Nortel Multiservice Switch 7400

Operations: Remote Server Agent

NN10600-765

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*.

RSA configuration

Configure remote server agent (RSA) using default settings provided with the package, or configure RSA to meet your specific requirements. With exceptions such as addresses,

There are some exceptions to this procedure, such as configuring addresses.

Refer to Remote server agent fundamentals (page 15) for an overview of RSA and its associated components.

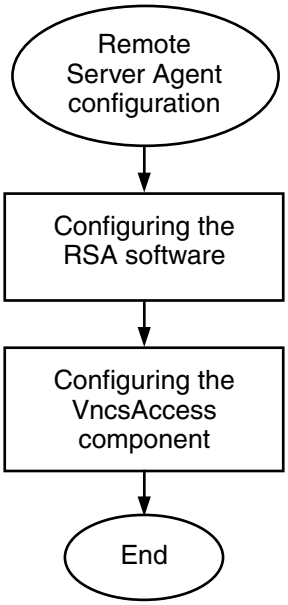
Prerequisites to RSA configuration

- The number of RSAs required in the network to handle the Passport 4400 units has been determined.
- If RSA is used to access VNCS, the VNCS and RSA must be provisioned on the same Multiservice Switch node. See the provisioning procedures in NN10600-755 *Nortel Multiservice Switch 7400 Operations: Voice Networking*.

RSA configuration procedures

This task flow shows you the sequence of procedures you perform to configure RSA. To link to any procedure, go to RSA configuration procedures navigation (page 6).

RSA configuration procedures



MSS 3420 009 AA

RSA configuration procedures navigation

- Configuring the RSA software (page 7)
- Configuring the VncsAccess component (page 9)

Configuring the RSA software

Configure the RSA software to perform the initial configuration.

Procedure steps

Step	Action
1	Include the RSA feature on the LogicalProcessorType (LPT) feature list for the supporting FP. **`set sw lpt/RSA fl serverAccessRsa`**
2	Add the Rsa component to the module. **`add Rsa/<rsa_name>`**
3	Specify the LP that will run the RSA application. **`set Rsa/<rsa_name> lp lp/<lp_number>`**
4	Assign the Rsa component a Dna component. **`set Rsa/<rsa_name> Dna dna <dna>`**
5	Optionally, set the incAccess attribute under the *Dna* component. **`set Rsa/<rsa_name> Dna incAccess allowed`**
6	Optionally, add a Cug component for the RSA. **`add Rsa/<rsa_name> Dna Cug/<cug_number>`**
7	Optionally set the attributes under the Cug component (for example, interlockCode). **`set Rsa/<rsa_name> Dna Cug/<cug_number> interlockCode 101`**

