NORTEL NETWORKS

Passport 7400

Remote Server Agent Guide

241-7401-765

Passport 7400

Remote Server Agent Guide

Publication: 241-7401-765
Document status: Standard
Document version: 5.2S1
Document date: November 2003

Printed in Canada

Publication history

November 2003

5.2S1 Standard
General availability. Contains information on Passport 7400 for the PCR5.2 GA release.

Contents

List of figures

List of tables

About this document

This document describes the Remote Server Agent (RSA) for the Passport system.

The following topics are discussed in this section:

Who should read this document

This document is intended for those who use the Passport 4400 access units for voice service and need an overview of the RSA. It is also intended for those personnel responsible for one or more of the following tasks on a Passport 7400 product that has the RSA:

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

What you need to know

Before you read this document, you should be familiar with fundamental data communications, particularly general principles of packet switching, and switching communication products. You should also read 241-5701-030 *Passport 7400, 15000, 20000 Overview*.

For installation procedures

If you are performing the installation procedures in this document, you should have one to two years of experience installing services. You must be familiar with installation techniques and terminology. You must also be aware of all pertinent electrical and physical safety procedures and standards.

For provisioning procedures

If you are performing provisioning procedures, Nortel Networks recommends that you have at least one to two years experience in your field. You should read NN10600-605 *Passport - MDM Network Security: Operations* and refer to document 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

How this document is organized

The 241-7401-765 *Passport 7400 Remote Server Agent Guide* contains the following information about the RSA:

- “RSA configuration” (page 17) provides the installation and provisioning procedures for the Remote Server Agent.
- “Remote server agent fundamentals” (page 25) introduces the RSA and describes its features and benefits.
- “Operations and maintenance” (page 37) provides the common operational mode commands and examples of how these commands are used to monitor the RSA.

What’s new in this document

There were no new features added to this document.

This document was restructured into a modular, task-based format to improve the usability of the information. The following changes were made to this document:

- Procedures were grouped into higher-level tasks.
- Task flow charts were added to improve navigation through tasks and procedures, to set tasks and procedures in context, and to provide a visual representation of prerequisites and configuration paths.
- Procedures were restructured into a modular format.
- Purpose statements were added to tasks and procedures to provide context.
- Prerequisites were divided into those applicable to an entire task. those applicable only to a specific procedure, and those applicable only to a specific procedure step. Prerequisites applicable to an entire task were placed in the appropriate task-level prerequisite section, prerequisites applicable only to a specific procedure were placed in the perquisites section of the procedure, and prerequisites applicable only to a specific step were placed in the step.
- 'Where' statements were removed from procedures and the content placed in the 'Variable values' table following the procedure.
- A 'Procedure Job Aid' section was added to procedures where appropriate. This consists of information that supports the procedure, such as a component hierarchy figure, a checklist, or a diagram.
- Conceptual and reference information were removed from procedures, placed in the appropriate conceptual or reference section, and cross-referenced from the procedure where appropriate.

Conventions

There are a number of documentation conventions you should know about.

- `nonproportional spaced plain type`

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

- **nonproportional spaced bold type**

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

- *italics*

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

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

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

- `<general_term>`

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

- UPPERCASE, lowercase

  Passport 7400 commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string option values (for example, file and directory names) and string attribute values.

- |

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

- ...

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

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

Related documents

For the complete list of documents contained in the Passport document library, see 241-5701-001 *Passport 7400, 15000, 20000 Documentation Guide*.

Passport references

It may be necessary for you to refer to the following documents to install, provision, and operate the RSA in your network:

- 241-5701-030 *Passport 7400, 15000, 20000 Overview*
- NN10600-605 *Passport - MDM Network Security: Operations*
- 241-7401-480 *Passport 7400 Multiservice Passport Access Network Link Guide*
- 241-7401-755 *Passport 7400 Voice Networking Guide*
- 241-5701-060 *Passport 7400, 15000, 20000 Components*
- 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*

How to get more help

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

Chapter 1
RSA configuration

With exceptions such as addresses, you can configure RSA using default settings provided with the package or you can configure it to meet specific requirements that you may have.

Prerequisites to RSA configuration

It is assumed that the following installation and provisioning steps have been completed before provisioning RSA:

- The Passport system has been installed, powered up, and commissioned.
- The Passport control processors and function processors have been installed according to 241-7401-240 *Passport 7400 Hardware Installation, Maintenance and Upgrade*.
- The number of RSAs required in the network to handle the Passport 4400 units is determined.
- VNCS is provisioned on the Passport node. See 241-7401-755 *Passport 7400 Voice Networking Guide*.

