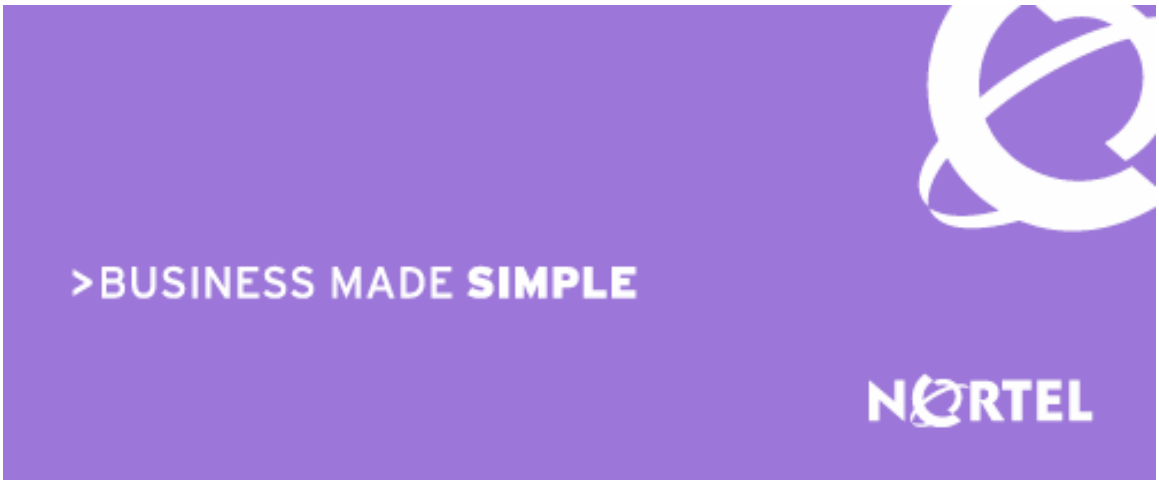


Ethernet Routing Switch 8600
Engineering

> Simple Network Management Protocol (SNMP) for ERS 8600 Technical Configuration Guide

Enterprise Business Solutions
Document Date: April 4, 2007
Document Number: NN48500-564
Document Version: 2.1

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Abstract

This Technical Configuration Guide (TCG) provides an overview on how to configure SNMP (Simple Network Management Protocol) on the Nortel Ethernet Routing Switch (ERS) 8600.

Table of Contents

1. SNMPV3 OVERVIEW 5

2. SNMP UPGRADE CONSIDERATIONS 6

2.1 HIDDEN FILE DETAILS 6

3. BLOCKING SNMP 7

3.1 BLOCKING SNMPV1/2 ONLY 7
3.2 BLOCKING SNMP VIA AN ACCESS POLICY – PRIOR TO SOFTWARE RELEASE 3.7.9 OR 4.1 7
3.3 SNMP GROUP ACCESS POLICY – RELEASE 3.7.9, 4.1 OR HIGHER 9
3.4 NEW DEFAULT COMMUNITY STRINGS IN HIGH SECURE (HSECURE) MODE 20

4. SNMP SETTINGS 21

5. SNMP WITH RADIUS AUTHENTICATION AND ACCOUNTING 23

6. CONFIGURING SNMPV3 24

6.1 LOADING THE DES OR AES ENCRYPTION MODULE 24
6.2 ADDING A NEW SNMPV3 USER TO USM TABLE 24
6.3 ASSIGN USM USER TO USM GROUP 25
6.4 ASSIGNING THE USM GROUP ACCESS LEVEL 27
6.5 ASSIGNING THE MIB VIEW TO THE USM GROUP 28
6.6 CREATING A MIB VIEW 29

7. CONFIGURATION EXAMPLE: CHANGING SNMP COMMUNITIES 30

7.1 CONFIGURATION EXAMPLE: SNMP COMMUNITIES WITH RELEASE 3.5 30
7.2 CONFIGURATION EXAMPLE: CHANGING THE DEFAULT SNMP COMMUNITY NAME WITH RELEASE 3.7 OR 4.1 31
7.3 CONFIGURATION EXAMPLE: ADDING A NEW SNMP COMMUNITY TO AN EXISTING SNMP GROUP MEMBER 31
7.4 TESTING SNMP USING DEVICE MANAGER 34
7.5 CONFIGURATION EXAMPLE: CHANGING THE MIB VIEW FOR AN SNMPV1/2 COMMUNITY 34

8. CONFIGURATION EXAMPLE USING SNMPV3 36

8.1 TESTING SNMPV3 USING DEVICE MANAGER 37

9. SOFTWARE BASELINE 39

10. REFERENCE DOCUMENTATION 40

11. APPENDIX A: CONFIGURATION FILES 41

11.1 FROM CONFIGURATION EXAMPLE 7.5 41
11.2 FROM CONFIGURATION EXAMPLE 8 41

List of Figures

Figure 1: SNMPv3 USM 5
Figure 2: MIB Structure 29

List of Tables

Table 1: New Default Password Settings 20
Table 2: New Default Community Settings 20

1. SNMPv3 Overview

SNMPv3 is the third version of the Internet-Standard Management Framework and is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2). SNMPv3 is not a stand-alone replacement for SNMPv1 and/or SNMv2. It defines security capabilities to be used in conjunction with SNMPv2 (preferred) or SNMPv1. As shown in the Figure 1 below, SNMPv3 specifies a User Security Model (USM) that uses a payload of either a SNMPv1 or a SNMPv2 protocol data unit (PDU).

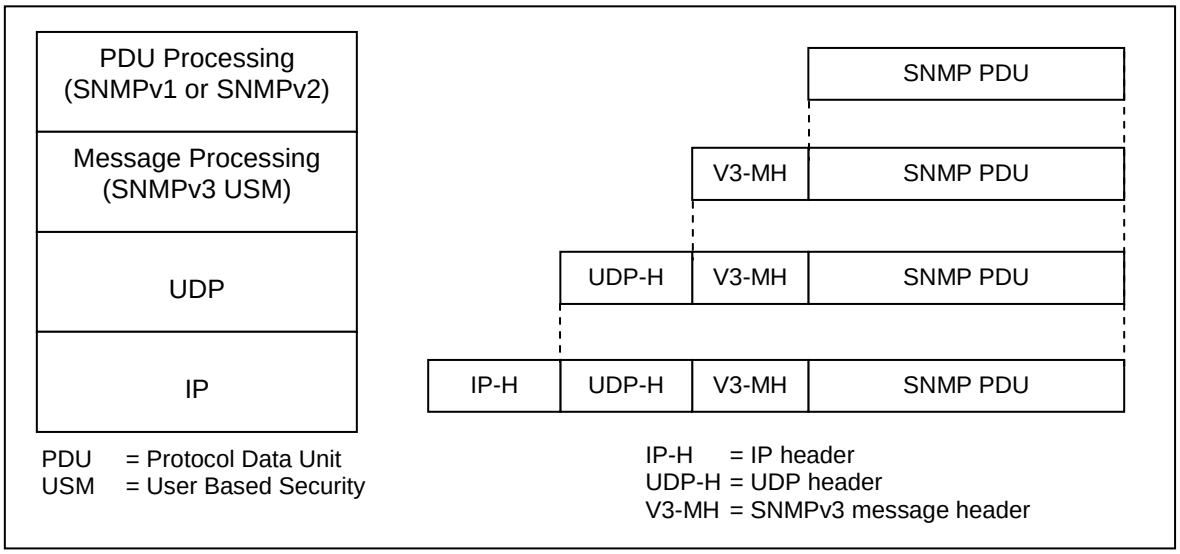


Figure 1: SNMPv3 USM

Authentication within the User-based Security Model (USM) allows the recipient of the message to verify whom the message is from and whether the message has been altered. As per RFC 2574, if authentication is used, the entire message is checked for the integrity. Authentication uses a secret key to produce a fingerprint of the message, which is included in the message. The receiving entity uses the same secret key to validate the fingerprint. Currently there are 2 authentication protocols defined, HMAC-MD5 and HMAC-SHA-96 for use with USM.

While the USM provides the user-name/password authentication and privacy services, control access to management information (MIB) must be defined. The View-based Access Control Module (VACM) is used to define a set of services that an application can use for checking access rights (read, write, notify) to a particular object. VACM uses the ASN.1 notation (3.6.1.4) or the name of the SNMP MIB branch, i.e. Org.Dod.Internet.Private. The administrator can define a MIB group view for a user to allow access to an appropriate portion of the MIB matched to an approved security level. The three security levels are:

- ***NoAuthNoPriv***-Communication without authentication and privacy
- ***AuthNoPriv***-Communication with authentication (MD5 or SHA) and without privacy
- ***AuthPriv***-Communication with authentication (MD5 or SHA) and privacy (DES or AES)

NOTE: Please refer to the Ethernet Routing Switch 8600 4.1 release notes (Part number 317177-D Rev 01) regarding important information regarding SNMPv3. Special considerations need to be considered regarding hidden and encrypted that contains community table information.

