Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

SNMP Configuration Overview

This section describes how to configure SNMP components which apply to SNMPv1 and SNMPv2c, and SNMPv3 on the router.

Configuring SNMPv1 and SNMPv2c

Alcatel-Lucent routers are based on SNMPv3. To use the routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three pre-defined access methods are available when SNMPv1 or SNMPv2c access is required. Each access method (**r**, **rw**, or **rwa**) is associated with an SNMPv3 access group that determines the access privileges and the scope of managed objects available. The **community** command is used to associate a community string with a specific access method and the required SNMP version (SNMPv1 or SNMPv2c). The access methods are:

- Read-Only — Grants read only access to the entire management structure with the exception of the security area.

- Read-Write — Grants read and write access to the entire management structure with the exception of the security area.

- Read-Write-All — Grants read and write access to the entire management structure, including security.

If the predefined access groups do not meet your access requirements, then additional access groups and views can be configured. The **usm-community** command is used to associate an access group with an SNMPv1 or SNMPv2c community string.

SNMP trap destinations are configured in the **config>log>snmp-trap-group** context.

Configuring SNMPv3

The OS implements SNMPv3. If security features other than the default views are required, then the following parameters must be configured:

- Configure views
- Configure access groups
- Configure SNMP users

Basic SNMP Security Configuration

This section provides information to configure SNMP parameters and provides examples of common configuration tasks. The minimal SNMP parameters are:

For SNMPv1 and SNMPv2c:

- Configure community string parameters.

For SNMPv3:

- Configure view parameters
- Configure SNMP group
- Configure access parameters
- Configure user with SNMP parameters

The following displays SNMP default views, access groups, and attempts parameters.

```
A:ALA-1>config>system>security>snmp# info detail
----------------------------------------------
                view iso subtree 1
                    mask ff type included
                exit
                view no-security subtree 1
                    mask ff type included
                exit
                view no-security subtree 1.3.6.1.6.3
                    mask ff type excluded
                exit
                view no-security subtree 1.3.6.1.6.3.10.2.1
                    mask ff type included
                exit
                view no-security subtree 1.3.6.1.6.3.11.2.1
                    mask ff type included
                exit
                view no-security subtree 1.3.6.1.6.3.15.1.1
                    mask ff type included
                exit
                access group snmp-ro security-model snmpv1 security-level no-auth-no-
privacy read no-security notify no-security
                access group snmp-ro security-model snmpv2c security-level no-auth-no-
privacy read no-security notify no-security
                access group snmp-rw security-model snmpv1 security-level no-auth-no-
privacy read no-security write no-security notify no-security
                access group snmp-rw security-model snmpv2c security-level no-auth-no-
privacy read no-security write no-security notify no-security
                access group snmp-rwa security-model snmpv1 security-level no-auth-no-
privacy read iso write iso notify iso
                access group snmp-rwa security-model snmpv2c security-level no-auth-no-
privacy read iso write iso notify iso
                access group snmp-trap security-model snmpv1 security-level no-auth-no-
privacy notify iso
                access group snmp-trap security-model snmpv2c security-level no-auth-
no-privacy notify iso
                attempts 20 time 5 lockout 10
```

Configuring SNMP Components

Use the CLI syntax displayed below to configure the following SNMP scenarios:

- Configuring a Community String on page 297
- Configuring View Options on page 297
- Configuring Access Options on page 298
- Configuring USM Community Options on page 299
- Configuring Other SNMP Parameters on page 300

CLI Syntax:
```
config>system>security>snmp
    attempts [count] [time minutes1] [lockout minutes2]
    community community-string access-permissions [version SNMP
        version]
    usm-community community-string group group-name
    view view-name subtree oid-value
      mask mask-value [type {included|excluded}]
    access group group-name security-model security-model secu-
        rity-level security-level [context context-name [pre-
        fix-match]] [read view-name-1] [write view-name-2]
        [notify view-name-3]
```

Configuring a Community String

SNMPv1 and SNMPv2c community strings are used to define the relationship between an SNMP manager and agent. The community string acts like a password to permit access to the agent. The access granted with a community string is restricted to the scope of the configured group.

One or more of these characteristics associated with the string can be specified:

- Read-only, read-write, and read-write-all permission for the MIB objects accessible to the community.
- The SNMP version, SNMPv1 or SNMPv2c.

