>THIS IS **THE WAY**

>THIS IS **NORTEL**™

Nortel Multiservice Switch 7400/15000/20000

Security Management

NN10600-601

Document status: Standard
Document issue: 7.2S2
Document date: April 2006
Product release: PCR7.2 and up
Job Function: Administration and Security
Type: NTP
Language type: US English

Contents

What’s new

The following features were added to this document:

- Secure shell (Ssh) on Nortel Multiservice Switch 15000 and 20000 (page 6)
- IKE support for IPSec on Nortel Multiservice Switch 15000/20000 (page 6)
- Telnet or Ssh command logging (page 7)

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*.

Secure shell (Ssh) on Nortel Multiservice Switch 15000 and 20000

The following sections were updated for this feature:

- Multiservice Switch OAM security configuration (page 8)
- Adding a new userID (page 14)

The following sections were added for this feature:

- Configuring secure shell (Ssh) (page 78)
- Secure shell (Ssh) (page 106)

IKE support for IPSec on Nortel Multiservice Switch 15000/20000

The following sections were added for this feature:

- IP security configuration on a Multiservice Switch node procedures (page 42)
- Configuring an IKE proposal and policy on a Multiservice Switch 15000/20000 node (page 54)
- Configuring an IP security proposal and policy on a Multiservice Switch 15000/20000 node (page 59)

- Configuring a link between an IP security policy and an IKE policy on a Multiservice Switch 15000/20000 node (page 64)
- Example 1 of configuring IKE proposal and policy (page 66)
- Example 2 of configuring IP security proposal and policy for FTP traffic (page 68)
- Example 3 of configuring IP security proposal and policy for ICMP traffic (page 70)
- Example 4 of configuring IP security proposal and policy for UDP traffic (page 72)
- Example 5 of configuring the sample bypass policy for IKE traffic (page 74)
- Internet key exchange (page 99)
- Internet key exchange processing (page 99)
- Automated key management (page 104)
- Anti-replay (page 105)
- IP security and secure shell interworking (page 106)

The following sections were updated for this feature:

- Multiservice Switch OAM security configuration tasks (page 9)
- Configuring IP security manually on a Multiservice Switch node (page 44)

Telnet or Ssh command logging

The following sections were added for this feature:

- Telnet or Ssh command logging (page 109)
- Pre-login warning banner (page 108)

Multiservice Switch OAM security configuration

Use the Multiservice Switch operations, administration and maintenance (OAM) security configuration work flow to perform the tasks needed to configure the userID authentication method, create and change userIDs, and monitor and control user sessions.

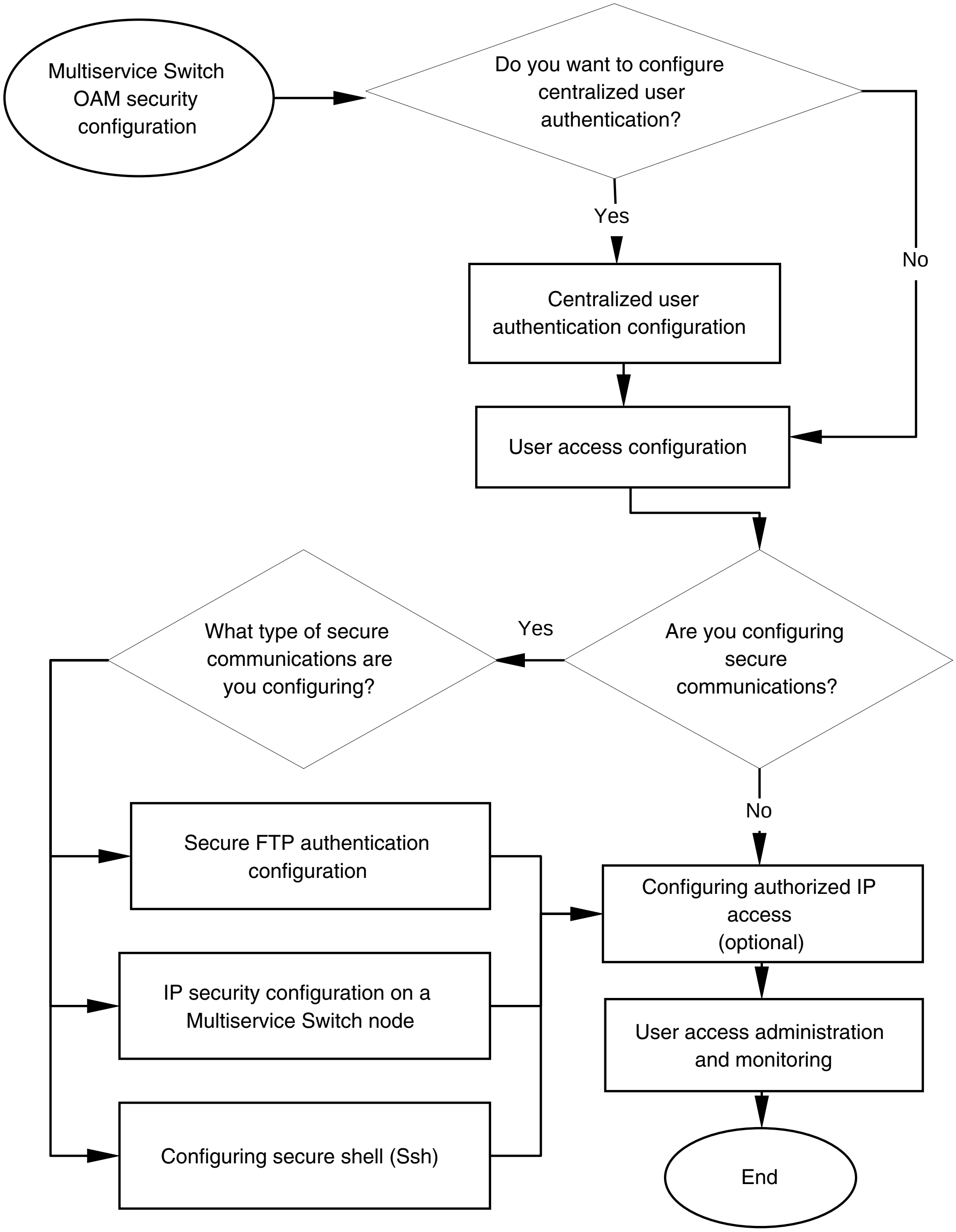
Prerequisites to Multiservice Switch OAM security configuration

- Install the base software. For more information, see NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*.
- If you need to understand the different ways of controlling user access, see Understanding user access (page 91).

Multiservice Switch OAM security configuration tasks

This work flow shows you the sequence of tasks you perform to configure Multiservice Switch OAM security. To link to any task, go to Multiservice Switch OAM security configuration task navigation (page 10).

Multiservice Switch OAM security configuration tasks


Multiservice Switch OAM security configuration
Do you want to configure centralized user authentication?
Yes
No
Centralized user authentication configuration
User access configuration
Are you configuring secure communications?
Yes
What type of secure communications are you configuring?
No
Secure FTP authentication configuration
IP security configuration on a Multiservice Switch node
Configuring secure shell (Ssh)
Configuring authorized IP access (optional)
User access administration and monitoring
End

MSS 3604 001 AD

Multiservice Switch OAM security configuration task navigation

User access configuration

Configure the user access to control user access to the Multiservice Switch from the Multiservice Switch itself.

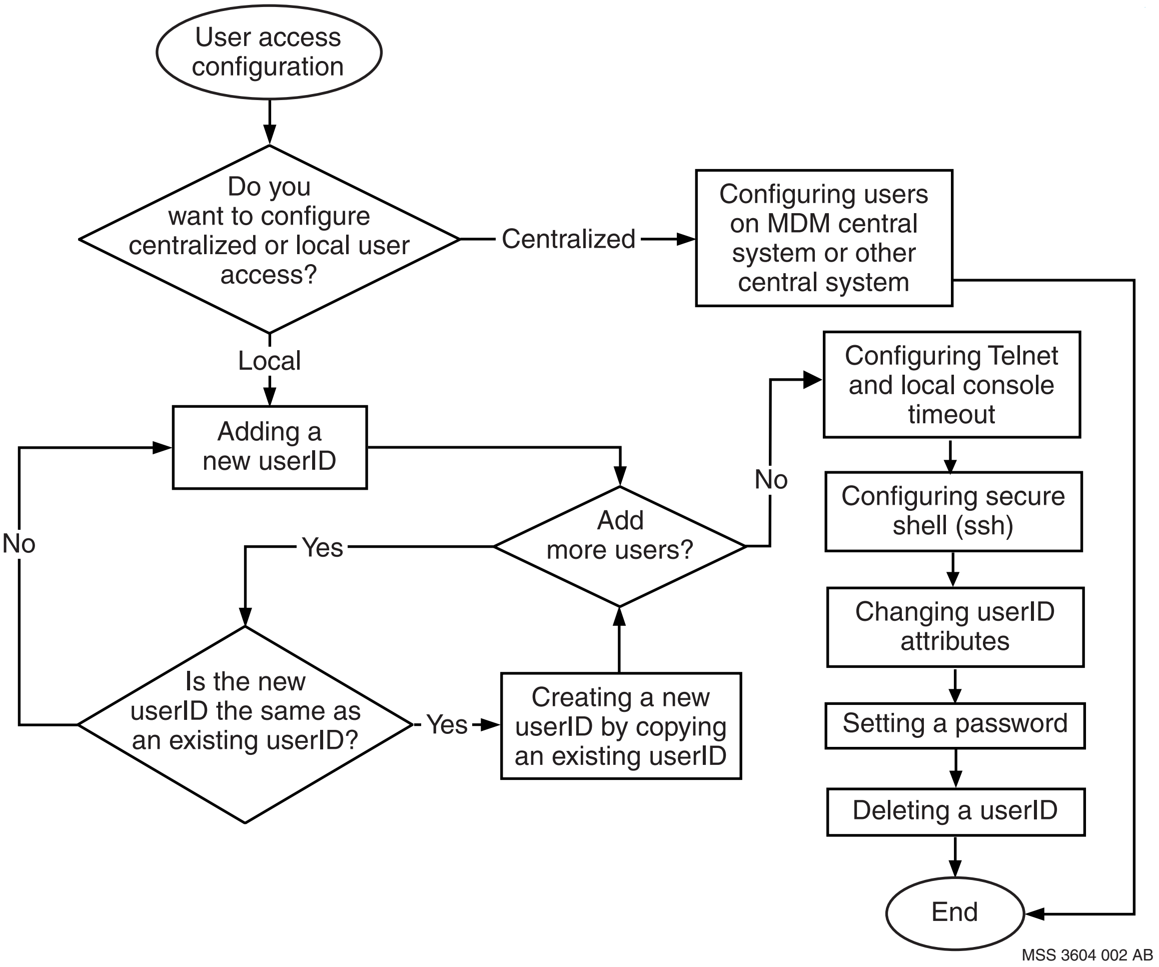
Prerequisites to user access configuration

- If you need to understand userID authentication, see Multiservice Switch userID authentication (page 91).
- To ensure absolute protection, use a local session or IP security (IPSec) when you set a password. When you are not using a local session or IPSec, the information you enter travels over the network in easy-to-read ASCII format.

User access configuration procedures

This task flow shows you the sequence of procedures you perform to configure user access. To link to any procedure, go to User access configuration procedure navigation (page 12).

User access configuration procedures


User access configuration
Do you want to configure centralized or local user access?
Centralized
Configuring users on MDM central system or other central system
Local
Adding a new userID
Add more users?
No
Yes
Configuring Telnet and local console timeout
Configuring secure shell (ssh)
Changing userID attributes
Setting a password
Deleting a userID
End
No
Is the new userID the same as an existing userID?
Yes
Creating a new userID by copying an existing userID
MSS 3604 002 AB

User access configuration procedure navigation

- Adding a new userID (page 14)
- Configuring users on MDM central system or other central system. For information on the Multiservice Data Manager (MDM) central system, see NN10400-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration* and NN10400-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*. For information on other central systems, see the documentation provided with that system.
- Creating a new userID by copying an existing userID (page 18)
- Configuring Telnet and local console timeout (page 20)
- Configuring secure shell (ssh) (page 22)

- Changing userID attributes (page 24)
- Setting a password (page 26)
- Deleting a user ID (page 28)

Adding a new userID

Add new userIDs to allow only those users to access the Multiservice Switch node. You can add new userIDs when you are setting up a new Multiservice Switch and any time after that.

Prerequisites

- Unless this is a new Multiservice Switch node, you must be logged in with a userID with a command impact of systemAdministration.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- If you are using only locally defined userIDs, it is recommended that you define at least the following userIDs:
  - Two userIDs with command impact of systemAdministration
  - A userID that lets you view Multiservice Switch alarms on Nortel Multiservice Data Manager (MDM). This userID must have a command scope of network, command impact of service, and allowed access of FMIP.
- If you are using remote authentication dial-in service (RADIUS) authentication, it is recommended that you define at least one locally defined userID with a command scope of network, command impact of systemAdministration, and allowed access of all network management interfaces. However, the userID defined locally needs to be different than those on the RADIUS server. Otherwise the authentication method defaults to local.

Procedure steps

Step	Action
1	Add a *userID* component. **`add Ac Userid/<user_id>`**
2	Set the *password (passwd)* attribute. **`set Ac Userid/<user_id> passwd <pswd>`**
3	Set the *customerIdentifier (cid)* attribute. **`set Ac Userid/<user_id> cid <cust_id>`**
4	Set the *commandScope (scope)* attribute. **`set Ac Userid/<user_id> scope <scope>`**
5	Set the *commandImpact (impact)* attribute. **`set Ac Userid/<user_id> impact <impact>`**

6 Set the allowed network management interfaces with the *allowedAccess (nmifs)* attribute.

```
set Ac Userid/<user_id> nmifs <nmifs>
```

To disallow a network management interface, enter the attribute value preceded by a tilde (~). For example, to allow access from all interfaces except FTP, enter the following:

```
set Ac Userid/<user_id> nmifs local fmip remote ~ftp
```

Attention: The *remote* attribute allows access to both Telnet and Secure shell (Ssh) network management interfaces.

7 Set the *allowedOutAccess (outAccess)* attribute.

```
set Ac Userid/<user_id> outAccess <out_access>
```

8 Set the *remoteAuth* attribute.

```
set Ac Userid/<user_id> remoteAuth <remote_auth>
```

9 Optionally, set the *timeoutProtocol* attribute.

```
set Ac Userid/<user_id> timeoutProtocol
<timeoutProtocol>
```

10 Optionally, set the user *loginDirectory (dir)* attribute for file system commands or FTP commands.

```
set Ac Userid/<user_id> dir <directory>
```

--End--

Variable definitions

Variable	Value
<cust_id>	is a number between 0 and 8191. The customer identifier restricts a user's access to those components with the same CID. However, 0 (zero) can access any component. Only userIDs with a CID of 0 (zero) can provision. When you assign a CID to a component, its subcomponents that do not already have a CID assume the CID of the parent component. Those subcomponents that already have a CID retain it, regardless of the CID of the parent component.
<directory>	is the login directory for the userID. This is similar to a home directory in UNIX. The default is /, which is the root directory.
<nmifs>	is one or more allowed network management interfaces for the userID: • *local* (for a directly connected terminal) • *fmip* (for Nortel Multiservice Data Manager (MDM)) • *telnet* (for a standard telnet connection) • *ftp* (for a standard FTP connection) The default is *local*.
<impact>	is one of *passive*, *service*, *configuration*, or *systemAdministration*. The default is *passive*.
<out_access>	is either *telnet* or ~*telnet* If you want the userID to be able to establish outgoing telnet connections from the node, use *telnet*. If not, use ~*telnet*.
<pswd>	is the initial password for the new userID. It needs to be five to eight characters long. Passwords are case sensitive. The *password* attribute holds a password for this user only if the user is to be authenticated locally by the node. If this user is to be authenticated remotely by such a device as a RADIUS server, then the password is left blank. When you are setting a password, it displays on the screen. Once set, the password cannot be displayed again. Locally defined passwords do not expire.
<remote_auth>	specifies whether the user is to be authenticated locally by the node or remotely by an off-switch device such as a RADIUS server. If the *remoteAuth* attribute is set to enabled, the user is authenticated remotely but the locally stored information is still used with the exception of the local password which is left blank.
<scope>	is one of *application*, *device*, or *network*. The default is *application*. For Nortel Multiservice Data Manager (MDM) configuration tools for Multiservice Switch devices, set <scope> to network.

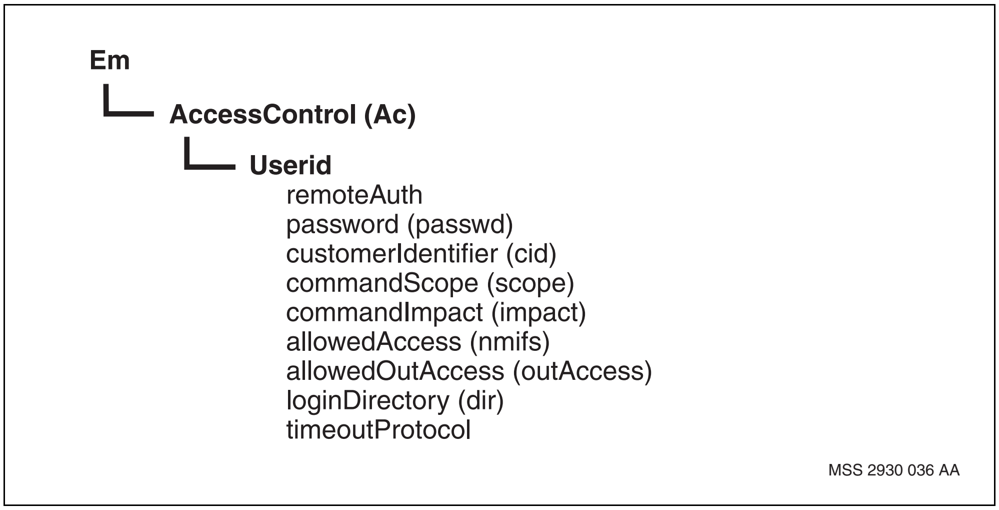
(1 of 2)

Variable	Value
<timeoutProtocol>	is when a timeoutPeriod is configured under telnet or the local operator, the length of time that a session can be idle before being terminated, applies to all sessions under that NMIS interface. However, individual users can be exempted from the configured timeoutPeriod, meaning specific sessions can remain idle without being tracked for inactivity. A user with a command impact of systemAdministration can override the timeoutPeriod for specific users by disabling the timeoutProtocol. The timeoutProtocol is enabled by default, meaning the timeoutPeriod applies to all users. For more information about telnet or local timeout, see NN10600-030 *Nortel Multiservice Switch 7400/15000/20000 Overview*.
<user_id>	is a new user identifier. It needs to be one to eight alphanumeric characters long.

(2 of 2)

Procedure job aid

New userID component hierarchy



Creating a new userID by copying an existing userID

Use this procedure to create a new userID and all of its attributes, except the password. Once you copy a *userID* component, you only need to change the password. This procedure is useful for creating a large number of userIDs that need the same attributes.

Prerequisites

- You must be logged in with a userID with command impact of systemAdministration.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Copy the *Userid* component. **`copy -s(Ac Userid/<old_user_id>) -d(Ac Userid/<new_user_id>) Prov`**
2	Set the *password (passwd)* attribute for the new userID. **`set Ac Userid/<new_user_id> passwd <pswd>`**
3	To change any other attribute of the new userID use the *set* command, as shown in Changing userID attributes (page 24).