2. SNMP Upgrade Considerations

Please note the following when upgrading software on the ERS8600.

Starting in software release 3.7 and continued to software release 4.1.x, the CLI command *save config* creates a hidden and encrypted file that contains the SNMP community table information. For security purposes, the *save config* command also removes reference to the existing SNMP community strings in the newly created configuration file. Please note that if you only have one CPU, and if you swap the CPU, you must backup all hidden files or else all the password and SNMP references will be lost. If you do not backup the hidden files, you must reconfigure your trap receivers and community strings every time you change the CPU.

The commands to change the SNMP Community strings and trap receivers in software release 3.3 have changed in software releases 3.5, 3.7, 4.0, and 4.1.x. However, even though software releases 3.5, 3.7, 4.0, and 4.1.x use the same commands, in software release 3.7 and 4.1.x only, the SNMP community strings and trap receivers are stored in a hidden and encrypted file and are not found in the configuration file. This is similar with software releases 3.5 and 4.0; however the files are stored in a hidden non-encrypted file. Upgrades from 3.7 to 4.1.x, all files are translated as-is. Please see section 3.3.3 for more details.

2.1 Hidden File Details

Backup the following configuration files to either via FTP, a TFTP server or a PCMCIA card:

- shadov.txt
- snmp_usm.txt
- snmp_comm.txt
- password.txt

3. Blocking SNMP

By default, SNMP access is enabled. You can disable SNMP; this includes SNMPv1/v2 and SNMPv3, access to the ERS 8600 by using the following commands:

- ERS-8610:5# ***config bootconfig flags block-snmp true***
- ERS-8610:5#***save boot***
- ERS-8610:5#***boot -y***

To re-enable SNMP access, type in the following command:

- ERS-8610:5# ***config bootconfig flags block-snmp false***

3.1 Blocking SNMPv1/2 Only

If you wish to allow only SNMPv3 access, you can disable SNMPv1/2 by configuring the SNMPv3 MIB view. Portions of the MIB can be configured to either include or exclude access at an MIB OID level. This is explained in section 5.5. For SNMPv3, this can be done on a per-user basic. For SNMPv1/v2, it can be done on a global/community basis. By default, SNMPv1/v2 is permitted access to all MIB OIDs under 1.3 in the MIB OID tree with the exception with sections related to the SNMP USM, VACM, and Community MIBs. This cannot be altered, but, if an additional exclusion statement is added, the entire usable MIB can be disabled through SNMPv1/v2. Specifically, if the entire MIB tree under 1.3.6 (iso org dod) is excluded, none of the switches public or private MIBs will be accessible.

To disable SNMPv1/v2 only, enter the following command:

- PP8600-B:6# ***config snmp-v3 mib-view create v1v2only 1.3.6 type exclude***

At this point, SNMPv1/v2 will be disabled and only SNMPv3 will be allowed.

3.2 Blocking SNMP via an Access Policy – Prior to Software Release 3.7.9 or 4.1

You can also enable or disable SNMP via an Access Policy. Overall, the Access Policy feature on the ERS 8600 supports the following feature:

- ***Access level:*** Specifies the access level of the trusted as hostreadOnly (ro), readWrite (rw), or readWriteAll (rwa)
- ***Mode:*** Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access.
- ***Service***: Indicates the protocol to which this entry should be applied. Choices are telnet, snmp, tftp, ftp, http, rlogin, and/or ssh.
- ***Precedence:*** Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128).
- ***Network Address and Network Mask:*** Indicates the source network IP address and mask. An address of 0.0.0.0 specifies any address on the network.
- ***Host:*** Indicates the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh.

- ***Access-strict:*** Sets the access level strictly.

To add an access policy, you must first enable the access policy feature globally by entering the following command:

- ERS-8606:5# ***config sys access-policy enable <true/false>***

After the access policy feature has been enabled globally, to add a new access policy, enter the following command:

a) Add a new policy

- ERS-8606:5# ***config sys access-policy policy <1..65535>***

b) After entering the above command, enter the appropriate parameters:

- ERS-8606:5# ***config sys access-policy policy <1..65535> ?***

```
Sub-Context: service
Current Context:

    accesslevel <ro|rw|rwa>
    access-strict <true|false>
    create
    delete
    disable
    enable
    host <ipaddr>
    info
    mode <allow|deny>
    name <name>
    network <addr/mask>
    precedence <precedence>
    username <string>
```

c) Add the services to the newly created access policy:

- ERS-8606:5# ***config sys access-policy policy <1..65535> service ?***

```
Sub-Context:
Current Context:

    ftp <enable|disable>
    http <enable|disable>
    info
    rlogin <enable|disable>
    snmp <enable|disable>
    ssh <enable|disable>
    telnet <enable|disable>
    tftp <enable|disable>
```

Please refer to publication number 314997-C titled *Important Security Information for the 8000 Series Switch* for more details on Access Policies.

3.2.1 Configuration Example: Blocking SNMP via an Access Policy

In this example, we will create an access policy to not allow SNMP for any user coming from network 172.30.x.y/16.

a) Enable access policy globally:

- ERS-8606:5# ***config sys access-policy enable true***

b) Add a new policy, in this example, since it is the first policy, we will simply create policy 2 and name it *policy2*:

- ERS-8606:5# ***config sys access-policy policy 2 create***
- ERS-8606:5# ***config sys access-policy policy 2 name policy2***

c) Add network 172.30.0.0/16 to policy 2:

- ERS-8606:5# ***config sys access-policy policy 2 network 172.30.0.0/16***

d) Add read/write/all access level to policy 2:

- ERS-8606:5# ***config sys access-policy policy 2 accesslevel rwa***

e) Disable SNMP service for policy 2:

- ERS-8606:5# ***config sys access-policy policy 2 service snmp disable***

After the policy has been created, enter the following command to view policy 2:

- ERS-8606:5# ***show sys access-policy info policy2***

```
AccessPolicyEnable: on

                Id: 2
              Name: policy2
      PolicyEnable: true
              Mode: allow
           Service: http|telnet|ssh
        Precedence: 128
           NetAddr: 172.30.0.0
           NetMask: 255.255.0.0
    TrustedHostAddr: 0.0.0.0
TrustedHostUserName: none
       AccessLevel: readWriteAll
      AccessStrict: false
             Usage: 337
```

3.3 SNMP Group Access Policy – Release 3.7.9, 4.1 or Higher

In release 3.7.9 or 4.1, a new policy enhancement was added that allows the administrator to specify a group or groups for SNMPv3 access. With SNMPv3, the community name is not mapped to an access level, but determined only through VACM. This allows the administrator to create separate policies for SNMP users based on USM or community and associate them to groups.

The following items where added high-lighted in red below.

ERS-8610:5# ***config sys access-policy policy 1 ?***

```
Sub-Context: service
Current Context:

    accesslevel <level>
    access-strict <true|false>
    create
    delete
    disable
    enable
    host <ipaddr>
    info
    mode <mode>
    name <name>
    network <addr/mask>
    precedence <precedence>
    snmp-group-add <group name> <model>
    snmp-group-del <group name> <model>
    snmp-group-info
    username <string>
```

ERS-8610:5# ***config sys access-policy policy 1 service ?***

```
Sub-Context:
Current Context:

    ftp <enable|disable>
    http <enable|disable>
    info
    rlogin <enable|disable>
    snmpv3 <enable|disable>
    ssh <enable|disable>
    telnet <enable|disable>
    tftp <enable|disable>
```

3.3.1 SNMPv3 Group Access Policy: Configuration Example

For this example, we wish to create a policy for read-write-all access and only allow telnet and SNMPv3 access only for SNMPv3 usm group named group_example. Please see Section 5 in regards to how to configure SNMPv3.

a) Enable access policies globally

- ERS-8606:5# ***config sys access-policy enable true***

b) Assuming no access policies have been created, we can start with policy 2 and name the policy *policy2*.

- ERS-8606:5# ***config sys access-policy policy 2 create***
- ERS-8606:5# ***config sys access-policy policy 2 name policy2***

c) Add read/write/all access level to policy 2:

- ERS-8606:5# ***config sys access-policy policy 2 accesslevel rwa***

d) Add the usm group ‘group_example’ to policy 2:

- ERS-8610:5# ***config sys access-policy policy 2 snmp-group-add group_example usm***

e) Enable access strict enable

- ERS-8610:5# ***config sys access-policy policy 2 access-strict true***

f) Enable telnet and SNMPv3 service:

- ERS-8610:5# ***config sys access-policy policy 2 service telnet enable***
- ERS-8610:5# ***config sys access-policy policy 2 service snmpv3 enable***

g) Enable policy 2:

- ERS-8610:5# ***config sys access-policy policy 2 enable***

h) After the policy has been created, enter the following command to view policy 2:

- ERS-8606:5# ***show sys access-policy info policy2***

```
  AccessPolicyEnable: on

                  Id: 2
                Name: policy2
        PolicyEnable: true
                Mode: allow
             Service: telnet|snmpv3
          Precedence: 10
             NetAddr: 0.0.0.0
             NetMask: 0.0.0.0
     TrustedHostAddr: 0.0.0.0
 TrustedHostUserName: none
         AccessLevel: readWriteAll
        AccessStrict: true
               Usage: 3777
```

- ERS-8610:5# ***show sys access-policy snmp-group-info***

```
  snmpv3-groups :

  Policy 1 snmpv3-groups :
                   Group Name    Snmp-Model

  Policy 2 snmpv3-groups :
                   Group Name    Snmp-Model
            group_example             usm
```

3.3.2 SNMPv1/2 Group Access Policy: Configuration Example

As release 3.7 and 4.1 is based on the SNMPv3, you must add the SNMPv3 group name and model for both SNMPv1 and SNMPv2 when setting up an access policy. To view the SNMPv3 group name and model, please use the following as shown below. Note that the items high-lighted in red need to be added when setting up the access policy.