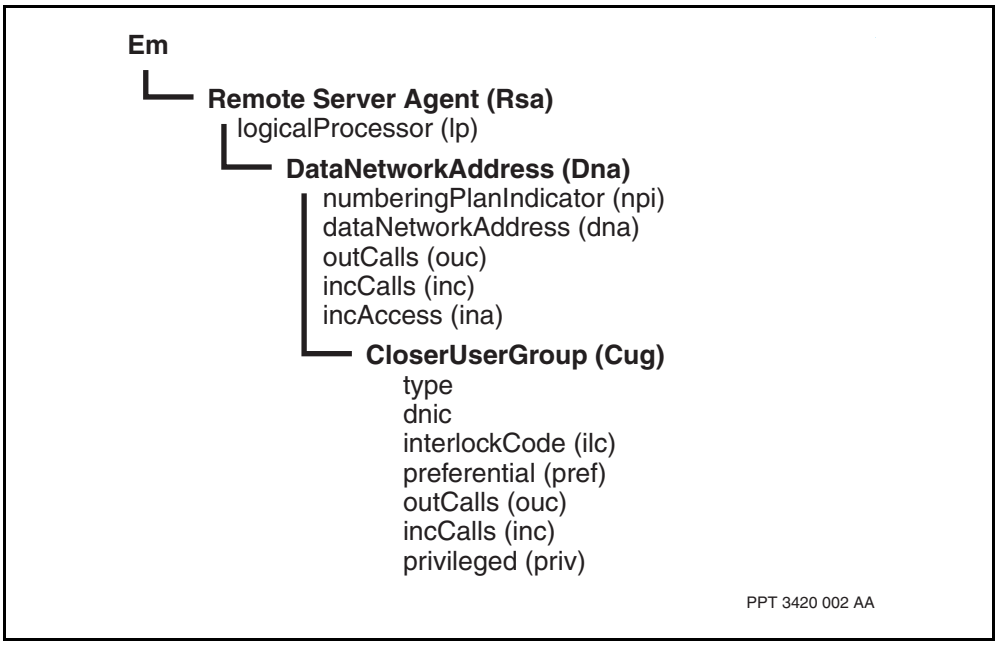
--End--

Variable definitions

Variable	Value
<cug_number>	is the *Cug* index range, value from 0 to 255.
<dna>	is the dna attribute value.
<lp_number>	is the instance number of the LP.
<rsa_name>	is the name assigned to this instance of the *Rsa* component.

Procedure job aid

RSA software component hierarchy



Configuring the VncsAccess component

Configure the *VncsAccess* component to access the VNCS so that voice interworking can occur between Passport 4400 access units and other nodes in the Nortel Multiservice Switch network.

Prerequisites

- Knowledge of how to provision VNCS to support voice interworking with Passport 4400 units, as described in NN10600-755 *Nortel Multiservice Switch 7400 Operations: Voice Networking*.

Procedure steps

Step	Action
1	Add the VncsAccess component to the RSA. **`add Rsa/<rsa_name> VncsAccess`**
2	Optionally, set the *timeToLive* attribute of the *VncsAccess* component to specify the length of time (in seconds) that a VNCS request may remain in the RSA queue before it is considered too old and is purged. **`set Rsa/<rsa_name> VncsAccess timeToLive <timeToLive_seconds>`**

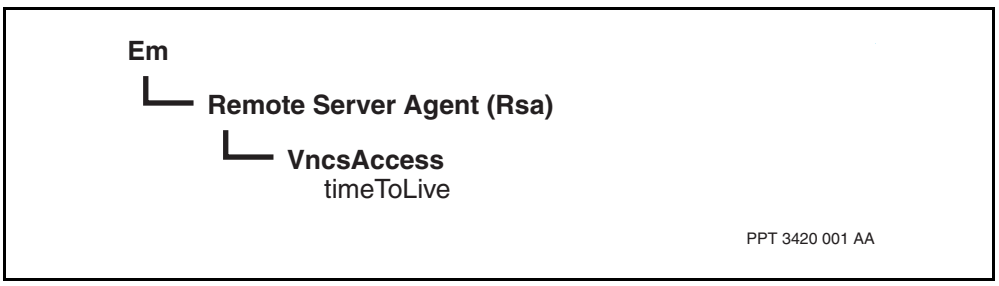
--End--

Variable definitions

Variable	Value
<rsa_name>	is the name assigned to this instance of the *Rsa* component.
<timeToLive_seconds>	*is the timeToLive* attribute value, from 1 to 5 seconds. The default value is 2 seconds.

Procedure job aid

VncsAccess component hierarchy



Operations and maintenance

This chapter describes how to maintain and control the Remote Server Agent (RSA).

Navigation

Attention: For information on commands, see NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

Operational mode states

The operational states are listed in following tables, Operational states reported by the Rsa component (page 10), and Operational states reported by the VncsAccess component (page 11).

Operational states reported by the Rsa component

Operational states reported	Details
administrativeState: unlocked operationalState: disabled usageState: idle	This state is valid when the RSA has failed to activate properly due to a lack of resources.
administrativeState: unlocked operationalState: enabled usageState: idle	This state combination is transient. It is valid when the RSA changes its operational state from disabled to enabled.
administrativeState: unlocked operationalState: enabled usageState: active	This state is valid when the RSA is fully operational with free LCNs available for RSI connections. This is the normal state for the Rsa component.
administrativeState: unlocked operationalState: enabled usageState: busy	This state is valid when the RSA not longer has any free LCNs available for RSI connections; but it is operational.

Operational states reported by the VncsAccess component

Operational states reported	Details
administrativeState: unlocked operationalState: disabled usageState: idle	This state is valid when the *VncsAccess* component is unable to locate the VNCS. This can be caused by the VNCS not being provisioned or during a CP switchover.
administrativeState: unlocked operationalState: enabled usageState: idle	This state combination is transient. It is valid when the *VncsAccess* component changes its operational stated from disabled to enabled.
administrativeState: unlocked operationalState: enabled usageState: active	This state is valid when the *VncsAccess* component can locate the VNCS and is able to forward translations. This is the normal state for the VncsAccess component.