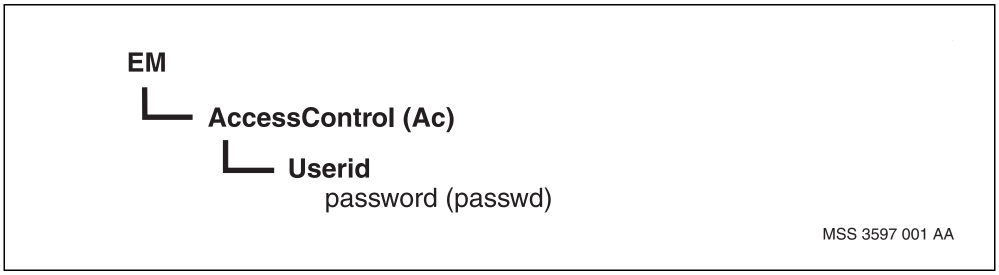
--End--

Variable definitions

Variable	Value
<new_user_id>	is the new user identifier. It needs to be one to eight alphanumeric characters long.
<old_user_id>	is the old user identifier.
<pswd>	is the password for the new userID. It needs to be five to eight characters long. Passwords are case sensitive. When you set a password, it displays on the user interface. Once set, the password cannot be displayed again.

Procedure job aid

Creating a new userID by copying an existing userID component hierarchy



Configuring Telnet and local console timeout

Configure Telnet and local console session timeout on a node, to set the amount of time a session can remain idle before it is terminated.

Prerequisites

- Your userID must have a command impact of systemAdministration.
- The new *timeoutPeriod* attribute that is set only applies to new sessions.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Configure the *timeoutPeriod* attribute to specify how long all local or Telnet sessions can remain idle before they are terminated. `set Nmis <telnet or local> timeoutPeriod <newValue>`
2	If you want to make a particular user exempt from this setting, disable the *timeoutPeriod* attribute for that user ID. `set Ac Userid/<userid> timeoutProtocol disabled`

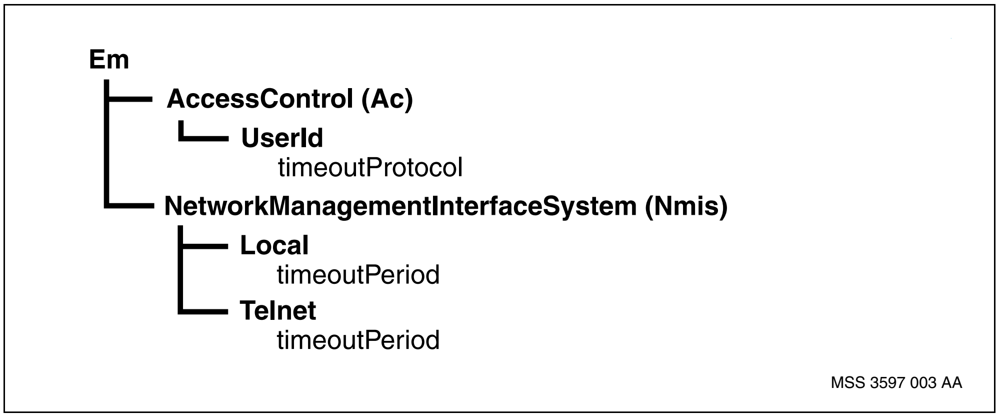
--End--

Variable definitions

Variable	Value
<newValue>	is a value between 5 and 120 minutes.
<telnet or local>	specifies the NMIS interface to be affected.
<userid>	is the user ID of the session to be exempt from being terminated due to inactivity.

Procedure job aid

Telnet and local console timeout component hierarchy



Configuring secure shell (ssh)

Configure secure shell (ssh) to provide a secure alternative to telnet when accessing Nortel Multiservice Switch through a command line interface (CLI).

Procedure steps

Step **Action**

1 Add ssh software to the feature list.

```
set sw dld avl secureShell_<version>
```

2 Start.

```
start -h(<ip_address>) -u(<user_id>) -p(<pswd>) sw dld
```

3 Add.

```
set sw avl secureShell
```

4 Add the ssh software to the feature list.

```
set sw lpt/cp fl secureShell
```

5 Check, activate and confirm the provisioning changes. See Activating configuration changes (page 114).

6 Enable secure shell.

```
set Nmis SecureShell -Mode sshTelnet
```

7 Modify your user IDs associated with this MSS to include ssh in their allowed access.

Attention: If you do not modify the user IDs and disable telnet, you will be locked out of OAM-ENET access to the switch.

8 Disable telnet.

```
set Nmis SecureShell -Mode sshonly.
```

--End--

Variable definitions

Variable	Value
<user_id>	is the user ID of the session.
<version>	is the software version of ssh.

(1 of 2)

Variable	Value
<ip_address>	is the IP address of the node.
<pswd>	is the password for the user ID. It needs to be five to eight characters long. Passwords are case sensitive.
(2 of 2)	

Changing userID attributes

Use this procedure to change one or more attributes of an existing userID.

Prerequisites

- You must be logged in with a userID with command impact of systemAdministration.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Use the following command for each attribute of the userID component you need to change. `set Ac userID/<user_id> <attribute> <value>`

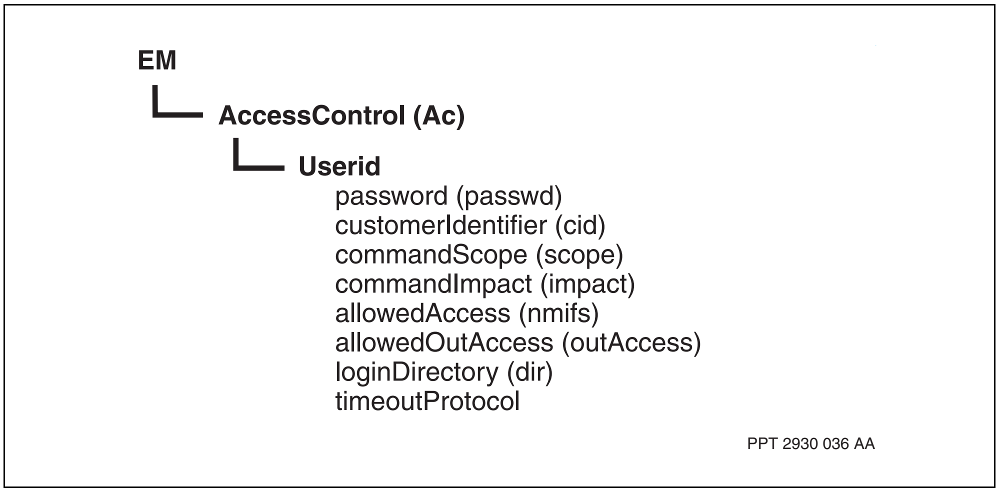
--End--

Variable definitions

Variable	Value
<attribute>	is the name of the attribute you want to change for this userID.
<user_id>	is an existing userID.
<value>	is the new value for the attribute you are changing.

Procedure job aid

UserID attributes component hierarchy



Setting a password

Use this procedure to set a password or change an existing password for a userID.

Prerequisites

- You must be logged in with a userID with command impact of systemAdministration.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- When you set or change a password, the actual characters of the password appear on the user interface. To keep passwords private, make sure your workstation is in a secure area before changing a password.
- To ensure absolute protection, use a local session or IP security (IPSec) when you set a password. When you are not using a local session or IPSec, the information you enter travels over the network in easy-to-read ASCII format.

Procedure steps

Step	Action
1	Set the *password (passwd)* attribute. `set Ac userid/<user_id> passwd <pswd>`
2	Activate the configuration changes. See Activating configuration changes (page 114).

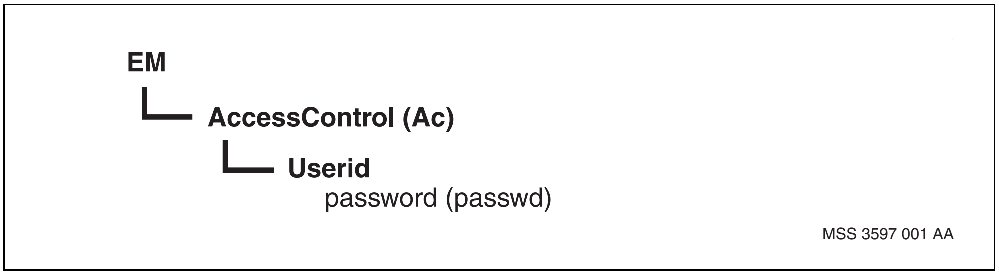
--End--

Variable definitions

Variable	Value
<pswd>	is the new password for the userID. It needs to be five to eight characters long. Passwords are case sensitive. When you set a password, it displays on the user interface. Once set, the password cannot be displayed again.
<user_id>	is the user identifier whose password you are changing.

Procedure job aid

Password component hierarchy



Deleting a user ID

Use this procedure to delete an existing userID.

Prerequisites

- You must be logged in with a userID with command impact of systemAdministration.
- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Remove the *userID* component. **`delete Ac userID/<user_id>`**

--End--

Variable definitions

Variable	Value
<user_id>	is the existing userID that you want to delete.

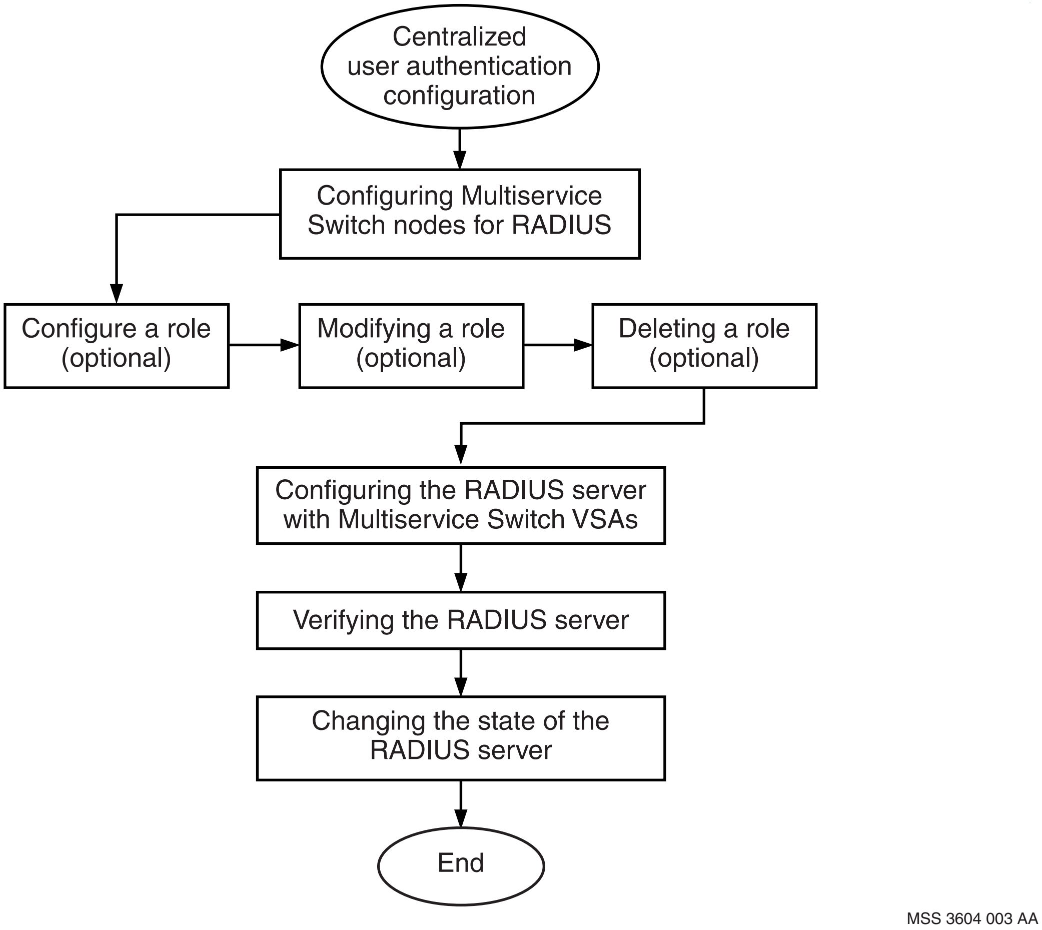
Centralized user authentication configuration

Configure the centralized user authentication on Nortel Multiservice Switch nodes to enable a node to work with a remote authentication dial-in service (RADIUS) server.

Centralized user authentication configuration procedures

This task flow shows you the sequence of procedures to configure centralized user authentication. To link to any procedure, go to Centralized user authentication configuration procedure navigation (page 30).

Centralized user authentication configuration procedures


Centralized user authentication configuration
Configuring Multiservice Switch nodes for RADIUS
Configure a role (optional)
Modifying a role (optional)
Deleting a role (optional)
Configuring the RADIUS server with Multiservice Switch VSAs
Verifying the RADIUS server
Changing the state of the RADIUS server
End
MSS 3604 003 AA

Centralized user authentication configuration procedure navigation

- Configuring Multiservice Switch nodes for RADIUS (page 31)
- Configuring a role (page 34)
- Modifying a role (page 37)
- Deleting a role (page 38)
- Verifying the RADIUS server (page 39)
- For information on Configuring the RADIUS server with Multiservice Switch VSAs, see the documentation for your RADIUS server or NN10400-605 *Nortel Multiservice Data Manager Network Security Fundamentals*.

Configuring Multiservice Switch nodes for RADIUS

Configure Multiservice Switch nodes for the remote authentication dial-in service (RADIUS) as part of implementing authentication between your network management system and the node.

Prerequisites

CAUTION
Risk of denied access to the Multiservice Switch
If the RADIUS server is unavailable and you do not have any userIDs defined locally, access to the Multiservice Switch is not possible.

- It is highly recommended that you define at least one userID locally on the Multiservice Switch in order to have a backup authentication method if the RADIUS server is unavailable. The local userID should have a command scope of network, command impact of systemAdministration, and allowed access to all network management interfaces.
- If IP security (IPSec) is enabled, you must provision security policies to allow RADIUS traffic to be forwarded correctly. If component Vr Ip Spd exists, IPSec is enabled. For more information on IPSec, see NN10400-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*.
- IP connectivity must be configured on the node. To configure IP on the VR, see OAM Ethernet port configuration in NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*. To configure ipiFr and ipiVc, see NN10600-271 *Nortel Multiservice Switch 7400/15000/20000 Network Management Connectivity*.
- For security reasons, it is recommended that you use a local session, particularly when provisioning the *sharedSecret* attribute. When you are not using a local session, the information you enter travels over the network in easy-to-read ASCII format.
- The oamRadius feature must be provisioned in the feature list of the CP that is providing management access (for example, set sw lpt/cp fl oamradius).

Procedure steps

Step **Action**

1 Add a primary RADIUS server. This server is also called the active RADIUS server.

```
add -s Ac Radius Server/0
```

2 Specify the IP address that the node uses to communicate with the RADIUS server.

```
set Ac Radius nasIdentifier <nas_id_addr>
```

3 Set the attributes for the RADIUS server.

```
set Ac Radius Server/0 sharedSecret <prm_ss>,
serverPortNumber <port_nbr>, serverIpAddress
<prm_ip_addr>, ipStack <ip_stk>
```

4 If required, configure another RADIUS server as a backup. This server is the standby RADIUS server.

```
add -set Ac Radius Server/1 sharedSecret <bkup_ss>,
serverPortNumber <port_nbr>, serverIpAddress
<bkup_ip_addr>, ipStack <ip_stk>
```

5 Activate the configuration changes. See Activating configuration changes (page 114).

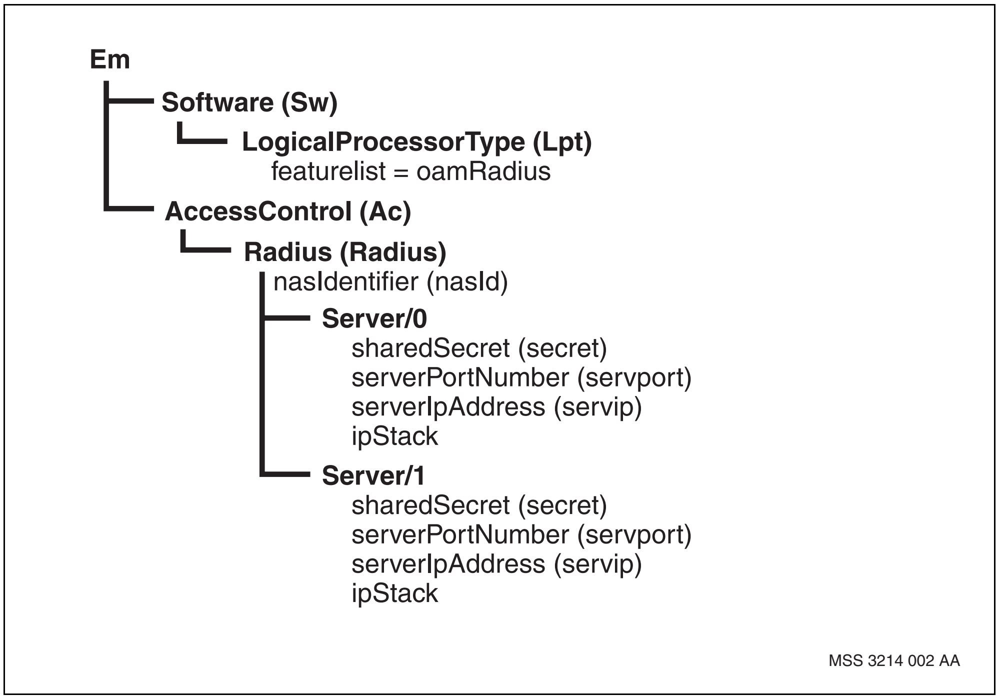
--End--

Variable definitions

Variable	Value
<bkup_ip_addr>	is the IP address of the backup RADIUS server.
<bkup_ss>	is the shared secret of the backup RADIUS server.
<ip_stk>	is the Vrip or the ipiFr ipiVc depending on the connection between the node and RADIUS. If a backup RADIUS server has been provisioned, the ip_stk value must be the same for both servers.
<nas_ip_addr>	is an IP address. If the connection between the node and RADIUS uses oamEnet, this is the IP address of the management VR. If the connection between the node and RADIUS uses ipiFr or ipiVc, this is the ipiFr or ipiVc address respectively.
<port_nbr>	is the UPD port the node is using to send requests to the RADIUS server.
<prm_ip_addr>	is the IP address of the primary RADIUS server.
<prm_ss>	is the shared secret of the primary RADIUS server.

Procedure job aid

Multiservice Switch nodes for RADIUS component hierarchy



Configuring a role

Configure a role to assign centralized user access privilege to groups of users based on a job function.

Procedure steps

Step **Action**

1 Add a role.

```
add Ac Role/<role_name>
```

2 Set the *customerIdentifier (cid)* attribute.

```
set Ac Role/<role_name> cid <cust_id>
```

3 Set the *commandScope (scope)* attribute.

```
set Ac Role/<role_name> scope <scope>
```

4 Set the *commandImpact (impact)* attribute.

```
set Ac Role/<role_name> impact <impact>
```

5 Set the allowed network management interfaces with the *allowedAccess (nmifs)* attribute.

```
set Ac Role/<role_name> nmifs <nmifs>
```

Attention: To disallow a network management interface, enter the attribute value preceded by a tilde (~).