- ERS8610-B:5# ***show snmp-v3 group-access***

```
=============================================================================
                          VACM Group Access Configuration
=============================================================================
Group       Prefix Model    Level        ReadV      WriteV     NotifyV
-----------------------------------------------------------------------------
initial            usm      noAuthNoPriv root       root       root
initial            usm      authPriv     root       root       root
readgrp            snmpv1   noAuthNoPriv v1v2only               org
readgrp            snmpv2c  noAuthNoPriv v1v2only               org
v1v2grp            snmpv1   noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp            snmpv2c  noAuthNoPriv v1v2only   v1v2only   v1v2only
esegroup           usm      authPriv     org        org
sBladeGrp          snmpv1   noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp          snmpv2c  noAuthNoPriv sBladeView sBladeView sBladeView

9 out of 9 Total entries displayed
-----------------------------------------------------------------------------
```

The following example will add a new access policy that will allow SNMPv1/2 and telnet.

a) Enable access policies globally

- ERS-8606:5# ***config sys access-policy enable true***

b) Assuming no access policies have been created, we can start with policy 2 and name the policy *policy2*.

- ERS-8606:5# ***config sys access-policy policy 2 create***
- ERS-8606:5# ***config sys access-policy policy 2 name policy2***

c) Add read/write/all access level to policy 2:

- ERS-8606:5# ***config sys access-policy policy 2 accesslevel rwa***

d) Add the SNMPv1/2 group name and models to policy 2:

- ERS-8610:5# ***config sys access-policy policy snmp-group-add readgrp snmpv1***
- ERS-8610:5# ***config sys access-policy policy 2 snmp-group-add readgrp snmpv2c***
- ERS-8610:5# ***config sys access-policy policy snmp-group-add v1v2grp snmpv1***
- ERS-8610:5# ***config sys access-policy policy snmp-group-add v1v2grp snmpv2c***

If the ERS 8600 also contains a Web Switching Module (WSM) then access to the SNMPv1/2 Group “sBladeGrp” must also be configured. Enter the following commands to enable SNMP management of the WSM:

- ERS-8610:5# ***config sys access-policy policy snmp-group-add sBladeGrp snmpv1***
- ERS-8610:5# ***config sys access-policy policy snmp-group-add sBladeGrp snmpv2c***

e) Enable telnet and SNMPv3 service:

- ERS-8610:5# ***config sys access-policy policy 2 service telnet enable***
- ERS-8610:5# ***config sys access-policy policy 2 service snmpv3 enable***

f) Enable policy 2:

- ERS-8610:5# ***config sys access-policy policy 2 enable***

g) After the policy has been created, enter the following command to view policy 2:

- ERS-8606:5# ***show sys access-policy info policy2***

```
  AccessPolicyEnable: on

                  Id: 2
                Name: policy2
        PolicyEnable: true
                Mode: allow
             Service: telnet|snmpv3
          Precedence: 10
         NetAddrType: ipv4
             NetAddr: 0.0.0.0
             NetMask: 0.0.0.0
    TrustedHostAddr: 47.133.58.69
 TrustedHostUserName: none
         AccessLevel: readWriteAll
        AccessStrict: false
               Usage: 385
```

- ERS-8610:5# ***show sys access-policy snmp-group-info***

```
          snmpv3-groups :

Policy 1 snmpv3-groups:
                         Group Name      Snmp-Model

Policy 2 snmpv3-groups:
                         Group Name      Snmp-Model
                         readgrp          snmpv1
                         readgrp         snmpv2c
                         v1v2grp          snmpv1
                         v1v2grp         snmpv2c
```

3.3.3 SNMP Community Strings

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request. This is accomplished by verifying that the manager belongs to a valid SNMP community. An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (community string), and all members of a community have the same access privileges, either read-only or read-write:

- Read-only: members can view configuration and performance information.
- Read-write: members can view configuration and performance information, and also change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

SNMP community strings are required for access to the switch using Device Manager or other SNMP-based management software. You set the SNMP community strings using the CLI. If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Device Manager.

In the ERS 8000 Series switch software release 3.7, the CLI command *save config* creates a hidden and encrypted file that contains the SNMP community table information. The SNMP

community strings are not referenced in the ERS 8600 configuration file. Please see publication number 317177-A titled *Release Notes for the ERS 8000 Series Switch Software Release 3.7* for more details regarding upgrading SNMP to release 3.7.

Caution: For security reasons, Nortel Networks recommends that you set the passwords to values other than the factory defaults.

3.3.3.1 Setting the SNMP Community String and Trap Receivers with Software Release 3.3

In the ERS 8000 Series Switch Release 3.3, SNMP community strings and traps are added by using the two commands shown below. In the 3.3 release, these commands appear in the configuration file.

- ERS-8606:5# ***config sys set snmp community < ro|rw|l2|l3|rwa> <commstring>***
- ERS-8606:5# ***config sys set snmp trap-recv <ipaddr> v2c public***

  Where:
  - ***ro|rw|l2|l3|rwa*** is the choice of community. ro is read-only, rw is read/write, l2 is layer 2 read/write, l3 is layer 3 (and layer 2) read/write, and rwa is read/write/all.
  - ***commstr*** is the input community string up to 1024 characters.

3.3.3.2 Setting the SNMP Community String and Trap Receivers with Software Release 3.5, 4.0, 3.7 and 4.1

The two commands shown above in section 3.3.3.1 are now obsolete. To set the ERS 8600 community strings, enter the following command:

- ERS-8606:5# ***config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]***

  Where:

config snmp-v3 community create followed by:	
Comm Idx	The unique index value of a row in this table. The range is 1-32 characters.
name	The community string for which a row in this table represents a configuration
security	Maps community string to the security name in the VACM Group Member Table.
tag <*value*> (optional)	The transport tag name in the table. The range is 1-32 characters.

In release 3.7 or 4.1, after you save the configuration, information regarding SNMP community strings are stored in a separate file and will not be found in the configuration file. This is not the case for software release 3.5.

3.3.4 Modifying and/or Adding Community Strings

Initially, there are 4 communities: first, second, index1 and index2. ***first*** represents the default read-only access (public) and ***second*** represents the default read-write access (private) created by the SNMPv3 engine. The access rights are determined by the Security Name from the VACM table.

Previously existing default communities prior to software upgrade to release 3.7 appear as ***index1*** (private) and ***index2*** (public). They can be modified or deleted. If you had other communities defined, they will appear converted as ***index3***, ***index4***, etc…

You can modify or delete those, but you can not delete the default communities ***first*** and ***second***, however, you can change the community strings for them.

- ERS-8606:5# ***config snmp-v3 community info***

```
================================================================================
                                    Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
index1          ********        initialview
index2          ********        readview
second          ********        initialview

4 out of 4 Total entries displayed
--------------------------------------------------------------------------------
```

Please note that in software release 3.5, the community name is displayed as shown below.

- ERS8600G:3# ***config snmp-v3 community info***

```
================================================================================
                                    Community Table
================================================================================
INDEX           NAME            SECURITYNAME
--------------------------------------------------------------------------------
first           public          initialview
second          private         initialview

2 out of 2 Total entries displayed
--------------------------------------------------------------------------------
```

To change the default communities, for example, the index named first with a new community name of readonly and the index named second with a new community name of readwrite, enter the following commands:

- ERS-8606:5# ***config snmp-v3 community commname first new-commname readonly***
- ERS-8606:5# ***config snmp-v3 community commname second new-commname readwrite***

You will now not be able to access the switch with the default communities public and private; you will need to use readonly and readwrite instead.

Note: You will not be able to see those new communities as they are now encrypted and hidden. However, you can still always modify them.

If you wish to change or create further communities, alter the existing communities, create a new community or delete a community (for example, in case you have forgotten the community string, which is now encrypted and hidden).

