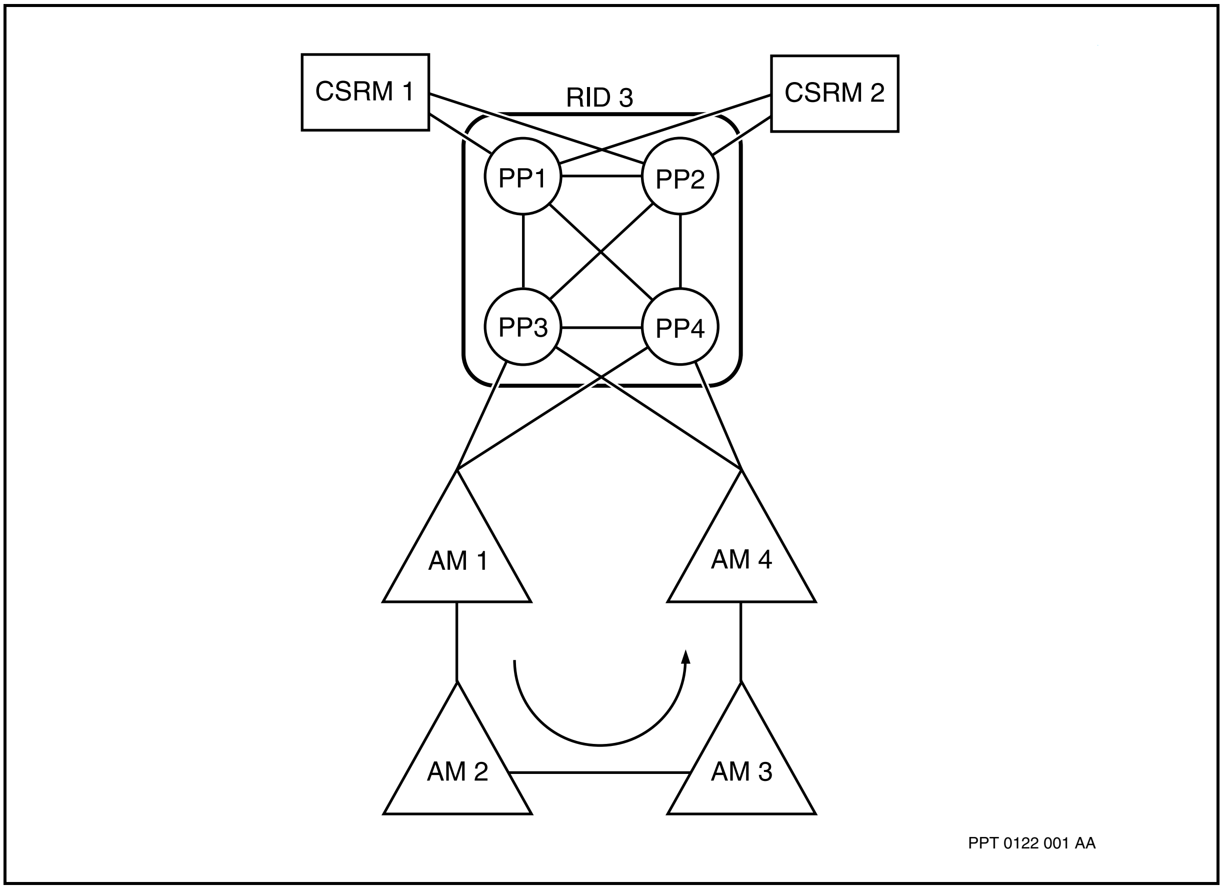
Using stub-AMs


CSRM
CSRM
PP
PP
PP
PP
AM
AM
AM
AM
AM
AM
45 AMs; each with 45 stub-AMs connected
2000 stub-AM with primary link to 1 connector-AM and a DBNL or 2nd connection to a 2nd concentrator-AM
45 stub-AMs with DBNL connection to a second AM
PPT 0934 004 AA

AM cluster routing

The information about AMs reachable through Nortel Multiservice Switch nodes is not propagated from Multiservice Switch nodes to AMs. This means that intra-cluster packets are not routed up to the Multiservice Switch node. Instead, this traffic is routed between the AMs themselves. See figure Intra-AM cluster routing (page 75). Packets originating at AM1 and destined for AM4 are routed through modules AM2 and AM3. Only packets destined for modules outside the cluster are routed to the Multiservice Switch node.

Intra-AM cluster routing



You must consider intra-cluster routing when engineering the use of links in a cluster. If you do not want intra-cluster routing through lower levels of the cluster, establish links at higher levels or partition the cluster so that traffic is forced through the RID subnet.

Other options prevent AM cluster traffic from routing down through lower-level AMs in the cluster. For example, in the AM cluster in the figure Intra-AM cluster routing (page 75), you can define the AM1-AM2 link and the AM3-AM4 link as standby network links (SBNL). An SBNL is assigned a metric value of 3, which is higher than a normal network link metric of 1.

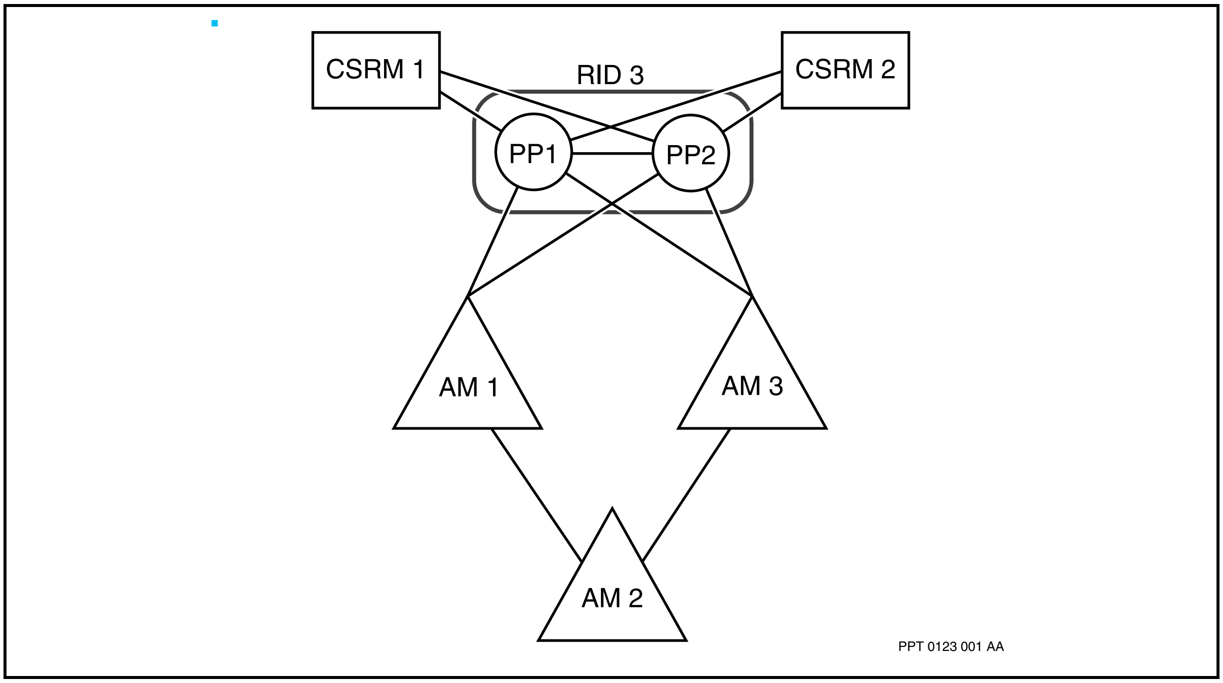
By defining both ends of the AM1-AM2 and AM3-AM4 links as SBNLs, the overall metric for the path through the cluster from AM1 to AM4 equals the MID routing cutoff value of 7. When the metric value for a MID is equal to or greater than this cutoff, MID routing considers the MID to be unreachable. In this example, AM1 does not view AM4 as reachable within its cluster, and routes up to the network level through the Multiservice Switch node to reach AM4. The same routing also occurs for traffic from AM4 to AM1.

In this topology, all other routing remains the same as with normal network links defined. AM2 routes up to the network level through AM1 under normal conditions, and through AM3 under failure conditions on its primary path. AM2 is still able to route to AM4 through the cluster. For more information about SBNL and its implications for MID routing, see 241-1001-111 *DPN-100 Routing & Call Establishment General Description* and 241-1001-015 *DPN-100 Network Link and Trunk User Guide*.

The figure, Intra-AM cluster routing using a DBNL (page 76) shows another option for AM cluster topology. If the AM1-AM2 and AM2-AM3 links are defined as SBNLs, the resulting metric on AM1 for the MID of AM3 is 6, which is less than the cutoff value. In this scenario, one option is to define AM2 as tandem-suppressed. This option prevents AM2 from sending traffic in tandem to and from other modules. AM2 is still reachable from both AM1 and AM3. See 241-1001-111 *DPN-100 Routing & Call Establishment General Description* for more information.

Another option is to define one of AM2's network links as a dial backup network link (DBNL). For example, AM2 could be singly connected to AM1, and connect to AM3 only under failure conditions. (The impact of AM2 becoming part of AM3's cluster must be taken into consideration for AM3's cluster limit of 28 modules.) See 241-1001-015 *DPN-100 Network Link and Trunk User Guide* for more information about DBNL.

Intra-AM cluster routing using a DBNL



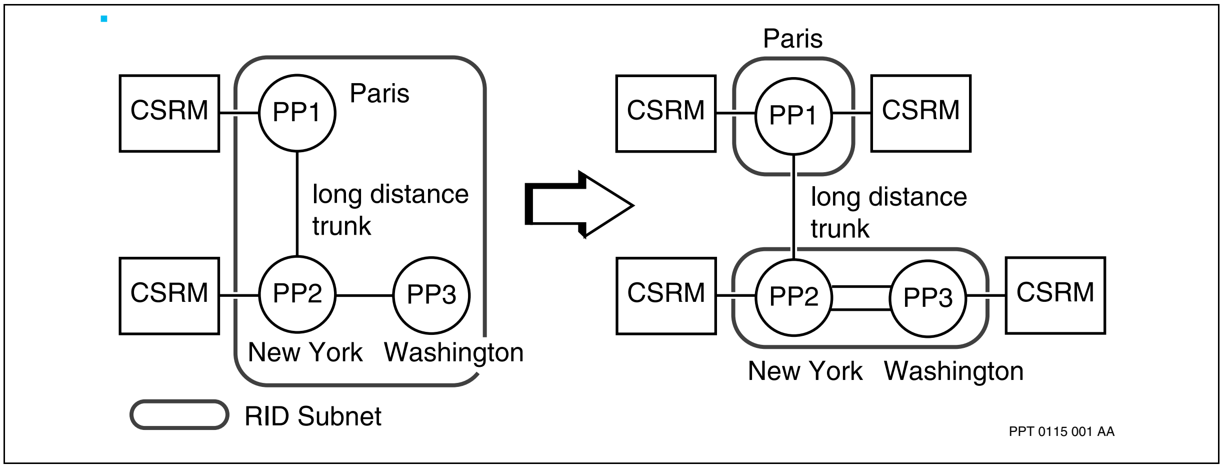
CSRMs in a combined network

A Nortel Multiservice Switch RID subnet supports two CSRMs for redundancy purposes. This two-CSRM limit reduces the amount of DNA-associated traffic generated by the RID subnet's Multiservice Switch nodes, as well as all AMs connected to the RID subnet.

The ability to interconnect Multiservice Switch RID subnets eliminates the impact that the two-CSRM limit has on geographically disperse networks. It is preferable to segregate geographically-separated Multiservice Switch nodes into different RID subnets for other routing reasons as well. For example, it is not cost-effective to propagate internal RID subnet routing information across a transatlantic trunk each time a routing event occurs in the subnet.

The figure, CSRM proximity (page 77) illustrates how partitioning an existing RID subnet into two RID subnets can address CSRM proximity and density issues.

CSRM proximity



Another method of limiting the impact of two CSRMs for a RID subnet is to designate and configure more than two CSRMs. Although only two CSRMs are active at any one time, a maximum of ten RMs can be defined as CSRMs for a RID subnet. The two active CSRMs are selected based on their RID values. The CSRMs with the two lowest RID values are selected to be the active CSRMs. If one of the active CSRMs fails, the CSRM with the next-lowest RID becomes active, and the RID subnet continues to operate with two CSRMs. There is a slight delay (less than 60 seconds) for the backup CSRM to become fully functional. When the backup CSRM becomes active and functional, DNA association is initiated by all Multiservice Switch nodes and AMs in the RID subnet. X.25/X.75 gateways on all AMs immediately report their availability to the new CSRM.

When the original CSRM recovers from its failure, it becomes active, and the backup CSRM returns to a backup state. In this case, the GDCR on the backup CSRM immediately removes the information about the RID subnet X.25/X.75 gateways from its tables to ensure that it no longer advertises the availability of these gateways. The DCR on the backup CSRM never deletes its DNA entries. The RID subnet DNAs remain in the backup CSRM DCR tables until a DCR associate command is entered, or all DCRs on the module restart, or the entire module restarts.