6 Set the *allowedOutAccess (outAccess)* attribute.

```
set Ac Role/<role_name> outAccess <out_access>
```

7 Optionally, set the *timeoutProtocol* attribute.

```
set Ac Role/<role_name> timeoutProtocol
<timeoutProtocol>
```

8 Optionally, set the user *loginDirectory (dir)* attribute for file system commands or FTP commands.

```
set Ac Role/<role_name> dir <directory>
```

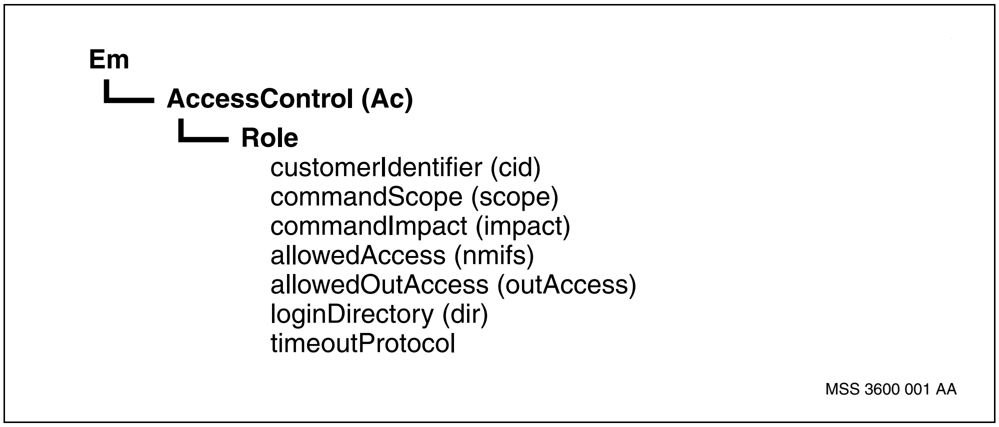
--End--

Variable definitions

Variable	Value
<cust_id>	is a number between 0 and 8191. The customer identifier restricts a user's access to those components with the same CID. However, 0 (zero) can access any component. Only userIDs with a CID of 0 (zero) can provision. When you assign a CID to a component, its subcomponents that do not already have a CID assume the CID of the parent component. Those subcomponents that already have a CID retain it, regardless of the CID of the parent component.
<directory>	is the login directory for the role. This is similar to a home directory in UNIX. The default is /, which is the root directory.
<impact>	is one of *passive*, *service*, *configuration*, or *systemAdministration*. The default is *passive*.
<nmifs>	is one or more allowed network management interfaces for the role: • *local* (for a directly connected terminal) • *fmip* (for Nortel Multiservice Data Manager (MDM)) • *telnet* (for a standard telnet connection) • *ftp* (for a standard FTP connection) The default is *local*.
<out_access>	is either *telnet* or ~*telnet* If you want the role to be able to establish outgoing telnet connections from the node, use *telnet*. If not, use ~*telnet*.
<role_name>	is a new role identifier that describes a job function for a group of users.
<scope>	is one of *application*, *device*, or *network*. The default is *application*. For Nortel Multiservice Data Manager (MDM) configuration tools for Multiservice Switch devices, set <scope> to network.
<timeoutProtocol>	specifies whether a user session with this role will override the *timeoutPeriod* attribute of the Telnet component. This setting exempts individual users from the configured *timeoutPeriod*, meaning specific sessions can remain idle without being tracked from inactivity. A user with a command impact of systemAdministration can override the *timeoutPeriod* for specific users with this role by disabling the *timeoutProtocol*. The *timeoutProtocol* is enabled by default, meaning the *timeoutPeriod* applies to all users with this role.

Procedure job aid

Role component hierarchy



Modifying a role

Modify role attributes to change the profile of an existing role that is defined on the Multiservice Switch system.

Prerequisites

- You must be logged in to the Multiservice Switch node with a userID with command impact of systemAdministration.

Procedure steps

Step	Action
1	Use the following command for each attribute of the role component you need to change. **set Ac Role/<role_name> <attribute> <value>**

--End--

Variable definitions

Variable	Value
<attribute>	is the name of the attribute you want to change for this role.
<role_name>	is the name of an existing role.
<value>	is the value for the attribute you are changing.

Deleting a role

Delete a role to remove an existing role and its associated privileges.

Prerequisites

- You must be logged in to the Multiservice Switch node with a userID with command impact of systemAdministration.

Procedure steps

Step	Action
1	Remove the *userId* component. **`del Ac Role/<role_name>`**

--End--

Variable definitions

Variable	Value
<role_name>	is the name of the existing role that you want to delete.

Verifying the RADIUS server

Use this procedure to verify that the RADIUS server can be used. Nortel Networks recommends that you perform this procedure on a regular basis.

Prerequisites

- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step **Action**

1 Lock the active server 0 so that authentication requests are sent to the standby server 1. Statistics such as attributes *Ac Radius Server accessRequests* and *accessAccepts* are updated under the server with which you are authenticating, in this case the standby server 1.

```
lock Ac Radius Server/0
```

2 Once you have verified that the standby server 1 can authenticate userIDs and passwords, unlock the server 0.

```
unlock Ac Radius Server/0
```

3 Lock the standby server 1 to force authentication requests to be sent to server 0.

```
lock Ac Radius Server/1
```

4 Log in to the Multiservice Switch with a userID that is defined in the database and not locally. This authentication request is processed through the active server. Statistics are now updated under the active server.

5 Unlock the server 1. This server is now on standby in case server 0 fails.

```
unlock Ac Radius Server/1
```

--End--

Changing the state of the RADIUS server

Change the state of the RADIUS server to force a switchover between two RADIUS servers. Locking an active RADIUS server, forces the second RADIUS server to become active.

When a primary RADIUS server fails, the second RADIUS server takes over. However, when the primary RADIUS is working again, the Multiservice Switch does not automatically switchover from the second RADIUS server to the primary. Locking the second RADIUS server, forces the primary server to become active again.

Procedure steps

Step **Action**

1 Determine which server is the active RADIUS server.

```
d Ac Radius Server/*
```

2 Lock the active RADIUS server.

```
lock Ac Radius Server <server>
```

3 Once the primary server is active again, unlock the RADIUS server that you locked in step 2.

```
unlock Ac Radius Server <server>
```

--End--

Variable definitions

Variable	Value
<server>	is the instance of the RADIUS server.

IP security configuration on a Multiservice Switch node

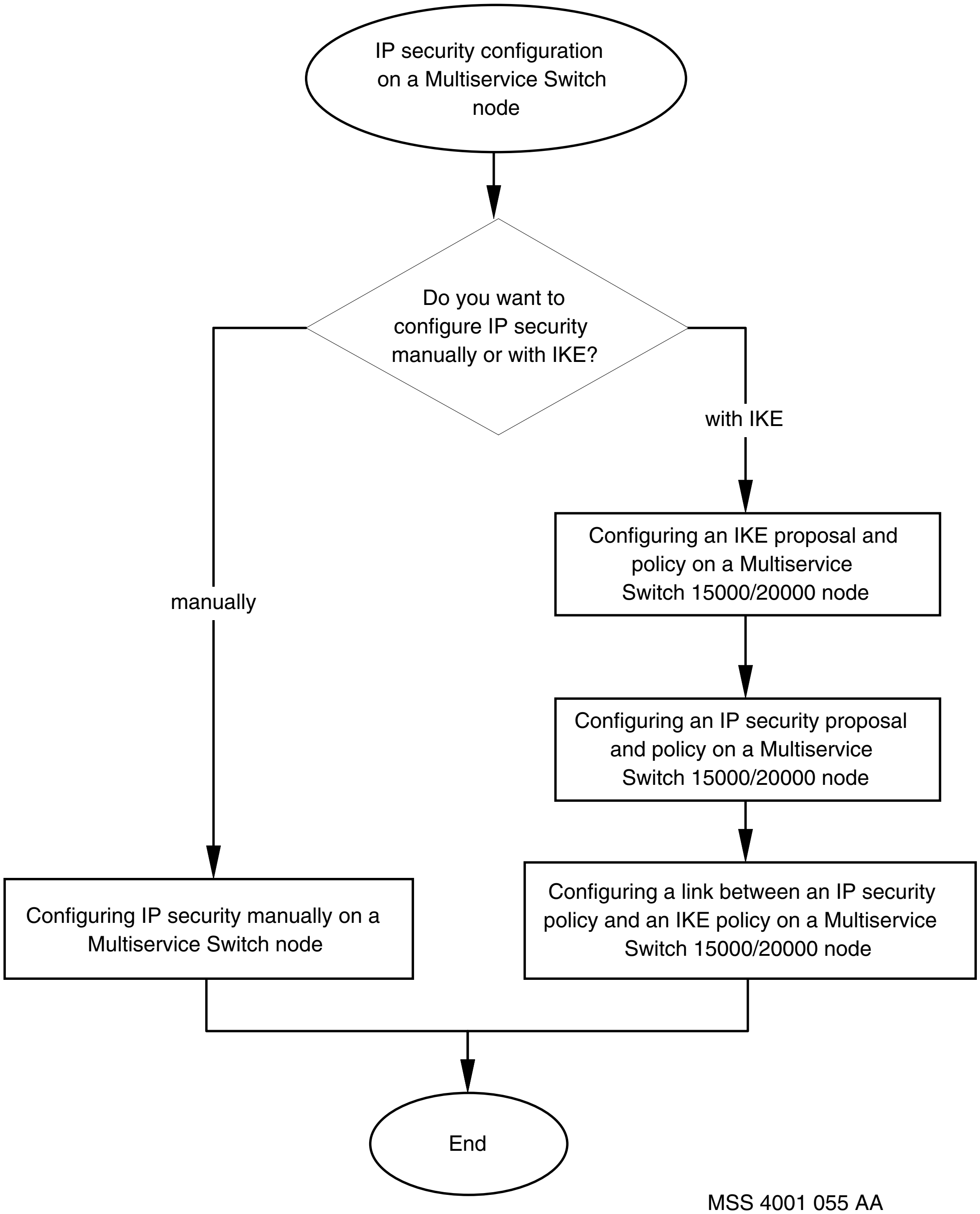
IP security (IPSec) configuration on a Multiservice Switch node, either manually or with the Internet key exchange (IKE), allows for the negotiation of a security association (SA). This security association is negotiated between the Multiservice Switch and the Multiservice Data Manager requiring secure communication for operations, administration and maintenance (OAM) traffic.

You can configure IPSec on Multiservice Switch 7400/15000/20000. Multiservice Switch 15000/20000 supports IPSec with IKE.

IP security configuration on a Multiservice Switch node procedures

This task flow shows you the sequence of procedures you perform to configure user access. To link to any procedure, go to IP security configuration on a Multiservice Switch node navigation (page 43).

IP security configuration on a Multiservice Switch node procedures


IP security configuration on a Multiservice Switch node
Do you want to configure IP security manually or with IKE?
manually
with IKE
Configuring an IKE proposal and policy on a Multiservice Switch 15000/20000 node
Configuring an IP security proposal and policy on a Multiservice Switch 15000/20000 node
Configuring a link between an IP security policy and an IKE policy on a Multiservice Switch 15000/20000 node
Configuring IP security manually on a Multiservice Switch node
End

MSS 4001 055 AA

IP security configuration on a Multiservice Switch node navigation

Configuring IP security manually on a Multiservice Switch node

Configure IP security (IPSec) manually on a Multiservice Switch node to provide secure IP-based OAM packets terminating on the Multiservice Switch node. You must configure a security association (SA) on both the Nortel Multiservice Data Manager (MDM) workstation and the Multiservice Switch node in order to apply advanced encryption standard (AES), data encryption standard (DES), triple DES encryption, message digest 5 (MD5), or secure hash algorithm1 (SHA1) on all traffic exchanged between MDM and the Multiservice Switch node.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- Prior to completing this procedure, you must ensure that you perform the following procedures on the Nortel Multiservice Data Manager (MDM) workstation:
  - Downloading encryption packages and patches
  - Installing the encryption packages
  - Configuring a default SA between the workstation and node

For more information about the Multiservice Data Manager procedures, see NN10400-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*.

- IPSec is supported for the OAM Ethernet, Ethernet, and ATM MPE media types. Before configuring IPSec, you must first configure the required media type. For more information, see NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- Download the IPSec software. For more information, see NN10600-270 *Nortel Multiservice Switch 7400/15000/20000 Software Installation*. Ensure to conform to the export control guidelines and requirements. The IPSec software is separately packaged and can be ordered.
- The IPSec feature must be configured in the software AVL. For more information on adding features to the AVL, see NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*.
- To ensure absolute protection, the node IPSec policy must be set by connecting directly to the serial port with a local console, so that the encryption or authentication key can not be compromised. The key used on the node is the same key that must be used on the Nortel Multiservice Data Manager workstation, otherwise you will need to delete the policy and create it again.

Refer to the following examples for more information:

- Example 1 of configuring the sample IP security provisioning for FTP traffic (page 49)
- Example 2 of configuring the sample discard policy for ICMP traffic (page 51)
- Example 3 of configuring the sample bypass policy for UDP traffic (page 52)

Procedure steps

Step **Action**

1 Add the *SecurityPolicyDatabase (Spd)* component for the IPSec policy database.

```
add Vr/0 Ip Spd/<spd_name>
```

2 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
```

3 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
```

4 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> action
<action>, direction in
```

5 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> action
<action>, direction out
```

6 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

7 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

8 Add the *securityAssociation (Sa)* component for the inbound policies that have *Vr Ip Spd Policy action* set to apply.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
<sa_addr_1>,<esp>,<spi_1>
```

Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

9 Add the *securityAssociation (Sa)* for the outbound policies that have *Vr Ip Spd Policy action* set to apply.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
<sa_addr_2>,<esp>,<spi_2>
```

Adding the *Sa* component automatically creates a *ManEspSa* subcomponent.

10 Set the algorithms and keys for the inbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> Sa/
<sa_addr_1>,<esp>,<spi_1> ManEspSa encAlgorithm
<enc_alg>, encKey <enc_key_1>, authAlgorithm <auth_alg>,
authKey <auth_key_1>
```

11 Set the algorithms and keys for the outbound policy security association.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> Sa/
<sa_addr_2>,<esp>,<spi_2> ManEspSa encAlgorithm
<enc_alg>, encKey <enc_key_2>, authAlgorithm <auth_alg>,
authKey <auth_key_2>
```

12 Activate the configuration changes. See Activating configuration changes (page 114).

--End--

Variable definitions

Variable	Value
<action>	is the action to be taken when a packet is received that matches the policy.
<auth_alg>	is the authentication algorithm for the security association. Specify at least one of the *encAlgorithm* and *authAlgorithm* attributes; they cannot both be set to none.
<auth_key_1> <auth_key_2>	is the symmetric key for the keyed-hash function for the security association.
<dst_addr>	is the destination IP address for traffic flows to which the policy applies.
<dst_port>	is the destination TCP or UDP port number for traffic flows to which the policy applies.
<enc_alg>	is the encryption algorithm for the security association. Specify at least one of the *encAlgorithm* and *authAlgorithm* attributes; they cannot both be set to none.

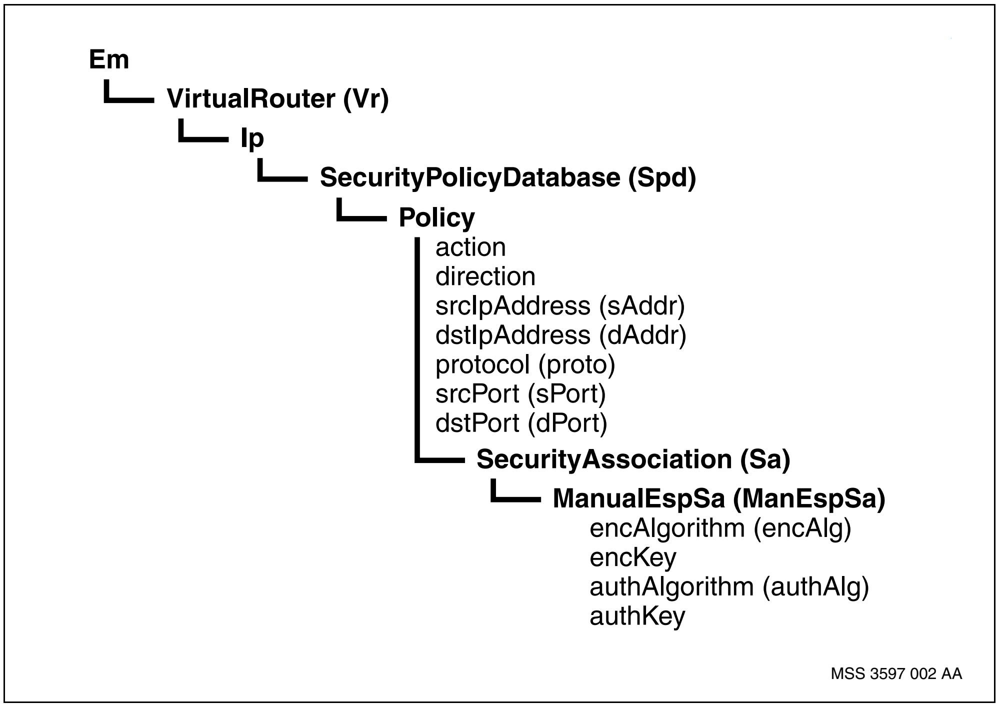
(1 of 2)

Variable	Value
<enc_key_1> <enc_key_2>	is the symmetric encryption key for the security association.
<esp>	is the IPSec protocol type for the security association.
<pol_in>	is the instance value of the policy for inbound traffic. The instance value specifies the policy precedence. Policy lookup occurs in order of increasing precedence value.
<pol_out>	is the instance value of the policy for outbound traffic. The instance value specifies the policy precedence. Policy lookup occurs in order of increasing precedence value.
<protocol>	is the layer 4 protocol to which the policy applies.
<sa_addr_1>	is the IP address of the local node (for inbound SAs).
<sa_addr_2>	is the IP address of the workstation (for outbound SAs).
<spd_name>	is the name of the security policy database.
<spi_1> <spi_2>	is the security parameter index for the security association.
<src_addr>	is the source IP address for traffic flows to which the policy applies.
<src_port>	is the source TCP or UDP port number for traffic flows to which the policy applies.

(2 of 2)

Procedure job aid

Manual IP security configuration on a node component hierarchy



Example 1 of configuring the sample IP security provisioning for FTP traffic

This example shows IP security provisioning for file transfer protocol (FTP) traffic where:

- IPSec processing is applied.
- The FTP connection is from the workstation to the node.
- Encryption and authentication is applied to the control channel.
- Authentication is applied to the data channel.

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Procedure steps

Step **Action**

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/10
add Vr/0 Ip Spd/1 Policy/20
add Vr/0 Ip Spd/1 Policy/30
add Vr/0 Ip Spd/1 Policy/40
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/10 action apply, direction out
set Vr/0 Ip Spd/1 Policy/20 action apply, direction in
set Vr/0 Ip Spd/1 Policy/30 action apply, direction out
set Vr/0 Ip Spd/1 Policy/40 action apply, direction in
```

3 Set the traffic flow policy selectors for the FTP control channel.

```
set Vr/0 Ip Spd/1 Policy/10 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, protocol tcp, srcPort ftp
set Vr/0 Ip Spd/1 Policy/20 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, protocol tcp, dstPort ftp
```

4 Set the traffic flow policy selectors for the FTP data channel.

```
set Vr/0 Ip Spd/1 Policy/30 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, protocol tcp, scrPort ftpdata
set Vr/0 Ip Spd/1 Policy/40 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, protocol tcp, dstPort ftpdata
```

5 Add security associations (SAs) for the FTP control channel. A security association is required when attribute *Vr Ip Spd Policy action* is set to apply.

```
add Vr/0 Ip Spd/1 Policy/10 Sa/x.x.x.xB,esp,300
add Vr/0 Ip Spd/1 Policy/20 Sa/x.x.x.xA,esp,301
```

6 Set the algorithms and keys for the FTP control channel.

