snmpd command (SNMP daemon)

Description

This command enables/disables the SNMP daemon (Simple Network Management Protocol) version 1, 2c and 3.

SNMP protocol support is an important feature of all communication devices, it allows system administrator to use a uniform mechanism to manage the operation of a whole network and it's components separately.

Although versions 1 and 2c of the SNMP protocol lack security in the operation of the protocol itself, which hinders it's use for network management, it is widely used to monitor and analyze network operation.

Support of SNMP V3 with USM (User-based Security Model), MD5 authentication and confidentiality mode are also available. For access granting, a user account with username, access passwords and access rights (with or without authentication and confidentiality) is created.

SNMP daemon implementation supports MIB-II, as well as private MIBs.

Syntax:

```
user NAME (add|set) [pass PASSWORD] [sec[urity] (noAuthNoPriv|authNoPriv|authPriv)]
            [acc[essRights] (readOnly|readWrite)] [cla[ss] (guest|admin)]
            [privpass PRIVPASS]
user NAME del[ete]
comm[unity] NAME
(nodebug|debug  [prox] [trap] [stat] [mibs] [user] [cryp] [time] [flow])
(v1disable|v1enable) # SNMPv1 and SNMPv2c disable/enable
(start|stop)
clear
```

Parameters

Parameters	Description
user NAME (add|set)	Add/set a username to which parameters are referred
[pass PASSWORD]	Set a password of SNMP user account.
[privpass PRIVPASS]	Set a "*privacy*" password if a confidentiality mode is required.
[sec[urity] (noAuthNoPriv|authNoPriv|authPriv)]	Set the level of security: • *"noAuthNoPriv"* – SNMP messages are sent unauthenticated and without confidentiality, only username needs to be specified. • "*authNoPriv"* – SNMP messages are sent authenticated but without confidentiality, username and password need to be specified. • "*authPriv"* – SNMP messages are sent authenticated and confidential, username, password and password "*privacy*" need to be specified.

[acc[essRights] (readOnly|readWrite)]	Provides access management of the resources: • *"readOnly"* – only reading. • "readWrite" – reading and changing some variables, set by default.
[cla[ss] (guest|admin)]	Set an access level to the variables: • *"guest"* – limited access, set by default. • *"admin"* – full access.
user NAME del[ete]	Deletes a user account.
comm[unity] NAME	Allows changing the default community name. The default SNMP v1 and 2c community name for read operations is "*public*".
(v1disable|v1enable)	Enables / disables support of SNMPv1 and SNMPv2c. Disabling as a result fastens incoming SNMP-requests processing.
(nodebug|debug [prox] [trap] [stat] [mibs] [user] [pack] [time] [flow])	Disables/enables printing of SNMP service information into the system log. Allows to filter records out by the following parameters: • *"[prox]"* – redirecting SNMP-requests from an IP-network to a MINT network and SNMP-responses in the opposite direction (R5000 devices have own SNMP-proxy function). • *"[trap]"* – redirecting of traps (subset of the "*flow*" function). • *"[stat]"* – statistics of the processing time of SNMP-requests (the response time for this request, the longest response time and the average response time). • *"[mibs]"* – detection of SNMP-values in the MIB of the device and insertion values in the response datagram. • *"[user]"* – authentication and reasons for not responding to incorrect SNMP-requests in the protocol version 3. • *"[time]"* – recording the exact time of receiving and sending SNMP-packets. • *"[flow]"* – logging information about receiving, confirming and analysing of received SNMP-requests, about forming and sending SNMP-responses, redirecting of traps.
(start|stop)	Disables/enables SNMP daemon.
clear	Resets the SNMP configuration.

Examples

Set the password "*mypassword*" for user "*john*" and select second level of security with authentication but without confidentiality.

```
snmpd user john add pass mypassword security authNoPriv
```