Source Call Routing

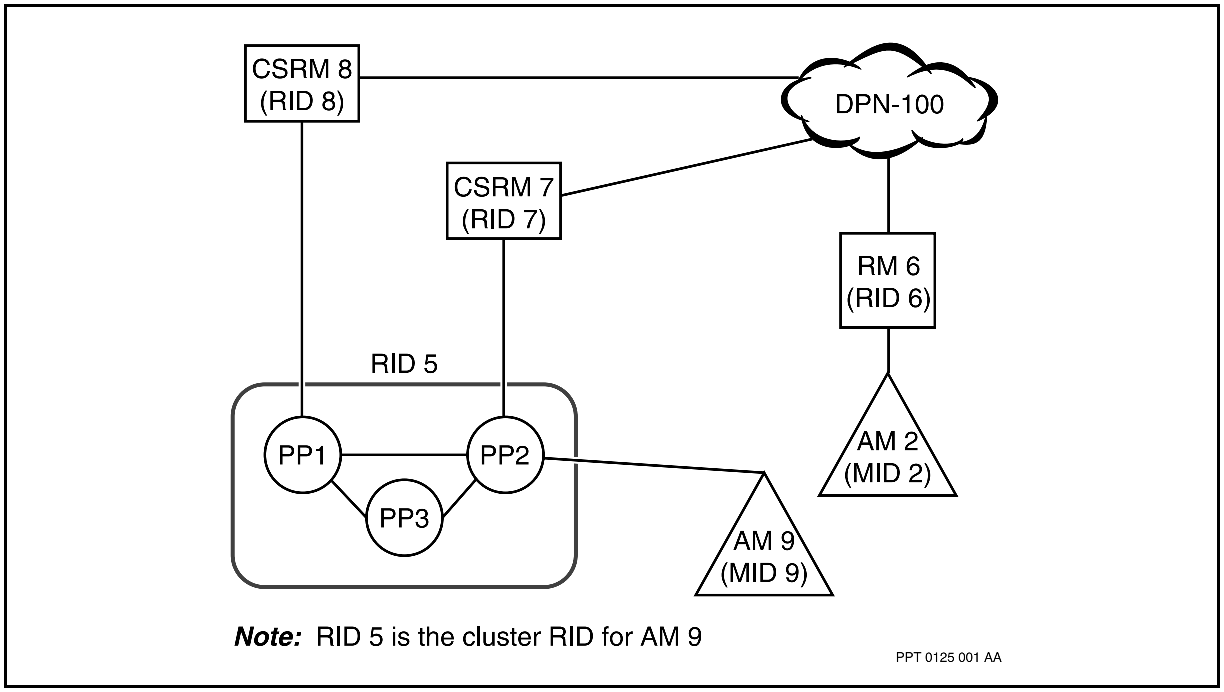
In a DPN-100 network, the source call router (SCR) maps the prefix of the destination data network address (DNA) to its destination module's RID for further address resolution by the destination call routing (DCR) system on that node. This RID is called the prime RID for that DNA. The SCR tables that map prefix DNAs to RIDs, network identifiers (NIDs), or dial-out server region identifiers (DSRIDs) are configured in service data. When Nortel Multiservice Switch call services are provided on a CSRM, the prefix DNAs of Multiservice Switch nodes and supported AMs of the RID subnet have the Multiservice Switch subnet RID as their prime RID.

The following examples detail AM interconnections to a RID subnet and to both a RID subnet and an RM.

AM connected to a RID subnet

In the sample configuration shown in the figure, AM connected to RID subnet (page 79), AM 9 is connected to a Multiservice Switch node in RID 5. Connected in this manner, RID 5 is therefore the cluster RID for AM 9. As in DPN-100, an AM can connect to a maximum of two cluster RIDs. These cluster RIDs can be either an RM and a RID subnet, two RMs, or two RID subnets. The prime RID value for AM 9 in this example configuration is also RID 5.

AM connected to RID subnet

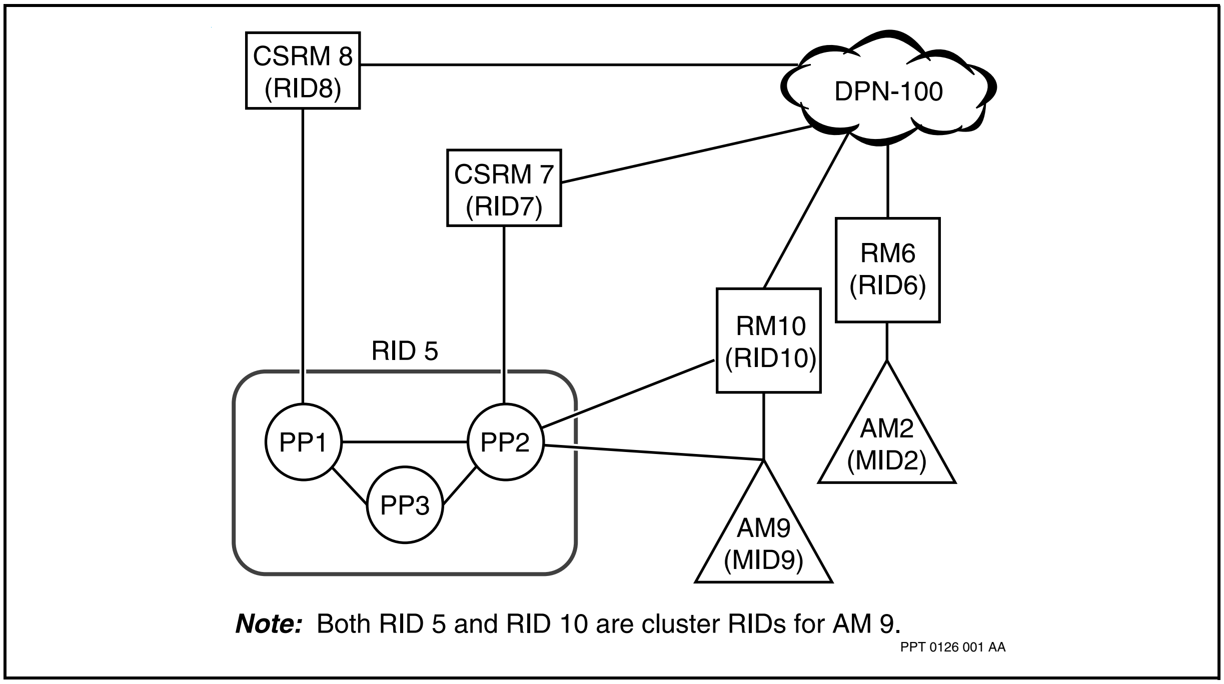


Note: RID 5 is the cluster RID for AM 9

AM connected to a RID subnet and an RM

In a second sample configuration, shown in AM connected to RID subnet and RM (page 80), AM 9 has two cluster RIDs, RID subnet RID 5 and RM RID 10. Therefore, the SCR prime RID value for AM 9 DNAs could be either RID 5 or RID 10.

AM connected to RID subnet and RM



Note: Both RID 5 and RID 10 are cluster RIDs for AM 9.

PPT 0126 001 AA

Destination call routing

In a DPN-100 network, the destination call router (DCR) maps a complete data network address (DNA) to the value of the module identifier (MID) that supports the DNA. To support Multiservice Switch call services on an RM, the destination call routing system stores RID as well as MID information for the DNA addresses in its mapping tables. This is because DNAs associated to the DCR system within the RID subnet have a different RID than the CSRM RID of the DCR.

Deployment strategies

This section details the deployment strategies for combined networks. The topics include:

- Introducing a new Multiservice Switch RID subnet (page 80)
- Splitting a RID subnet (page 87)
- Merging RID subnets (page 93)
- Deploying CSRMs (page 95)

Introducing a new Multiservice Switch RID subnet

You can install Nortel Multiservice Switch nodes and subnets in a DPN-100 network to provide a high-capacity network backbone. After Multiservice Switch nodes are deployed in the network, AMs can migrate from RM connection to direct connection with the Multiservice Switch nodes of a RID subnet. You can then remove the RMs in the network for deployment elsewhere, or configure them as AMs or CSRMs.

You can add a new RID subnet to a network using one of two approaches:

- You can define the new RID subnet with a single Multiservice Switch node, connect the RID subnet to the network, and then include additional Multiservice Switch nodes in the RID subnet.
- You can configure the RID subnet with multiple Multiservice Switch nodes, and then connect it to the network.

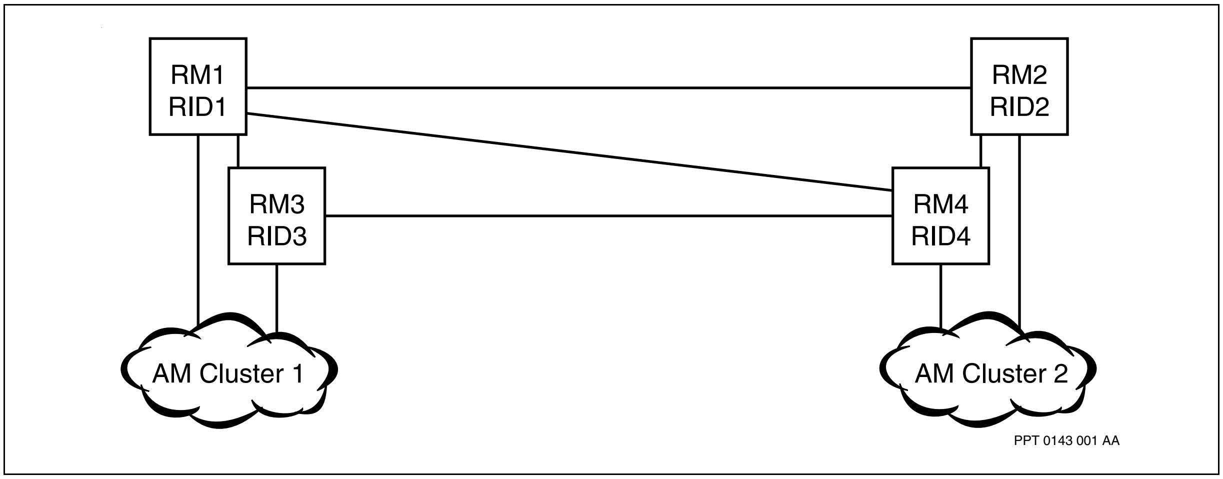
To prepare for the RID subnet deployment, you must designate and configure the CSRMs to serve the new RID subnet. CSRMs can be shared amongst RID subnets. A CSRM can support up to eight RID subnets, subject to engineering guidelines. See Deploying CSRMs (page 95).

Adding a Multiservice Switch RID subnet to an interworking network

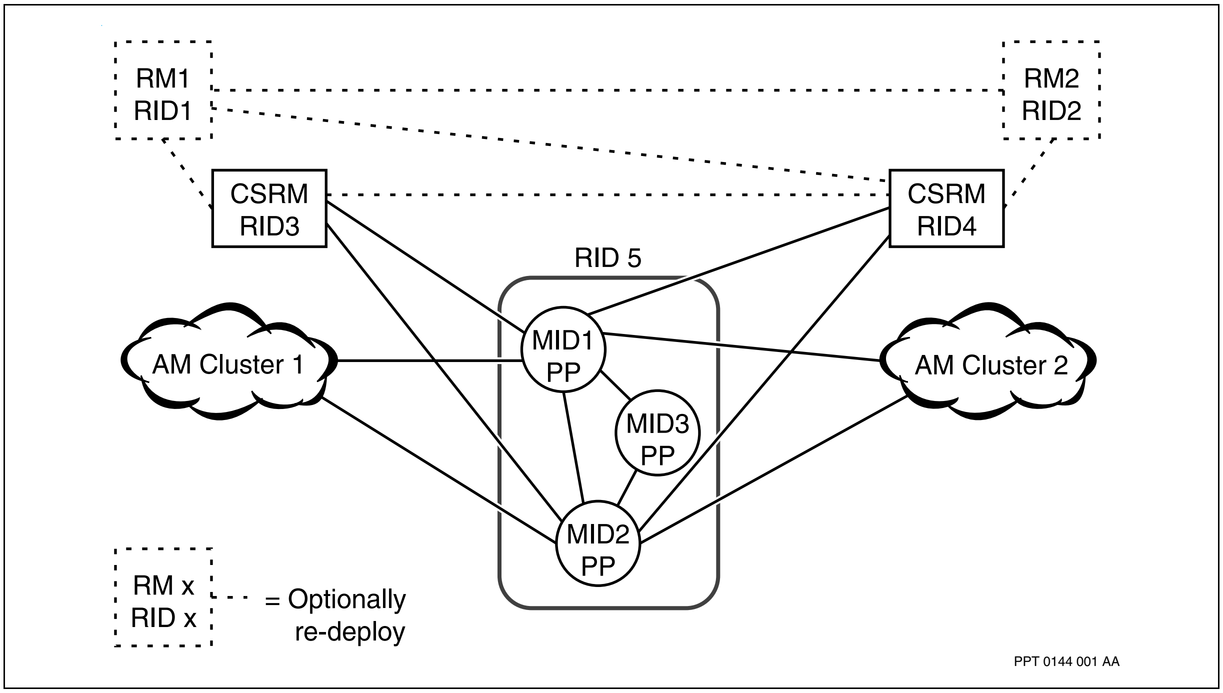
This section provides an example of how to add a Nortel Multiservice Switch RID subnet to the DPN-100 network shown in DPN-100 network (page 81). After deployment of the Multiservice Switch RID subnet backbone, the new interworking network is configured as shown in Multiservice Switch/DPN-100 interworking network (page 82).