```
set Vr/0 Ip Spd/1 Policy/10 Sa/x.x.x.xB,esp,300 ManEspSa
encAlgorithm des, enckey d0efbc8a79462513, authAlgorithm
md5, authKey fedcba98765432100123456789abcdef
set Vr/0 Ip Spd/1 Policy/20 Sa/x.x.x.xA,esp,301 ManEspSa
encAlgorithm des, enckey 132546798abcefd0, authAlgorithm
md5, authKey 0123456789abcdeffedcba9876543210
```

7 Add security associations (SAs) for the FTP data channel. The security parameter indexes (SPIs) can be the same for both SAs, as in this example.

```
add Vr/0 Ip Spd/1 Policy/30 Sa/x.x.x.xB,esp,400
add Vr/0 Ip Spd/1 Policy/40 Sa/x.x.x.xA,esp,401
```

8 Set the algorithms and keys for the FTP data channel.

```
set Vr/0 Ip Spd/1 Policy/30 Sa/x.x.x.xB,esp,400 ManEspSa
authAlgorithm sha1, authKey
fedcba98765432100123456789abcdeffedcba9876543210
set Vr/0 Ip Spd/1 Policy/30 Sa/x.x.x.xA,esp,401 ManEspSa
authAlgorithm sha1, authKey
0123456789abcdeffedcba98765432100123456789abcdef
```

Since the security policies are unidirectional and there are two separate traffic flows (FTP control channel and FTP data channel), four security policies are provisioned.

--End--

Example 2 of configuring the sample discard policy for ICMP traffic

This example shows IPSec provisioning for Internet control message protocol (ICMP) traffic, where all ICMP packets are discarded. This example applies to all ICMP traffic originating from either the node or workstation, and destined for either the workstation or node, respectively.

Procedure steps

Step **Action**

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/50
add Vr/0 Ip Spd/1 Policy/60
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/50 action discard, direction out
set Vr/0 Ip Spd/1 Policy/60 action discard, direction in
```

3 Set the traffic flow policy selectors for all ICMP traffic.

```
set Vr/0 Ip Spd/1 Policy/50 protocol icmp
set Vr/0 Ip Spd/1 Policy/60 protocol icmp
```

--End--

Example 3 of configuring the sample bypass policy for UDP traffic

This example shows IPSec provisioning for user datagram protocol (UDP) traffic, where IPSec processing is bypassed. This example applies to all UDP traffic originating from either the node or workstation, and destined for either the workstation or node, respectively.

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Procedure steps

Step	Action

1	Add the policies.
	`add Vr/0 Ip Spd/1 Policy/70`
	`add Vr/0 Ip Spd/1 Policy/80`

2	Specify the action and direction for the policies.
	`set Vr/0 Ip Spd/1 Policy/70 action bypass, direction out`
	`set Vr/0 Ip Spd/1 Policy/80 action bypass, direction in`

3	Set the traffic flow policy selectors for the UDP traffic.
	`set Vr/0 Ip Spd/1 Policy/70 srcIpAddr x.x.x.xA, dstIpAddr x.x.x.xB, protocol udp`
	`set Vr/0 Ip Spd/1 Policy/80 srcIpAddr x.x.x.xB, dstIpAddr x.x.x.xA, protocol udp`

--End--

Example 4 of configuring the sample bypass policy for secure shell traffic

This example is used to bypass IPSec processing when the Multiservice Switch has IPSec enabled and a system wants to access the Multiservice Switch using the secure shell (SSH).

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Procedure steps

Step **Action**

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/70
add Vr/0 Ip Spd/1 Policy/80
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/70 action bypass, direction out
set Vr/0 Ip Spd/1 Policy/80 action bypass, direction in
```

3 Set the traffic flow policy selectors for the secure shell traffic.

```
set Vr/0 Ip Spd/1 Policy/70 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, srcPort 22
set Vr/0 Ip Spd/1 Policy/80 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, dstPort 22
```

--End--

Configuring an IKE proposal and policy on a Multiservice Switch 15000/20000 node

Configure an IKE proposal and policy on a Multiservice Switch 15000/20000 node to set up the phase 1 of the security association (SA). This SA between the Multiservice Switch 15000/20000 and the Nortel Multiservice Data Manager (MDM) acts as the control channel. This control channel is used to exchange messages to set up the IPSec SA, also called phase 2 SA.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- You must select an authentication and encryption algorithm combination. You will need this information to complete step 5 and step 6 of this procedure. For more information, refer to Authentication and encryption algorithms (page 104).
- Nortel Multiservice Data Manager (MDM) initiates a session using one of the network management interfaces: telnet, file transfer protocol (FTP), or fast management interface protocol (FMIP).

For an example procedure, refer to:

- Example 1 of configuring IKE proposal and policy (page 66)

Procedure steps

Step **Action**

1 Add the *SecurityPolicyDatabase (Spd)* component for the IPSec policy database.

```
add Vr/0 Ip Spd/<spd_name>
```

2 Add the *InternetKeyExchange (Ike)* component.

```
add Vr/0 Ip Spd/<spd_name> Ike
```

3 Add the *IkeSaProposal* (*Proposal*) component for IKE.

```
add Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
```

4 Add the *Transform (Trans)* component for IKE. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform1_ike>
```

```
add Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform2_ike>
```

5 Specify the *authAlgorithm (authAlg)* attribute, for each direction.

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform1_ike> authAlg <auth_alg>
```

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform2_ike> authAlg <auth_alg>
```

6 Specify the *encAlgorithm (encAlg)* attribute, for each direction.

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform1_ike> encAlg <enc_alg>
```

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform2_ike> encAlg <enc_alg>
```

7 Specify the *diffieHellmanGroup (dhg)* attribute, for each direction.

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform1_ike> dhg <dhg>
```

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
Trans/<transform2_ike> dhg <dhg>
```

8 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
ttl <time_to_live_ike>
```

9 Set the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Proposal/<proposal_ike>
softLifeTime <soft_life_time_ike>
```

10 Add the *IkeSaPolicy* (*Policy)* component for IKE.

```
add Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike>
```

11 Specify the *description (desc)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike> desc
<description_ike>
```

12 Specify the *presharedKey (key)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike> key
<preshared_key>
```

13 Specify the *retryTimerValue* (*rtv*) attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike> rtv
<retry_timer_value>
```

14 Specify the *numRetryAttempts* (*retryAttempts*) attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike>
retryAttempts <num_retry_attempts>
```

15 Specify the *destinationIpAddress (destAddr)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike>
destAddr <dest_ip_address>
```

16 Specify the *ikeProposalLink* (*proposalLink*) attribute.

```
set Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike>
proposalLink ! Vr/0 Ip Spd/<spd_name> Ike Proposal/
<proposal_ike>
```

17 Display the list of IKE policies.

```
display Vr/0 Ip Spd/<spd_name> Ike Proposal/
<proposal_ike> ikePolicyList <ike_policy_list>
```

18 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
```

Attention: From step 18 onwards, you are configuring the IKE port bypass IPSec policy to allow the IKE messaging to go through.

19 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
```

20 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> action
bypass, direction in
```

21 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> action
bypass, direction out
```

22 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, dstPort IKE
```

23 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, srcPort IKE
```

--End--

Variable definitions

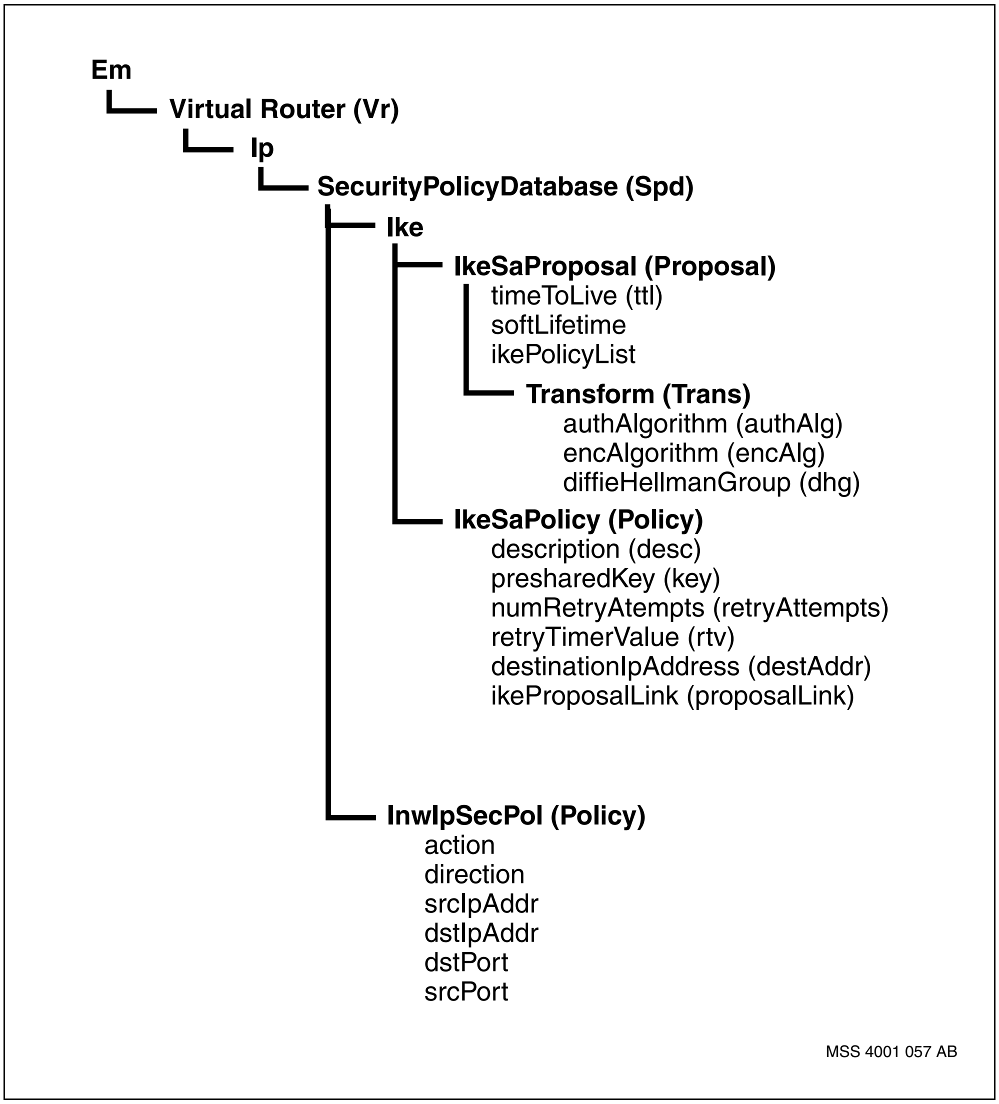
Variable	Value
<auth_alg>	is the authentication algorithm to use for the security association. Specify at least one of the *encAlgorithm* and *authAlgorithm* attributes; they cannot both be set to none.
<description_ike>	is the reason for the creation of this policy.
	(1 of 2)

Variable	Value
<dest_ip_address>	is the IP address of the IKE peer.
<dhg>	is the Diffie-Hellman group number used for this SA.
<enc_alg>	is the encryption algorithm to be proposed in negotiation of the IKE SA.
<ike_policy_list>	specifies the list of IKE policy components which will use the *Proposal* component in an attempt to negotiate an IKE phase 1 SA.
<num_retry_attempts>	is the number of retransmission attempts of any IKE message.
<policy_ike>	represents the IKE requirements for a specific IKE security association (SA).
<preshared_key>	specifies the preshared key to be used at both ends of an IKE SA for authentication. **Attention:** This is a write-only attribute. The operator cannot read back the value of this attribute.
<proposal_ike>	represents a set of security parameters to be negotiated between two peers.
<retry_timer>	is the initial time, in milliseconds, that IKE waits for a reply from the IKE peer before attempting to resend a message.
<soft_life_time_ike>	is the percentage of the *timeToLive* attribute that must pass before the renegotiation of phase 1 SA can start.
<spd_name>	is the name of the security policy database.
<time_to_live_ike>	specifies the proposed time-to-live value for an IKE security association that is negotiated using this *Proposal* component.
<transform1_ike> <transform2_ike>	represents information contained in the transform payload that is used during the negotiation of the IKE SA. The information consists of specific security attributes that need to be negotiated with the IKE peer.

(2 of 2)

Procedure job aid

IKE proposal and policy on a node component hierarchy



- **Em**
  - **Virtual Router (Vr)**
    - **Ip**
      - **SecurityPolicyDatabase (Spd)**
        - **Ike**
          - **IkeSaProposal (Proposal)**
            - timeToLive (ttl)
            - softLifetime
            - ikePolicyList
            - **Transform (Trans)**
              - authAlgorithm (authAlg)
              - encAlgorithm (encAlg)
              - diffieHellmanGroup (dhg)
          - **IkeSaPolicy (Policy)**
            - description (desc)
            - presharedKey (key)
            - numRetryAtempts (retryAttempts)
            - retryTimerValue (rtv)
            - destinationIpAddress (destAddr)
            - ikeProposalLink (proposalLink)
        - **InwIpSecPol (Policy)**
          - action
          - direction
          - srcIpAddr
          - dstIpAddr
          - dstPort
          - srcPort

MSS 4001 057 AB

Configuring an IP security proposal and policy on a Multiservice Switch 15000/20000 node

Configure an IP security (IPSec) proposal and policy on a Multiservice Switch 15000/20000 node to set up the phase 2 of the security association (SA). The attributes are negotiated for the IPSec SA over messaging done on the phase 1 SA. The IPSec or phase 2 SA is the final data channel required by the user.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- You must select an authentication and encryption algorithm combination. You will need this information to complete step 6 and step 7 of this procedure. For more information, refer to Authentication and encryption algorithms (page 104).

For example procedures, refer to:

- Example 2 of configuring IP security proposal and policy for FTP traffic (page 68)
- Example 3 of configuring IP security proposal and policy for ICMP traffic (page 70)
- Example 4 of configuring IP security proposal and policy for UDP traffic (page 72)
- Example 5 of configuring the sample bypass policy for IKE traffic (page 74)

Procedure steps

Step **Action**

1 Add the *SecurityAssociationProposal* (*Proposal*) component.

```
add Vr/0 Ip Spd/<spd_name> Proposal/<proposal>
```

2 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> ttl
<time_to_live>
```

3 Specify the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal>
softLifeTime <soft_life_time>
```

4 Add the *IpSecSaTransform (Trans)* component. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform1>
```

```
add Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform2>
```

5 Specify the *antiReplay (replay)* attribute, for each direction.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform1> replay <replay>
```

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform2> replay <replay>
```

6 Specify the *authAlgorithm (authAlg)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform1> authAlg <auth_alg>
```

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform2> authAlg <auth_alg>
```

7 Specify the *encAlgorithm (encAlg)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform1> encAlg <enc_alg>
```

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform2> encAlg <enc_alg>
```

8 Specify the *diffieHellmanGroup (dhg)* attribute.

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform1> dhg <dhg>
```

```
set Vr/0 Ip Spd/<spd_name> Proposal/<proposal> Trans/
<transform2> dhg <dhg>
```

9 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_in>
```

10 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/<spd_name> Policy/<pol_out>
```

11 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> action
<action>, direction in
```

12 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> action
<action>, direction out
```

13 Specify the *description* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> description
<description>
```

14 Specify the *description* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> description
<description>
```

15 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_in> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

16 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/<spd_name> Policy/<pol_out> srcIpAddr
<src_addr>, dstIpAddr <dst_addr>, protocol <protocol>,
srcPort <src_port>, dstPort <dst_port>
```

17 Specify the *saProposal* attribute.

```
set Vr/0 Ip Spd/<spd_name> Policy/<policy> saProposal
Vr/0 Ip Spd/<spd_name> Proposal/<proposal>
```

--End--

Variable definitions

Variable	Value
<action>	is the action to be taken when a packet is received that matches the policy.
<replay>	specifies whether the anti-replay protection is on or off.
<description>	is the reason for the creation of this policy.
<dst_addr>	is the destination IP address for traffic flows to which the policy applies.
<dst_port>	is the destination TCP or UDP port number for traffic flows to which the policy applies.
<pol_in>	is the instance value of the policy for inbound traffic. The instance value specifies the policy precedence. Policy lookup occurs in order of increasing precedence value.
<pol_out>	is the instance value of the policy for outbound traffic. The instance value specifies the policy precedence. Policy lookup occurs in order of increasing precedence value.
<policy>	is the instance value that specifies the policy precedence. The *Policy* component defines an IPSec policy to be applied for a virtual router.
<proposal>	represents a set of security parameters to be negotiated between two IPSec peers.

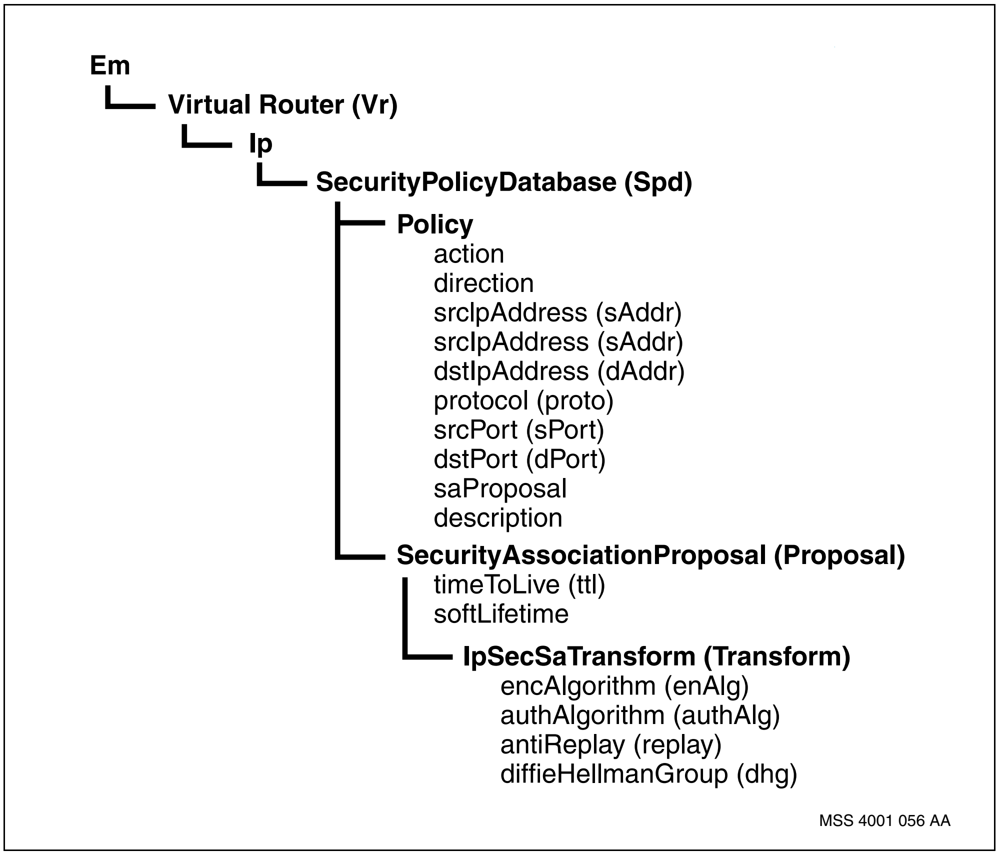
(1 of 2)

Variable	Value
<protocol>	is the layer 4 protocol to which the policy applies.
<soft_life_time>	is the percentage of the *timeToLive* attribute that must pass before the renegotiation of phase 2 SA can start.
<spd_name>	is the name of the security policy database.
<src_addr>	is the source IP address for traffic flows to which the policy applies.
<src_port>	is the source TCP or UDP port number for traffic flows to which the policy applies.
<time_to_live>	is the maximum time-to-live period, in seconds, that the IPSec SA exists unless it is renegotiated.
<transform>	represents the encryption and authentication parameters that can be used to negotiate an IPSec SA.