Maintenance

This section provides guidelines on how to solve problems that may occur after the RSA is operational. This section contains the following information:

- Alarms (page 11)
- Handling problems (page 13)

Alarms

It is possible that after the RSA is operational, alarms may appear at the user interface to indicate faults or failure conditions on the node.

Alarms are generated asynchronously by Nortel Multiservice Switch 7400 components. When a component generates an alarm, it does so to signal one of the following:

- It is in need of repair.
- It has detected a fault elsewhere on the node.

Alarms contain a relatively large amount of information, which assist you in the monitoring and surveillance of the network. The figure Example of an alarm as it appears on the text interface (page 12), shows an example of an alarm. Because alarms are such an important and integral part of Multiservice Switch 7400 fault management, they are described separately in their own document, NN10600-500 *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*.

When do alarms occur?

As a general rule, expect to see an alarm in the following situations:

- degradation or quality-of-service conditions (for example, if a threshold is reached)
- processing errors (for example, protocol violations)

- failures or out-of-service conditions (for example, hardware or facility failures)
- engineering alarms (out of memory)

Example of an alarm as it appears on the text interface

```
      Rsa/8 VncsAccess; 1997-08-27 14:51:42.22
SET critical communications commSubsystemFailure  7050001
      ADMIN: unlocked   OPER: disabled    USAGE: idle
      AVAIL:      PROC:       CNTRL:
      ALARM:      STBY: notsetUNKNW: false
      Id: 08000003 Rel: Lp/8
      Com: The RSA cannot access the VNCS server.
           Server requests are discarded.
      Int: 8/1/3/8224; vncsIf.cc;374; p4.2d.14



      Rsa/8 VncsAccess; 1997-08-27 14:53:55.32
CLR cleared communications commSubsystemFailure 7050001
      ADMIN: unlocked   OPER: disabled    USAGE: active
      AVAIL:      PROC:       CNTRL:
      ALARM:      STBY: notsetUNKNW: false
      Id: 08000004 Rel:
      Com: The RSA is able to access the VNCS server.
           Int: 8/1/3/8224; vncsIf.cc;374; p4.2d.14
```

PPT_2210_001_AA

RSA alarms

There are four RSA-specific alarms.

- 7050 0001 - The Remote Server Agent cannot forward a request to the VNCS. While this alarm is set, all request for the VNCS are discarded. A clear is issued when the first request is successfully forwarded to the VNCS.
- 7050 0002 - The LAPF transmit queue has exceeded a 300 frame maximum and all frames from the queue are purged.
- 7050 0003 - The LAPF transmit queue has been purged due to a peer LAPF reset.
- 7050 0004 - The RSA has received a request for an unknown server. The request is discarded.

Handling problems

The table Handling problems (page 13), provides guidelines on how to respond to problems that may occur when using the RSA. This table contains three columns. The first column describes the problem, the second column provides a possible cause for that problem, and the third column explains how to correct the problem.

Problems that occur when your service is up and running may not be confined to the *Rsa* components only.

Handling problems

Problems that may occur	Possible cause	Corrective measures
The RSI call fails to connect or clears unexpectedly. The RSI reports the cause of the most recent failure as a decimal number and its hexadecimal equivalent.	No route to destination (RSI cause 3, 03 Hex)	Verify that the RSI is correctly provisioned with the DNA of the RSA. Verify that the path to the RSA is enabled (MPANL, trunks).
	User busy (RSI cause 17, 11 Hex)	The RSA already has 1000 RSI connections established. Provision this connection to another RSA.
	Destination out of order (RSI cause 27, 1B Hex)	The RSA has cleared the call because it is out of memory. Address a memory issue as detailed in problem 5. The RSA has cleared the call because the RSA is being deleted. Provision the RSI calls to another RSA.
	Switching congestion (RSI cause 42, 2A Hex)	Verify that the path to the RSA is enabled (MPANL, trunks).
	Service not implemented (RSI cause 79, 4F Hex)	Contact your local Nortel Networks Networks technical support group.
	User not member of CUG (RSI cause 87, 57 Hex)	Verify that the RSI is provisioned in the same CUG as the RSA.
	Protocol error (RSI cause 111, 6F Hex)	Contact your local Nortel Networks Networks technical support group.
The RSA cannot access the VNCS. Alarm 7050 0001 is generated.	The VNCS is not provisioned.	Provision the VNCS on the CP.
	The CP is in a switchover.	No action is required. The alarm clears when the VNCS accepts requests.