Although this example illustrates the deployment of a Multiservice Switch RID subnet in a DPN-100 subnet, the same considerations apply when adding a new RID subnet to an existing interworking network.

DPN-100 network



Multiservice Switch/DPN-100 interworking network



Before deploying the new RID subnet, you must take the same steps as when a new RM is introduced into the network. You must update the network-wide SCR tables to contain the prefix-DNA mapping for the new RID. This step is necessary before the SCR can route to the new RID. This process is particularly important for establishing Preside Multiservice Data Manager VCs to the new Multiservice Switch modules.

Example of adding a Multiservice Switch RID subnet to an interworking network

1 Select the CSRMs for the new Multiservice Switch RID subnet. See the figure Define and connect CSRMs to the Multiservice Switch RID subnet (page 84).

In this example, configure RM3 and RM4 as CSRMs connected to Multiservice Switch MID1 and Multiservice Switch MID2.

If the network contains X.25 or X.75 gateways, ensure that the CSRMs' RIDs are provisioned in the gateway call routing system's common envelope RID map on all network RMs and CSRMs in the gateway region. (For most networks this is all RMs and CSRMs in the network.) Do not include the RID subnet RID in this RID map. See 241-1001-313 *DPN-100 X.75 Gateway Call Routing System User Guide* for more details.

2 Connect the CSRMs to the RID subnet, as shown in the figure Define and connect CSRMs to the Multiservice Switch RID subnet (page 84), and ensure that the network connection is functioning. See Configuring the Multiservice Switch node (page 11) for specific steps.

The CSRMs have two connections to the RID subnet for redundancy. The connections are DPN-100 gateways using a UTP trunk.

— Ensure that the gateway between each Multiservice Switch MID and CSRM has staged successfully.

— Verify that the CSRMs can route to the Multiservice Switch MIDs by using the ppath operator command from each CSRM. (See 241-1001-303 *DPN-100 Operator Commands and Responses* for information on operator commands.)

— Verify that each Multiservice Switch MID can route to the CSRMs by using the ping command. (See NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.)

— Verify that each CSRM is operating correctly. Use the csr display interfaces command to display the RID and MID of Multiservice Switch MID1 and MID2.

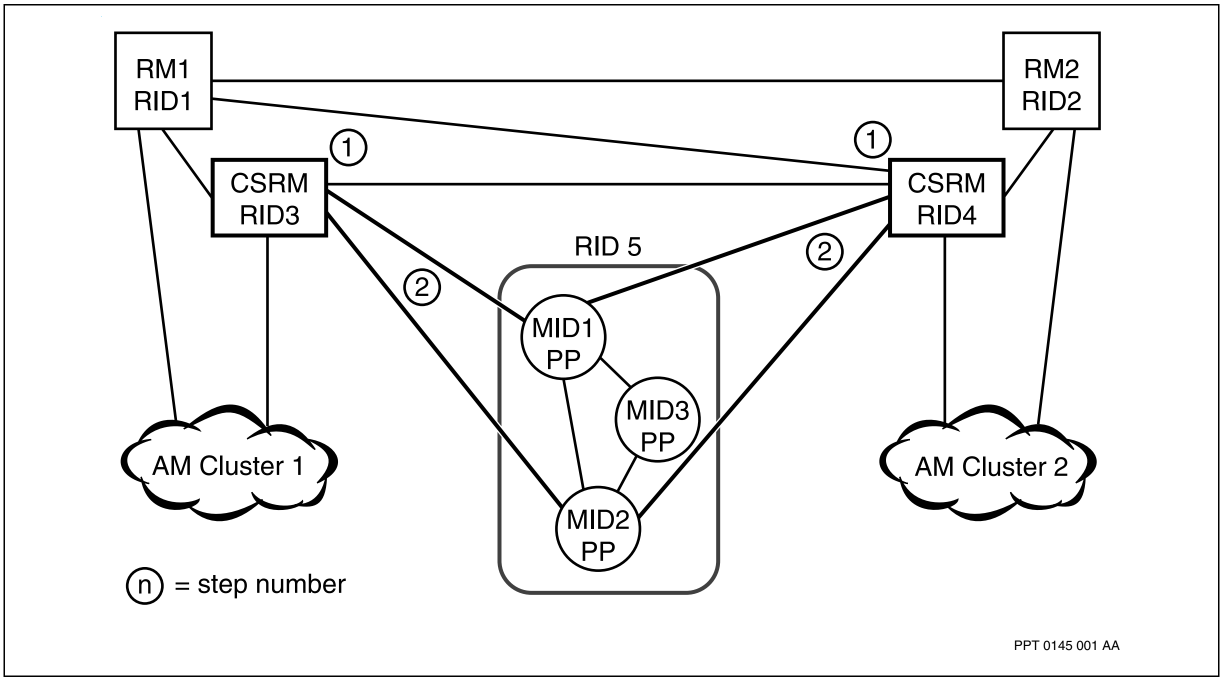
— Verify that Multiservice Switch MID1 and MID2 view the CSRM as their call server RID by using the display rtg dpn command.

— Ensure that the Multiservice Switch DNAs are associated in the DCR on each CSRM.

— Ensure that Preside Multiservice Data Manager connectivity to the Multiservice Switch modules is established (ensure that the DNAs are provisioned properly on the Multiservice Switch node).

— Ensure that incoming and outgoing calls can be set up to and from the Multiservice Switch MIDs in the new RID subnet.

Define and connect CSRMs to the Multiservice Switch RID subnet



Migrating an AM cluster

This section provides an example on how to migrate an AM cluster from an RM to a Multiservice Switch RID subnet.

Example of migrating an AM cluster

1 Prepare to connect AM clusters 1 and 2 to the RID subnet.

Because AM clusters 1 and 2 are migrating from their home RIDs (RM3 and 4, which are also the CSRMs for the RID subnet), it is not necessary to RID-split these RMs to the Multiservice Switch RID. This is because the AM DNAs are associated on these CSRMs through the RID subnet. However, when migrating to a RID subnet from an RM which is not a CSRM for the RID subnet, the RM should be RID-split to the RID subnet if it is the home RID of the AM cluster. In addition, once the AM cluster is disconnected from the RM, it is necessary to enter a DCR associate command on the RM. This command removes the DNAs of the disconnected AMs from the RM DCR tables. Any calls to the AMs that are still prefix-mapped to the RM are RID-split to the RID subnet and processed by the DCR on the CSRMs. Once the SCR tables in the network are updated to reflect the new prefix mappings for the AM cluster, the RID splitting can be removed. For additional information, see Splitting a RID subnet (page 87).

— Reduce the number of AMs in the AM cluster to 28 or less.

— The AM DNAs do not need to be changed when migrating an AM cluster to a RID subnet, but verify that they are correctly prefix-mapped to the RID subnet.

2 Connect the AM cluster to the Multiservice Switch node (and disconnect from the RM). See the figure Migrate an AM cluster - connect to the first Multiservice Switch node (page 86).

An AM cluster can connect to a maximum of two nodes at the network level.

— Verify connectivity to the AM cluster from the RID subnet by using the list rtg dpn mid/* command. Then use the ping command to query the AM cluster. (See NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.)

— Verify connectivity to the RID subnet from the AM cluster by using the midr d clust command, and verify that the AMs in the cluster list the CSRMs as their CS RIDs.

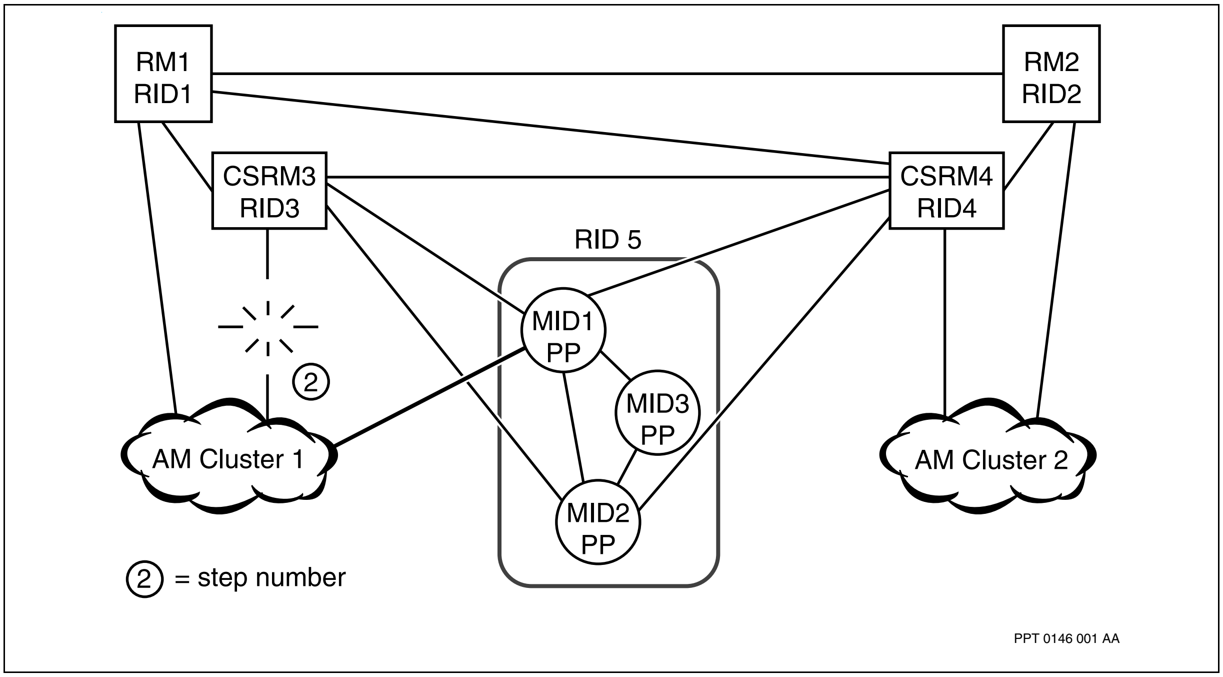
— Verify support of the AM cluster from the CSRMs. Check that the DNAs in the AM cluster are correctly associated using the subnet’s RID in the DCR system. Check that all X.25 and X.75 gateways in the AM cluster are supported using the subnet’s RID in the GDCR system.

3 Optionally, connect the AM to another Multiservice Switch MID in the RID subnet and disconnect from the RM. See the figure Migrate an AM cluster - connect to another Multiservice Switch node (page 86).

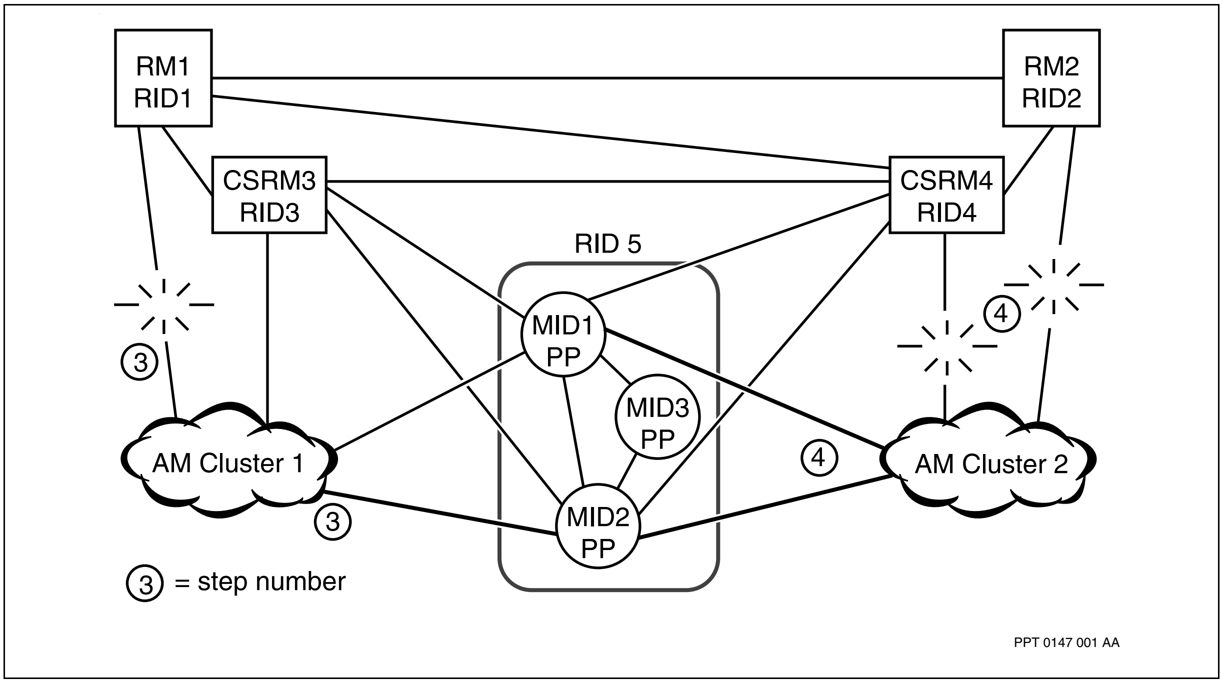
4 Connect another AM cluster to the RID subnet by repeating this procedure.

