

Chapter 27

Summary of SNMP Configuration Statements

The following sections explain each of the SNMP configuration statements. The statements are organized alphabetically.

authorization

Syntax	<code>authorization <i>authorization</i>;</code>
Hierarchy Level	[edit snmp community]
Description	Set the access authorization for SNMP Get, GetNext, and Set requests. The JUNOS SNMP implementation currently does not support Set requests.
Options	<i>authorization</i> —Access authorization level: read-only—Enable Get, GetNext, and GetBulk requests. read-write—Enable all requests, including Set requests. Default: read-only
Usage Guidelines	See “Configure the SNMP Community String” on page 286.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

categories

Syntax	<code>categories category;</code>
Hierarchy Level	[edit snmp trap-group]
Description	Define the types of traps in a named trap notification.
Default	If you omit the categories statement, all trap types are included in trap notifications.
Options	<i>category</i> —One or more trap types. Values: all, authentication, routing, chassis, link, startup Default: all
Usage Guidelines	See “Configure SNMP Trap Groups” on page 287.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

clients

Syntax	<code>clients { default restrict; address <restrict>; }</code>
Hierarchy Level	[edit snmp community]
Description	Specify the SNMP clients that are authorized to access this router.
Default	If you omit the clients statement, all SNMP clients are authorized to access the router.
Options	<i>address</i> —Address of an SNMP client that is authorized to access this router. You must specify an address, not a host name. To specify more than one client, include multiple <i>address</i> options. Default: If you do not specify any addresses, all clients are authorized.
	<i>default restrict</i> —Do not allow any SNMP clients to access the router unless they are explicitly given access. We recommend that you always include the default restrict option to limit SNMP client access to the local router. Default: If you omit the default restrict statement, all SNMP clients can access the router.
	<i>restrict</i> —(Optional) Do not allow the specified SNMP client to access the router. Default: If you omit the restrict option after the address, access is permitted.
Usage Guidelines	See “Configure the SNMP Community String” on page 286.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

community

Syntax	community <i>community-name</i> { authorization <i>authorization</i> ; clients { default restrict; <i>address</i> <restrict>; } }
Hierarchy Level	[edit snmp]
Description	Define an SNMP community string, which acts as a password when determining whether an SNMP server can access a client. The community string is used by SNMP Get, GetNext, and Set requests. The JUNOS SNMP implementation currently does not support Set requests.
Default	If you omit this statement, all SNMP requests are denied.
Options	<i>community-name</i> —Community string. It can be any name you choose. If the name includes spaces, enclose it in quotation marks (" "). The remaining statements are explained separately.
Usage Guidelines	See "Configure the SNMP Community String" on page 286.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

contact

Syntax	contact <i>contact</i> ;
Hierarchy Level	[edit snmp]
Description	Define the value of the MIB II sysContact object, which is the contact person of the managed system.
Options	<i>contact</i> —Name of contact person. If the name includes spaces, enclose it in quotation marks (" ").
Usage Guidelines	See "Configure the System Contact" on page 284.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

description

Syntax	description <i>description</i> ;
Hierarchy Level	[edit snmp]
Description	Description of the system being managed.
Options	<i>description</i> —System description. If the name includes spaces, enclose it in quotation marks (“ ”).
Usage Guidelines	See “Configure the System Description” on page 285.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

interface

Syntax	interface [<i>interface-names</i>];
Hierarchy Level	[edit snmp]
Description	Configure the interfaces on which SNMP requests can be accepted.
Default	If you omit this statement, all interfaces are granted SNMP access privileges.
Options	<i>interface-name</i> —Name of one or more logical interfaces.
Usage Guidelines	See “Configure the Interfaces on which SNMP Requests Can Be Accepted” on page 288.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

location

Syntax	location <i>location</i> ;
Hierarchy Level	[edit snmp]
Description	Define the value of the MIB II sysLocation object, which is the physical location of the managed system.
Options	<i>location</i> —Location of local system. You must enclose the name within quotation marks (“ ”).
Usage Guidelines	See “Configure the System Location” on page 285.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

snmp

Syntax	snmp { ... }
Hierarchy Level	[edit]
Description	Configure SNMP.
Usage Guidelines	See “Configure SNMP” on page 283.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

targets

Syntax	targets { <i>address</i> ; }
Hierarchy Level	[edit snmp trap-group <i>group-name</i>]
Description	Configure one or more systems to receive SNMP traps.
Options	<i>address</i> —Address of the system. You must specify an address, not a host name.
Usage Guidelines	See “Configure SNMP Trap Groups” on page 287.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

traceoptions

Syntax traceoptions {
 file <files *number*> <size *size*>;
 flag *flag* <disable>;

Hierarchy Level [edit snmp]

Description Configure SNMP tracing options.

To specify more than one tracing operation, include multiple flag statements. The output of the tracing operations is placed into two files:

 /var/log/snmpd—Errors and communications between the server and subagents

 /var/log/mib2d—All interface statistics

Options disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

files *number*—(Optional) Maximum number of trace files. When a trace file (for example, snmpd) reaches its maximum size, it is renamed snmpd.0, then snmpd.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1000 files

Default: 10 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

 all—Trace all SNMP events.

 interface-stats—Trace physical and logical interface statistics.

 pdu—Trace SNMP request and response packets.

 protocol-timeouts—Trace SNMP response timeouts.

 routing-socket—Trace routing socket calls.

 subagent—Trace subagent restarts.

 timer—Trace internal timer events.

 varbind-error—Trace variable binding errors.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, snmpd) reaches its maximum size, it is renamed snmpd.0, then snmpd.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option.

Range: 10 KB through the maximum file size supported on your system

Default: 1000 KB

Usage Guidelines See “Trace SNMP Traffic” on page 288.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

trap-group

Syntax

```
trap-group group-name {
    categories category;
    targets {
        address;
    }
    version version;
}
```

Hierarchy Level [edit snmp]

Description Create a named group to receive the specified trap notifications. The name is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name.

Options *group-name*—Name of the trap notification. It can be any name you want. If the name includes spaces, enclose it in quotation marks (“ ”).

The remaining statements are explained separately.

Usage Guidelines See “Configure SNMP Trap Groups” on page 287.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