(1 of 2)

Handling problems (continued)

Problems that may occur	Possible cause	Corrective measures
The RSA does not reply to VNCS translation requests.	The RSA is overloaded with VNCS requests and is forced to discard those requests that have been queued longer than the *timeToLive* attribute value.	Re-engineer the RSA to decrease the combined traffic from its connections. This involves configuring an additional RSA in the network and provisioning some of the connections to this new RSA.
The RSA connection resets frequently. Alarms 7050 0002 and 7050 0003 are generated.	The RSA connection is congested.	Re-engineer the RSA as detailed in the corrective measure of problem 3.
	Software error	Contact your local Nortel Networks Networks technical support group.
The RSA fails to activate properly. An engineering alarm is generated and the RSA OSI state becomes unlocked, disabled and idle.	The RSA FP is low on memory.	Provision the RSA on a stand-alone FP or upgrade the RSA FP to a PM2.

(2 of 2)

Remote server agent fundamentals

This chapter provides a fundamental overview of the Remote Server Agent (RSA).

Navigation

What is an RSA?

The Remote Server Agent (RSA) is an entry point for applications requiring access to Nortel Multiservice Switch servers.

How is the RSA used?

The RSA provides access to the Nortel Multiservice Switch Voice Networking Call Server (VNCS) by the Passport 4400 access units such that 4400-based voice applications can interwork with the Nortel Multiservice Switch network.

How is the RSA accessed?

The RSA is accessed through the Remote Server Interface (RSI) on a Passport 4400 unit over a frame relay switched virtual circuit (SVC) connection. The RSA can reside anywhere in the network. For load sharing and backup purposes, there can be multiple RSAs located in the network.

This document only deals with the Nortel Multiservice Switch 7400 part of server access by Passport 4400 units.

Why you need an RSA

The RSA provides the following benefits:

- access to the VNCS for voice applications on nodes permitting voice interworking between Passport 4400 units and other Nortel Multiservice Switch nodes
- a centralized access to the servers

- freedom of location in the network; it is not restricted to modules that support the applications that require access to the RSA services
- load sharing and backup capabilities through a multiple RSA configuration

RSA features

The following sections detail the features of the RSA:

System capabilities

The RSA has the following system capabilities:

- resides on a V11 or V35 FP or CFP1 on the Nortel Multiservice Switch node
- supports a maximum of 1000 RSI connections where RSA is on a dedicated V.11 or V.35
- supports a maximum of 100 RSI connections on a CFP1
- can be distributed in the network (for loadsharing and backup)
- provides access to the VNCS
- can handle up to 100 VNCS translations per second