5 Update the network-wide SCR service data to map the prefix DNAs of the AM clusters to the RID subnet.

Migrate an AM cluster - connect to the first Multiservice Switch node



Migrate an AM cluster - connect to another Multiservice Switch node

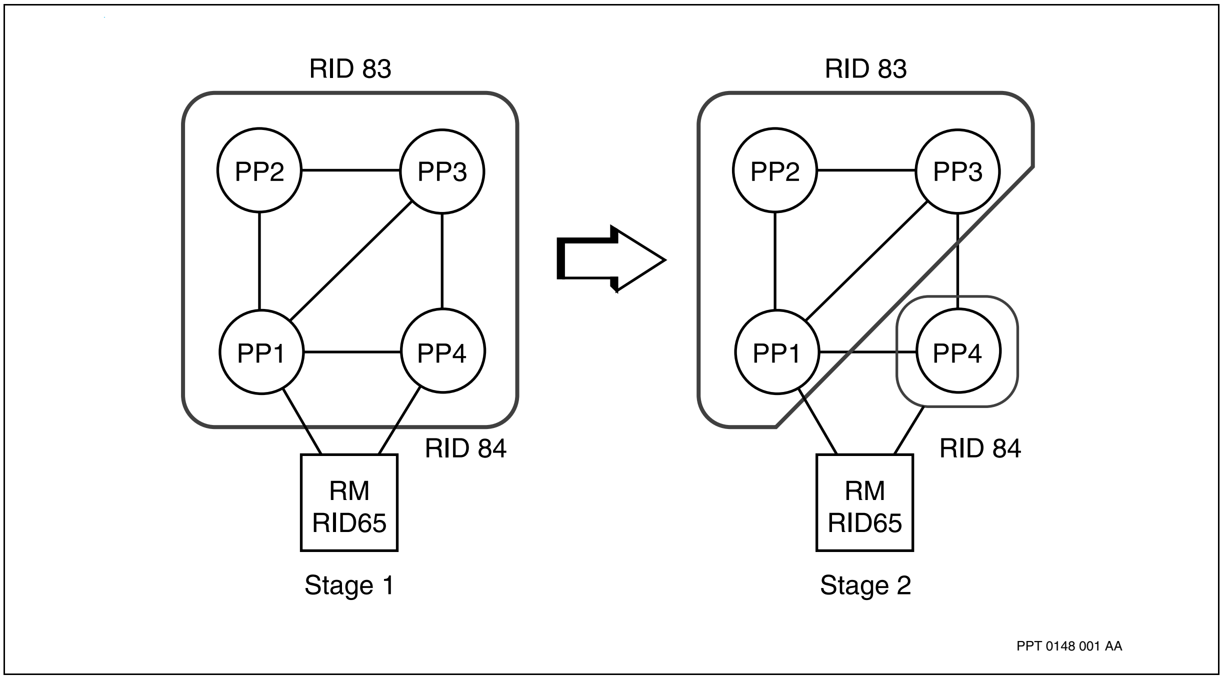


Splitting a RID subnet

Splitting a RID subnet causes a critical service data change on the Nortel Multiservice Switch nodes that are being split off into the new RID subnet. This is because changing the RID of a Multiservice Switch node causes the module to restart.

When splitting a RID subnet, you must consider the impact on routing. DPRS favors routing within the RID subnet rather than tandeming through another RID. Splitting a RID subnet can alter the existing routing behavior. The figure, Splitting a RID subnet (page 87) shows this impact.

Splitting a RID subnet



Preparing to split the subnet: In the figure, Splitting a RID subnet (page 87), the topology in Stage 1 represents an existing RID subnet that is to be split into the topology depicted in Stage 2. In Stage 1, this topology results in two equal-cost paths from node PP3 to RM 65. These paths are PP3-PP1-RM65, and PP3-PP4-RM65. When the RID subnet is split in Stage 2, these paths are no longer of equal cost, and routing will always favor the path through the RID subnet, PP3-PP1-RM65. This behavior results because of the difference in resolution between the Multiservice Switch metrics used for routing within the RID subnet, and the DPN metrics used when routing over DPN internal or external gateways. The better resolution of the Multiservice Switch metric results in the RID subnet route being the chosen path even though the link costs along the two paths are equal.

As in the case of adding a new RID subnet, the first step in planning to split a RID subnet is to determine the CSRM deployment for the resulting two RID subnets. Since the CSRMs are already defined to support the existing RID of the subnet, you must ensure that CSRM connectivity to that RID is unaffected after the subnet is split. You must also configure the CSRMs for the new RID subnet to support the new RID. CSRMs can be shared across RID subnets. If a CSRM is connected to two Multiservice Switch nodes that are to be split into two separate RID subnets, you can configure the CSRM with the new RID value as well as the old RID value. The CSRM will continue to provide call services for all the Nortel Multiservice Switch nodes in the two subnets.

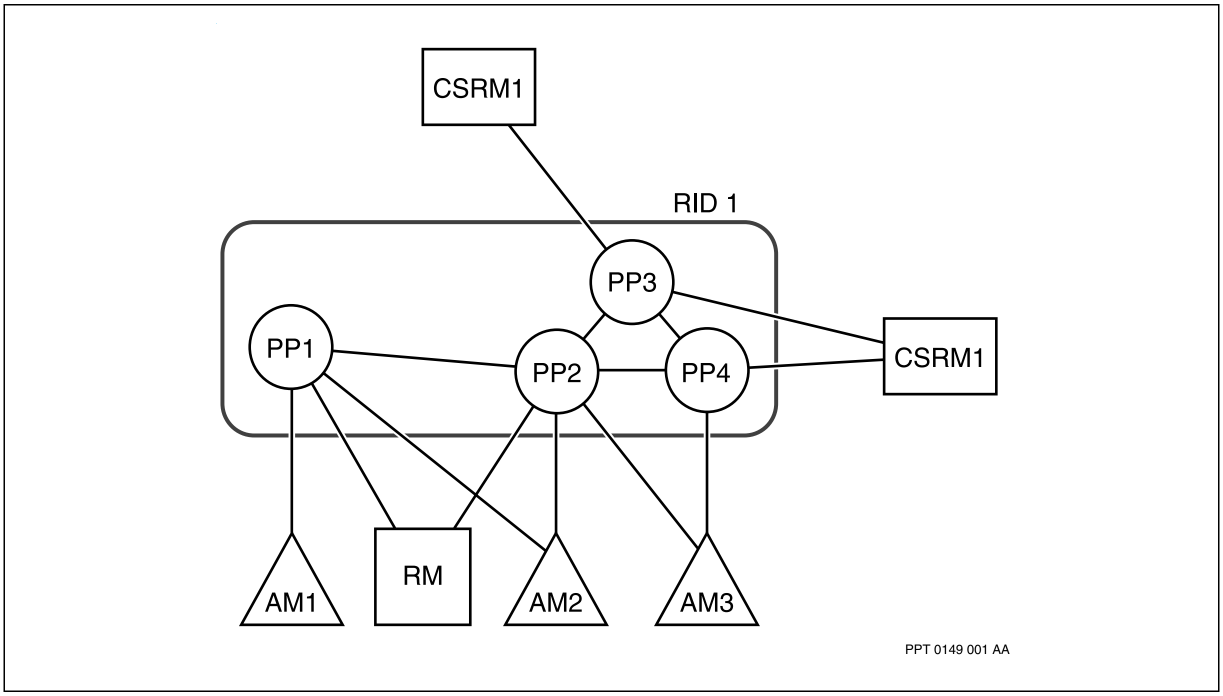
The next step is to consider is the AM connectivity to the subnet. Three scenarios are possible after the subnet split:

1. The AM cluster remains connected only to Multiservice Switch nodes in the original RID subnet. This has no impact on the routing to the AM.
2. The AM cluster is connected to two Multiservice Switch nodes, each in different RID subnets. This has no impact on the routing to the AM. Network SCR service data continues to map the DNAs on the AM using the original RID subnet as the AM's home RID. The AM inbound loadshares across its links up to the network level. Outbound loadsharing to the AM from the network occurs as the AM's calls are balanced across its two links up to the two network RIDs.
3. The AM cluster is connected only to Multiservice Switch nodes in the new RID subnet. This will have an impact on routing to the AM DNAs. RID splitting should be defined on the CSRMs of the original RID subnet in order to send incoming calls to the CSRMs of the new RID subnet. Over time, the network-wide SCR prefix DNA map should be updated to reflect the new home RID for the AMs in the AM cluster.

You must also consider the Preside Multiservice Data Manager connectivity to the Multiservice Switch nodes in the new RID subnet. It is essential to ensure that Preside Multiservice Data Manager connectivity is still maintained to all Multiservice Switch nodes after the RID subnet has been split. In some numbering plans, the Multiservice Switch IPIVC or IPIFR DNAs may begin with the same prefix on the Multiservice Switch nodes that are to be in separate RID subnets.

Splitting the subnet: The figure, Splitting a RID subnet (page 89) displays a RID subnet with a RID value of 10 to be split into two separate RID subnets (RID 10 and RID 20). The CSRMs for RID 10 are both called CSRM1. In this example, nodes PP1 and PP2 are to be split into a separate RID subnet. The three possible AM connectivity scenarios are shown in this diagram.

Splitting a RID subnet



Example of splitting a RID subnet

1 Configure CSRMs for the new RID subnet

Add the new RID to the list of RIDs supported by the CSRMs. Ensure that at least one of the CSRMs for the new RID is connected to the first Multiservice Switch node to be split off into the new RID subnet (node PP1 in this case).

If new CSRMs are being defined to support the RID subnet in a network that contains X.25 or X.75 gateways, ensure that the new CSRM’s RID is provisioned in the gateway call routing system’s common envelope RID map.

Before each Multiservice Switch node is activated with a new RID, it must have a direct trunk connection to the new RID subnet. In addition, each Multiservice Switch node in the old RID subnet must maintain a direct trunk connection to its RID subnet when any other Multiservice Switch node in the subnet is having its RID changed.

2 Configure RID splitting on both CSRMs for RID 10 split to RID 20. See Configure and RID-split CSRMs for new RID subnet (page 91).

In preparation for assigning a new RID to node PP1, the CSRMs for RID 10 must have RID splitting provisioned in their DCR system to RID-split to the new RID 20. This will ensure that the DNAs on node A and AM1 can still be reached after node A has restaged with the new RID value.

At this point, no special consideration is required for AM2, which is connected to both nodes PP1 and PP2. On reassignment of a new RID to node PP1, AM2 will still be connected to node PP2, so calls can still be routed to DNAs on AM2.

3 Configure the new RID on the Multiservice Switch node. See Configure new RID on Multiservice Switch node (page 92).

Configure the new subnet RID on the first Multiservice Switch node to be split into the new RID subnet (node PP1 in this example). Activating the changed service data results in a critical service data change, causing the module to restart. Immediately after the module loads, enter a DCR associate command on the CSRMs for RID 10 to clear out the DNAs for node PP1 and its connected AMs. This process ensures that RID splitting will take effect. In this topology, because AM1 is singly connected to node PP1, calls on AM1 will go down when node PP1 reloads with its new RID value. To avoid any impact to AM1, configure a second connection to another Multiservice Switch node in the RID subnet or another RID.

On rejoining the network, node PP1 advertises its new RID value, and the Multiservice Switch trunks between node PP1 and nodes PP2 and PP3 restage as internal gateways for DPRS. (However, the topology system will still have a global network view of all the interconnected Multiservice Switch nodes.) Configure new RID on Multiservice Switch node (page 92) depicts the topology resulting from this step.

At this time, perform the following steps:

— Ensure that the CSRMs for the new RID are functioning correctly. (See Configuring the Multiservice Switch node (page 11)). Use the csr display interfaces command to make sure the RID and MID of the Multiservice Switch node (node PP1) in the new RID subnet are included in the interface list.

— Ensure that call setup can be established to node PP1 and its connected AMs. This should occur as a result of RID splitting on the CSRMs of the RID 10 subnet.

— Check that the DNAs in the attached AMs are correctly associated with the new RID subnets’ CSRMs.

— If any X.25 or X.75 gateways are supported in the attached AMs, verify that they are correctly displayed by GDCR on the RID 20 CSRMs.

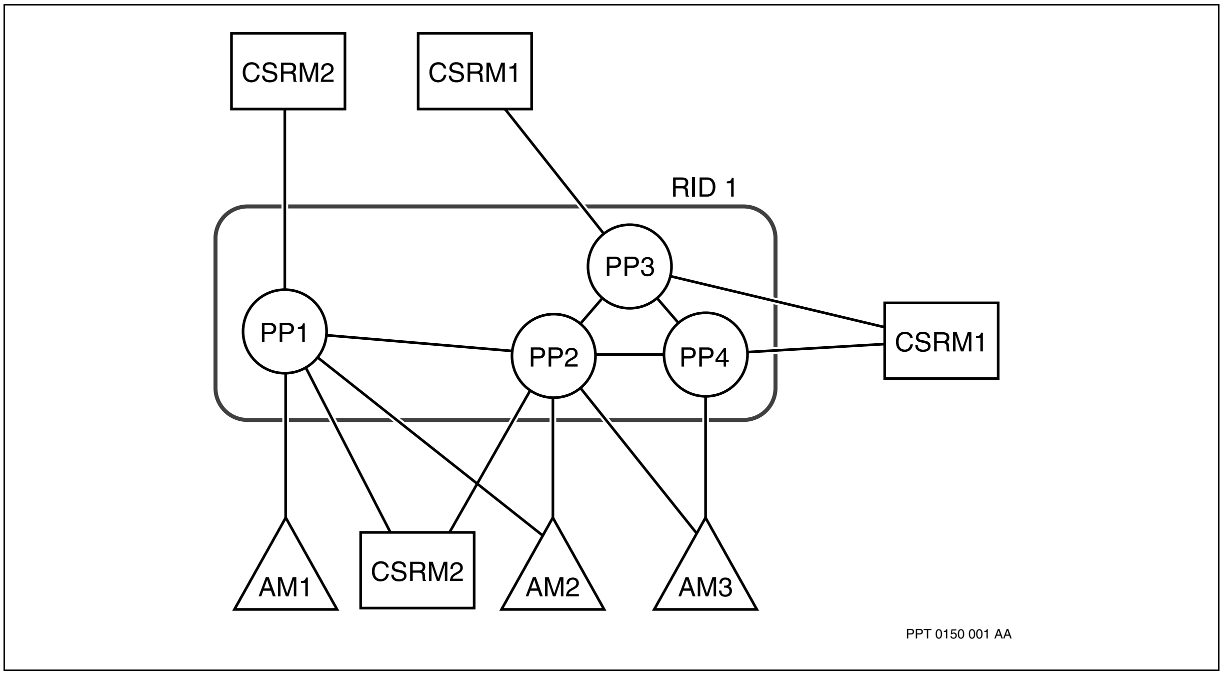
4 Configure the new RID on other Multiservice Switch nodes. Refer to Configure new RID on other Multiservice Switch nodes (page 92).