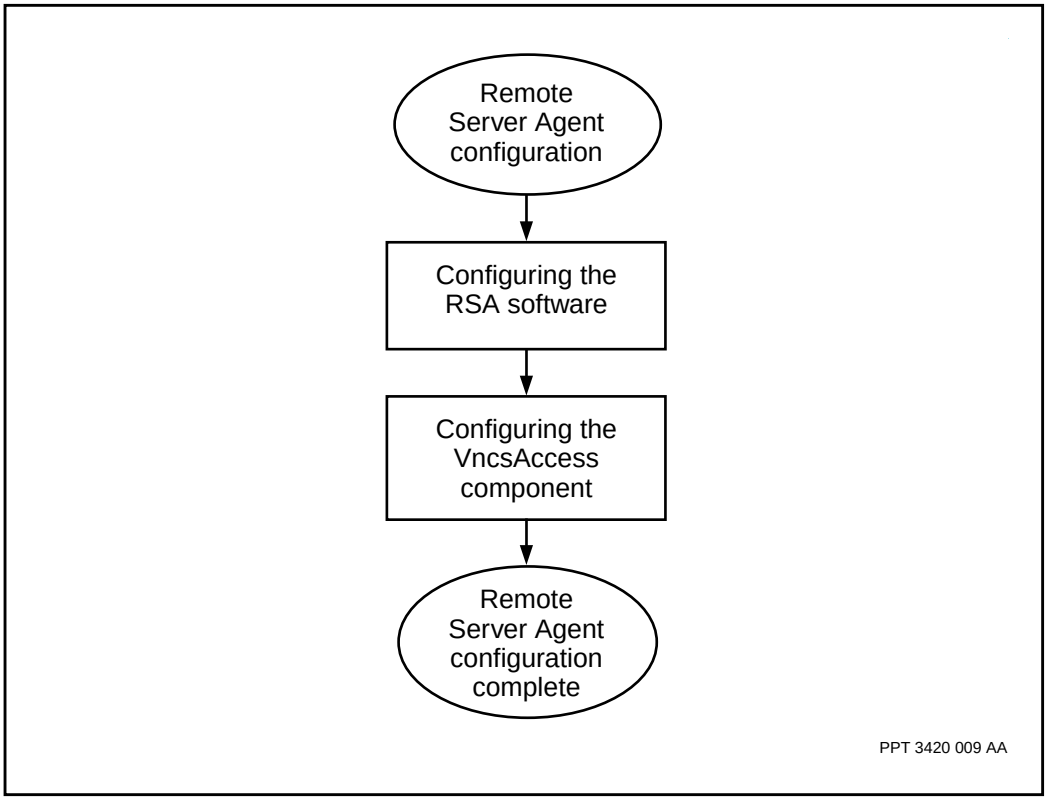
Other prerequisites are

- If you choose to provision attributes associated with the service, be sure that you understand what each attribute does. Default values can be viewed using the online help for the components and attributes. Detail on components and attributes can be found in 241-5701-060 *Passport 7400, 15000, 20000 Components*.
- For basic provisioning information, see NN10600-605 *Passport - MDM Network Security: Operations*.
- Your user ID must have a command impact of at least configuration to perform the provisioning procedures in this section.
- If access to the VNCS is required, the VNCS and the RSA must be provisioned on the same Passport node. See the provisioning procedures in 241-7401-755 *Passport 7400 Voice Networking Guide*.

RSA configuration flow

"RSA configuration task flow" (page 19) shows you the sequence of tasks and procedures you perform to configure RSA. To link to any task or procedure, go to "Task navigation" (page 19).

Figure 1
RSA configuration task flow



Task navigation

- “Configuring the RSA software” (page 20)
- “Configuring the VncsAccess component” (page 22)

Configuring the RSA software

Perform the initial configuration and set the attributes of the RSA software.

Procedure steps

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*).