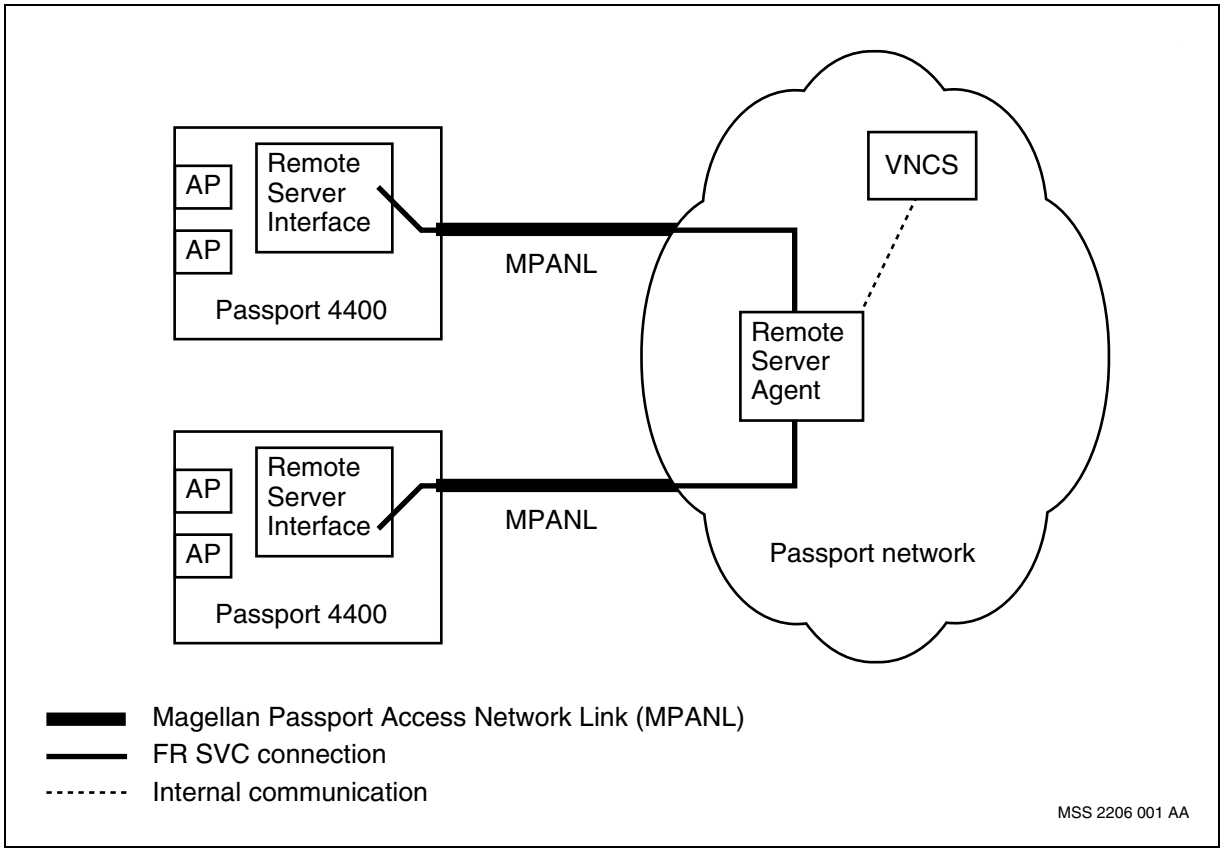
System overview

The RSI is an interface located on a Passport 4400 unit that communicates with the RSA to gain access to the Multiservice Switch 7400 servers. There can be a maximum of one thousand RSIs communicating with a single RSA at the same time. The RSI communicates with the RSA over a semi-permanent frame relay switched virtual circuit (FR SVC) connection. This connection is considered semi-permanent because it is set up only once and then it is used for all server requests and replies between the RSI and the Multiservice Switch 7400 servers.

It is recommended that the RSA be provisioned on a dedicated V11 or V35 function processor (FP) on the Nortel Multiservice Switch node.

The figure Passport 4400 units to VNCS access (page 17), shows the system architecture for units accessing the VNCS.

Passport 4400 units to VNCS access



Frame relay SVC connection establishment

The RSA is identified by a unique Data Network Address (DNA). The RSI is provisioned with this DNA in order to initiate the FR SVC call establishment using standard Q.933 signalling procedures.

When there is a failure, the RSI is responsible for the call re-establishment. The RSI reports the cause information element (IE) from the Q.933 release message of the last unsuccessful FR SVC connection attempt for troubleshooting purposes.