Configure the new subnet RID on the next Multiservice Switch node to be split into the new RID subnet (node PP2 in this example). While node PP2 reloads, enter a DCR associate command on the CSRMs for the RID 10 subnet to ensure that RID splitting takes effect. In this topology, all calls on AM2 will stay up since AM2 still has a connection to the network while node PP2 reloads.

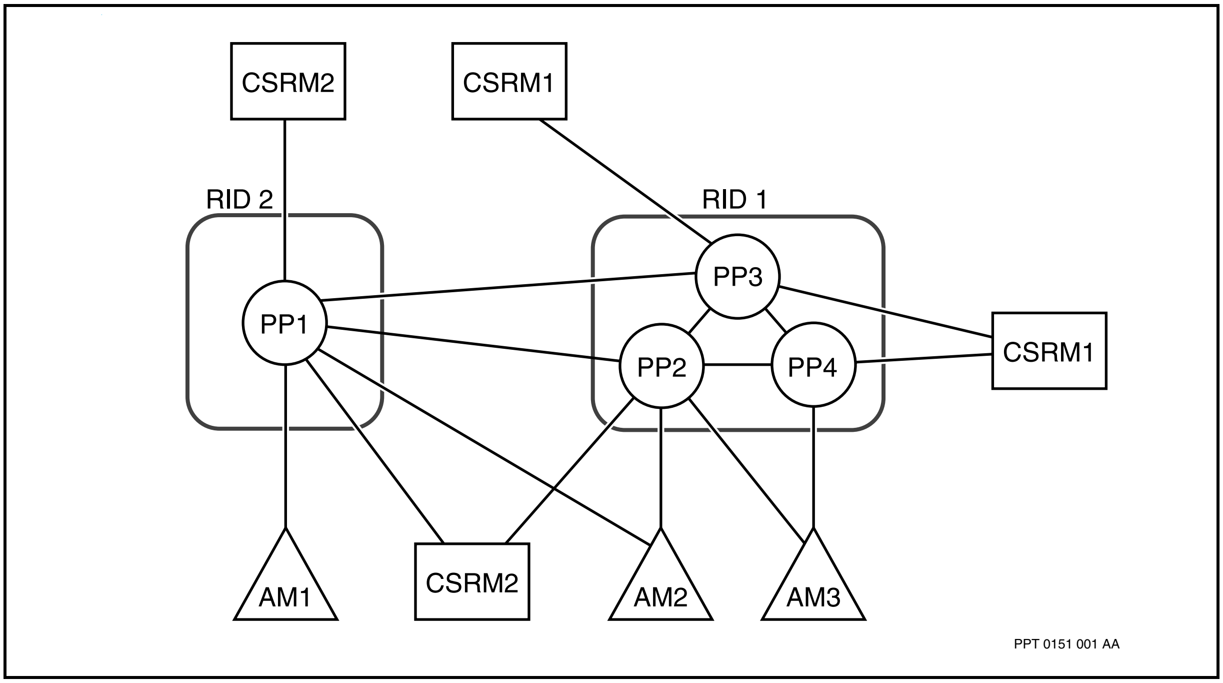
5 Update the network-wide SCR prefix-DNA map.

The SCRs across the network must be updated with the new prefix-DNA mappings required to route calls to the local DCR system in the new RID subnet.

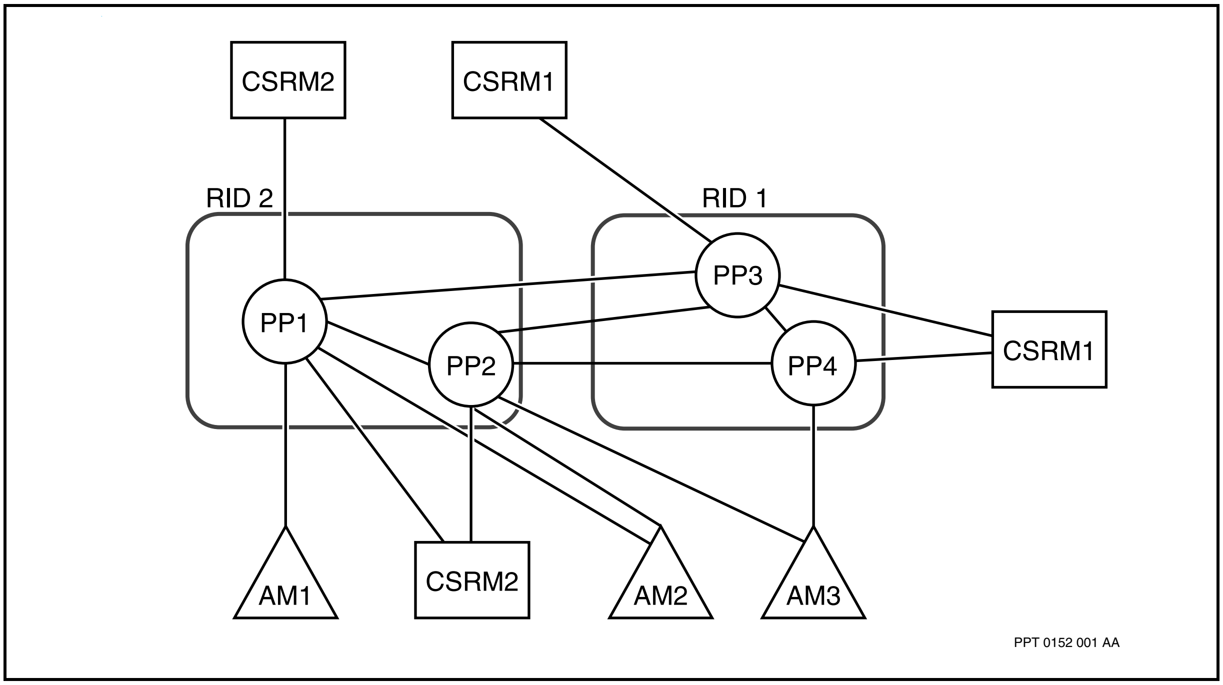
Configure and RID-split CSRMs for new RID subnet



Configure new RID on Multiservice Switch node



Configure new RID on other Multiservice Switch nodes



Merging RID subnets

Merging RID subnets is the opposite process to RID splitting. Configure new RID on other Multiservice Switch nodes (page 92) shows the sample RID subnets to be merged.

Example of merging RID subnets

1 Plan CSRM deployment.

When you are merging two RID subnets, take into consideration the geographical considerations of CSRM deployment. The CSRMs of the resulting merged RID subnet should be geographically located so that call setup can be achieved within a reasonable proximity to most call sources. If you need to reassign the CSRMs, you can do this more easily after the subnet merge is complete.

2 Set up RID backup for the two subnet RIDs.

3 If all the Multiservice Switch nodes in a RID subnet are to be merged into another RID subnet, the RID to be eliminated (RID 20 in this example) should be redirected to the merged RID value (RID 10) in the network-wide access to call redirection RID redirection map.

— The CSRMs of the RID 20 subnet should be RID-split to RID 10 (the merged RID subnet). This handles two possible scenarios of RID subnet merging:

The RID subnets are not to be completely merged; only some Multiservice Switch nodes are to be merged to the other RID subnet. Both RIDs remain in the network and RID splitting handles routing calls to the merged modules until the network SCR prefix maps are updated.

The RID subnets are to be completely merged. During the intermediate steps in which Multiservice Switch nodes are reassigned RIDs one by one, both RIDs are reachable in the network. In this case, RID splitting handles routing calls to the modules that have been merged so far, until all the modules are merged into the single RID subnet.

4 Configure the new RID on the Multiservice Switch nodes.

Before each Multiservice Switch node is activated with a new RID, it must have a direct trunk connection to the new RID subnet. In addition, each Multiservice Switch node in the old RID subnet must maintain a direct trunk connection to its RID subnet when any other Multiservice Switch node in the subnet is having its RID changed.

In this step, Multiservice Switch nodes in the RID subnet to be eliminated (RID 20) can be provisioned one by one with the merged RID value (RID 10). This is a critical service data change and results in the Multiservice Switch node restarting. After the restart, the Multiservice Switch trunks, which were previously internal gateways to RID 10, are now simply perceived as Multiservice Switch trunks to DPRS. DPRS broadcasts are now exchanged across the trunks. The newly provisioned Multiservice Switch node now learns all the MIDs in the RID 10 subnet, and uses the RID 10 subnet's CSRMs for its call services.

Configure new RID on Multiservice Switch node (page 92) shows the first step in this subnet merging process. At this point, all calls destined to node B or its connected AM are still routed to their old RID value (RID 20) due to the mapping in the network SCR tables. While the Multiservice Switch node is restarting, use the DCR associate command on the CSRMs for the RID 20 subnet to clear out the DNAs for node B and its connected AMs. This ensures that RID splitting will take effect.

5 Configure the new RID on last Multiservice Switch node in RID subnet.

At this point, the last Multiservice Switch node in a RID subnet is defined with the merged RID value. The RID to be eliminated (RID 20) will no longer be reachable. This will have the following implications:

Calls that were established to AMs connected to this last Multiservice Switch go into VC recovery. If the AM is still reachable through its alternative RID, the calls recover successfully and are subsequently rerouted through the alternative RID. If not, the Multiservice Switch node should restart fast enough for the VC recovery to occur through the restarted Multiservice Switch node. These calls use the new RID.

New calls destined for the now unreachable RID (due to SCR prefix mapping) are sent to the call redirection system. They are backed up to the merged RID value as defined in step 2.

Check that the DNAs in the attached AMs are correctly associated with the new RID subnets' CSRMs.

If any X.25 or X.75 gateways are supported in the attached AMs, verify that they are correctly displayed by GDCR on the RID 10 CSRMs.

6 Update the network-wide SCR prefix-DNA map.

At this point, you must update the SCRs across the network with the new prefix-DNA mappings to route calls to the local DCR system in the merged RID subnet.

Splitting and Merging RID subnets that contain Multiservice Switch clusters

There is no extra configuring or operating procedures required for migrating RID subnets in an inter-worked network, when Nortel Multiservice Switch clusters are deployed. Simply ensure that each Multiservice Switch cluster node maintains at least one path to reach a backbone node within its own RID subnet during the migration. The goal is simply to avoid isolation of any of the Multiservice Switch cluster nodes. See NN10600-425 *Nortel Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System* for more information.

Deploying CSRMs

This section describes deployment considerations for CSRMs.

Server PE performance

For each CSRM call server type (for example, SCR, DCR, GSCR, GDCR), up to eight instances can be configured on the CSRM. Only one instance of each server type can be provisioned on a call server PE. For optimal performance, configuring all server types on the same call server PE is recommended.

However, this may not be feasible for CSRMs supporting large RID subnets. If there are many DNAs supported in the RID subnet, you may need to separate the DCR onto its own PE for memory considerations. (See Server PE memory (page 95)). The higher call throughput demands of a large RID subnet can be accommodated by configuring more instances of the required server types. The packet routing system on the CSRM evenly loadshares traffic across all instances of any server type.

When two CSRMs are engineered for a RID subnet, each one must be engineered to support all network traffic in case the other CSRM fails.

For additional information, see 241-1001-156 *DPN-100 Access/Resource Module Engineering*.