(2 of 2)

Procedure job aid

IP security proposal and policy on a node component hierarchy



Configuring a link between an IP security policy and an IKE policy on a Multiservice Switch 15000/20000 node

Configure a link between an IP security (IPSec) policy and an Internet key exchange (IKE) policy on a Multiservice Switch 15000/20000 node to assign the phase 1 SA to the IPSec SA, also called phase 2 SA. The assignment determines which phase 1 SA will be used for the phase 2 SA negotiation. More than one phase 2 SA can be negotiated over the same phase 1 SA. When you have completed this procedure, the Multiservice Switch 15000/20000 and the Multiservice Data Manager are ready to exchange data.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Specify the *ikePolicy* attribute. `set Vr/0 Ip Spd/<spd_name> Policy/<policy> ikePolicy Vr/0 Ip Spd/<spd_name> Ike Policy/<policy_ike>`
2	Activate the configuration changes. See Activating configuration changes (page 114).

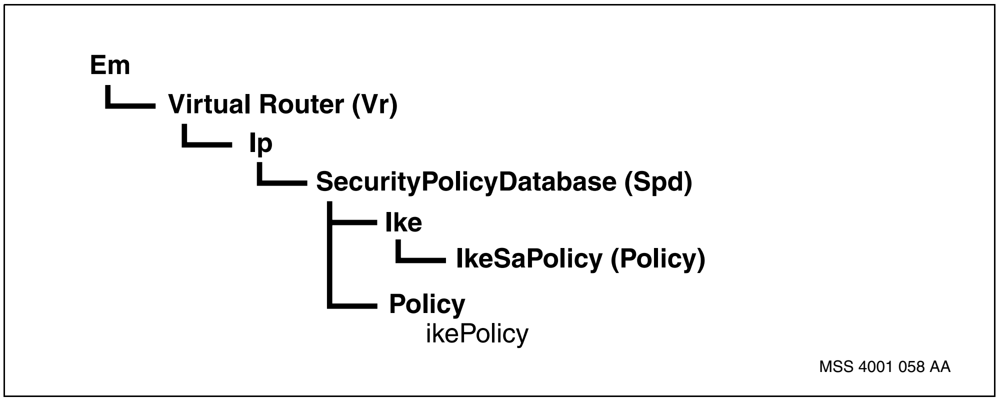
--End--

Variable definitions

Variable	Value
<policy_ike>	represents the IKE requirements for a specific IKE security association (SA).
<policy>	is the instance value that specifies the policy precedence. The *Policy* component defines an IPSec policy to be applied for a virtual router.
<spd_name>	is the name of the security policy database.

Procedure job aid

Link between an IP security policy and an IKE policy component hierarchy



Example 1 of configuring IKE proposal and policy

This example procedure shows the configuration of an IKE proposal and policy on a Multiservice Switch 15000/20000 node to set up the phase 1 of the security association (SA).

In this example procedure, the IP address in the network is identified as x.x.x.xA.

Procedure steps

Step **Action**

1 Add the *SecurityPolicyDatabase (Spd)* component for the IPSec policy database.

```
add Vr/0 Ip Spd/t
```

2 Add the *InternetKeyExchange (Ike)* component.

```
add Vr/0 Ip Spd/t Ike
```

3 Add the *IkeSaProposal* (*Proposal*) component for IKE.

```
add Vr/0 Ip Spd/t Ike Proposal/1
```

4 Add the *Transform (Trans)* component for IKE. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/t Ike Proposal/1 Trans/1
add Vr/0 Ip Spd/t Ike Proposal/1 Trans/2
```

5 Specify the *authAlgorithm (authAlg)* attribute.

```
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/1 authAlg md5
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/2 authAlg md5
```

6 Specify the *encAlgorithm (encAlg)* attribute.

```
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/1 encAlg aes
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/2 encAlg aes
```

7 Specify the *diffieHellmanGroup (dhg)* attribute.

```
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/1 dhg group1
set Vr/0 Ip Spd/t Ike Proposal/1 Trans/2 dhg group2
```

8 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/t Ike Proposal/1 ttl 43200
```

9 Set the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/t Ike Proposal/1 softLifeTime 85
```

10 Add the *IkeSaPolicy* (*Policy)* component for IKE.

```
add Vr/0 Ip Spd/t Ike Policy/1
```

11 Specify the *description (desc)* attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 desc MDM 1
```

12 Specify the *presharedKey (key)* attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 key <you enter a key>
```

13 Specify the *retryTimerValue* (*rtv*) attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 rtv 2000
```

14 Specify the *numRetryAttempts* (*retryAttempts*) attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 retryAttempts 1
```

15 Specify the *destinationIpAddress (destAddr)* attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 destAddr x.x.x.xA
```

16 Specify the *ikeProposalLink* (*proposalLink*) attribute.

```
set Vr/0 Ip Spd/t Ike Policy/1 proposalLink ! Vr/0 Ip
Spd/1 Ike Proposal/1
```

17 Display the list of IKE policies.

```
display Vr/0 Ip Spd/t Ike Proposal/1 ikePolicyList
<ike_policy_list>
```

--End--

Example 2 of configuring IP security proposal and policy for FTP traffic

This example procedure shows the configuration of an IP security proposal and policy for file transfer protocol (FTP) traffic.

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Procedure steps

Step **Action**

1 Add the *SecurityAssociationProposal* (*Proposal*) component.

```
add Vr/0 Ip Spd/t Proposal/1
```

2 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/t Proposal/1 ttl 14400
```

3 Specify the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/t Proposal/1 softLifeTime 90
```

4 Add the *IpSecSaTransform (Trans)* component. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/t Proposal/1 Trans/1
add Vr/0 Ip Spd/t Proposal/1 Trans/2
```

5 Specify the *antiReplay (replay)* attribute, for each direction.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/1 replay off
set Vr/0 Ip Spd/t Proposal/1 Trans/2 replay off
```

6 Specify the *authAlgorithm (authAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 authAlg sha1
```

7 Specify the *encAlgorithm (encAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 encAlg des
```

8 Specify the *diffieHellmanGroup (dhg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 dhg none
```

9 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/t Policy/100
```

10 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/t Policy/101
```

11 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 action apply, direction in
```

12 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 action apply, direction out
```

13 Specify the *description* attribute for the inbound traffic.

```
set Vr/0 Ip Spd/t Policy/100 description MDM FTP in
traffic
```

14 Specify the *description* attribute for the outbound traffic.

```
set Vr/0 Ip Spd/t Policy/101 description MDM FTP out
traffic
```

15 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, protocol tcp, srcPort any, dstPort
ftp
```

16 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, protocol tcp, srcPort ftp, dstPort
any
```

17 Specify the *saProposal* attribute for both policies.

```
set Vr/0 Ip Spd/t Policy/100 saProposal Vr/0 Ip Spd/1
Proposal/1
```

```
set Vr/0 Ip Spd/t Policy/101 saProposal Vr/0 Ip Spd/1
Proposal/1
```

--End--

Example 3 of configuring IP security proposal and policy for ICMP traffic

This example procedure shows the configuration of an IP security proposal and policy for Internet control message protocol (ICMP) traffic.

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Prerequisites

- Ensure you complete the procedure, Example 1 of configuring IKE proposal and policy (page 66).

Procedure steps

Step **Action**

1 Add the *SecurityAssociationProposal* (*Proposal*) component.

```
add Vr/0 Ip Spd/t Proposal/1
```

2 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/t Proposal/1 ttl 14400
```

3 Specify the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/t Proposal/1 softLifeTime 90
```

4 Add the *IpSecSaTransform (Trans)* component. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/t Proposal/1 Trans/1
add Vr/0 Ip Spd/t Proposal/1 Trans/2
```

5 Specify the *antiReplay (replay)* attribute, for each direction.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/1 replay off
set Vr/0 Ip Spd/t Proposal/1 Trans/2 replay off
```

6 Specify the *authAlgorithm (authAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 authAlg sha1
```

7 Specify the *encAlgorithm (encAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 encAlg des
```

8 Specify the *diffieHellmanGroup (dhg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 dhg none
```

9 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/t Policy/100
```

10 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/t Policy/101
```

11 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 action apply, direction in
```

12 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 action apply, direction out
```

13 Specify the *description* attribute for the inbound traffic.

```
set Vr/0 Ip Spd/t Policy/100 description MDM ICMP in
traffic
```

14 Specify the *description* attribute for the outbound traffic.

```
set Vr/0 Ip Spd/t Policy/101 description MDM ICMP out
traffic
```

15 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, protocol icmp, srcPort any, dstPort
any
```

16 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, protocol icmp, srcPort any, dstPort
any
```

17 Specify the *saProposal* attribute for both policies.

```
set Vr/0 Ip Spd/t Policy/100 saProposal Vr/0 Ip Spd/1
Proposal/1
```

```
set Vr/0 Ip Spd/t Policy/101 saProposal Vr/0 Ip Spd/1
Proposal/1
```

--End--

Example 4 of configuring IP security proposal and policy for UDP traffic

This example procedure shows the configuration of an IP security proposal and policy for user datagram protocol (UDP) traffic.

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Prerequisites

- Ensure you complete the procedure, Example 1 of configuring IKE proposal and policy (page 66).

Procedure steps

Step **Action**

1 Add the *SecurityAssociationProposal* (*Proposal*) component.

```
add Vr/0 Ip Spd/t Proposal/1
```

2 Specify the *timeToLive* (*ttl*) attribute.

```
set Vr/0 Ip Spd/t Proposal/1 ttl 14400
```

3 Specify the *softLifeTime* attribute.

```
set Vr/0 Ip Spd/t Proposal/1 softLifeTime 90
```

4 Add the *IpSecSaTransform (Trans)* component. Add this component twice, one for each direction.

```
add Vr/0 Ip Spd/t Proposal/1 Trans/1

add Vr/0 Ip Spd/t Proposal/1 Trans/2
```

5 Specify the *antiReplay (replay)* attribute, for each direction.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/1 replay off

set Vr/0 Ip Spd/t Proposal/1 Trans/2 replay off
```

6 Specify the *authAlgorithm (authAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 authAlg sha1
```

7 Specify the *encAlgorithm (encAlg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 encAlg des
```

8 Specify the *diffieHellmanGroup (dhg)* attribute. For the *Trans/1* component, keep the default value.

```
set Vr/0 Ip Spd/t Proposal/1 Trans/2 dhg none
```

9 Add a policy for inbound traffic.

```
add Vr/0 Ip Spd/t Policy/100
```

10 Add a policy for outbound traffic.

```
add Vr/0 Ip Spd/t Policy/101
```

11 Specify the *action* attribute and *direction* attribute for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 action apply, direction in
```

12 Specify the *action* attribute and *direction* attribute for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 action apply, direction out
```

13 Specify the *description* attribute for the inbound traffic.

```
set Vr/0 Ip Spd/t Policy/100 description MDM UDP in
traffic
```

14 Specify the *description* attribute for the outbound traffic.

```
set Vr/0 Ip Spd/t Policy/101 description MDM UDP out
traffic
```

15 Specify the selector attributes for the inbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/100 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, protocol udp, srcPort any, dstPort
any
```

16 Specify the selector attributes for the outbound traffic policy.

```
set Vr/0 Ip Spd/t Policy/101 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, protocol udp, srcPort any, dstPort
any
```

17 Specify the *saProposal* attribute for both policies.

```
set Vr/0 Ip Spd/t Policy/100 saProposal Vr/0 Ip Spd/1
Proposal/1
```

```
set Vr/0 Ip Spd/t Policy/101 saProposal Vr/0 Ip Spd/1
Proposal/1
```

--End--

Example 5 of configuring the sample bypass policy for IKE traffic

This example procedure shows the configuration of a sample bypass policy for Internet key exchange (IKE) traffic

In this example procedure, the two IP addresses in the network are identified as x.x.x.xA and x.x.x.xB.

Procedure steps

Step **Action**

1 Add the policies.

```
add Vr/0 Ip Spd/1 Policy/50
add Vr/0 Ip Spd/1 Policy/60
```

2 Specify the action and direction for the policies.

```
set Vr/0 Ip Spd/1 Policy/50 action bypass, direction out
set Vr/0 Ip Spd/1 Policy/60 action bypass, direction in
```

3 Set the traffic flow policy selectors for the secure shell traffic.

```
set Vr/0 Ip Spd/1 Policy/50 srcIpAddr x.x.x.xA,
dstIpAddr x.x.x.xB, srcPort ike
set Vr/0 Ip Spd/1 Policy/60 srcIpAddr x.x.x.xB,
dstIpAddr x.x.x.xA, dstPort ike
```

--End--

Secure FTP authentication configuration

File transfer protocol (FTP) authentication between Nortel Multiservice Switch and another system can be secured on a best-effort basis or restricted to the secure type only.

In the case of best effort, the FTP authentication depends on whether the Multiservice Switch is communicating with a system that is secure or not. If the Multiservice Switch is communicating with a Nortel Multiservice Data Manager (MDM) workstation that is running the FTP daemon, then the FTP authentication will be secure, otherwise the FTP authentication will not be secured.

If the Multiservice Switch is configured to support secure FTP authentication, the Multiservice Switch can only communicate with an MDM workstation that is running the FTP secure daemon.

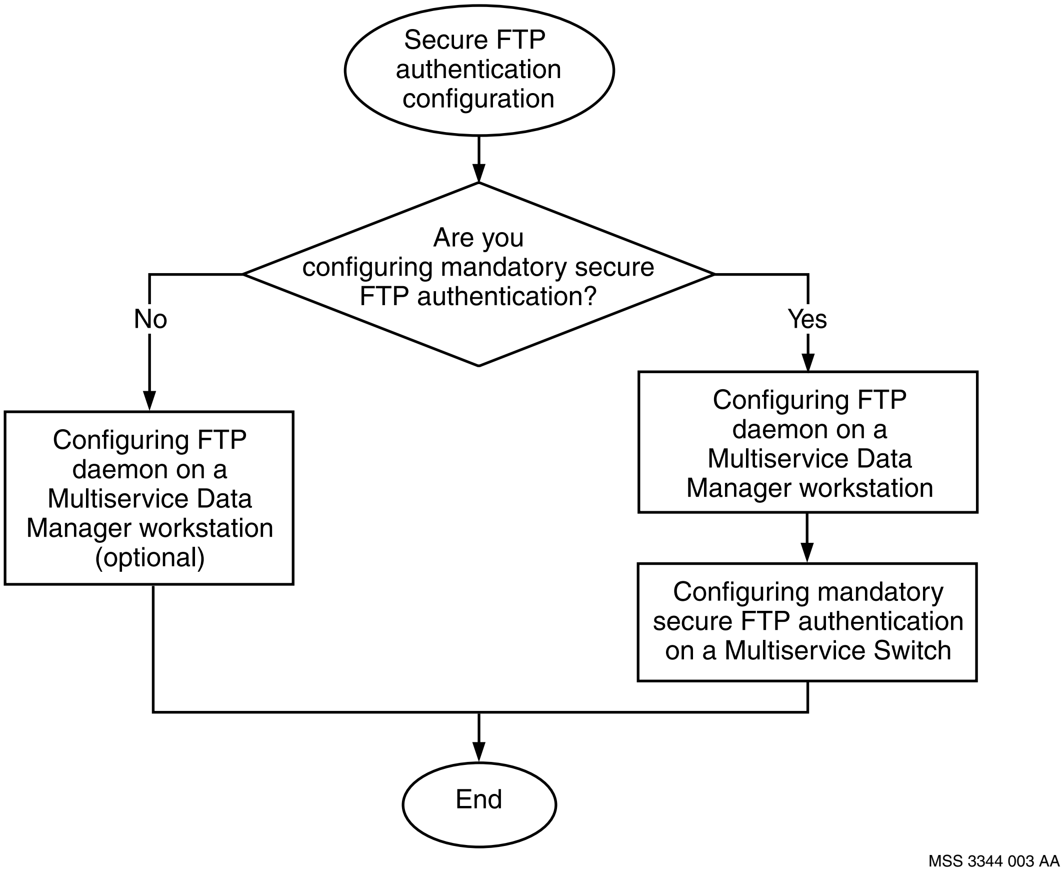
Prerequisites to secure FTP authentication configuration

- If you need to understand secure FTP authentication, see Password encryption between Multiservice Switch and Multiservice Data Manager (page 97).

Secure FTP authentication configuration procedures

This task flow shows you the sequence of procedures you perform to configure secure FTP authentication. To link to any procedure, go to Secure FTP authentication configuration procedure navigation (page 76).

Secure FTP authentication configuration procedures


Secure FTP authentication configuration
Are you configuring mandatory secure FTP authentication?
No
Yes
Configuring FTP daemon on a Multiservice Data Manager workstation (optional)
Configuring FTP daemon on a Multiservice Data Manager workstation
Configuring mandatory secure FTP authentication on a Multiservice Switch
End
MSS 3344 003 AA

Secure FTP authentication configuration procedure navigation

- For Configuring FTP daemon on a Multiservice Data Manager workstation, see NN10400-607 *Nortel Multiservice Data Manager Network Security: Secure Communications Configuration*.
- Configuring mandatory secure FTP authentication on a Multiservice Switch (page 77)

Configuring mandatory secure FTP authentication on a Multiservice Switch

Configure mandatory secure FTP authentication on a Multiservice Switch to force both the FTP client and the FTP server to support secure FTP authentication communication only.

If you do not configure the mandatory secure FTP authentication, the FTP authentication on the Multiservice Switch is a best effort. The FTP authentication depends on whether the Multiservice Switch is communicating with a system that is secure or not.The best-effort FTP authentication is the default setting.

Attention: The secure FTP authentication feature is provisioned under the CP and removing it from the feature list causes a complete shelf reload.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).

Procedure steps

Step	Action
1	Add the new security feature to the feature list of the CP. `set Software Lpt/CP0 featurelist secureFtpAuth1Only`
2	Activate the configuration changes. See Activating configuration changes (page 114).

--End--

Configuring secure shell (Ssh)

Configure secure shell (Ssh), which is a secure alternative to Telnet, to allow users to communicate with a Nortel Multiservice Switch securely via the Component Administration System (CAS). Userids and passwords used for authentication are encrypted.

Prerequisites

- If you need to understand authorized IP access, see Authorized IP access (page 96).
- For general information about secure shell and Telnet, see NN10600-030 *Nortel Multiservice Switch 7400/15000/20000 Overview*.
- The procedure in this section describes configuring secure shell (Ssh) only. Basic configuration of the node (in this case, creating an instance of a logical processor type (LPT), and adding the services to the featureList component) must be performed first. For that, add *OamEnet*, *ip* and *base* features to the feature list.
- If you have a firewall around your Multiservice Switch, open port 22, which is the port used by Ssh.

Procedure steps

Step **Action**

1 Add the feature to the feature application version list (AVL).

```
set sw avl secureShell_<version>
```

2 Add the feature to the feature list.

```
set sw lpt/cp featureList secureShell
```

3 Activate the configuration changes. See Activating configuration changes (page 114).

4 Modify your userids associated with this Multiservice Switch to include *remote* in their allowed access. *Remote* allows both Telnet and Ssh connectivity.