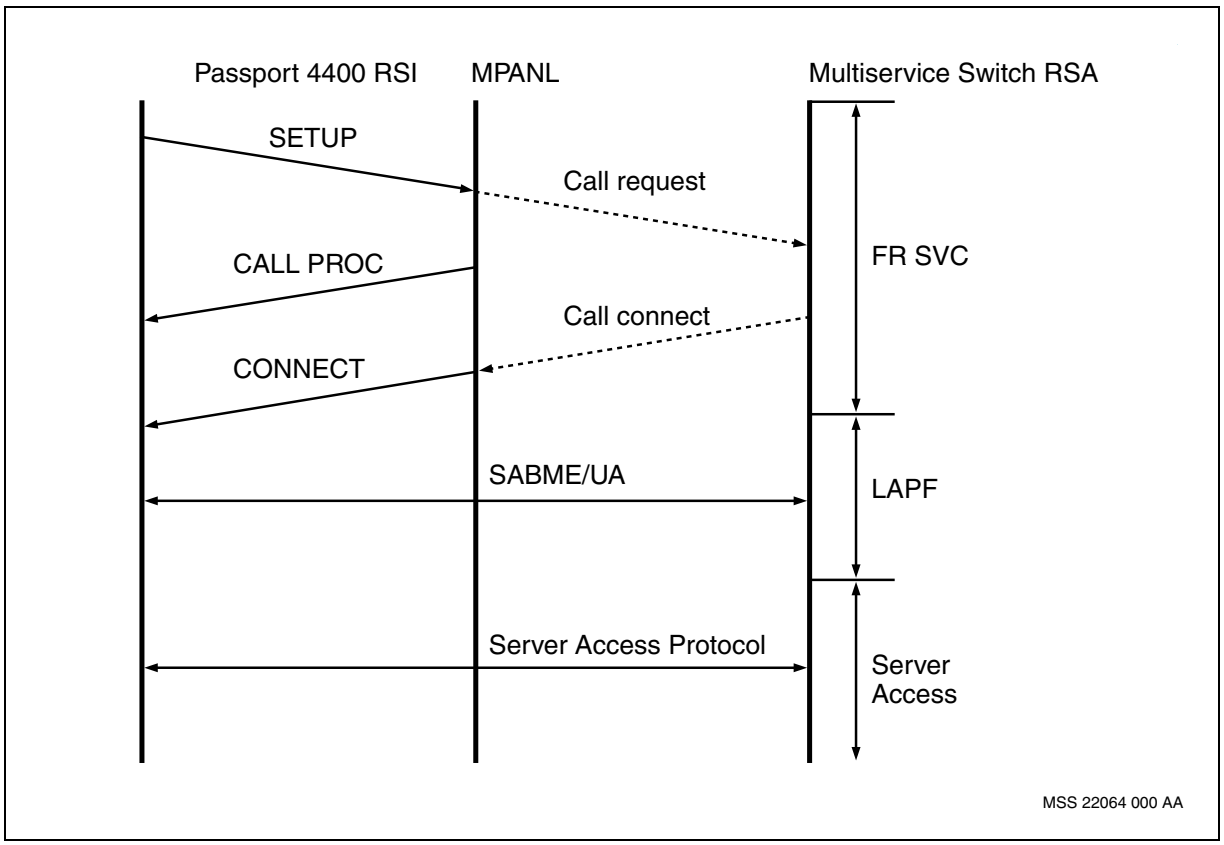
As an optional security feature, a single Closed User Group (CUG) or multiple CUGs can be provisioned on the RSA. If this option is required, then the RSI must also be provisioned with a matching CUG in order for the FR SVC to connect.

The RSI identifies itself to the RSA by providing an optional identification string in the user-user IE of the setup message. This string is displayed by the RSA as part of the *DteComponentName* attribute.

To provide a reliable RSI to RSA SVC connection, Link Access Procedure Frame (LAPF) protocol is run on top of the FR SVC.

The figure Connection establishment (page 18), shows the time line diagram for the connection establishment between the RSI on a Passport 4400 unit and the RSA on a node in the Nortel Multiservice Switch network.