For example, assuming we have upgraded to release 3.7 and now wish to delete community's index1 and index2:

- ERS-8606:5# ***config snmp-v3 community delete index1***
- ERS-8606:5# ***config snmp-v3 community delete index2***

A new SNMP community can be added by using the following command:

- ERS-8606:5# config snmp-v3 community create <Comm Idx> <name> <security> [tag <value>]

where:

Parameter	**Description**
Comm Idx	The unique index value of a row in this table. The range is 1-32 characters.
name	The community string for which a row in this table represents a configuration
security	Maps community string to the security name in the VACM Group Member Table.
tag <*value*> (optional)	The transport tag name in the table. The range is 1-32 characters.

For example, to add a new community with a community index named *third* with a community name of *readonly*, and a community index named *forth* with a community name of *readwrite*, enter the following:

- ERS-8606:5# ***config snmp-v3 community create third readonly readview***
- ERS-8606:5# ***config snmp-v3 community create forth readwrite initialview***
- ERS-8606:5# ***config snmp-v3 community info***

```
================================================================
                        Community Table
================================================================
Index           Name            Security Name   Transport Tag
----------------------------------------------------------------
first           ********        readview
forth           ********        initialview
second          ********        initialview
third           ********        readview

4 out of 4 Total entries displayed
----------------------------------------------------------------
```

Please see section 7 for more details in regards to configuring SNMP communities.

3.3.5 Creating or Deleting Trap Receivers with Software Release 3.7 or 4.1

With software release 3.7 or 4.1, you create trap receivers by creating SNMP-v3 trap notifications and then specifying the target address where you wish to send the notifications along with specific target parameters.

By default, the ERS8600 has a default trap notification of “trapTag”. You can use this default notification when setting up the SNMP trap target address or if you wish, you can create a new trap notification using the following command:

- ERS-8606:5# ***config snmp-v3 notify ?***

```
Sub-Context:
Current Context:

    create <Notify Name> [tag <value>] [type <value>]
    delete <Notify Name>
    info
    tag <Notify Name> new-tag <value>
    type <Notify Name> new-type <value>
```

For example, to create a new trap notification named “Trap2” with a tag value of “Trap2”, please enter the following command

- ERS-8606:5# ***config snmp-v3 notify create Trap2 tag trapTag2 type trap***

You can view the notification table by using the following command:

- ERS-8606:5# ***show snmp-v3 notify info***

```
================================================================================
                        Notify Configuration
================================================================================
Notify Name                     Tag                                 Type
--------------------------------------------------------------------------------
Inform                          informTag                           inform
Trap                            trapTag                             trap
Trap2                           trapTag2                            trap
```

The SNMP target address is configured using the following command:

- ERS-8606:5# ***config snmp-v3 target-addr ?***

```
Sub-Context:
Current Context:

    create <Target Name> <Ip addr:port> <Target parm>         [timeout
<value>] [retry <value>] [taglist <value>] [mask <value>] [mms <value>]
    delete <Target Name>
    info
    address <Target Name> new-addr <value>
    mask <Target Name> new-mask <value>
    mms <Target Name> new-mms <value>
    parms <Target Name> new-parms <value>
    retry <Target Name> new-retry <value>
    taglist <Target Name> new-taglist <value>
    timeout <Target Name> new-timeout <value>
```

For example, to add a SNMPv1 trap-receiver, enter the following assuming the Target Name is *TAddr1* and assuming you are using the default trap notify of *trapTag* and the default target-param of TparamV1 for SNMPv1 traps:

- ERS-8606:5# ***config snmp-v3 target-addr create TAddr1 X.X.X.X:162 TparamV1 timeout 1500 retry 3 taglist trapTag mask 0xff:ff:00:00:00:00 mms 484***

Where X.X.X.X is the IP-Address of your trap-receiver. Enter **TparamV1** for SNMPv1 and **TparamV2** for SNMPv2c. For each subsequent trap receiver that you add, you must give it a new target address, for example **TAddr2**, **mgmtstation**, etc.

The following is an example of adding an SNMP target address of 10.10.1.102 using the default notification tag "trapTag" for SNMPv1 traps.

- ERS-8606:5# ***config snmp-v3 target-addr create TAddr1 10.10.1.102:162 TparamV1 timeout 1500 retry 3 taglist trapTag mask 0xff:ff:00:00:00:00 mms 484***

NOTE: If you wish, you can also manually set the source IP address for all trap messages sent by the ERS 8600. For example, you could create a circuit-less IP address and use this address as the source IP for all traps generated. Please see section 4 for more details.

NOTE: You also configure the ERS 8600 to send authentication traps. Please see section 4 for more details.

To delete a trap receiver, delete the target name, for example:

- ERS-8606:5# ***config snmp-v3 target-addr delete TAddr1***

To view the trap receiver table, enter the following command:

- ERS-8606:5# ***config snmp-v3 target-addr info***

```
================================================================================
                        Target Address Configuration
================================================================================
Target Name                     TDomain   TAddress                TMask

--------------------------------------------------------------------------------
TAddr1                          ipv4      10.10.1.102:162         0xff:ff:00:0
0:00:00


================================================================================
                        Target Address Configuration
================================================================================
Target Name                     Timeout Retry TagList
Params                          MMS
--------------------------------------------------------------------------------
TAddr1                          1500    3     trapTag
TparamV1                        484
```

To view the SNMPv3 target parameters, enter the following command:

- ERS-8610:5# ***config snmp-v3 target-param info***

```
================================================================================
                        Target Params Configuration
================================================================================
Target Name                     MP Model  Security Name                   Sec
Level
--------------------------------------------------------------------------------
TparamV1                        snmpv1    readview                        noAu
thNoPriv
TparamV2                        snmpv2c   readview                        noAu
thNoPriv
```

3.4 New Default Community Strings in High Secure (hsecure) Mode

If the ERS 8600 has been configured for high security mode (config bootconfig flags hsecure true) after a factory default setting, the software will change the default password and SNMP communities. All new passwords must be at least 8 characters and in release 4.1, all new passwords must be at least 10 characters. All old passwords less than 8 or 10 (for release 4.1) characters are no longer valid and you will be prompted to change the password to the mandatory character length.

To enable or disable hsecure, enter the following commands:

- ERS-8606:5# ***config bootconfig flags hsecure {false|true}***
- ERS-8606:5# ***save boot***
- ERS-8606:5# ***boot –y***

From a previous default factory setting, without changes made to the password or SNMP community strings, the following tables display the default hsecure settings.

Table 1: New Default Password Settings

User ID	New Default Password
rwa	rwarwarrw
rw	rwrwrwrw
ro	rorororo
l3	l3l3l3l3
l2	l2l2l2l2
l1	l1l1l1l1
l4admin	l4adminl
slbadmin	slbadmin
oper	operoper
l4oper	l4operl4
slboper	slbopers
ssladmin	ssladmin

Table 2: New Default Community Settings

User ID	New Default Password
ro	publiconly
l1	privateonly
l2	privateonly
l3	privateonly
rw	privateonly
rwa	secretonly

4. SNMP Settings

To configure the SNMP settings, enter the following command:

- ERS-8606:5# ***config sys set snmp ?***

```
Sub-Context:
Current Context:

    force-iphdr-sender <true|false>
    force-trap-sender <true|false>
    info
    sender-ip <ipaddr> <ipaddr>
Where:
```

config sys set snmp followed by:	
force-iphdr-sender *<true|false>*	If set to true, the configured source address is sent in the IP header of the notification message as the source address.
force-trap-sender *<true|false>*	If set to true, the configured source address is sent in the notification message as the sender network.
info	Displays the current SNMP settings.
sender-ip *<target_address> <source_address>*	Configures a source IP address which is set in the notification sent to the target. The source IP add`ress should be a circuitless IP address.

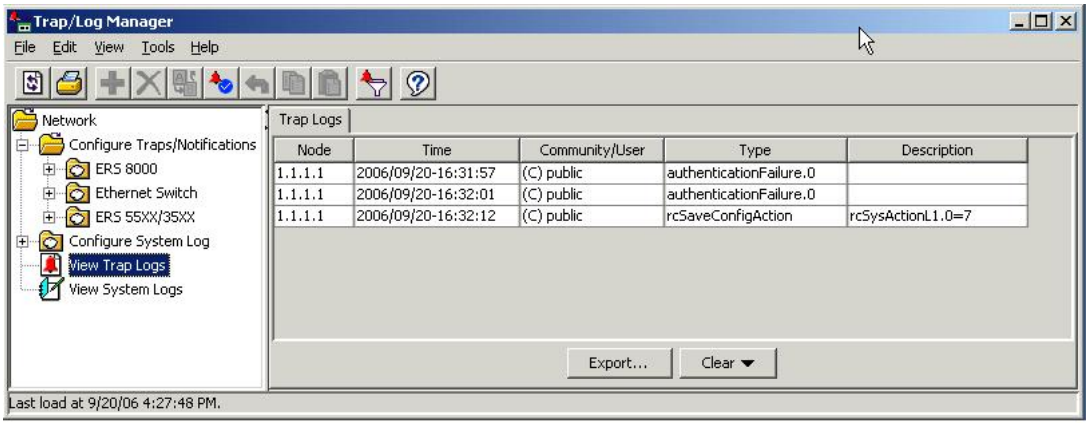
For example, assume we have an ERS 8600 switch with software release 4.1 and we wish to send SNMPv2 traps using the circuitless IP address. For this example, let's assume the trap receiver IP address is 10.1.50.10, the circuitless IP address is 1.1.1.1/32, and OSPF is used as the IGP.