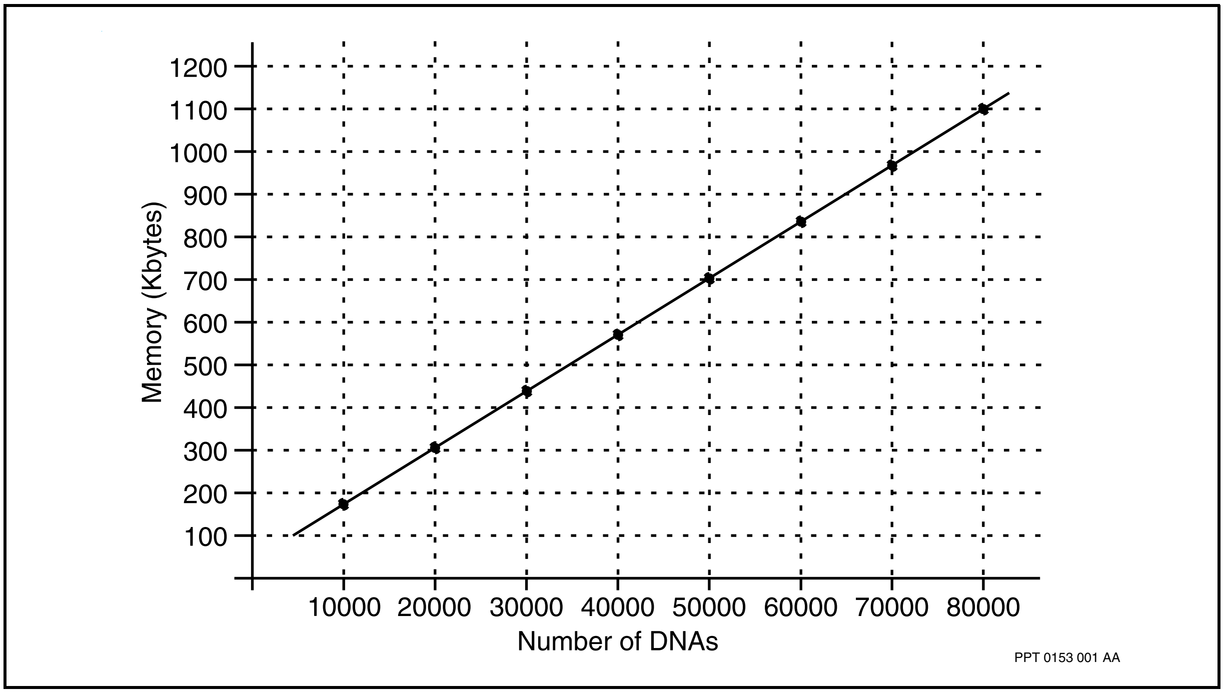
Server PE memory

The largest consumers of PE memory on the server PE are the SCR and the DCR systems. In the case of the SCR, its heap usage increases with the number of prefix DNA entries provisioned in its tables. When migrating a DPN-100 network to an interworking network, the SCR prefix-mapping table should be reviewed for entries that can be deleted due to the migration of AMs to Nortel Multiservice Switch and the redeployment of RMs.

DCR heap usage is dynamic and is affected by the number of DNAs in the supported RID subnet, as well as the network numbering plan. Because of the numbering plan implications for DCR memory use, it is not possible to state a precise DCR memory consumption figure based solely on the number of DNAs. The graph in the figure Average DCR heap usage (page 96) represents the heap usage computed using a formula which averages the spread of DNA digits in a numbering plan.

For some numbering plans, the DCR memory consumption graph shown in Average DCR heap usage (page 96) may be conservative. This graph does not take into account the efficiency of the DNA tree structure used for storing DNAs in the DCR database. For example, most numbering plans use the same four digits to represent the DINT in the first four digit positions of every DNA. This leads to more efficient memory usage by the DCR. Alternatively, in a numbering plan where there is very little replication of DNA digits the efficiency of the structure is minimized, resulting in potentially greater memory use than shown in the graph.

Average DCR heap usage



The heap usage of the CSRM server PE should be monitored to ensure timely action for network growth. As heap memory consumption on the PE increases, the following actions can be taken to accommodate the increased heap requirement. These actions are listed in the order in which they should be applied until the heap requirements are met.

1 Increase the provisioned value for percent heap in the server PE loader service data.

2 Separate DCR servers onto their own separate server PEs.

3 Use 4 Megabyte 386 PE for DCR server PEs.

4 Split the RID subnet.

Checklist of CSRM engineering considerations (page 97) shows information you should consider when determining CSRM engineering requirements.

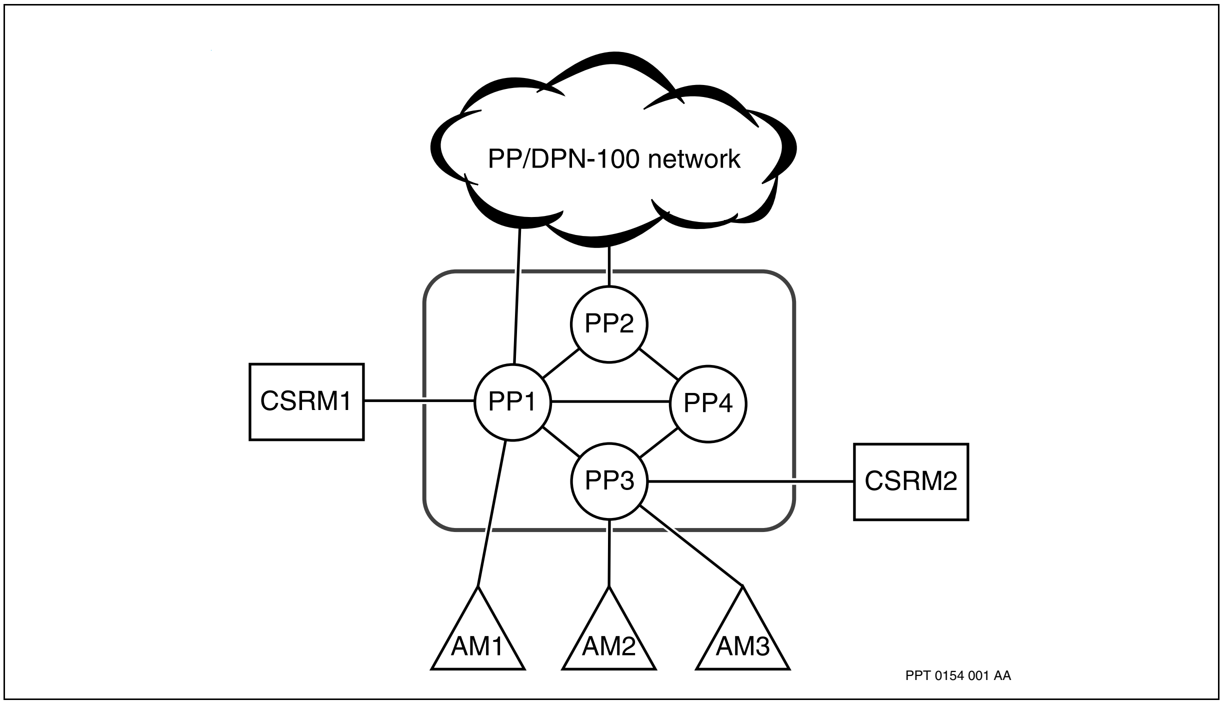
Checklist of CSRM engineering considerations

÷	Item	Notes
	Number of calls per second expected during peak hours from the supported RID subnet as well as the community of interest of these calls (that is, all within the RID subnet or some to other RID subnets or RMs in the network).	This information should be used to determine the required number of SCR/DCR servers based on the server calls per second performance characteristics.
	Number of calls per second expected during peak hours to X.25/X.75 gateways in the RID subnet.	This information should be used to determine the required number of GSCR/GDCR servers based on the server calls per second performance characteristics.
	Estimated number of calls from the RID subnet requiring NUI translation.	This information should be used to determine the required number of NUI-RSI servers based on the server calls per second performance characteristics.
	Estimated number of calls to the RID subnet requiring call redirection or RID redirection.	This information should be used to determine the number of CRD-RSI servers that should be configured.
	Number of DNAs supported in the RID subnet.	This information should be used to determine whether or not to isolate the DCR to its own PE for heap purposes, and to determine the RAM requirement for the PE 386 (for example, 2 or 4 Megabytes).
	DPNGateways to CSRM throughput.	A call originating from and destined to the same RID subnet traverses the CSRM link four times for SCR and DCR processing. This is because the SCR maps the RID subnet prefixes to the subnet RID and then the call is routed to the RID. On arriving at the RID subnet, the call is sent to the CSRM for subsequent DCR processing. This aspect should be considered when analyzing bandwidth use of the CSRM trunks. Note that calls originating from other RIDs simply traverse the link to the CSRM two times since they require only DCR processing.

CSRM location

In a combined network, you should consider the location of the RID subnet CSRMs with respect to the rest of the network. CSRM deployment (page 98) shows a sample topology in which a RID subnet connects to a combined network.

CSRM deployment



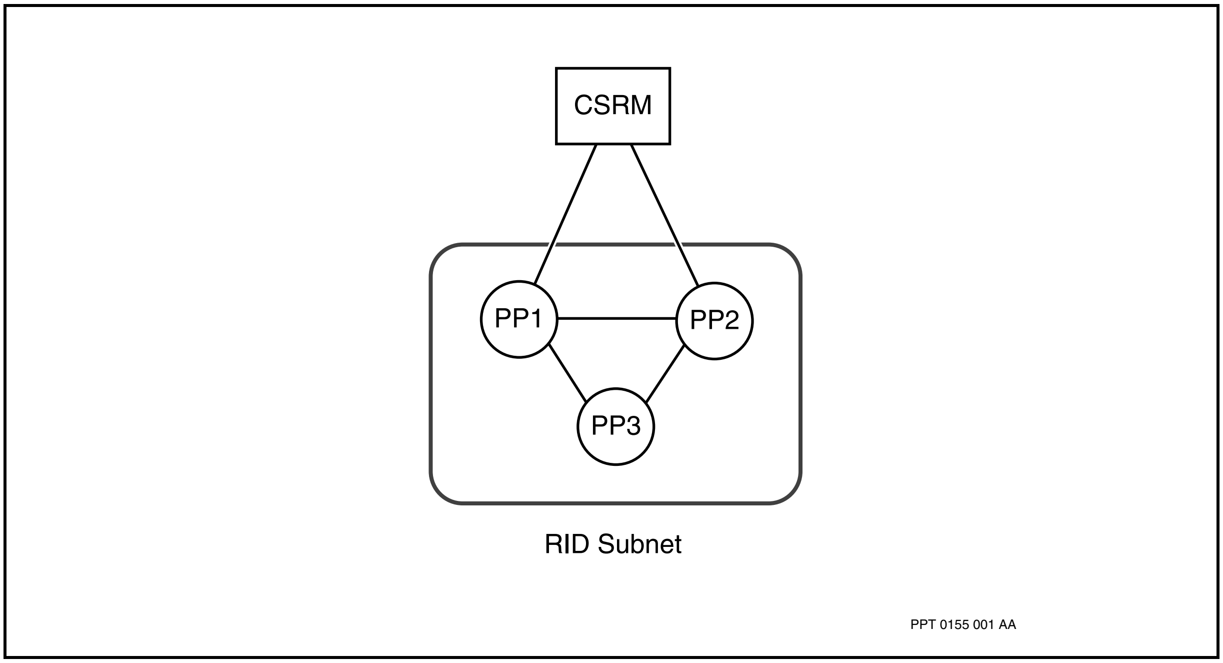
In this example, CSRM1 is located closer than CSRM2 to the two entry points into the RID subnet from the rest of the network. The impact of this topology is that the CSRM1 DCR receives all calls destined for the RID subnet from the rest of the network, because it is always the CSRM closest to the calls' point of entry into the RID subnet. For calls generated within the subnet, CSRM2 is used if it is closest to the call's point of origin.

The topology depicted in CSRM deployment (page 98) is an extreme case in order to explain the traffic implications. In a more typical network, there would be connectivity to the rest of the network from node PP3 or PP4. If this is not the case, then the CSRM connectivity should be considered. If an alternative connectivity strategy is not feasible, it is necessary to ensure that CSRM1 is engineered to handle the network call traffic that it will receive.

CSRM routing

When selecting an RM to act as a CSRM for a RID subnet in an interworking network, you should consider certain engineering aspects. Dual-connected CSRM (page 99) shows a simple RID subnet configuration with a CSRM dual-connected to the RID subnet for redundancy purposes.

Dual-connected CSRM



In this topology, traffic from the RID subnet to the CSRM is evenly loadspread across the two links to the CSRM if the links are of equal cost. However, traffic from the CSRM to the RID subnet uses only one path, even though they are equal. This is because the CSRM uses RM RID routing behavior and selects one of the links as a primary over which all traffic flows. See Selecting paths (page 32). The other link is considered an alternative path. If overflow routing is provisioned on the CSRM, high-reliability traffic is routed over the alternative path if the primary path is congested.

Shared CSRMs

The purpose of sharing a CSRM between two or more RID subnets is to minimize the number of CSRMs required in an interworking network. Adding or removing a RID in the CSRM service data is a non-critical change, and has no impact on the CSRM operation.

CSRMs can be shared amongst several RID subnets, subject to engineering guidelines which take into account the number of calls as well as memory consumption to support the RID subnet DNAs.

If a CSRM is shared by two RID subnets, the CSRM is directly connected to both RID subnets and provides a backup path for traffic if there is a trunk failure. To avoid this potential failure scenario, the shared CSRM should be tandem-suppressed. See Tandem through RM (page 67) for an example of tandeming through an RM under Nortel Multiservice Switch trunk failure.

It is important to consider the routing implications for other RIDs when tandem-suppressing a shared CSRM. Under failure of the other CSRM in one of its supported RID subnets, the shared CSRM must be engineered so that it can handle the full load for that RID subnet while still handling part of the load for any other supported RID subnets. For this reason, sharing CSRMs is really only applicable when the RID subnets are small with few connected AMs.