Connection establishment

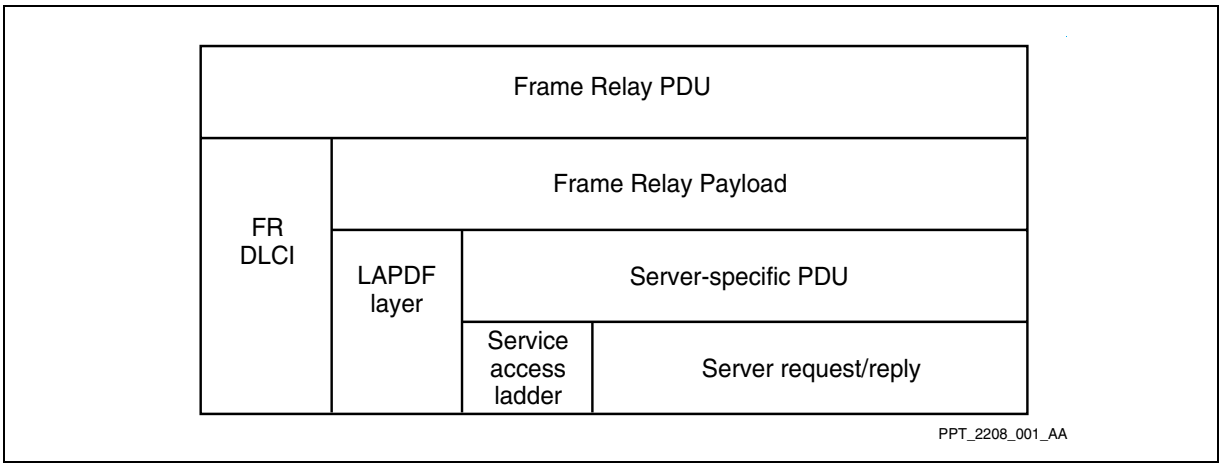


Server access protocol

Individual server requests and replies are formatted by the RSI and the server respectively. A server access header is added by the RSI, or the server, to form a server-specific Protocol Data Unit (PDU).

The server-specific PDU is then encapsulated in a LAPF I-frame and sent over the FR SVC connection. See the figure Frame relay PDU (page 19), for details.

Frame relay PDU



LAPF layer

The LAPF protocol is normally defined over a frame relay link; for the RSI connection, it includes the virtual circuit (VC) and the frame relay or MPANL link. See the table LAPF system parameters (page 20), for a list of the LAPF parameters and their values.

The RSI on a Passport 4400 unit initiates the SABME/UA exchange with its peer on the Nortel Multiservice Switch 7400 RSA as soon as the FR SVC connection is established. After the SABME/UA exchange is complete, the RSI on a Passport 4400 unit and the Multiservice Switch 7400 RSA can start exchanging data using LAPF I-frames.

If the LAPF protocol experiences an unrecoverable error condition, an alarm is issued. The error should not impact the operation of the FR SVC call, except that there may be some lost messages. Once the LAPF protocol recovers after another SABME/UA exchange, server transactions can be resumed.

LAPF system parameters

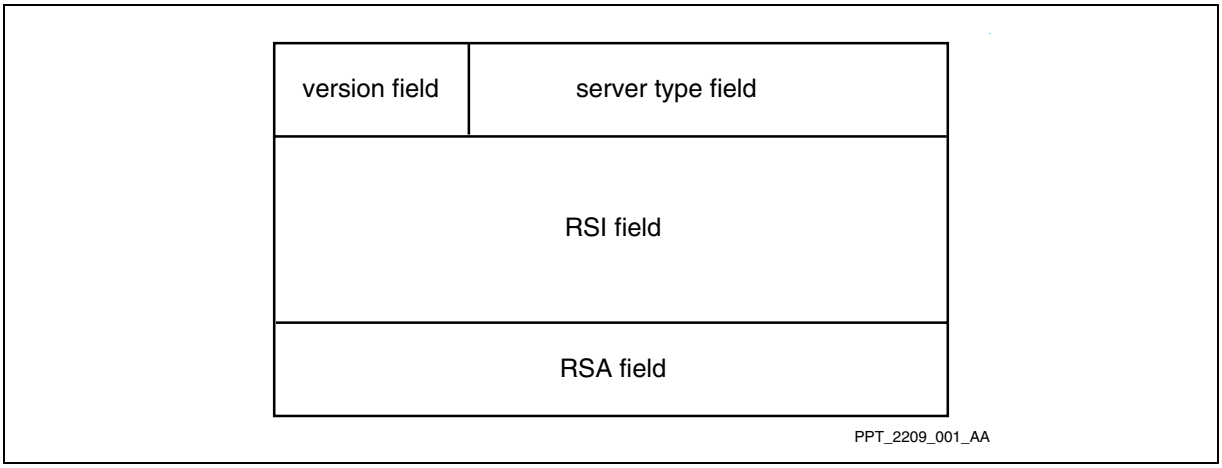
System parameter	Default value	Meaning
T200	1.5 seconds	This parameter is the retransmission (T200) timer. It is started after the transmission of a command frame that requires a response. It stops when the RSA receives the response. If this timer expires, the command frame is retransmitted.
N200	3 retransmissions	This parameter is the maximum number of retransmissions. After each T200 timer expiry, a frame is retransmitted. The number of times a frame can be retransmitted is specified by this parameter. If this parameter is exceeded, the LAPF connection is reset.
N201	4096 octets	This parameter specifies the maximum number of octets in an information field. Frames received with an information field size greater than this parameter are discarded.
k	7 frames	This parameter is the maximum number of unacknowledged I-frames allowed. This is the LAPF window size. If the window closes, transmission of the I-frames stops until an acknowledgment is received.
T203	30 seconds	This parameter is the idle timer. It detects the loss of the peer LAPF at the other end of the connection. If this timer expires, the LAPF connection is reset.