1. First, add the circuitless IP address and enable OSPF
   - ERS-8606:5# ***config ip circuitless-ip-int 1 create 1.1.1.1/32***
   - ERS-8606:5# ***config ip circuitless-ip-int 1 ospf enable***
2. Add the SNMP trap target address using the default trap notification "trapTag"
   - ERS-8606:5# ***config snmp-v3 target-addr create TAddr1 10.1.50.10:162 TparamV2 timeout 1500 retry 3 taglist trapTag mask 0xff:ff:00:00:00:00 mms 484***
3. Finally, set the SNMP sender IP address using the CLIP address
   - ERS-8606:5# ***config sys set snmp sender-ip 10.1.50.10 1.1.1.1***
   - ERS-8606:5# ***config sys set snmp force-iphdr-sender true***
   - ERS-8606:5# ***config sys set snmp force-trap-sender true***

Also, you can enable authentication traps by entering the following command:

- ERS-8606:5# ***config sys set sendAuthenticationTrap true***

After the ERS 8600 has been configured, the trap receiver should display traps from the ERS 8600 with a source IP address of 1.1.1.1 as shown below using Enterprise Switch Manager.



5. SNMP with RADIUS Authentication and Accounting

Radius-SNMP authentication and accounting is supported in release 3.5 for SNMPv1 and SNMPv2. Radius-SNMP authentication operates by passing the community string to a RADIUS server. The RADIUS server will in return will send an integer value indicating the level of access allowed or no access at all.

Please note that software releases 3.7 and 4.1.x do not support this feature.

6. Configuring SNMPv3

The following are the configuration steps required to enable SNMPv3:

- Load the DES or AES (release 4.1 only) Encryption Module
- Adding a SNMP User USM
- Assigning the USM as a member to a SNMPv3 USM group
- Assigning the USM group access level of either authPriv, authNoPriv, or noAuthNoPriv
- Assigning a MIB view to the USM group

6.1 Loading the DES or AES Encryption Module

Prior to configuring SNMPv3 on the ERS 8600, the DES or AES encryption module must be loaded. Note that Advanced Encryption Standard (AES) is supported only release 4.1. The DES or AES module is required in order to provide secure communications between the user and the ERS 8600.

The AES standard is the current encryption standard (FIPS-197) intended to be used by the U.S. Government organizations to protect sensitive information. It is also becoming a global standard for commercial software and hardware that uses encryption or other security features.

Once the DES or AES encryption module is uploaded to the ERS 8600 (the file ends with a .des or .aes extension, i.e. p80c3700.des or p80c4100.aes), it can be loaded by typing the following command:

For single DES:

- ERS-8610:5# ***config load-encryption-module DES /flash/<filename>.des***

For single 3DES:

- ERS-8610:5# ***config load-encryption-module 3DES /flash/<filename>.des***

For AES:

- ERS-8610:5# ***config load-encryption-module AES /flash/<filename>.aes***

6.2 Adding a New SNMPv3 User to USM Table

After the DES or AES module has been loaded, the switch is now ready for SNMPv3 configuration. The first step is to add a user to the USM (User-based Security Model) table. You can add a new user to the USM table by typing in the following command:

- ERS-8610:5# ***config snmp-v3 usm create [User Name<1-32>] [authentication protocol <md5|sha>] auth [authentication password<1-32>] [priv-protocol <des|aes>] priv [privacy password<1-32>]***

In release 4.1, there is one additional change to support AES:

- ERS-8610:5# ***config snmp-v3 usm create [User Name<1-32>] [authentication protocol <md5|sha>] auth [authentication password<1-32>] priv [privacy password<1-32>]***

For example, the following will create a new user named “user1”, set the authentication protocol to MD5 with a password of “user1234” and a privilege password of userpriv:

For release 3.7, the command will be:

- ERS-8610:5# ***config snmp-v3 usm create user1 md5 auth user1234 priv userpriv***

For release 4.1, if using AES, the command will be:

- ERS-8610:5# ***config snmp-v3 usm create user1 md5 auth user1234 priv-prot aes priv userpriv***

After the user has been installed, you can view the users in the USM table by typing in the following command:

- ERS-8610:5# ***config snmp-v3 usm info***

```
Engine ID = 80:00:08:E0:03:00:E0:7B:82:9C:00

================================================================================
                              USM Configuration
================================================================================
User/Security Name    Engine Id                          Protocol
--------------------------------------------------------------------------------
user1                800008E00300E07B829C00           HMAC_MD5, DES PRIVACY

1 out of 1 Total entries displayed
--------------------------------------------------------------------------------
```

6.3 Assign USM User to USM Group

The next step is to assign the user to a USM group. The USM group is used to define the access level and MIB view given to a user. The USM access level and MIB view will be added in the next two steps.

You can add a new USM Group by entering the following command:

- ERS-8610:5# ***config snmp-v3 group-member create <user name> usm <group name>***

Example: the following example adds the user ‘user1’ created above to a USM group named ‘group_example’:

- ERS-8610:5# ***config snmp-v3 group-member create user1 usm group_example***

To view the USM group, enter the following command:

- ERS-8610-C:5# ***config snmp-v3 group-member info***

```
================================================================================
                  VACM Group Membership Configuration
================================================================================
Sec Model  Security Name                 Group Name
--------------------------------------------------------------------------------
snmpv1     readview                      readgrp
snmpv1     sBladeUser                    sBladeGrp
snmpv1     initialview                   v1v2grp
snmpv2c    readview                      readgrp
snmpv2c    sBladeUser                    sBladeGrp
snmpv2c    initialview                   v1v2grp
usm        user1                         group_example
usm        initial                       initial
usm        OpsQosPolicyUser              OpsQosPolicyUser

9 out of 9 Total entries displayed
--------------------------------------------------------------------------------
```

6.4 Assigning the USM Group Access Level

The next step is to assign the access level to the USM Group. One of the following three USM access levels must be configured:

- ***NoAuthNoPriv***-Communication without authentication and privacy
- ***AuthNoPriv***-Communication with authentication (MD5 or SHA) and without privacy
- ***AuthPriv***-Communication with authentication (MD5 or SHA) and privacy (DES or AES in release 4.1)

The ERS 8600 has a number of default groups, with one default USM group named 'initial'. The default groups can be examined by typing in the following command:

- ERS-8610:5# ***config snmp-v3 group-access info***

```
================================================================================
                                    VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm     noAuthNoPriv root       root       root
initial           usm     authPriv     root       root       root
readgrp           snmpv1  noAuthNoPriv v1v2only              org
readgrp           snmpv2c noAuthNoPriv v1v2only              org
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
sBladeGrp         snmpv1  noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c noAuthNoPriv sBladeView sBladeView sBladeView
OpsQosPolicyUser        usm     noAuthNoPriv org        org        org


9 out of 9 Total entries displayed----------------------------------------------
```

The default USM level, named 'initial', has both authentication and encryption (authPriv) with full read-write views. You can use this group for initial SNMPv3 access to the ERS 8600. The name of the read-write view starts at 'org' – please see next step in regards to setting up the MIB view.

To set the SNMP USM security level, type in the following command:

- ERS-8610:5# ***config snmp-v3 group-access create [group name <0-32>] [prefix <0-32>] usm [noAuthNoPriv|authNoPriv|authPriv]***

Example: the following will add USM security level of 'authPriv' to the USM group named 'group_example':

- ERS-8610:5# ***config snmp-v3 group-access create group_example "" usm authPriv***

NOTE: The prefix entered above is entered using double quotes. If you wish, you can define the 'exact' context match that should be matched against the context of the incoming PDU; i.e. exact prefix match of read or write. There is no read or write view associated with the group yet. This will be defined in the next step.

6.5 Assigning the MIB View to the USM Group

We can assign the USM group to either an existing MIB view or create a new MIB view fist (next step) and then assign it to the USM group. The next section will describe how to add a new MIB view.