The call routing system, specifically the source call router (SCR), maps the prefix of the DNAs supported in each RID subnet to the RID of that subnet. This is the case when a CSRM is supporting a single RID subnet. This may also be the case when a CSRM is supporting multiple RID subnets. If a RID subnet is split into two subnets, for example, the DNA prefix for the original subnet may no longer easily identify a single RID to which the calls can be mapped. Since one destination call router (DCR) is capable of supporting both subnets, it is possible to split a RID subnet and have DNAs with the same prefix span two RID subnets. This allows a call to be mapped to one RID and terminate in another RID subnet. However, when CSRM connectivity fails in this scenario, potential routing constraints exist. For more information on the specific limitations, see Shared CSRM constraints (page 103).

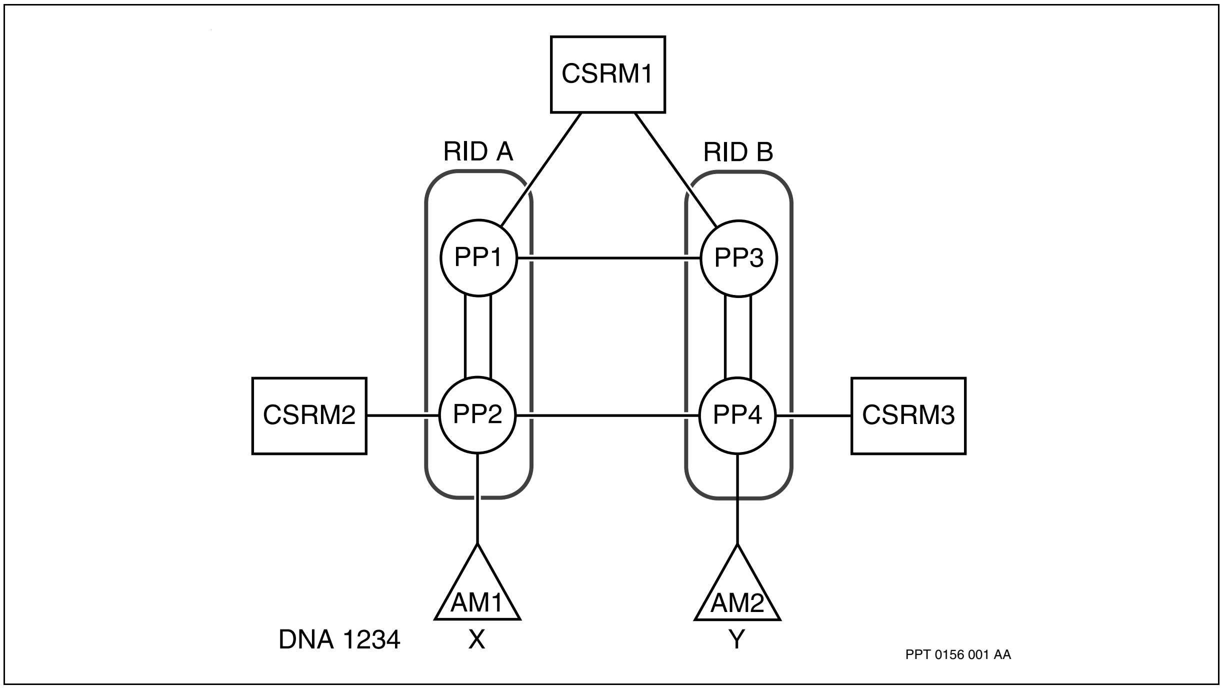
RID splitting: If a CSRM is shared between two or more RID subnets, it is important to consider the effect on some networking features. A CSRM can be RID-split only to a single RID at any one time. If RID splitting is in effect on the shared CSRM, then no other RID subnets supported by the CSRM can RID-split to a different RID. Once the first migration is complete and the necessary RID splitting removed, RID splitting can then be defined for any of the other RID subnets on a one by one basis. As well, while RID splitting is defined on a shared CSRM, the RID-split RID is the first level of call backup for all calls processed by the shared CSRM. Any call failures that result because of a DNA missing in the CSRM's DCR tables result in the calls being sent to the RID-split RID.

AM DNA association: AMs connected to a Nortel Multiservice Switch RID subnet provide the RID of the subnet to the DCR on the CSRMs when they associate their DNAs. When an AM is connected to two RID subnets, and these RID subnets share a CSRM, the AM will associate only one of the RIDs to the DCR on the shared CSRM. If the AM is connected to both a RID subnet and its CSRM, the AM non-deterministically associates one of its two cluster RIDs to the DCR on the CSRM in question. The RID selected may not necessarily be the best path to the AM, but this RID only comes into effect during call setup. The AM selects the best RID for the VC setup.

Although it is technically possible to connect an AM cluster to two RID subnets, it is preferable to connect the cluster to two Multiservice Switch nodes in the same RID subnet. This engineering guideline results in simplified backup scenarios under failure conditions.

DNA call forwarding: Another special consideration with respect to shared CSRMs is the configuring of call forward DNAs. If a DNA is moved from one RID subnet to another RID subnet, DNA call forwarding does not have to be provisioned on a shared CSRM which supports both subnets. For example, the figure Sample topology for CSRMs (page 101) shows a sample topology.

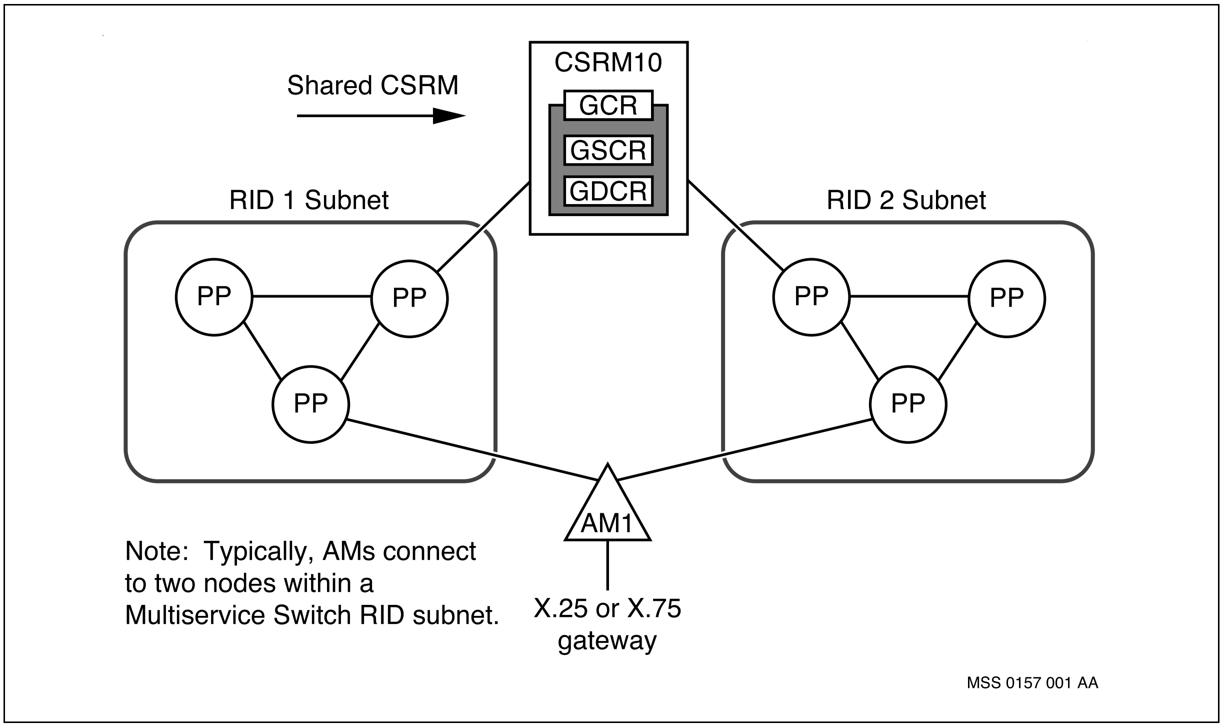
Sample topology for CSRMs



In this example, DNA 1234 is to be moved from location x to location y. Call forwarding service data does not have to be defined for this DNA on the shared CSRM since the DNA is associated to the shared CSRM by AM2. Call forwarding must still be defined on CSRM2.

Shared CSRMs for X.25/X.75 gateways: In the special case topology shown in the figure Shared CSRM for X.25/X.75 gateways (page 102), AM1 reports its gateway availability to the shared CSRM through two Nortel Multiservice Switch RID subnets. As a result, the shared CSRM maintains a primary and an alternative (backup) RID for AM1. The GDCR routes all calls through the primary RID only, even though the call originated from the alternative RID.

Shared CSRM for X.25/X.75 gateways



If access to the gateway through the primary RID (for example RID 10) fails (due to failure of either the AM link or the CSRM link to RID 10), the alternative RID (RID 20) immediately becomes the primary RID to the gateway. In this example, when access to the gateway through RID 10 is restored, RID 10 becomes the alternative RID and RID 20 remains the primary RID.

The primary and alternative RIDs can be displayed through the GDCR display gateway command. For further information, see DPN document 241-1001-303 *DPN-100 Operator Commands and Responses*.

Shared CSRM constraints

There are potential issues associated with Nortel Multiservice Switch subnets supporting shared CSRMs.

When sharing CSRMs, the topology illustrated in the figure Shared CSRM topology-two CSRMs (page 104) is the most recommended. Here, Subnet A (RID A) and Subnet B (RID B) are interconnected as well as connected to CSRM X and CSRM Y. CSRMs X and Y are considered to be dual-homed CSRMs because they support two subnets. CSRMs X and Y share all the call-setup requests from the two supported subnets.

Each CSRM is assigned its own RID number, therefore, by including dual-homed CSRMs in your network you can help reduce the consumption of RID numbers (the maximum number of RIDs in a network is 126).

If either CSRM X or CSRM Y fails, it will take some time for the remaining CSRM to take on 100% of the call load. During this transition, some traffic may be lost. The same issue arises when the down CSRM becomes active again. In this case, the DCR tables must be updated, which can take time. Keep in mind that traffic loss is a possibility during transition in any CSRM sparing arrangement.

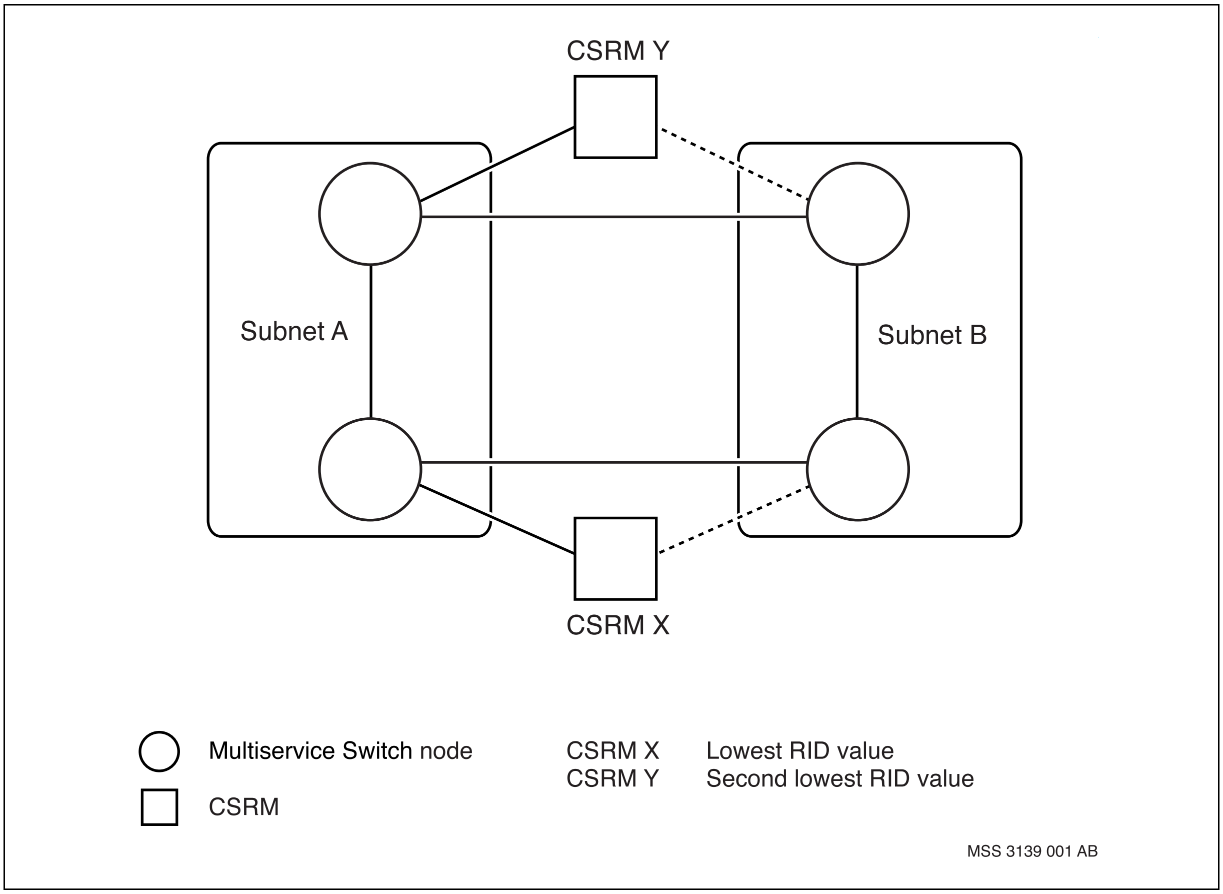
This appendix discusses situations in which source call routing tables in the network's CSRMs include data network addresses (DNAs) for calls mapped to RID A, calls mapped to RID B, and also calls mapped to RID A but actually supported by RID B. Refer to figure Shared CSRM topology-two CSRMs (page 104). The benefit of call routing with the latter mapping is that if a connection between RID B and either CSRM goes down, the destination call router (DCR) in that CSRM can still direct the calls to RID A.