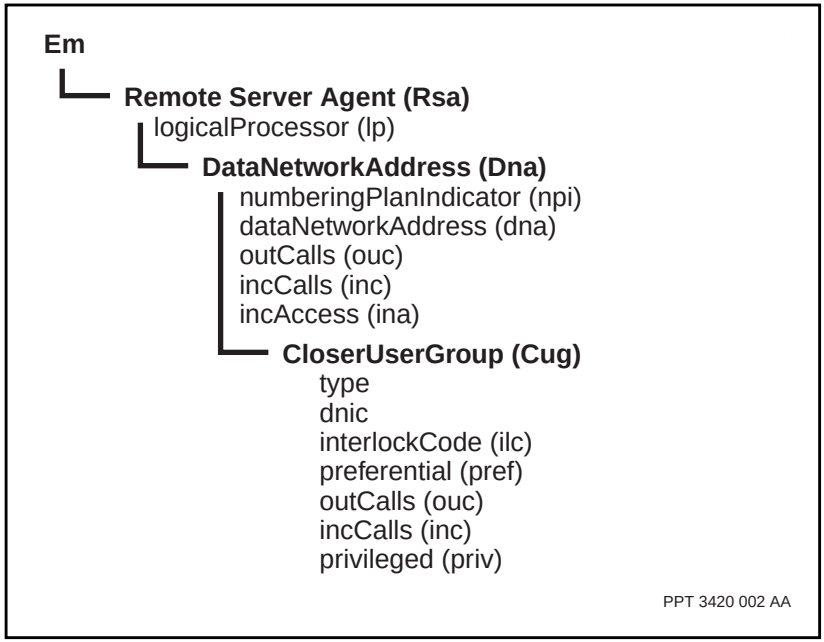
   ```
   set Rsa/<rsa_name> Dna Cug/<cug_number> interlockCode
   101
   ```

Variable definitions

Variable	Definition
<cug_number>	The CUG index range is from 0 to 255.
<dna>	The value of the dna attribute.
<lp_number>	The instance number of the LP.
<rsa_name>	The name assigned to this instance of the Rsa component.

Procedure job aid

Figure 2
Configuring the RSA software component hierarchy



Configuring the VncsAccess component

Configure the RSA to access the VNCS so that voice interworking can occur between Passport 4400 access units and other nodes in the Passport network.

Prerequisites

- For details on provisioning VNCS to support voice interworking with Passport 4400 units, see 241-7401-755 *Passport 7400 Voice Networking Guide*.