Default access features are pre-configured by the agent for SNMPv1/SNMPv2c.

Use the following CLI syntax to configure community options:

CLI Syntax: `config>system>security>snmp`
        `community community-string access-permissions [version SNMP`
            `version]`

The following displays an SNMP community configuration example:

```
*A:cses-A13>config>system>security>snmp# info
---------------------------------------------
                community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
                community "Lla.RtAyRW2" hash2 r version v2c
                community "r0a159kIOfg" hash2 r version both
---------------------------------------------
*A:cses-A13>config>system>security>snmp#
```

Configuring View Options

Use the following CLI syntax to configure view options:

CLI Syntax: `config>system>security>snmp`
        `view view-name subtree oid-value`
            `mask mask-value [type {included|excluded}]`

The following displays a view configuration example:

```
*A:cses-A13>config>system>security>snmp# info
---------------------------------------------
                view "testview" subtree "1"
                    mask ff
                exit
                view "testview" subtree "1.3.6.1.2"
                    mask ff type excluded
                exit
```

```
                   community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
                   community "Lla.RtAyRW2" hash2 r version v2c
                   community "r0a159kIOfg" hash2 r version both
---------------------------------------------
*A:cses-A13>config>system>security>snmp#
```

Configuring Access Options

The **access** command creates an association between a user group, a security model and the views that the user group can access. Access must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Use the following CLI syntax to configure access features:

CLI Syntax: config>system>security>snmp
    access group group-name security-model security-model secu-
        rity-level security-level [context context-name [pre-
        fix-match]] [read view-name-1] [write view-name-2]
        [notify view-name-3]

The following displays an access configuration with the view configurations.

```
*A:cses-A13>config>system>security>snmp# info
---------------------------------------------
                view "testview" subtree "1"
                    mask ff
                exit
                view "testview" subtree "1.3.6.1.2"
                    mask ff type excluded
                exit
                access group "test" security-model usm security-level auth-no-pr
ivacy read "testview" write "testview" notify "testview"
                community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
                community "Lla.RtAyRW2" hash2 r version v2c
                community "r0a159kIOfg" hash2 r version both
---------------------------------------------
*A:cses-A13>config>system>security>snmp#
```

Use the following CLI syntax to configure user group and authentication parameters:

CLI Syntax: config>system>security# user user-name
    access [ftp] [snmp] [console]
    snmp
        authentication [none]|[[hash]{md5 *key*|sha *key* } privacy
        {none|des-key|aes-128-cfb-key key}]
        group *group-name*

The following displays a user's SNMP configuration example.

```
A:ALA-1>config>system>security# info
----------------------------------------------
     user "testuser"
         access snmp
         snmp
           authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
           group testgroup
         exit
     exit
...
----------------------------------------------
A:ALA-1>config>system>security#
```

Configuring USM Community Options

User-based security model (USM) community strings associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

By default, the OS implementation of SNMP uses SNMPv3. However, to implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

CLI Syntax: `config>system>security>snmp`
`usm-community community-string group group-name`

The following displays a SNMP community configuration example:

```
A:ALA-1>config>system>security>snmp# info
----------------------------------------------
view "testview" subtree "1"
                  mask ff
              exit
              view "testview" subtree "1.3.6.1.2"
                  mask ff type excluded
              exit
              access group "test" security-model usm security-level auth-no-pr
ivacy read "testview" write "testview" notify "testview"
              community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
              community "Lla.RtAyRW2" hash2 r version v2c
              community "r0a159kIOfg" hash2 r version both
----------------------------------------------
A:ALA-1>config>system>security>snmp#
```

The group **grouptest** was configured in the **config>system>security>snmp>access** CLI context.

Configuring Other SNMP Parameters

Use the following CLI syntax to modify the system SNMP options:

CLI Syntax: `config>system>snmp`
          `engineID` *engine-id*
          `general-port` *port*
          `packet-size` *bytes*
          `no shutdown`

The following example displays the system SNMP default values:

```
A:ALA-104>config>system>snmp# info detail
----------------------------------------------
          shutdown
          engineID "0000xxxx000000000xxxxx00"
          packet-size 1500
          general-port 161
----------------------------------------------
A:ALA-104>config>system>snmp#
```