To view the default MIB views, enter the following command:

- ERS-8610:5# ***config snmp-v3 mib-view info***

```
================================================================================
                                  MIB View
================================================================================
View Name            Subtree                         Mask                Type

--------------------------------------------------------------------------------
org                  1                                                   include
root                 1                                                   include
snmp                 1.3.6.1.6.3                                         include
snmp                 1.3.6.1.2.1.1                                       include
layer1               1.3                                                 exclude
  .                      .                                                   .
  .                      .                                                   .
sBladeView           1.3.6.1.4.1.1872                                    include

50 out of 50 Total entries displayed-------------------------------------------
```

To associate the USM group to a MIB view, enter the following command:

- ERS-8610:5# ***config snmp-v3 group-access view <group name> <prefix> usm <noAuthNoPriv|authNoPriv|authPriv> read <value> write <value>***

Example: to assign both read and write view to the existing view of 'org' to the group 'group_example' created earlier, enter the following command:

- ERS-8610:5# ***config snmp-v3 group-access view group_example "" usm authPriv read org write org***

You can view the Group Access MIB view table by entering the following command:

- ERS-8610:5# ***config snmp-v3 group-access info***

```
================================================================================
                                    VACM Group Access Configuration
================================================================================
Group      Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm     noAuthNoPriv root       root       root
initial           usm     authPriv     root       root       root
readgrp           snmpv1  noAuthNoPriv v1v2only               org
readgrp           snmpv2c noAuthNoPriv v1v2only               org
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
sBladeGrp         snmpv1  noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c noAuthNoPriv sBladeView sBladeView sBladeView
group_example        usm     authPriv     org        org
OpsQosPolicyUser        usm     noAuthNoPriv org        org        org


10 out of 10 Total entries displayed
--------------------------------------------------------------------------------
```

6.6 Creating a MIB View

As mentioned in the previous step, the ERS 8600 has a number of default MIB views. The MIB view configures the branches of the SNMP MIB tree that are permitted or not permitted for a particular user or group. The ERS 8600 MIB tree follows the ASN.1 hierarchical structure for both private and enterprise (private) MIBs.

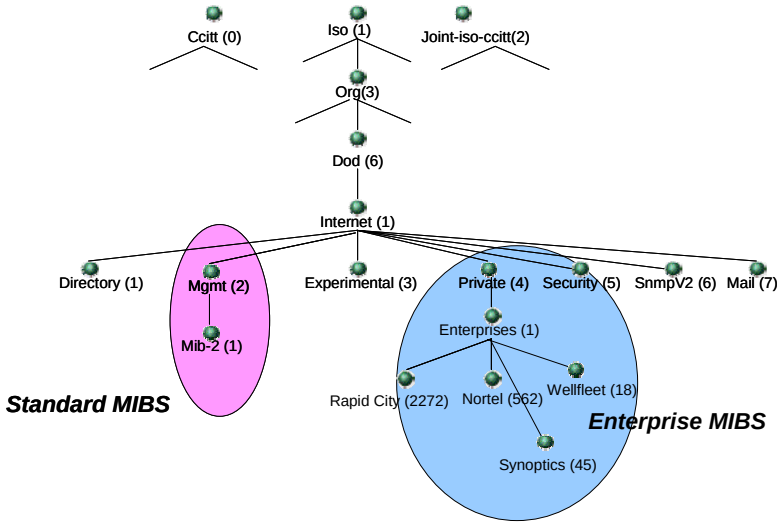


Figure 2: MIB Structure

To create a new MIB view, enter the following command:

- ERS-8610:5# ***config snmp-v3 mib-view create [view name<1..32>] <subtree oid> mask <value in hex> type <include|exclude>***

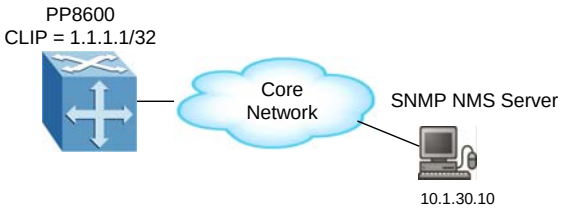
Example: to add a new MIB view named 'ro_private' to exclude the Private branch, enter the following command:

- ERS-8606:5# ***config snmp-v3 mib-view create ro_private 1.3.6.1.4 type exclude***
- ERS-8610:5# ***config snmp-v3 mib-view info***

```
================================================================================
                                  MIB View
================================================================================
View Name            Subtree                        Mask                Type

--------------------------------------------------------------------------------
org                  1                                                  include
root                 1                                                  include
snmp                 1.3.6.1.6.3                                        include
  .                      .                                                .
  .                      .                                                .

v1v2only             1.3.6.1.6.3.16                                     exclude
v1v2only             1.3.6.1.6.3.18                                     exclude
sBladeView           1.3.6.1.4.1.1872                                   include

50 out of 50 Total entries displayed


40 out of 40 Total entries displayed
--------------------------------------------------------------------------------
```

7. Configuration Example: Changing SNMP Communities

7.1 Configuration Example: SNMP Communities with Release 3.5



In this configuration example, we wish to accomplish the following:

- Change the 'rwa' community string to rwa123pp8600
- Change the 'ro' community string to ro567pp8600
- Add a trap receiver using the IP address of the SNMP NMS server

To accomplish the above, please complete the following steps:

A) Add the new rwa community string
   - ERS-8606:5# ***config sys set snmp community rwa rwa123pp8600***

B) Add the new ro community string
   - ERS-8606:5# ***config sys set snmp community ro ro567pp8600***

C) Add the SNMP trap receiver
   - ERS-8606:5# ***config sys set snmp trap-recv 10.1.30.10 v1 puplic***

NOTE: The Circuit-less IP (CLIP) can be used as the Source IP address for the SNMP traps. If you wish to use the CLIP address, assuming the CLIP address is 1.1.1.1/32, enter the following commands:

- ERS-8606:5# ***config sys set snmp trap-recv 10.1.30.10 v1 puplic 1.1.1.1***
- ERS-8606:5# ***config sys set snmp force-trap-sender true***

To view the SNMP communities, enter the following commands:

- ERS-8606:5# ***show sys community***

```
Community String
ro          ********
l1          ********
l2          ********
l3          ********
rw          ********
rwa         ********
```

7.2 Configuration Example: Changing the Default SNMP Community Name with Release 3.7 or 4.1

By default, the ERS 8600 public and private communities are configured using the names first and second respectively. You can view the SNMP community table by using the following command. Notice the community names, public and private by default, are asterisk out.

- ERS-8606:5# ***config snmp-v3 community info***

```
================================================================================
                                Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview

3 out of 3 Total entries displayed
--------------------------------------------------------------------------------
```

To change the default public/private SNMPv1, SNMPv2, and SNMPv3 community name, enter the following command:

- To change the default public community name, in this example to *ro567pp8600*, enter the following command:
  - ERS-8606:5# ***config snmp-v3 community commname first new-commname ro567pp8600***
- To change the default private community name, in this example to *rwa123pp8600*, enter the following command:
  - ERS-8606:5# ***config snmp-v3 community commname second new-commname rwa123pp8600***

7.3 Configuration Example: Adding a New SNMP Community to an Existing SNMP Group Member

If you use an existing group member in the VCAM table, a new community can be simply added. To view the SNMP VACM and MIB view, the following commands can be used

- To view the VACM Membership configuration, enter the following command:
  - ERS-8610-C:5# ***config snmp-v3 group-member info***
- To view the VCAM Group Access configuration, enter the following command:
  - ERS-8610-C:5# ***config snmp-v3 group-access info***
- To view the SNMP MIB View, enter the following command:
  - ERS-8610-C:5# ***config snmp-v3 mib-view info***

For example, if you wish to add a new community named *pp8600579* with read/write access, enter the following command:

- ERS-8610-C:5# ***config snmp-v3 community create third pp8600579 initialview***

After the community has been added, you can view the SNMP community table by using the following command:

- ERS-8610-C:5# ***config snmp-v3 community info***

```
================================================================================
                                      Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
OpsQosPolicyUser ********        OpsQosPolicyUser OpsQosPolicyUser
first           ********        readview
second          ********        initialview
third           ********        initialview

4 out of 4 Total entries displayed
--------------------------------------------------------------------------------
```

NOTE: Notice that we mapped the new community string to an existing security name named 'initialview'. You can view the VACM group member configuration by using the commands shown below.