5 If the node has IPSec enabled, then a Ssh bypass is required for all systems that require Ssh access. In the example below, the policy numbers 10 and 20 are arbitrary numbers chosen by the user.

```
add vr/0 ip spd/1 (if security policy database ‘spd’ is
not already there)

add vr/0 ip spd/1 policy/10

add vr/0 ip spd/1 policy/20

set vr/0 ip spd/1 policy/10 action bypass, direction in

set vr/0 ip spd/1 policy/20 action bypass, direction out

set vr/0 ip spd/1 policy/10 srcipaddr <ssh client ip
addr>, dstipaddr <mss IPaddr> dstport 22

set vr/0 ip spd/1 policy/20 dstipaddr <ssh client ip
addr>, srcipaddr <mss IPaddr> srcport 22
```

Optionally, you may add srcport = <ssh client port> in policy/10 and dstport = <ssh client port> in policy/20. The default value is “any” and it allows Ssh clients running on any ports to connect to the Multiservice Switch node.

Attention: In addition to the policies to bypass Ssh, you must also setup other security policies to allow access from your network management server using the required protocols. For more information, see IP security configuration on a Multiservice Switch node (page 41).

6 Disable Telnet.

```
set nmis ssh mode sshOnly
```

Attention: It is recommended that you disable non-secure interfaces, such as Telnet, once Ssh is activated.

7 If this is the first time that Ssh is setup on this Multiservice Switch node, generate a pair of server key files.

```
serverKeyGen nmis ssh
```

8 You may need to generate a pair of client key files on the Ssh client workstation and specify “dsa” as the key type. The following is an example of the command on a Solaris Ssh client. It may be different in other operating systems.

```
Ssh-keygen -t dsa
```

9 At any time, you may choose to switch back to insecure Telnet user login by deactivating the secureShell function. To deactivate Ssh, remove the feature from the feature list and the AVL (for more information, see NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures*). Ensure that you clear the Ssh component before activating the changes.

```
clear -rf prov
```

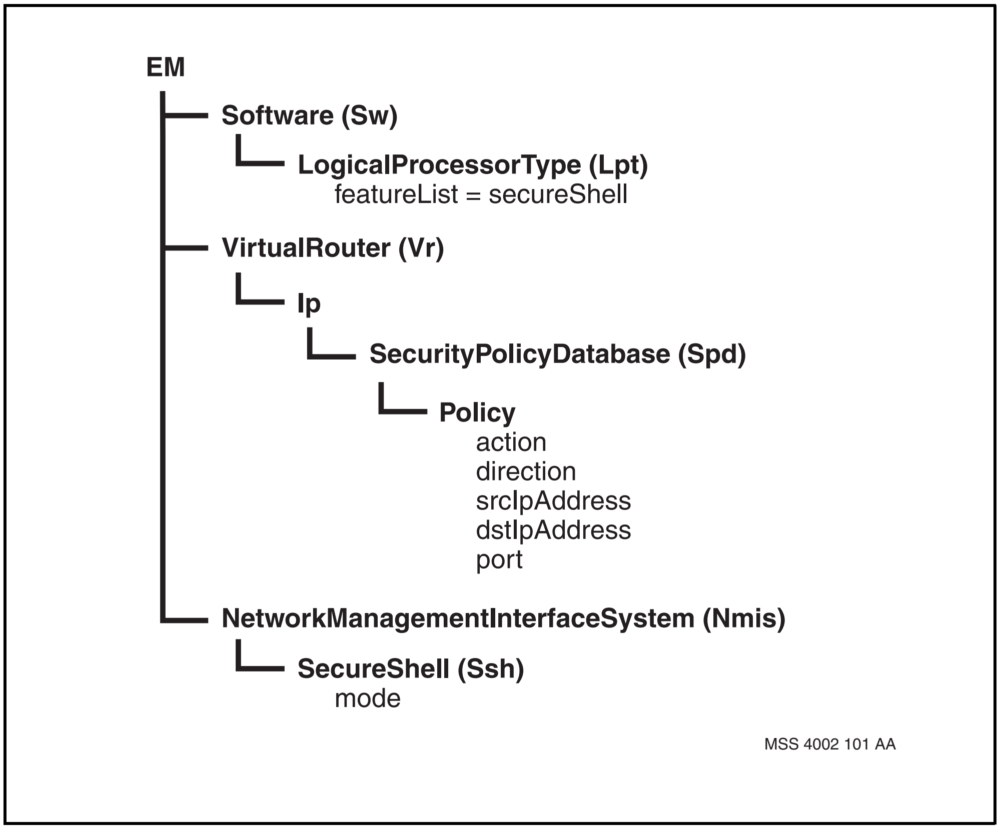
--End--

Variable definitions

Variable	Value
<mss Ipaddr>	is the IP address of the node.
<ssh client ip address>	is the IP address of the device that you want to allow access to the node.

Procedure job aid

Secure shell (Ssh) configuration component hierarchy



Configuring authorized IP access

Configure authorized IP access to specify the IP addresses of devices that you want to allow access to the node. You can also specify an entire IP subnetwork using an IP address and a subnetwork mask. The *IpAccess* component restricts access through telnet, FTP, and FMIP.

Prerequisites

- You must perform this procedure in provisioning mode. For more information, see Provisioning mode (page 114).
- If you need to understand authorized IP access, see Authorized IP access (page 96).

Procedure steps

Step	Action
1	Add an *IpAccess* component. **`add Ac IpAccess/<address>`**
2	To allow access to a subnetwork, set the subnetwork mask with the *ipAddressMask (mask)* attribute. **`set Ac IpAccess/<address> mask <mask>`**
3	Activate the configuration changes. See Activating configuration changes (page 114).

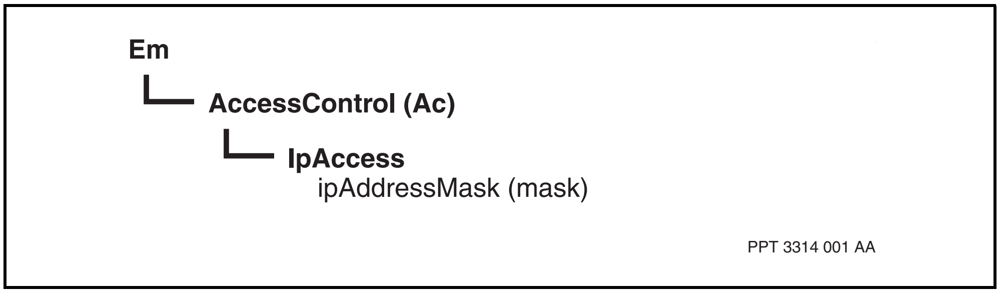
--End--

Variable definitions

Variable	Value
<address>	is the IP address of the device that you want to allow access to the node.
<mask>	is a special IP address that indicates which byte of the IP address to ignore when evaluating an incoming IP address. For example, setting the mask to 255.255.255.0 tells the node to ignore the last byte in the address. This allows all devices with their first three bytes identical to the IP address set in step 2 to access the node. The mask, combined with the IP address, defines a subnetwork.

Procedure job aid

Authorized IP access component hierarchy



User access administration and monitoring

Use the procedures in this section to monitor and control the user connections or sessions on the Multiservice Switch.

Navigation

Displaying the number of active user sessions on a node

Display the number of user sessions to determine how many users are logged in to the Nortel Multiservice Switch node and which network management interfaces they are using.

Prerequisites

- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step	Action
1	Display the number of simultaneous sessions currently active on a particular network management interface. `display Nmis <interface> activeSessions`
2	List the sessions logged in to a particular network management interface. `list Nmis <interface> Session/*`

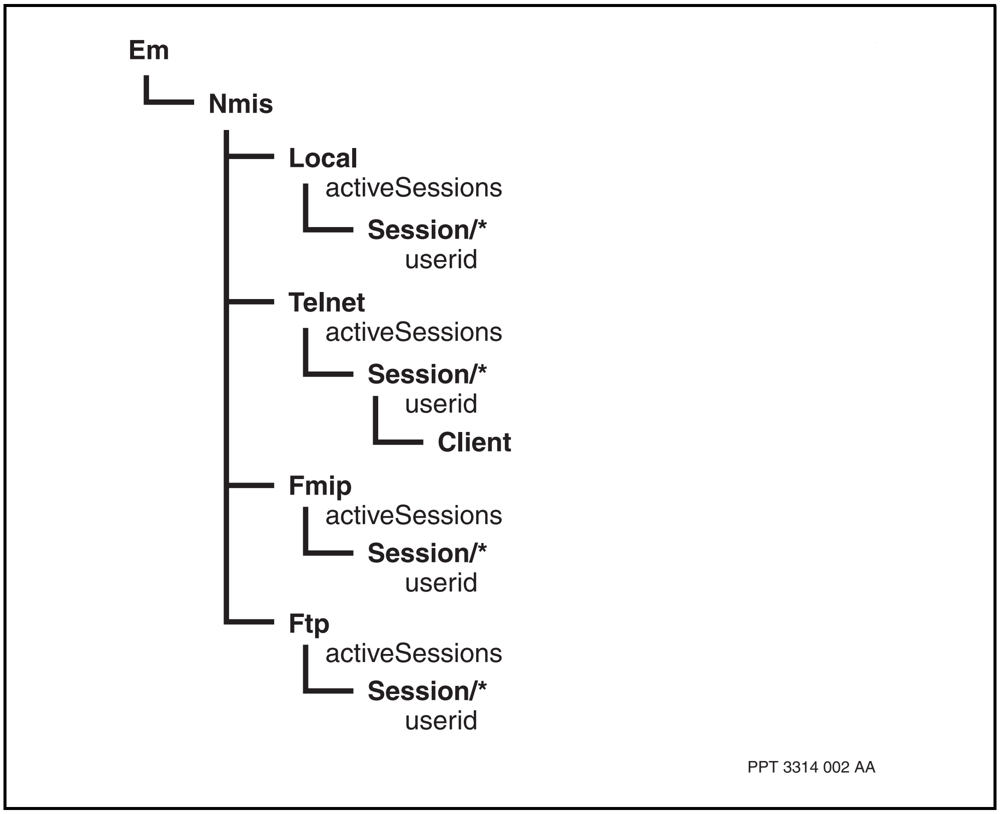
--End--

Variable definitions

Variable	Value
<interface>	is one of the network management interfaces: *Local*, *Fmip*, *Ftp*, or *Telnet*.

Procedure job aid

Active user sessions component hierarchy



Displaying the user IDs on a network management interface

Display the user IDs to determine which users are logged in to a particular network management interface.

Prerequisites

- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step	Action
1	Display all the users logged in to a network management interface. **`display Nmis <interface> Session/* userid`**

--End--

Variable definitions

Variable	Value
<interface>	is one of the network management interfaces, *Local*, *Fmip*, *Ftp*, or *Telnet*.

Restricting access through a node interface

Restrict access through a specified interface by placing the interface out of service. To place an interface out of service, lock the appropriate interface component. All current sessions continue until they are complete and no further sessions start until you unlock the interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step **Action**

1 Lock the interface component.

```
lock Nmis <interface>
```

The interface moves to a shutting-down state and does not allow setup of further sessions. All current sessions continue until they are complete.

If you lock the telnet interface while you have a current telnet session, you can still set up outgoing telnet client connections (using the *telnet Vr*, *telnet Rtr, or telnet Rtr Vrf* command), but you cannot set up new incoming telnet sessions.

--End--

Variable definitions

Variable	Value
<interface>	is one of the allowed network management interfaces: *Fmip*, *Ftp*, or *Telnet*. You cannot restrict access through the local interface. You can lock any other interface component except the interface you are currently using to access the node.

Releasing a locked network management interface

Use this procedure to release, or unlock, a locked network management interface. When you unlock an interface, it is once again available for users to set up new connections (sessions) on it.

Prerequisites

- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step	Action
1	Unlock the interface component. **`unlock Nmis <interface>`**

--End--

Variable definitions

Variable	Value
<interface>	is one of the allowed network management interfaces: *Fmip*, *Ftp*, or *Telnet*.

- Provisioning mode (page 114)

1 Activating configuration changes (page 114)

Terminating a user session on a network management interface

Terminate an individual user session on a specific interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step	Action
1	Display all current sessions. `list Nmis <interface> Session/*` This command lists all sessions on the interface. Each session has a unique instance number.
2	Find the session number belonging to the user session you want to terminate.
3	Clear the *Session* component. `clear Nmis <interface> Session/<n>` The user session terminates. If a telnet session has a client connection (as represented by the *Client* subcomponent), the command terminates the client connection too.

--End--

Variable definitions

Variable	Value
<interface>	is one of the allowed network management interface: *Fmip*, *Ftp*, or *Telnet*. You cannot terminate a user session on the local interface.
<n>	is the session number you want to terminate.

Terminating all user sessions on a network management interface

Use this procedure to terminate immediately all the user sessions on a particular interface and prevent the setup of new sessions on that interface.

Prerequisites

- You must be logged in with a user ID with a command impact of systemAdministration.
- You must perform this procedure in operational mode. For more information, see Operational mode (page 113).

Procedure steps

Step	Action
1	Force the lock on the interface component. `lock -force Nmis <interface>` The interface immediately terminates all its sessions, moves to a locked state, and does not set up further sessions.

--End--

Variable definitions

Variable	Value
<interface>	is one of the allowed network management interfaces: *Fmip*, *Ftp*, or *Telnet*. You cannot terminate user sessions on the local interface. You can lock any other interface component except the interface you are currently using to access the node.

Understanding user access

This section gives an overview of the different ways you can control access to the Multiservice Switches in your network.

Navigation

Multiservice Switch userID authentication

You access a Multiservice Switch node by logging in with a userID and password. In addition to granting or denying access to a Multiservice Switch, you can control the degree of access you grant. For example, read-only access prevents updates to any information that resides on the Multiservice Switch.

There are two different methods you can use for Multiservice Switch userID authentication:

- Centralized, by defining userIDs, passwords, and access permissions on a device other than the Multiservice Switch. Multiservice Switch uses a RADIUS server and database for this purpose. See Centralized user authentication using RADIUS (page 92).

- Local, by defining userIDs, passwords, and access permissions on the Multiservice Switch. See Local authentication (page 95).

Centralized user authentication using RADIUS

RADIUS (remote access dial-in user service) is an IP-based protocol that is commonly used to centralize the authentication of user access to network elements. It is described in RFC 2865.

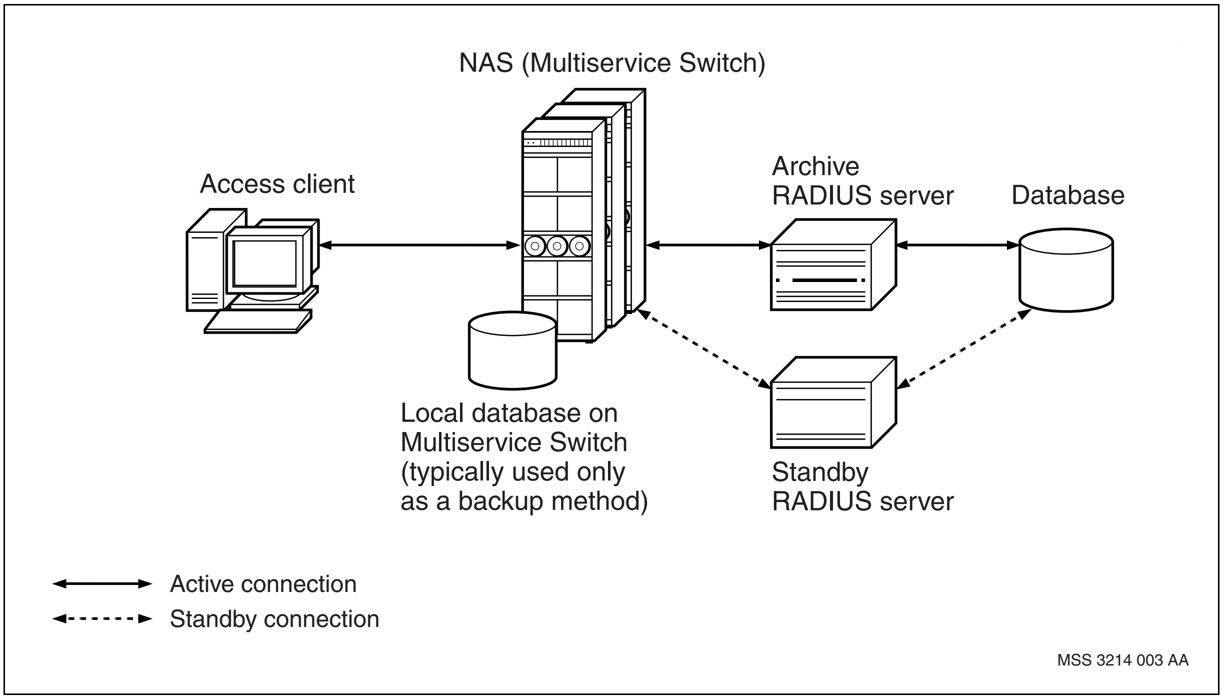
RADIUS centralized user authentication components

There are five parts to centralized user authentication using RADIUS:

- Access client, which is a user that is requesting access to the network. For example, a telnet session, a secure shell (Ssh) and an FTP session are access clients.
- Network access server (NAS), which is the Multiservice Switch itself. It receives connection requests from the access client and passes on the request and associated data, such as the userID and password, to the RADIUS server.
- RADIUS server, which authenticates the connection request. For successful connection requests, the RADIUS server returns an access authorization (Access-Accept PDU) and a list of access permissions for the userID in the form of vendor specific attributes (VSAs).
- Central database (ex: SUN ONE directory server), where each user ID associated password are stored and maintained. This server is used as a central authentication database for the Operator Client and the network elements. The User Administration system manages the information stored on this server.
- Optionally, the use of local authentication, by defining on the Multiservice Switch at least one userID with system administration permissions. This userID serves as a backup authentication method in case the RADIUS server is unavailable.
- The figure RADIUS authentication (page 93) presents the RADIUS authentication components.

> **CAUTION**
> **Risk of denied access to the Multiservice Switch**
> If the RADIUS server is unavailable and you do not have any userIDs defined locally, access to the Multiservice Switch is not possible.

RADIUS authentication



RADIUS authentication recommendations

> **CAUTION**
> **Risk of denied access to the Multiservice Switch**
> If the RADIUS server is unavailable and you do not have any userIDs defined locally, access to the Multiservice Switch is not possible.

Note the following:

- It is highly recommended that you define at least one userID locally on the Multiservice Switch in order to have a backup authentication method if the RADIUS server is unavailable. The local userID should have a command scope of network, command impact of systemAdministration, and allowed access to all network management interfaces.
- It is recommended that for redundancy purposes, each Multiservice Switch is configured with an active and a standby RADIUS server, each with its own database. For more information, see the figure Active and standby RADIUS servers.

The MDM Release 15.1 or later provides a security infrastructure that allows it to be used as a RADIUS server. For more information on centralized user authentication, see NN10400-605 *Nortel Multiservice Data Manager Network Security Fundamentals*.

Active and standby RADIUS servers

You can configure the Multiservice Switch to work with up to two RADIUS servers: one active and one standby. When using two RADIUS servers, the Multiservice Switch sends all authentication requests to the active RADIUS server, as long as it is reachable. In the event that the active server is no longer reachable, the Multiservice Switch sends authentication requests to the standby RADIUS server. When the standby RADIUS server becomes the active one, authentication requests are sent to this server until it is no longer available. This is a simple toggle mechanism with no mechanism to automatically switchover from the standby to the active server. If the user wants to force a switchover to the standby RADIUS server, the currently active RADIUS server can be locked to cause the authentication requests to switchover to the standby server. The standby server in turn becomes the active RADIUS server.