Navigation

Two CSRMs supporting two RID subnets

Two scenarios will be discussed here in order to describe what happens during different types of connection failures. See the figure Shared CSRM topology-two CSRMs (page 104) for a graphic representation of the following scenarios.

Shared CSRM topology-two CSRMs



The first scenario involves a connection failure between RID B and CSRM Y. The following situations will occur:

- Calls originating from and terminating in RID A continue using CSRM X and CSRM Y and are established as normal.
- Calls originating from RID B use CSRM X and are established as normal.
- Calls mapped to RID B use CSRM X only (until CSRM Y becomes active again) and are established as normal.
- Calls mapped to RID A but destined for RID B can be directed to either CSRM X or Y. If the calls are sent to CSRM X then the calls will establish as normal. If the calls are sent to CSRM Y the calls will establish as long as the destination DNA was learned from RID B before the CSRM

connection failed (these calls will get sent to RID B via RID A). The DNAs that would not be known would be those that were introduced to RID B after the CSRM link failed. In this case, 100% of the calls to those DNAs would fail.

Call packets sent to newly established nodes in RID B via CSRM Y will encounter 100% failure because the DNAs have not yet been learned by DCR.

The second scenario involves a connection failure between RID B and both CSRMs X and Y. The following situations will occur:

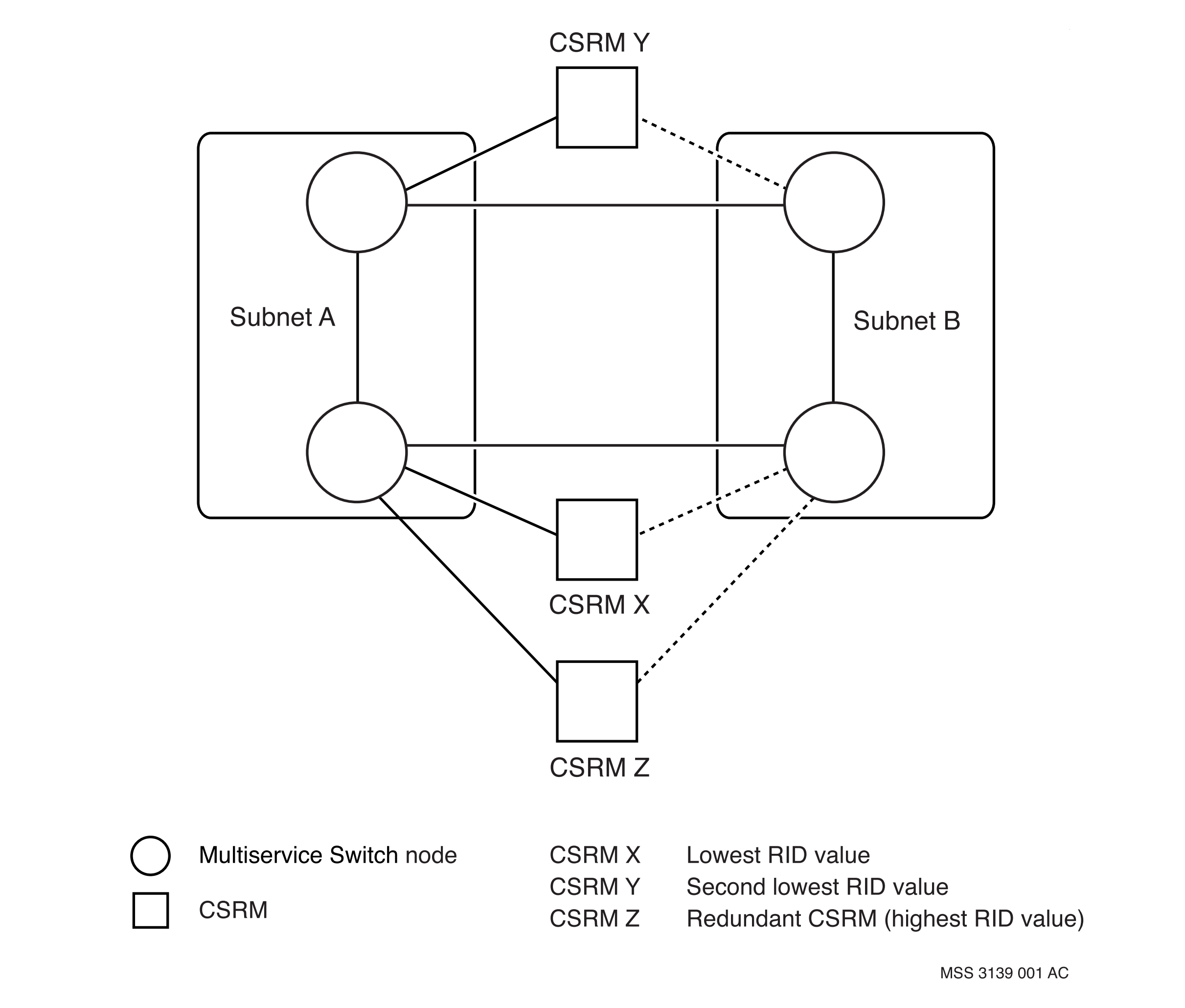
- Both originating and terminating calls of RID A continue using CSRM X and CSRM Y and are established as normal.
- Calls mapped to RID B will encounter 100% failure.
- Calls mapped to RID A but destined for RID B will learn of the destination node in RID B by either CSRM X or Y. The calls will then be sent to RID B via RID A, as long as the DNA was learned before the CSRM link failed.

Call packets sent to newly established nodes in RID B via CSRM X or Y will encounter 100% failure because the DNAs have not yet been learned by DCR.

Three CSRMs supporting two RID subnets

Two scenarios will be discussed here in order to describe what happens during different types of connection failures. In both scenarios, CSRM Z is the redundant CSRM, meaning if one CSRM (X or Y) fails, CSRM Z will become active. See the figure Shared CSRM topology-three CSRMs (page 106) for a graphic representation of the following scenarios.

Shared CSRM topology-three CSRMs



The first scenario involves a connection failure between RID B and CSRM Y. The following situations will occur:

- Calls originating from and terminating in RID A continue using CSRM X and CSRM Y and are established as normal.
- Calls mapped to RID B use CSRM X and CSRM Z (until CSRM Y becomes active again) and are established as normal.
- Calls originating in RID B will use CSRM X and CSRM Z (until CSRM Y becomes active again) and are established as normal.
- Calls mapped to RID A but destined for RID B can be directed to either CSRM X or Y. If the calls are sent to CSRM X then the calls will establish as normal. If the calls are sent to CSRM Y the calls will establish as long as the destination DNA was learned from the RID B subnet before the CSRM connection failed (these calls will get sent to RID B via RID A). The

DNAs that would not be known would be those that were introduced to RID B after the CSRM link failed. In this case, 100% of the calls to those DNAs would fail.

Calls sent to newly established nodes in RID B via CSRM Y will encounter 100% failure because the DNAs have not yet been learned by DCR.

The second scenario involves a connection failure between RID B and both CSRMs X and Y. The following situations will occur:

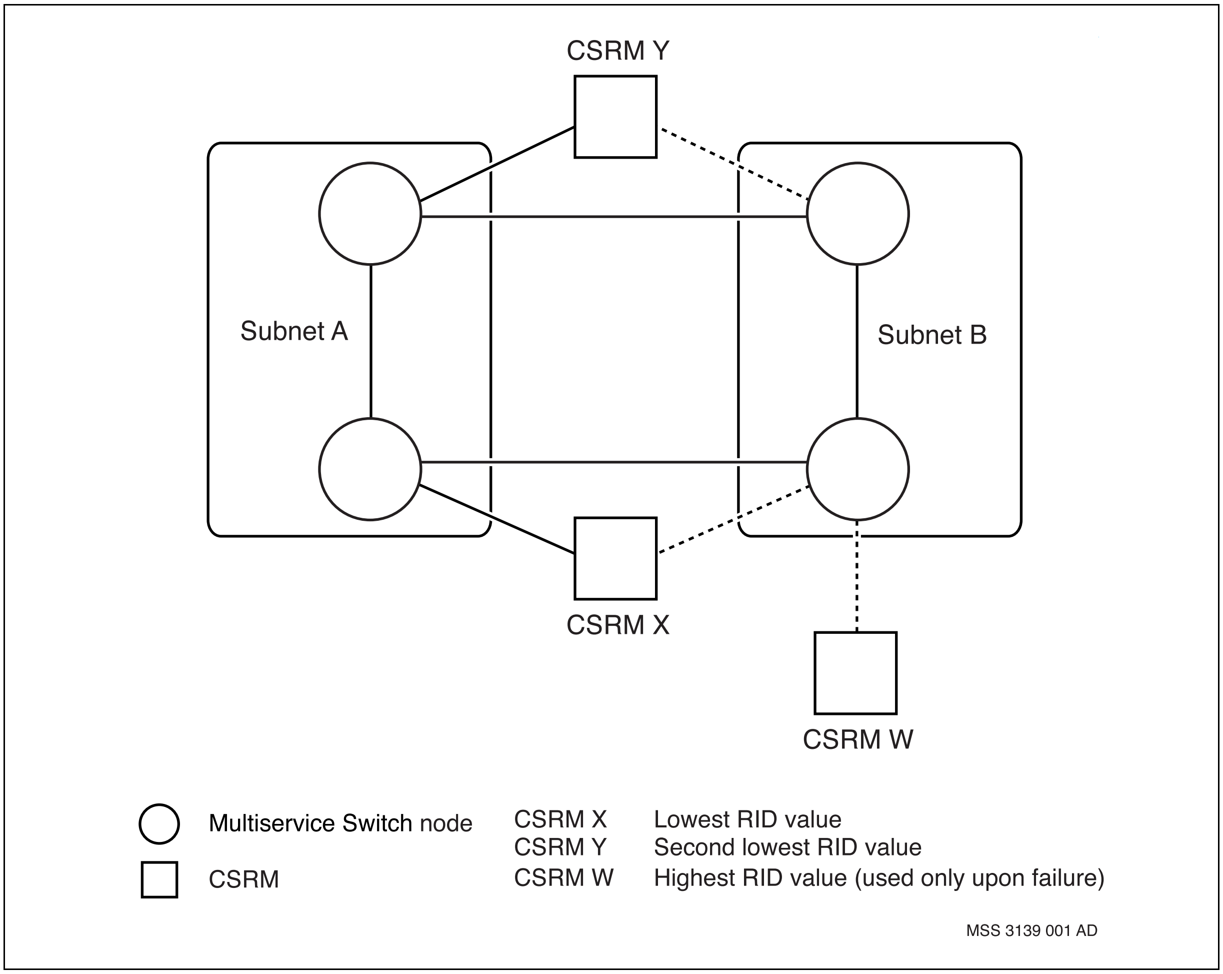
- Calls originating from and terminating in RID A continue using CSRM X and CSRM Y and are established as normal.
- Calls mapped to RID B will use CSRM Z only and are established as normal.
- Calls mapped to RID A but destined for RID B can be directed to either CSRM X or Y. The calls will establish as long as the destination DNA was learned from RID B before the CSRM connection failed (these calls will get sent to RID B via RID A). The DNAs that would not be known would be those that were introduced to RID B after the CSRM link failed. In this case, 100% of the call load would fail.

Calls sent to newly established nodes in RID B via CSRM X or Y will encounter 100% failure because the DNAs have not yet been learned by DCR.

Three CSRMs supporting two RID subnets (one CSRM is not shared)

This section describe a scenario that arises when one RID subnet has a CSRM (CSRM W) that does not support both RIDs. This scenario will describe what happens during a specific type of connection failure. See the figure Shared CSRM topology-three CSRMs (with one supporting a single RID) (page 108) for a graphic representation of the following scenario.

Shared CSRM topology-three CSRMs (with one supporting a single RID)



The following scenario involves a connection failure between RID B and CSRM Y. The following situations will occur:

- Calls originating from and terminating in RID A continue using CSRM X and CSRM Y and are established as normal.
- Calls mapped to RID B use CSRM X and CSRM W (until CSRM Y becomes active again) and are established as normal.
- Calls originating from RID B use CSRM X and W and are established as normal.
- Call packets mapped to RID A but destined for RID B can be directed to either CSRM X or Y. If the calls are sent to CSRM X then the calls will establish as normal. If the calls are sent to CSRM Y then the calls will establish as long as the destination DNA was learned from the RID B subnet before the CSRM connection failed. These calls will be sent to RID B via RID A. The DNAs that would not be known would be those that were introduced to the RID B after the CSRM link failed.

Call packets sent to newly established nodes in RID B via CSRM Y will encounter 100% failure because the DNAs have not yet been learned by DCR.

Nortel Multiservice Switch 7400

Operations: DPN-100 Interworking

Publication: NN10600-450
Document status: Standard
Document issue: 7.1S1
Document date: October 2005
Product release: PCR7.1 and up
Job function: Operations
Type: NTP
Language type: U.S. English