Server access header

The server access header provides multiplexing capabilities between the RSA and multiple RSI VCs. The server access header is shown in the figure Server access header format (page 21). This header is included in all server-specific PDUs passed between the RSI, the RSA, and the server in both directions.

For the VNCS, the server access header in the translation request is transparently prepended in front of the reply message by the VNCS.

Server access header format



The server type field is a 5-bit field that identifies the server type to which the server-specific PDU is destined. Currently, only one server type is supported (01 = VNCS).

The version field is a 3-bit field that identifies the server access header version. The initial version is set to 0.

The RSI field is a 32-bit field and is used by the RSI. It is passed transparently by the RSA and for transaction-oriented servers (like the VNCS), it is returned unmodified in the reply message.

The RSA field is a 16-bit field dedicated for RSA use.

Server-specific (VNCS)

The VNCS protocol is a simple request and reply protocol that queries the VNCS dialing plan database based on the dialed number. For details on VNCS, see NN10600-755 *Nortel Multiservice Switch 7400 Operations: Voice Networking*.

The VNCS must be provisioned on the same node as the RSA and the RSA must be provisioned with the *VncsAccess* subcomponent.

The *VncsAccess* subcomponent maintains statistics for the number of translation requests sent to the VNCS and the corresponding number of replies received from the VNCS. It also maintains statistics for the number of translation requests queued and discarded. Under normal, uncongested operation, the number of requests equals the number of replies. The number queued is small, and the number discarded is zero.

VNCS translation requests are queued by the RSA and forwarded in a controlled manner to the VNCS. This throttling mechanism ensures that requests that have been in the RSAs queue for a long time (due to congestion) are never sent to the VNCS. The requesting RSI has probably given up waiting for the reply. The RSA discards requests from its queue that are older than the provisioned *timeToLive* attribute (default is 2 seconds). To provision the *timeToLive* attribute, see Configuring the VncsAccess component (page 9).

For the VNCS, it is recommended that the maximum combined load from all RSI connections does not exceed 100 translations per second to avoid congestion.

Exception handling conditions

Although LAPF provides reliability for the FR SVC connection between the RSI and the RSA, messages can still be lost. The application is responsible for recovering from lost message conditions. Messages can be lost under the following conditions:

- The RSA queue to the server is congested.
- The server itself is congested.
- The FR SVC is congested.
- The FR SVC disconnects.
- ALAPF unrecoverable error occurs.
- The RSA cannot locate the specified server.

If the RSA cannot locate the specified server, an alarm is generated. The alarm is cleared on the next successful access to the same server. For details on RSA alarms, see Operations and maintenance (page 10) and NN10600-500 *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*.

CP switchover considerations

The RSA supports CP switchover. Access to the VNCS may be temporarily disrupted while the switchover is in progress. Failure to access the VNCS in this case is handled in the same manner as the general error when a server cannot be accessed.

Loadsharing and backup

For loadsharing or regionalization, multiple RSAs can be provisioned in the Nortel Multiservice Switch network.

For backup, at least two RSAs are provisioned on separate nodes to allow recovery from a node or LP failure. The RSI is provisioned with the DNAs of the primary and backup RSAs and establishes a connection to the primary RSA. If this call fails, the RSI establishes a connection to the backup RSA.

Semantic checks

The following semantic checks are performed for the RSA:

- A semantic check verifies that at least one server access subcomponent (for example, the *VncsAccess* subcomponent) is provisioned under the RemoteServerAgent component. This semantic check is run when a server access subcomponent is deleted.
- A semantic check verifies that VNCS is provisioned when the *VncsAccess* component is provisioned. This check is run whenever the *VncsAccess* component is added.

Nortel Multiservice Switch 7400

Operations: Remote Server Agent

Publication: NN10600-765
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