RADIUS VSAs for Multiservice Switch nodes

The RADIUS RFC 2865 defines a list of attributes that contain data about a specific user. Those attributes can be used for authentication and authorization. In order to use the RADIUS protocol to authenticate users wanting to access the Multiservice Switch, a set of vendor-specific attributes (VSAs) are defined to specify the authorization data that must be sent from the RADIUS server to the Multiservice Switch.

Each VSA required for centralized authentication is identical to a particular Multiservice Switch node attribute associated with a user that you must provision. The allowed values for each VSA and the corresponding attribute are the same.

When using remote authentication without locally defined permissions, the userIDs defined locally need to be different from those defined on the RADIUS server. If they are the same, the authentication method defaults to local for those userIDs defined both locally and remotely on the RADIUS server.

If the RADIUS server and a node are using roles, then only the role VSA needs to be returned from the RADIUS server. The other VSAs do not need to be returned to the Multiservice Switch nodes when using roles. A centrally authenticated user will get the permissions provisioned for a role whose name matches the value of the role VSA returned from the RADIUS server.

The table RADIUS VSA and matching userID and role attributes (page 95) shows a list of mandatory VSAs required to interoperate a Multiservice Switch with a RADIUS server.

For more information on the attributes associated with a user, see Multiservice Switch user requirements (page 110).

For more information on configuring the RADIUS server with Multiservice Switch VSAs, refer to NN10400-606 *Nortel Multiservice Data Manager Network Security: User Access Configuration*.

For more information on the Multiservice Switch components and attributes used with VSAs, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*.

RADIUS VSA and matching userID and role attributes

VSA	VSA value (integer)	Userid attribute (Ac Userid <attribute>)	Role attribute (Ac Role <attribute>)
Passport-Command-Scope	200	*Ac Userid commandScope*	*Ac Role commandScope*
Passport-Command-Impact	201	*Ac Userid commandImpact*	*Ac Role commandImpact*
Passport-Customer-Identifier	202	*Ac Userid customerIdentifier*	*Ac Role customerIdentifier*
Passport-Allowed-Access	203	*Ac Userid allowedAccess*	*Ac Role allowedAccess*
Passport-AllowedOut-Access	204	*Ac Userid allowedOutAccess*	*Ac Role allowedOutAccess*
Passport-Login-Directory	205	*Ac Userid loginDirectory*	*Ac Role loginDirectory*
Passport-Timeout-Protocol	206	*Ac Userid timeoutProtocol*	*Ac Role timeoutProtocol*
Passport-Role	207	na	*Ac Role*

Local authentication

The figure Local authentication (page 96) presents local authentication on the Multiservice Switch.

With this method, you maintain the userIDs and associated passwords and access permissions on each Multiservice Switch. You need to keep all associated userID information on your Multiservice Switches synchronized whenever you make any information modifications.

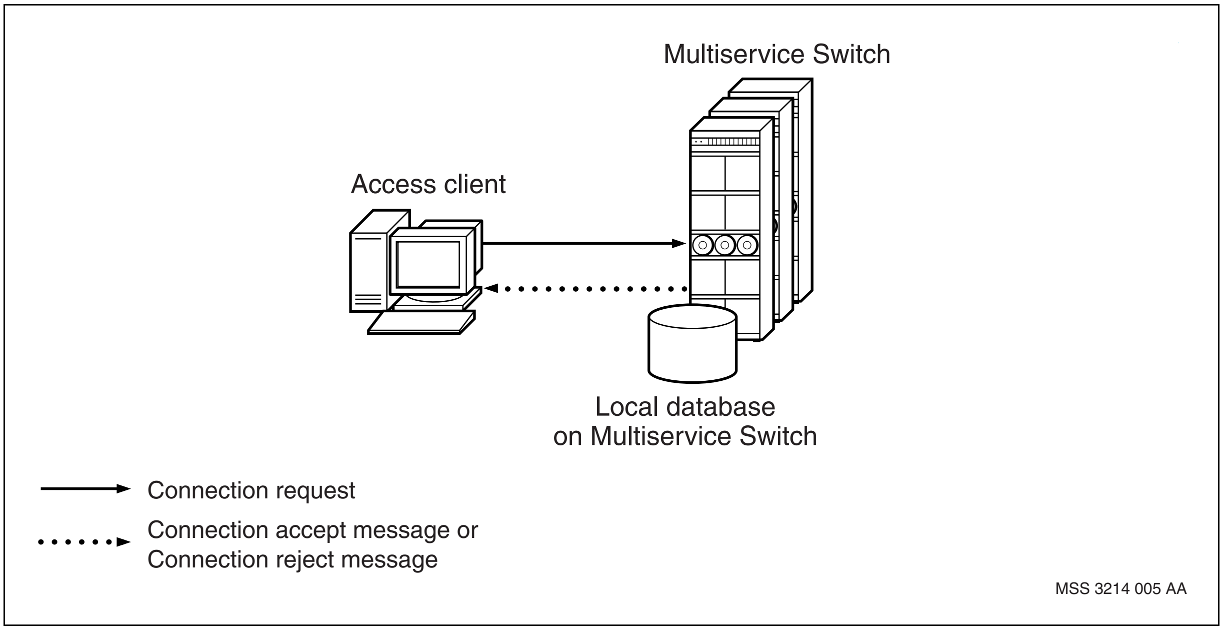
The *userId* component provides the ability to configure permissions to individual users specific to the node. If a *userId* component is configured on a node then that user is considered to be a local user.

Attention: Local does not imply a physical proximity to the node or access by way of the local console port, only that the *userId* component is defined “locally” in the local database on the Multiservice Switch. See figure, Local authentication (page 96).

A *userId* component may be defined on multiple nodes and with completely different permissions. Any permission change to the userId is independent of how the userId is configured on the other nodes.

If you use RADIUS authentication, you can still make use of local authentication as a backup method if the RADIUS server is unavailable.

Local authentication



Authorized IP access

Using the *IpAccess* component, you can specify the IP addresses of devices that you want to allow access to the node. You can also specify an entire IP subnetwork using an IP address and a subnetwork mask.

The *IpAccess* component prevents users from logging into a Multiservice Switch node from an unauthorized device. When one or more *IpAccess* components exist, the Multiservice Switch checks each authentication attempt against the list of valid IP addresses. If the authentication attempt is from a device with an invalid IP address, the Multiservice Switch rejects the attempt.

The *IpAccess* component restricts access only through telnet, FTP, and FMIP.

If you do not add an *IpAccess* component, all devices can access the node regardless of their IP address.

Password encryption between Multiservice Switch and Multiservice Data Manager

This section describes how password encryption between Nortel Multiservice Switch and Nortel Multiservice Data Manager (MDM) works, depending on which equipment initiates the connection.

Encryption on the FMIP interface

When you log in to a Multiservice Switch node from a Multiservice Data Manager workstation, the FMIP interface is used. The workstation automatically encrypts your password using a proprietary encryption algorithm before sending it to the Multiservice Switch for validation. The Multiservice Switch node decodes your password and validates it. This encryption ensures that your password travels across the network securely. All other data is sent unencrypted between the Multiservice Switch and the MDM.

Secure FTP authentication

Secure FTP authentication means that encrypted passwords are used for FTP sessions between a Nortel Multiservice Switch and a Nortel Multiservice Data Manager (MDM) workstation.

When a Multiservice Data Manager (MDM) or Management Data Provider (MDP) workstation initiates a file transfer protocol (FTP) session with a Multiservice Switch, MDM or MDP, secure FTP is used automatically. However, when a Multiservice Switch initiates an FTP session with a Multiservice Data Manager workstation, you need to configure an FTP daemon on the workstation to ensure that secure FTP authentication is used. Multiservice Switch switches initiate FTP sessions with Multiservice Data Manager workstations for the purposes of downloading software.

Client/server communication scenarios

The client and the server can use a best-effort or mandatory approach to FTP communications. The default is the best-effort approach. In a best-effort approach, either the client or the server attempts secure FTP authentication. If either end does not support the secure feature the transaction drops back to non-secure FTP communication. This applies to both the Multiservice Data Manager and Multiservice Switch sides of the communications link.

- **secure client with non-secure server:** the client first attempts secure FTP but the server fails the communications and causes the client to drop back to non-secure FTP.
- **non-secure client with secure server:** the client initiates non-secure FTP with the server. The Multiservice Switch server determines if the secure-only FTP feature is provisioned. If yes, the communication fails and

the connection is closed. If it is not provisioned, the non-secure FTP proceeds over this connection.

- **secure client with secure server:** both client and server proceed with the secure FTP communications and its authentication mechanism.

In addition to the ability to ensure secure FTP authentication for sessions between MDM/MDP workstations and Multiservice Switches, there is a provisionable feature that forces FTP communications on the Multiservice Switch to be restricted to the secure type only.

IP security

IP security (IPSec) is a standard for implementing security measures at the IP layer. IPSec helps to ensure a more secure overall network by protecting applications and securing communications across LANs, private WANs, public WANs, and the Internet.

Configuring IPSec provides security for OAM traffic flowing between Nortel Multiservice Switch nodes, or between Multiservice Switch nodes and Nortel Multiservice Data Manager (MDM) workstations. Security protocols such as encapsulating security payload (ESP), along with key management, help to secure communication across an insecure network. Security policies (SP) define the security services to be applied to specific IP traffic flows. It is the user or system administrator who selects the SPs.

Secure communication between two peers is established in a two stage process: authentication and key management. Mutual authentication is required to ensure the authenticity of both parties. Both peers must use the same key.

The following sections provide detailed conceptual information about IPSec:

- Security policies (page 99)
- Security associations (page 99)
- Authentication and encryption algorithms (page 104)
- Key management (page 105)
- Anti-replay (page 106)
- IP flow filtering versus IP security (page 106)
- IP security and secure shell interworking (page 106)

Security policies

Security policies determine what security services are applied to specific OAM traffic. All security policies are contained within the security policy database (SPD).

IPSec is applied to all IP traffic flows either terminating on or locally generated from the device (Multiservice Switch, Multiservice Data Manager workstation, or Windows-based PC), depending on the selector associated with the packet and how it relates to the SPD. Selectors define the criteria used in determining how IP security protocols are applied to a given packet. On Multiservice Switch nodes, one of three actions can be provisioned under the *policy* component: bypass, discard, or apply.

Security associations

IPSec services are defined and executed through security associations (SAs). An SA is a one-way relationship that is defined between a sending and receiving host. An SA is a set of policy and key used to protect information. IPSec services are applied to the traffic that is carried on SAs.

To create a peer relationship for a two-way secure exchange, you need to create two SAs. An SA is uniquely identified by three parameters: a security protocol identifier, an IP destination address, and a security parameter index (SPI). Nortel Multiservice Switch nodes and Nortel Multiservice Data Manager (MDM) workstations establish an SA by negotiating certain security parameters that are defined in the security policy database (SPD).

All active SAs within a node are contained in the security association database (SAD). For outbound processing, meaning packets that are generated locally and flow out of the workstation, each SA is associated with a security policy within the SPD. If an SA cannot be matched to a policy within the SPD, the OAM packet is discarded. For inbound traffic, meaning traffic that flows in from the workstation and is terminated locally, the SA entry applied to that packet is found within the SAD using fields in the IPSec packet. Both peers must be in agreement with the SA parameters specified.

Currently, SAs are limited to point-to-point type connections only: you cannot configure a point-to-multipoint SA. Therefore, if you do not plan your SAs in advance, you could end up with a potentially unmanageable number of connections as your network grows.

Internet key exchange

The Internet key exchange (IKE), as defined in RFC2409, is an hybrid protocol that implements the Oakley and Skeme key exchanges inside the ISAKMP framework. The IKE protocol reduces the required manual configuration to establish the IPSec SA used for secure communication between two peers (Nortel Multiservice Data Manager and Multiservice Switch 15000/20000).

Internet key exchange processing

IPSec SAs using IKE are set up in two phases: phases 1 and 2.

For details about supported authentication and encryption algorithms, see Authentication and encryption algorithms (page 104).

The purpose of phase 1 is to establish a secure and authenticated channel between ISAKMP peers. Phase 1 SA is the first level SA of IKE which provides the channel with which the nodes establishing IKE communicate. The phase 1 SA is the control channel connection.

During phase 1, there are two modes of exchange: main and aggressive. Only the main mode is supported on the Multiservice Switch 15000/20000 and is described here.

The main mode has the following characteristics:

- is a mandatory part of the IKE RFC 2409
- is used for identity protection and the ISAKMP identity protect exchange
- allows for greater flexibility than aggressive mode
- generates authenticated keying material from a Diffie-Hellman exchange
- must be selected when a pre-shared key approach of key management is used
- is a 6-message exchange

The following attributes are negotiated as part of phase 1, main mode:

- encryption algorithm
- hash algorithm
- authentication method
- information about a group over which to do Diffie-Hellman

The figure, Main mode, phase 1 SA set up (page 102), illustrates the following steps:

1 Initiation request. The initiator of the IKE exchange sends the initiation request. The initiator can propose several proposals for the responder to respond to. These proposals are in order of priority for the initiator.

2 Response message to the initiation message. This message contains the response proposal from the responder. The proposal is a selected one contained in the list of proposals sent by the initiator. The responder selects this proposal based on its own priority of proposals defined or supported. This ends the first exchange in the main mode messaging.

3 Response message to the initiation message. This is the second exchange in the main mode messaging which includes the key exchange payload.

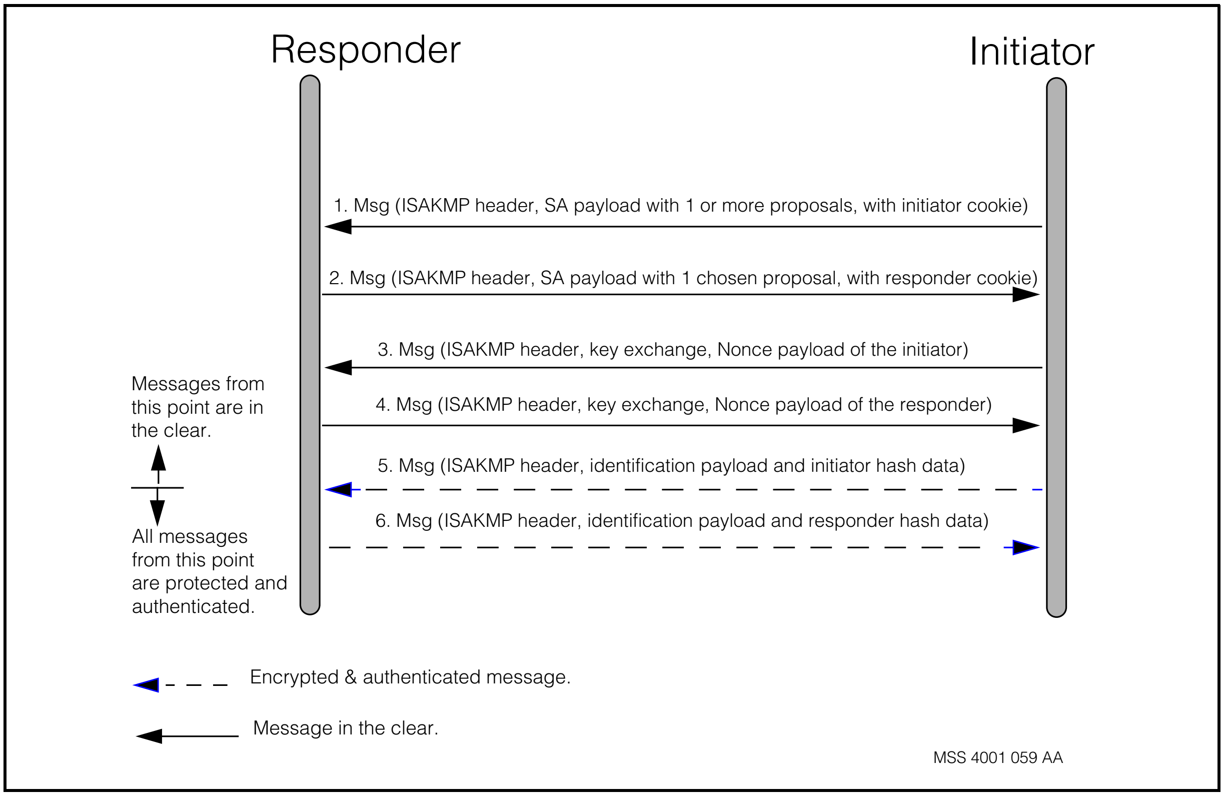
4 Response message to the key exchange message. This step completes the second exchange in the main mode messaging and is the last main mode message to go in the clear.

The key exchange message from the responder is the same as the key exchange message from the initiator, except that the key exchange data contains the responder Diffie-Hellman data and the nonce data is also that of the responder.

5 Hash data exchange. This is the third exchange for the main mode. The hash data exchange is authenticated or encrypted or both based on the negotiated transform and so are any following messages from this point.

6 Response message to the hash exchange message. This step completes the last exchange in the main mode messaging. This last message is similar to the message sent in step 5, with the exception that the hash data is from the responder.

Main mode, phase 1 SA set up


Responder
Initiator
1. Msg (ISAKMP header, SA payload with 1 or more proposals, with initiator cookie)
2. Msg (ISAKMP header, SA payload with 1 chosen proposal, with responder cookie)
3. Msg (ISAKMP header, key exchange, Nonce payload of the initiator)
4. Msg (ISAKMP header, key exchange, Nonce payload of the responder)
5. Msg (ISAKMP header, identification payload and initiator hash data)
6. Msg (ISAKMP header, identification payload and responder hash data)
Messages from this point are in the clear.
All messages from this point are protected and authenticated.
Encrypted & authenticated message.
Message in the clear.
MSS 4001 059 AA

The purpose of the IKE phase 2 negotiation is to set up the IPSec SA. The phase 2 SA is the data channel connection which uses the phase 1 control channel to set itself up. Other non-ISAKMP SAs can be set up as part of this phase as well. However, only IPSec ESP SAs are supported on the Nortel Multiservice Switch. In this phase, the keying material is exchanged as well as the time to live and the method of securing the SA is negotiated. The mode used during phase 2 for negotiating the IPSec SA is called the quick mode.

The figure, Quick mode, phase 2 SA set up (page 103), illustrates the three key messages for the quick mode exchange:

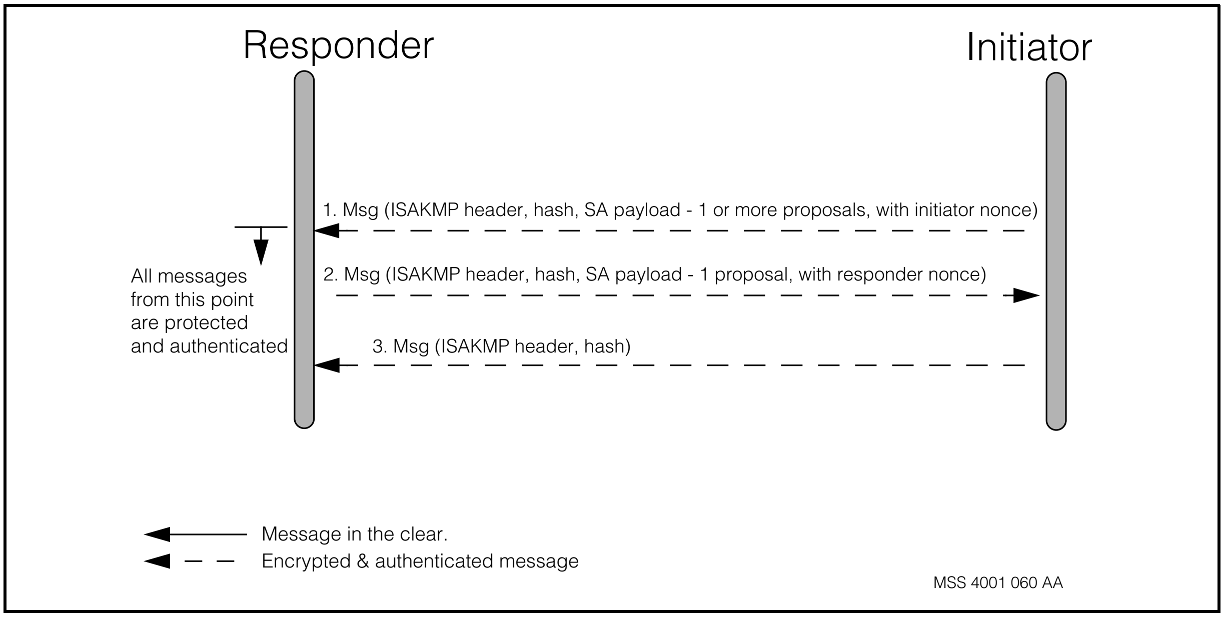
1 Proposal message. This is the initiation message for phase 2. The initiation message can be sent by either the initiator or the responder in the phase 1 exchange.