- ERS-8610-C:5# ***config snmp-v3 group-member info***

```
================================================================================
                         VACM Group Membership Configuration
================================================================================
Sec Model  Security Name                  Group Name
--------------------------------------------------------------------------------
snmpv1     readview                       readgrp
snmpv1     sBladeUser                     sBladeGrp
snmpv1     initialview                    v1v2grp
snmpv2c    readview                       readgrp
snmpv2c    sBladeUser                     sBladeGrp
snmpv2c    initialview                    v1v2grp
usm        initial                        initial
usm        OpsQosPolicyUser               OpsQosPolicyUser

8 out of 8 Total entries displayed
```

- ERS-8610-C:5# ***config snmp-v3 group-access info***

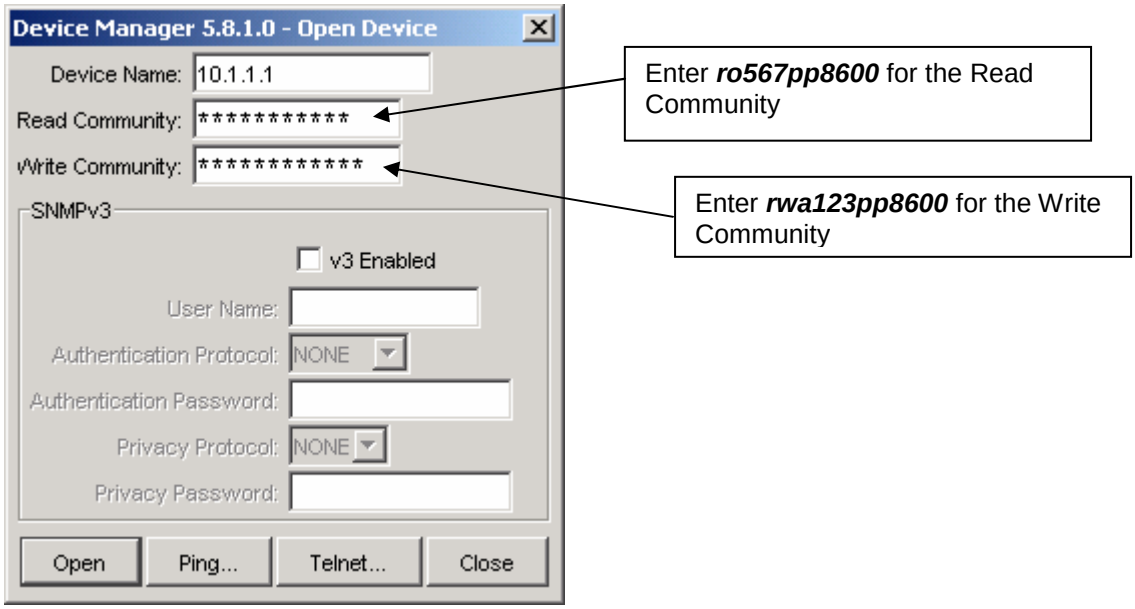
```
================================================================================
                                VACM Group Access Configuration
================================================================================
Group       Prefix Model   Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm      noAuthNoPriv root       root       root
initial           usm      authPriv     root       root       root
readgrp           snmpv1   noAuthNoPriv v1v2only               org
readgrp           snmpv2c  noAuthNoPriv v1v2only               org
v1v2grp           snmpv1   noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c  noAuthNoPriv v1v2only   v1v2only   v1v2only
sBladeGrp         snmpv1   noAuthNoPriv sBladeView sBladeView sBladeView
sBladeGrp         snmpv2c  noAuthNoPriv sBladeView sBladeView sBladeView
OpsQosPolicyUser        usm     noAuthNoPriv org        org        org
OpsQosPolicyUser        usm     authNoPriv   org        org        org

10 out of 10 Total entries displayed
```

- ERS-8610-C:5# ***config snmp-v3 mib-view info***

```
================================================================================
                                    MIB View
================================================================================
View Name            Subtree                          Mask                Type
--------------------------------------------------------------------------------
org                  1.3                                                  include
root                 1                                                    include
snmp                 1.3.6.1.6.3                                          include
snmp                 1.3.6.1.2.1.1                                        include
layer1               1.3                                                  exclude
layer1               1.3.6.1.2.1.2.2.1.7                                  include
layer1               1.3.6.1.4.1.2272.1.1.8                               include
layer1               1.3.6.1.4.1.2272.1.26.2                              include
layer1               1.3.6.1.4.1.2272.1.4.11.2                            include
layer1               1.3.6.1.4.1.2272.1.4.10.1.1.11                       include
layer1               1.3.6.1.4.1.2272.1.4.10.1.1.12                       include
layer1               1.3.6.1.4.1.2272.1.4.10.1.1.14                       include
layer1               1.3.6.1.4.1.2272.1.4.10.1.1.50                       include
layer2               1.3                                                  include
layer2               1.3.6.1.4.1.2272.1.8                                 exclude
layer2               1.3.6.1.4.1.2272.1.9                                 exclude
layer2               1.3.6.1.4.1.2272.1.19                                exclude

layer2               1.3.6.1.4.1.2272.1.24                                exclude
layer2               1.3.6.1.4.1.2272.1.29                                exclude
layer2               1.3.6.1.4.1.2272.1.31                                exclude
layer2               1.3.6.1.4.1.2272.1.34                                exclude
layer2               1.3.6.1.4.1.2272.1.51                                exclude
layer2               1.3.6.1.4.1.2272.1.23.15                             exclude
layer2               1.3.6.1.4.1.2272.1.30.9                              exclude
layer2               1.3.6.1.4.1.2272.1.30.10                             exclude
layer2               1.3.6.1.4.1.2272.1.100.2                             exclude
layer3               1.3                                                  include
layer3               1.3.6.1.4.1.2272.1.19                                exclude
layer3               1.3.6.1.4.1.2272.1.29                                exclude
layer3               1.3.6.1.4.1.2272.1.31                                exclude
layer3               1.3.6.1.4.1.2272.1.33                                exclude
layer3               1.3.6.1.4.1.2272.1.34                                exclude
v1v2only             1.0                                                  include
v1v2only             1.2                                                  include
v1v2only             1.3                                                  include
v1v2only             1.3.6.1.6.3.15                                       exclude
v1v2only             1.3.6.1.6.3.16                                       exclude
v1v2only             1.3.6.1.6.3.18                                       exclude
sBladeView           1.3.6.1.4.1.1872                                     include

39 out of 39 Total entries displayed

--------------------------------------------------------------------------------
```

7.4 Testing SNMP Using Device Manager

Now that you have changed the read and write communities, you can test the configuration by using Device Manager. The window shown below displays the parameters entered for the read and write communities.



7.5 Configuration Example: Changing the MIB View for an SNMPv1/2 Community

In software release 3.7 or 4.1, you can create a new MIB view and apply it to a specific SNMP community. This allows you, for example, to restrict write access to the ERS 8600 private MIB.

In this configuration example, we will create a new MIB view named private_restrict and apply it to a new community named no_private_comm. To accomplish these tasks, please enter the following commands:

A) Create a new MIB view named private_restrict. Note, as shown in section 6.6, the ERS 8600 Private OID is 1.3.6.1.4.

- ERS-8610:5# ***config snmp-v3 mib-view create private_restrict 1.3.6.1.4 type exclude***

B) Create a new SNMP group access named no_private:

1. Add SNMP group access with a security level of noAuthNoPriv for SNMPv1 with write restrict assigned to the MIB view 'private_restrict' create in step A above:

- ERS-8610:5# ***config snmp-v3 group-access create no_private "" snmpv1 noAuthNoPriv***
- ERS-8610-C:5# ***config snmp-v3 group-access view no_private "" snmpv1 noAuthNoPriv read org write private_restrict notify org***

2. Add SNMP group access with security level of noAuthNoPriv for SNMPv2 with write restrict assigned to the MIB view ‘private_restrict’ create in step A above:

   - ERS-8610:5# ***config snmp-v3 group-access create no_private "" snmpv2 noAuthNoPriv***
   - ERS-8610-C:5# ***config snmp-v3 group-access view no_private "" snmpv2 noAuthNoPriv read org write private_restrict notify org***

C) Create a new SNMP group member named “private” for SNMPv1/2 and add group access “no_private” created in step 2 above

1. In this example, we will add a new MIB view named ‘private’ to exclude access to the SNMP Private MIB

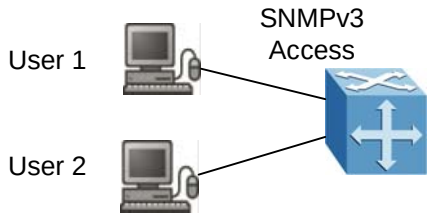
   - ERS-8610:5# ***config snmp-v3 group-member create private snmpv1 no_private***
   - ERS-8610:5# ***config snmp-v3 group-member create private snmpv2 no_private***

D) Create a new SNMP community named ‘forth’ with a community name of ‘no_private_comm’ and add group member ‘private’ created in step C above:

1. Assign to usm group ‘group_1’ read view to ‘org and write MIB view to ‘private’:

   - ERS-8610:5# ***config snmp-v3 community create forth no_private_comm private***

8. Configuration Example Using SNMPv3



For this configuration example, we wish to accomplish the following:

- Add User 1 to USM table with authentication protocol of MD5 and privacy protocol of DES, i.e. authPriv)
- Allow User 1 full MIB views with full permission starting the existing view “org”
- Add User 2 to USM table authentication protocol of MD5 with no privacy protocol, i.e. authNoPriv
- Allow User 2 full MIB read permission starting from the exiting “org” level, but exclude write permission from all Private Enterprise MIB’s

To accomplish the above, please follow the steps below.