Procedure steps

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>
```

Variable definitions

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

Procedure job aid

Figure 3
Configuring access to servers component hierarchy

Chapter 2
Remote server agent fundamentals

This section introduces the Remote Server Agent (RSA) and provides the following information:

What is an RSA?

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

How is the RSA used?

The RSA provides access to the Passport Voice Networking Call Server (VNCS) by the Passport 7400 4400 access units such that Passport 4400-based voice applications can interwork with the Passport 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.

Note: This document only covers the Passport 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 Passport 4400 units permitting voice interworking between Passport 7400 4400 units and other Passport nodes
- a centralized access to the Passport 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 Passport 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

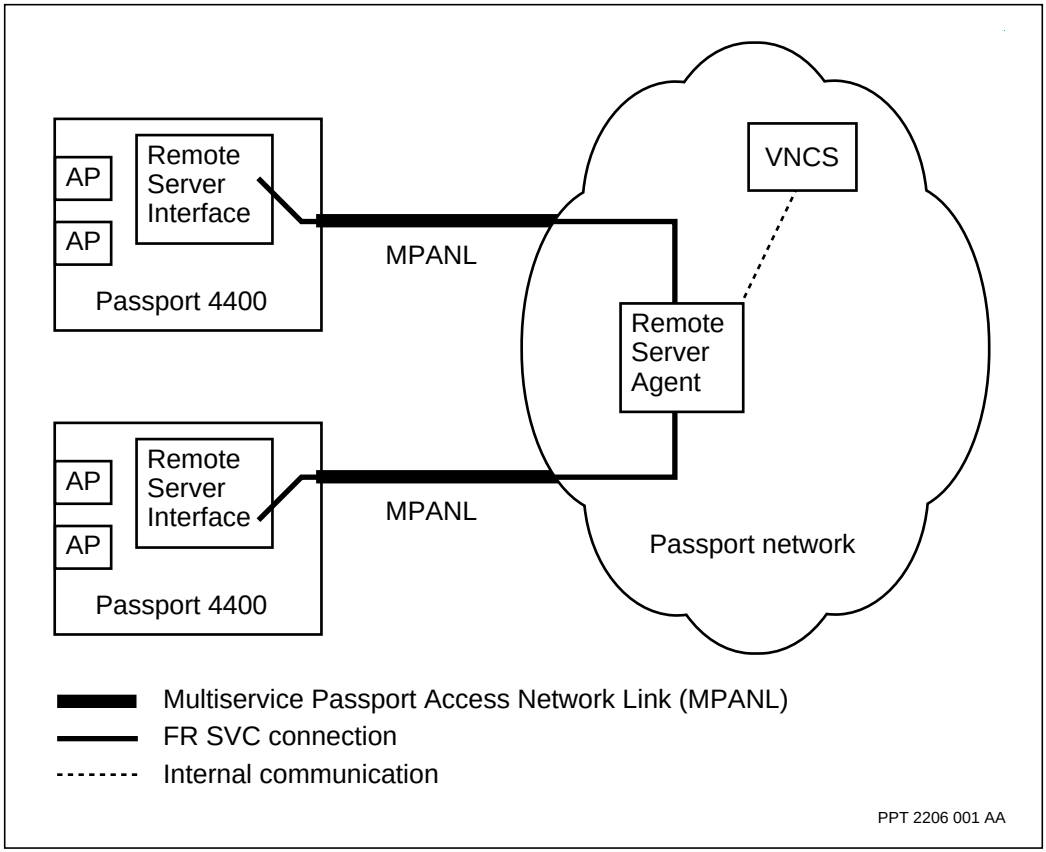
System overview

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

The RSI is an interface located on a Passport 7400 4400 unit that communicates with the RSA to gain access to the Passport 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 Passport 7400 servers.

The figure“Passport 4400 units to VNCS access” (page 28) shows the system architecture for Passport 7400 4400 units accessing the VNCS.

Figure 4
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.

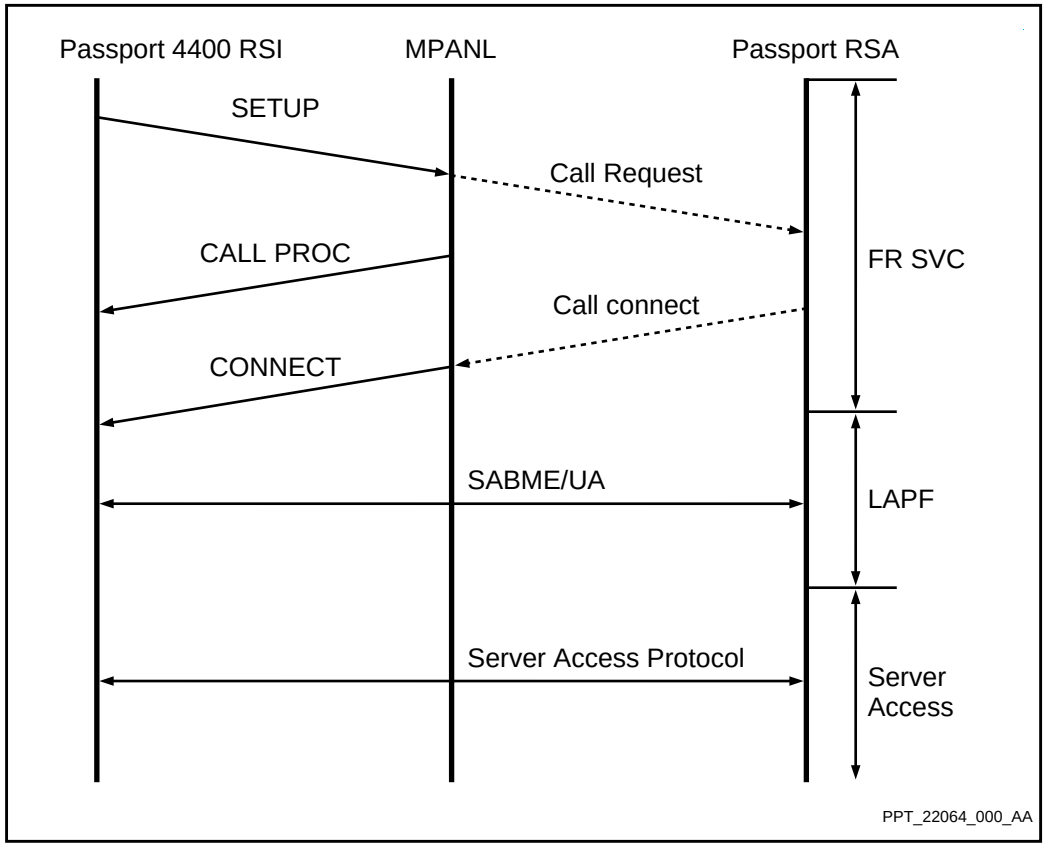
As an optional security feature, a single Closed User Group (CUG) or multiple CUGs can be provisioned on the RSA. If this option is required, then the RSI must also be provisioned with a matching CUG in order for the FR SVC to connect.

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" on page 22 shows the time line diagram for the connection establishment between the RSI on a Passport 7400 4400 unit and the RSA on a node in the Passport network.

Figure 5
Connection establishment

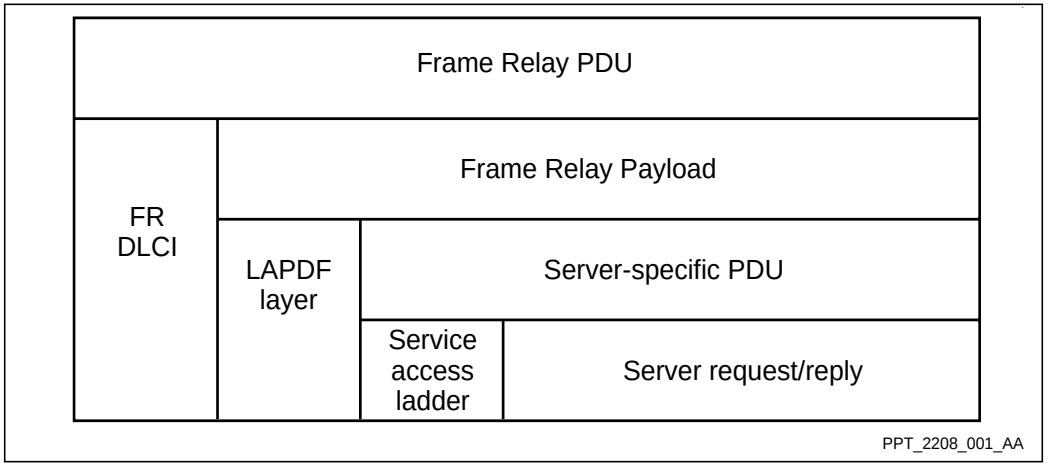


Server access protocol

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 31) for details.

Figure 6
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 32) for a list of the LAPF parameters and their values.