2 Reply message. The responder replies with a message that contains the selected AH transform.

3 Identity protect message. Upon receipt of the reply, the SA at the initiator end is set up. The initiator sends the hash message which is used to avoid replay attacks. The SA at the responder end is up once this message is received and processed successfully. This message is used for identity protection.

To support the perfect forward secrecy (PFS), the key exchange (KE) payload is exchanged as part of the base quick mode message from the initiator and then in response to the responder. The key exchange payload is included in the message after the nonce payload and before the identification payload.

Quick mode, phase 2 SA set up


Responder
Initiator
1. Msg (ISAKMP header, hash, SA payload - 1 or more proposals, with initiator nonce)
All messages from this point are protected and authenticated
2. Msg (ISAKMP header, hash, SA payload - 1 proposal, with responder nonce)
3. Msg (ISAKMP header, hash)
Message in the clear.
Encrypted & authenticated message
MSS 4001 060 AA

Security protocol identifier

The security protocol identifier specifies the type of security protocol you apply to an SA. Nortel Multiservice Switch supports encapsulating security payload (ESP) in transport mode only. ESP is used for data integrity protection.

Encapsulating security payload

The encapsulating security payload (ESP), as defined by RFC2406, can provide a mix of the following security services: confidentiality, data origin authentication, connectionless integrity, and traffic flow confidentiality. The set of security services provided depends on the options selected at the time the SA is established. Encryption and authentication are optional services, however at least one of them must be selected.

Transport mode

Transport mode extends protection to the payload of an IP packet. When a host runs ESP, the payload is the data that normally follows the IP header. Transport mode is typically used for end-to-end communications between two hosts and can be sufficient for securing a corporate network.

Destination IP address

With Nortel Multiservice Switch, you can only specify unicast addresses as the destination address.

Security parameter index

The security parameter index (SPI) is a hex string that is automatically assigned to an SA. The SPI is carried in the AH or ESP header.

Authentication and encryption algorithms

When you define an SA, you must also specify authentication and encryption algorithms.

For ESP, you must specify at least one of the authentication and encryption algorithms. Nortel Multiservice Switch supports the advanced encryption standard (AES), data encryption standard (DES) and the triple DES for encryption and secure hash algorithm 1 (SHA1) and message digest 5 (MD5) for authentication.

For manual SA configuration, you can use any authentication and encryption algorithms combination.

For automated SA configuration using IKE (phases 1 and 2), you can use the supported combinations of authentication and encryption algorithms.

IKE phase 1 supports the following combinations of authentication and encryption algorithms:

- DES and MD5
- DES and SHA1
- 3DES and MD5
- 3DES and SHA1

Attention: IKE phase 1 supports the Diffie-Hellman group 1 or 2.

IKE phase 2 supports the following combinations of authentication and encryption algorithms:

- AES and SHA1
- DES and MD5
- DES and SHA1
- 3DES and MD5
- 3DES and SHA1
- none and MD5
- none and SHA1

Attention: IKE phase 2 supports the Diffie-Hellman group 1 or 2.

Key management

Nortel Multiservice Switch nodes support automated and manual key management.

Automated key management

IKE supports the following authentication methods for automated key management:

- digital signatures
- two forms of authentication with public key encryption
- pre-shared keys

The current implementation of IKE between the Multiservice Switch 15000/20000 and the Multiservice Data Manager supports the pre-shared key only for automated key management. With the pre-shared key authentication method, the shared secret string is configured on both peers before they can authenticate each other. Sharing a pre-shared key among multiple nodes is not recommended because it reduces the key secret level.

The perfect forward secrecy (PFS) is a cryptographic property that ensures that one derived key is not used to derive subsequent keys for the IPSec SA set up. Therefore, if a key is compromised, PFS ensures that other previous or subsequent keys are not compromised.

To provide PFS for a particular IPSec SA, a Diffie-Hellman group must be selected and negotiated before the SA is established. The selection and negotiation of a Diffie-Hellman group can be done by setting that group within the ESP protocols of an IPSec proposal during the IKE phase 2 exchange.

Manual key management

Key distribution can be configured manually on Nortel Multiservice Switch nodes and Nortel Multiservice Data Manager. An encryption key, an authentication key, or both may be required to protect an IPSec session. These keys must be unique and random. They must also be symmetrical, meaning that for a given SA, those configured on a node must be the same as those configured on the workstation.

In order to ensure secure distribution of these keys, an SA must be established prior to sending provisioning data from the workstation to the node. The first SA must be added through a console port directly connected to the node. Distribution of the key to the console administrator of the node can be done by telephone, registered mail, or secure email. After the first SA is established and traffic is protected, keys can be refreshed using this SA.

Anti-replay

The Multiservice Switch IPSec SA supports an anti-replay mechanism to prevent packets from being processed more than once or replayed. The anti-replay capability can be disabled or enabled by the receiver on a per policy basis. The anti-replay is set to disabled by default.

Each packet is sent with a unique sequence number that is used to check for duplicate packets. The sequence number is initialized to zero when an SA is established and is incremented with each packet sent over the same SA. The first packet sent for a given SA has a value of one.

If the receiver has set anti-replay to enabled, the sequence number of each packet received on that SA is verified to ensure that it does not duplicate the sequence number of any other packet received during the life of that SA.

The sender checks to ensure that the counter has not cycled (32-bit value) before inserting the new value in the sequence number field. The sender does not send the packet if doing so can cause the sequence number to cycle. In this case, a new SA is established.

If the receiver disables the anti-replay for an SA, no inbound checks are performed on the sequence number. The sender still increments the counter. When the counter reaches the maximum value, the sequence number is set to zero.

IP flow filtering versus IP security

When IP security (IPSec) is enabled on OAM access cards (function processors) that support hardware IP flow filtering, use the deny functionality of IP flow filtering instead of IPSec. Packets will be discarded faster and there will be less congestion on the control processor (CP). However, IP flow filtering is not as granular as IPSec. For this reason, if you require filtering on the protocol or at the TCP/IP port level, use IPSec. For more information about IP flow filtering, see NN10600-800 *Nortel Multiservice Switch 7400/15000/ 20000 IP Technology Fundamentals*.

IP security and secure shell interworking

If IP security (IPSec) is enabled on the Multiservice Switch and a system wants to access the Multiservice Switch using the secure shell (Ssh), then you must configure a policy for Ssh. This policy is an Ssh bypass for all systems that require Ssh access to the Multiservice Switch in conjunction with IPSec. For more information on configuring this bypass policy, refer to Example 4 of configuring the sample bypass policy for secure shell traffic (page 53).

Secure shell (Ssh)

A secure shell (Ssh) server on the Multiservice Switch provides the capability for an operator to connect to the node in such a way that all authentication information and subsequent session traffic is encrypted for increased security.

The network management interface system (Nmis) framework provides Ssh server capability to secure authentication and encrypted transport. Customers are able to use Ssh as a replacement for telnet to access Multiservice Switch. Customers are able to configure their MSS to support:

- Ssh and telnet
- Ssh only

Ssh clients

When the Ssh server is activated and configured on the MSS switch (see Configuring secure shell (Ssh) (page 78), an operator can connect to the MSS using a Ssh client. The recommended Ssh clients are listed below.

- SSSH: Solaris SSH by Sun Microsystems on Solaris 9 of their operating system
- OpenSSH: from OpenSSH from a XP-based PC
- Mindterm (used by Java based Ssh client)

The Multiservice Switch Sshd provides support for Ssh clients that have the following capabilities:

- SSH version 2 support only for enhanced SSH security.

- Support SSH host to host public/private key authentication Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification.
- Support for HMAC-SHA1-160, HMAC-SHA1-96, HMAC-MD5-128, HMAC-MD5- 96 Message Integrity.
- Session Symmetric Cryptography to support AES256-CBC, RIJNDAEL256-CBC, AES192-CBC, RIJNDAEL192-CBC, AES128-CBC, RIJNDAEL128-CBC, BLOWFISH-128-CBC, 3DES-192-CBC, ARCFOUR-128.

Ssh server host key

When Ssh is provisioned, the server host key pair represents the identity of the Ssh server on the Multiservice Switch. This identity is generated when the secure shell feature is activated.

This key pair can be regenerated by the command *serverKeyGen* for security reasons or when the key files are corrupted. For more information on this command, see NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

Firewalls

For customers wishing to access the Multiservice Switch through a firewall device, the following list contains the ports used by the Multiservice Switch for operations, administration, and maintenance (OAM) functions:

- PING (packet internet groper): 9595
- FMIP (fast management information protocol): 5928
- SFTP (secure file transfer protocol): 2374, 2373

  The SFTP port is used for secure FTP authentication.
- FTP (file transfer protocol): 20, 21
- Telnet: 23
- RADIUS (remote authentication dial-in service): 1812
- NTP (network time protocol): 123

Multiservice Switch idle session timeout

Nortel Multiservice Switch nodes support a configurable inactivity interval timer that automatically detects and terminates idle Telnet and local console port sessions. When the idle session times out, system resources held by the session are released and new sessions can be created.

A single session can be held on each of the active and standby CPs through the local operator. The local and Telnet *timeoutPeriod* attribute is disabled by default, meaning sessions can remain idle indefinitely. This state of inactivity uses up system resources needlessly as well as offers a security risk since unauthorized access is a possibility. With a command impact of *systemAdministration*, you can provision the *timeoutPeriod*, meaning that each session will be tracked for inactivity. If a session remains idle for a provisioned length of time (5 to 120 minutes), the user is logged out. If that user wants to reconnect, username and password have to be re-entered.

Attention: A warning message will be issued one minute prior to the session being terminated. For example, if the *timeoutPeriod* has been set to 10 minutes and a session has been idle for 9 minutes, the user will receive a warning that they will be logged out of that session in 1 minute.

The *timeoutPeriod* is applicable to all sessions that are created after this attribute is set. If the value of the *timeoutPeriod* is changed, only new sessions created after the activation will be affected.

Any user can display the *idleTime* of an operator session. This attribute is read-only and indicates how long a session has been inactive, even if the *timeoutPeriod* attribute is disabled.

Attention: A local or Telnet session is only considered to be idle after the final response of a command has been printed on the interface and no subsequent commands have been entered.

All terminations due to inactivity are logged and an override capability is available. The override capability allows users with a command impact of *systemAdministration* to disable the *timeoutProtocol* for specific userIDs. Those userIDs for which the timeoutProtocol has been disabled are exempt from inactivity tracking. The timeoutProtocol is enabled by default, therefore, when a timeoutPeriod has been configured, it applies to all local sessions.

Pre-login warning banner

A pre-login default warning banner is displayed before the login prompt for any local, Telnet or Ssh session. This default warning banner is not a file, it is embedded into the code. Thus, the default banner cannot be modified or deleted by the operator.

As an alternative to the default banner, a user-defined static warning banner can be displayed. The text for this banner is saved as a banner.txt file. This file is not provisioned on the switch, instead it is downloaded via FTP and stored in the directory sfs/system/banner. If the banner.txt file is inaccessible, the default banner text is displayed instead.

The banner display makes the Multiservice Switch compliant with the following standards:

- Requirement number R3-83[51]; specs GR-815-CORE, Generic Requirements for Network Element/Network System (NE/NS) Security, Issue 2, March 2002, Telcordia.
- Requirement number M-48; specs T1.276-2003, OAM and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane, July 23, 2003, ANSI.

Telnet or Ssh command logging

To enhance the security of a Multiservice Switch, the commands issued from the originating node to establish and terminate a telnet or Ssh session are logged in the Multiservice Switch log stream, in two separate log records. A log record is also generated when an outgoing telnet or Ssh session fails. These commands are logged for components *Virtual Router* (*Vr*), *Router* (*Rtr*), and *VpnRouteForwarder* (*Vrf*). These log records are useful for auditing purposes. For more information on telnet commands, refer to NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

Multiservice Switch user requirements

To access Nortel Multiservice Switch nodes, privileges must be defined for the user that determine how the user can manipulate the node.

To manage the node, permissions must be defined regardless if a user is using Local authentication (page 95) or Centralized user authentication using RADIUS (page 92).

The permissions the user has for managing the node are defined using the following:

- Command scope (page 110)
- Command impact (page 110)
- Customer identifier (page 111)
- Allowed access (page 111)
- Allowed out access (page 112)
- Login directory (page 112)
- Timeout protocol (page 112)

Command scope

The command scope determines the components on which the user is allowed to execute commands. Each user and each component has a command scope. To execute a command on a component, you must have a command scope equal to or greater than the scope of that component. The table Component scope values (page 110) shows the possible scopes, from highest to lowest.

Component scope values

Impact	Components that
Network	Affect the operation of the entire network
Device	Affect the operation of a node
Application	Affect the operation of a single service application or access port

Command impact

Command impact defines the importance of the commands a user can execute. Each user has a command impact. As well, each command includes a verb with an associated impact. To execute a command, you must have a command impact equal to or greater than the verb impact. The table Command and verb impacts (page 111) shows the possible impacts, from highest to lowest.

Command and verb impacts

Impact	Verbs that
debug	Issue all commands including debugging commands. **Attention:** The debug level is not recommended for customer use and is typically limited for use by Nortel Networks support personnel, if required.
systemAdministration	Change the security of the node
configuration	Change the configuration of the node
service	Maintain services
passive	Display information about the node and services, but do not affect the operation or configuration of the node

Customer identifier

The customer identifier (CID) tells the system which customers have operational authority over each component. The CID is in the command messages that you send. You can perform operational commands only on those components that belong to the same CID as you. When you assign a

CID to a component, any subcomponents that are to be accessed by that user must have the CID manually provisioned to the same value as that of the CID assigned to the parent component. Those subcomponents that already have a CID provisioned retain that value, regardless of the CID assigned to the parent component.

The network owner, known as the network manager, has a special CID of 0 (zero). Only users with a CID of 0 (zero) can do provisioning procedures.

Allowed access

CAUTION

Risk of system failure

Do not use the file transfer protocol (FTP) access to delete files or directories from the Nortel Multiservice Switch provisioning file system because the Multiservice Switch can fail. To delete files or directories from the Multiservice Switch provisioning file system, use the *tidy prov* command. For more information about the *tidy prov* command, see NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*.

Allowed access specifies which network management interfaces (local, Telnet, Ssh, FMIP or FTP) the user can use to access the node. An allow access value of *remote* gives access to both Telnet and Ssh.

For more information on network management interfaces, see NN10600-030 *Nortel Multiservice Switch 7400/15000/20000 Overview*.

Allowed out access

Allowed out access indicates if the user is allowed outgoing Telnet access from the node. If it is set to *telnet*, you can Telnet out of a node.

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

Login directory

When you log into a node through FTP, the system places you into a default directory. Login directory specifies this default login directory, which is similar to the home directory in UNIX for a User ID.

Timeout protocol

Timeout protocol specifies whether the user can override the specified time period that a Telnet session and a local session can be idle before being terminated.

Roles on Multiservice Switch nodes

A role is used to assign centralized user access privilege to groups of users based on a job function.

Nortel Multiservice Switch nodes have a *role* component, which uses the same attributes for defining user requirements. See Multiservice Switch user requirements (page 110).

An operator's permissions can change depending on how the role is defined on each node in the network. Although the role is defined on each node the permissions associated with the role can differ, depending on the settings for that specific role.

If the role is defined differently on the remote server than on the node, the *remoteOverride* attribute determines which definition is used for defining the role permissions.

Procedure conventions

This document uses the following procedure conventions:

- You can enter commands using full component and attribute names, or you can abbreviate them. The commands used in the procedures contain the full component and attribute names in the first instance. In the second instance, the component and attribute names are abbreviated. For more information on abbreviating component and attribute names, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*. All component and attribute names are formatted in italics.
- The introduction of every procedure states whether you must perform the procedure in operational mode or provisioning mode. For more information on these modes, see Operational mode (page 113) or Provisioning mode (page 114).
- When you complete a procedure, you can verify your changes and then activate them as the new node configuration. For more information on completing configuration changes and exiting provisioning mode, see Activating configuration changes (page 114).

Operational mode

Procedures contained within this document can either be performed in operational mode or provisioning mode. When you initially log into a node, you are in operational mode. Nortel Multiservice Switch systems use the following command prompt when you are in operational mode:

```
#>
```

where:
# is the current command number

In operational mode, you work with operational components and attributes. In operational mode, you can

- list operational components and display operational attributes to determine the current operating parameters for the node
- control the state of parts of the node by locking and unlocking components

- set certain operational attributes and enter commands to perform diagnostic tests

Provisioning mode

To change from operational mode to provisioning mode, type the following command at the operator prompt:

```
start Prov
```

Only one user can be in provisioning mode at a time. Nortel Multiservice Switch systems use the following command prompt whenever you are in provisioning mode:

```
PROV #>
```

where:

# is the current command number

In provisioning mode, you work with the provisionable components and attributes that contain the current and future configurations of the node. You can add and delete components, and display and set provisionable attributes. For information on completing the configuration changes, exiting provisioning mode, and returning to operational mode see Activating configuration changes (page 114).

For information on operational and provisionable attributes, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*.

Activating configuration changes

Several procedures in this document ask that you complete the configuration changes. When you complete the configuration changes, you are activating the configuration changes, confirming that you want to activate them, and saving the changes. You are instructed to complete the configuration changes only at the end of procedures that you perform in provisioning mode.

CAUTION

Activating a provisioning view can affect service

Activating a provisioning view can result in a CP reload or restart, causing all services on the node to fail. See NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*, for more information.

CAUTION

Risk of service failure

When you activate the provisioning changes (see step 3), you have 20 minutes to confirm these changes. If you do not confirm these changes within 20 minutes, the shelf resets and all services on the node fail.

1 Verify that the provisioning changes you have made are acceptable.

```
check Prov
```

Correct any errors and then verify the provisioning changes again.

2 If you want to store the provisioning changes in a file, save the provisioning view.

```
save -f(<filename>) Prov
```

3 If you want these changes as well as other changes made in the edit view to take effect immediately, activate, confirm, and commit the provisioning changes.

```
activate Prov
confirm Prov
commit Prov
```

4 End the provisioning session.

```
end Prov
```

Nortel Multiservice Switch 7400/15000/20000

Security Management

Publication: NN10600-601
Document status: Standard
Document issue: 7.2S2
Document date: April 2006
Product release: PCR7.2 and up
Job function: Administration and Security
Type: NTP
Language type: US English