A) Load the DES module:

1. Assuming the DES module has been installed on the ERS 8600 switch, enter the following command:
   - ERS-8610:5# ***config load-encryption-module DES /flash/p80c3700.des***

B) Add User 1 to USM table. In this example, we will use a user name of ‘user1’, a MD5 password of ‘user1234’, and a DES privacy password of ‘userpriv’

- ERS-8610:5# ***config snmp-v3 usm create user1 md5 auth user1234 priv userpriv***

Or via 4.1.1

- ERS-8610:5# ***config snmp-v3 usm create user1 md5 auth user1234 priv-prot des priv userpriv***

C) Add User 1 to USM group. In this configuration example, we will add ‘user1’ to USM group named “group_1”

1. Add ‘user1’ to group ‘group_1’:
   - ERS-8610:5# ***config snmp-v3 group-member create user1 usm group_1***

D) Assign Access Level to USM group:

1. Assign access level of ‘authPriv’ to USM group ‘group_1’
   - ERS-8610:5# ***config snmp-v3 group-access create group_1 "" usm authPriv***

E) Assign the Read and Write view to the USM group:

1. Assign to usm group ‘group_1’ read and write view to ‘org’:
    - ERS-8610:5# ***config snmp-v3 group-access view group_1 "" usm authPriv read org write org***

F) Add User 2 to USM table. In this example, we will use a user name of ‘user2’, and a MD5 password of ‘user2abcd.

- ERS-8610:5# ***config snmp-v3 usm create user2 md5 auth user2abcd***

G) Add User 2 to USM group. We will add User 2 to the group named ‘group_1’ created above.

1. Add ‘user2’ to group ‘group_1’:
    - ERS-8610:5# ***config snmp-v3 group-member create user2 usm group_1***

H) Assign Access Level to USM group:

1. Assign access level of ‘authNoPriv’ to usm group ‘group_1’
    - ERS-8610:5# ***config snmp-v3 group-access create group_1 "" usm authNoPriv***

I) Create a new MIB view to exclude the private MIB for User 2

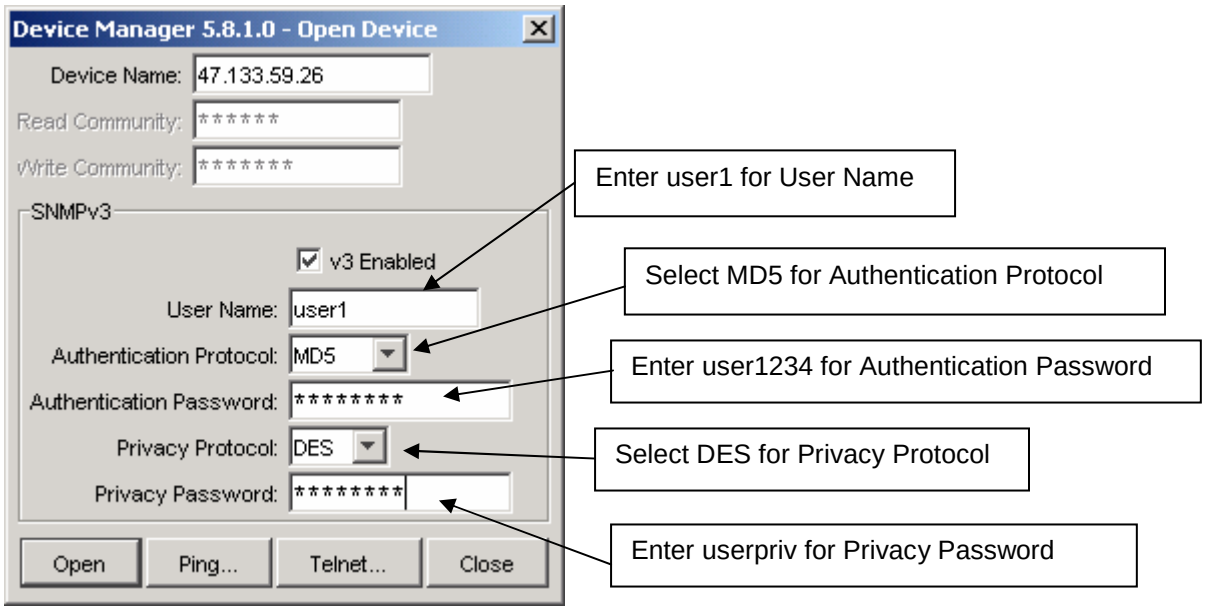
1. In this example, we will add a new MIB view named ‘private’ to exclude access to the SNMP Private MIB
    - ERS-8610:5# ***config snmp-v3 mib-view create private 1.3.6.1.4 type exclude***

J) Assign the Read and Write view to the usm group:

1. Assign to usm group ‘group_1’ read view to ‘org and write MIB view to ‘private’:
    - ERS-8610:5# ***config snmp-v3 group-access view group_1 "" usm authNoPriv read org write private***

8.1 Testing SNMPv3 Using Device Manager

Now that you have created two new users, you can test the configuration by using Device Manager. The window shown below displays the parameters entered for user1.



9. Software Baseline

All configuration examples are based on the ERS 8600 3.7 release with updated information release to AES support for release 4.1.

10. Reference Documentation

Document Title	Publication Number	Description
Configuring and Managing Security	314724-C	Passport 8000 Series Software Release 3.7
Configuring Network Management	314723-C	Passport 8000 Series Software Release 3.7
Important Security Information for the 8000 Series Switch	314997-C	Passport 8000 Series Software Release 3.7
Release Notes for the Ethernet Routing Switch 8600	317177-D Rev 01	Release 4.1.0
Configuring and Managing Security	314724-E Rev 00	Ethernet Routing Switch 8600 Software Release 4.1
Configuring Network Management	314723-E Rev 00	Ethernet Routing Switch 8600 Software Release 4.1

11. Appendix A: Configuration Files

11.1 From Configuration Example 7.5

```
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#

snmp-v3 group-member create private snmpv1 no_private
snmp-v3 group-member create private snmpv2c no_private
snmp-v3 group-member create user1 usm group_1
snmp-v3 group-member create user2 usm group_1

#
# SNMP V3 GROUP ACCESS CONFIGURATION
#

snmp-v3 group-access create group_1 "" usm authNoPriv
snmp-v3 group-access view group_1 "" usm authNoPriv read "org" write "private" notify ""
snmp-v3 group-access create group_1 "" usm authPriv
snmp-v3 group-access view group_1 "" usm authPriv read "org" write "org" notify ""
snmp-v3 group-access create no_private "" snmpv1 noAuthNoPriv
snmp-v3 group-access view no_private "" snmpv1 noAuthNoPriv read "org" write "private_restrict" notify "org"
snmp-v3 group-access create no_private "" snmpv2c noAuthNoPriv
snmp-v3 group-access view no_private "" snmpv2c noAuthNoPriv read "org" write "private_restrict" notify "org"
snmp-v3 group-access create OpsQosPolicyUser "" usm authNoPriv
snmp-v3 group-access view OpsQosPolicyUser "" usm authNoPriv read "org" write "org" notify "org"

#
# SNMP V3 MIB VIEW CONFIGURATION
#

snmp-v3 mib-view create private_restrict 1.3.6.1.4  type exclude
```

11.2 From Configuration Example 8

```
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#

snmp-v3 group-member create user1 usm group_1
snmp-v3 group-member create user2 usm group_1
snmp-v3 group-member create OpsQosPolicyUser usm OpsQosPolicyUser

#
# SNMP V3 GROUP ACCESS CONFIGURATION
#

snmp-v3 group-access create group_1 "" usm authNoPriv
snmp-v3 group-access view group_1 "" usm authNoPriv read "org" write "private" n
otify ""
snmp-v3 group-access create group_1 "" usm authPriv
snmp-v3 group-access view group_1 "" usm authPriv read "org" write "org" notify
""

snmp-v3 group-access create OpsQosPolicyUser "" usm authNoPriv
snmp-v3 group-access view OpsQosPolicyUser "" usm authNoPriv read "org" write "o
rg" notify "org"

#
# SNMP V3 MIB VIEW CONFIGURATION
#
```

```
snmp-v3 mib-view create private 1.3.6.1.4  type exclude

#
# SNMP V3 NOTIFY CONFIGURATION
#


#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#

snmp-v3 target-addr create OpsQosPolicyUser 47.133.56.105:8162 OpsQosPolicyUser
timeout 1500 retry 3 taglist OpsQosPolicyUser mms 484

#
# SNMP V3 TARGET PARAMS CONFIGURATION
#


snmp-v3 target-param create OpsQosPolicyUser mp-model usm sec-level authNoPriv s
ec-name OpsQosPolicyUser
snmp-v3 target-param create TparamV1 mp-model snmpv1 sec-level noAuthNoPriv sec-
name readview
snmp-v3 target-param create TparamV2 mp-model snmpv2c sec-level noAuthNoPriv sec
-name readview

#
# SNMP V3 NOTIFY FILTER CONFIGURATION
#

snmp-v3 ntfy-filter create OpsQosPolicyUser 1.3.6.1.4.1.562.42.5.1.3 type includ
e

#
# SNMP V3 NOTIFY FILTER PROFILE CONFIGURATION
#

snmp-v3 ntfy-profile create OpsQosPolicyUser profile OpsQosPolicyUser
```

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.