The RSI on a Passport 7400 4400 unit initiates the SABME/UA exchange with its peer on the Passport 7400 RSA as soon as the FR SVC connection is established. Once the SABME/UA exchange is complete, the RSI on a Passport 7400 4400 unit and the Passport 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.

Table 1
LAPF system parameters

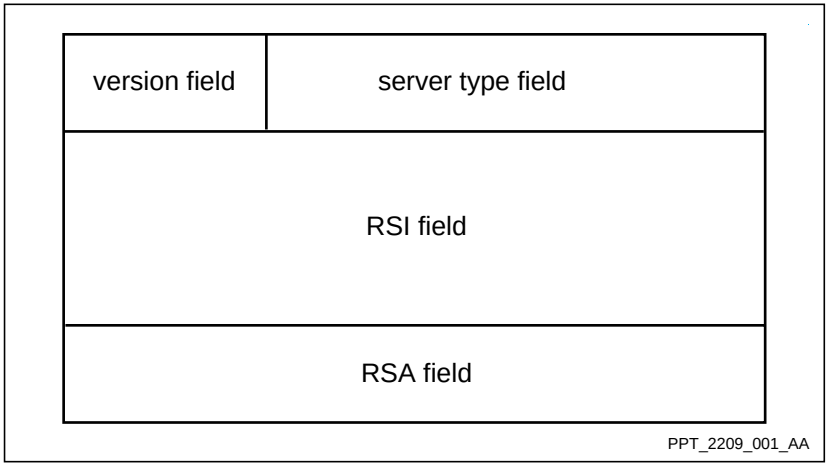
System parameter	Default value	Meaning
T200	1.5 seconds	This parameter is the retransmission (T200) timer. It is started after the transmission of a command frame that requires a response. It stops when the RSA receives the response. If this timer expires, the command frame is retransmitted.
N200	3 retransmissions	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 figure “Server access header format” (page 33). This header is included in all server-specific PDUs passed between the RSI, the RSA, and the server in both directions.

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

Figure 7
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 241-7401-755 *Passport 7400 Voice Networking Guide*.

The VNCS must be provisioned on the same Passport 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 22).

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 37) and 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

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 Passport 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.

RSA components and attributes

The table "RSA components" (page 35) describes RSA-specific components.

Table 2
RSA components

Component name	Description
Rsa	The *RemoteServerAgent* (Rsa) component provides access to Passport servers.
VncsAccess	The *VncsAccess* component is provisioned on RSA modules that provide access to the VoiceNetworkingCallServer (Vncs) application.
Connection	The operational *Connection* component is created for each RSI to RSA connection.
RsaDataNetworkAddress	The RSA local DNA is used for incoming calls.
RsaClosedUserGroup	The RSA Closed User Group provides security by restricting access to the RSA.

Note: *A* component requirement for the RSA feature also includes the *Dn* component; it is a subcomponent of the *Vncs* component.

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.

Chapter 3
Operations and maintenance

This section describes the tasks necessary to maintain and control the Remote Server Agent (RSA). It should be read by people responsible for the installation and day-to-day operation of the RSA. It consists of information on:

- "Operational mode states" (page 37)
- "Maintenance" (page 39)

For information on commands, see 241-5701-050 *Passport 7400, 15000, 20000 Commands*.

Operational mode states

The operational states are listed in the table "Operational states reported by the Rsa component" (page 38) and the table "Operational states reported by the VncsAccess component" (page 38).

Table 3
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.

Table 4
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 what steps you can take to solve problems that may occur after the RSA is operational. After reading this section, you will understand how to respond to these problems. This section is divided into the following sections:

- "Alarms" (page 39)
- "Handling problems" (page 41)

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 Passport 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.

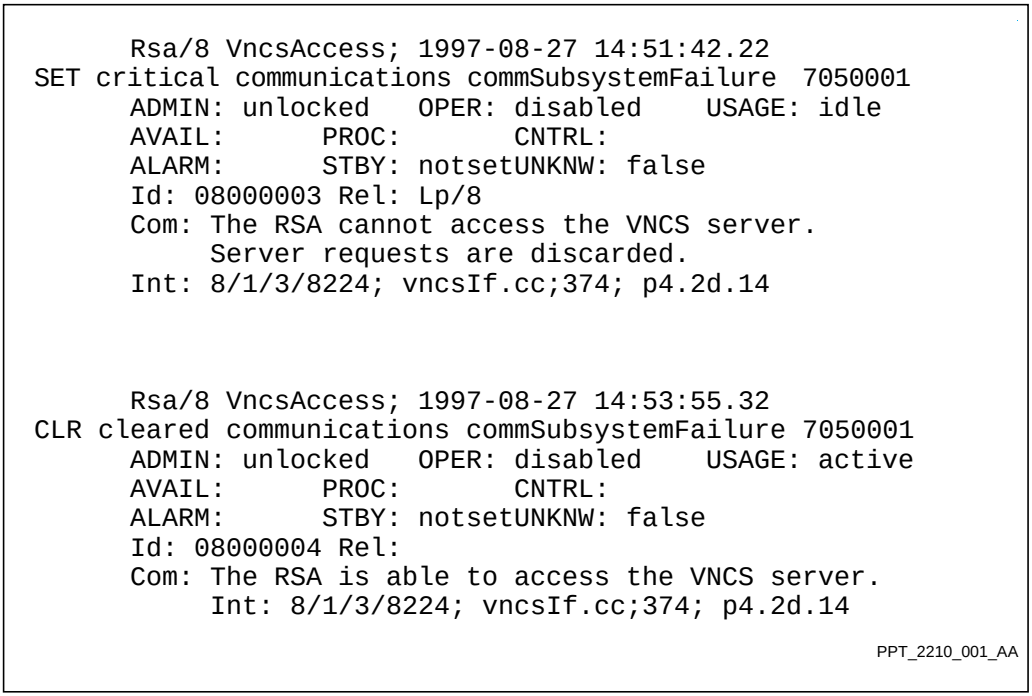
Alarms contain a relatively large amount of information; all of which assist you in the monitoring and surveillance of the network. The figure "Example of an alarm as it appears on the text interface" (page 40) shows an example of an alarm. Because alarms are such an important and integral part of Passport 7400 fault management, they are described separately in their own document, 241-5701-500 *Passport 6400, 7400, 15000, 20000 Alarms*.

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)

Figure 8
Example of an alarm as it appears on the text interface



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 41) 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.

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

Table 5
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.

(Sheet 1 of 2)

Table 5 (continued)
Handling problems

Problems that may occur	Possible cause	Corrective measures
	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.
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.

(Sheet 2 of 2)

Passport 7400
Remote Server Agent Guide

Release 5.2

Publication: 241-7401-765
Document status: Standard
Document version: 5.2S1
Document date: November 2003
Printed in Canada

NORTEL NETWORKS