Title

SNMP

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

The SNMP protocol support is an important feature of all communication devices because it allows the system administrator to manage the operation of a network as a whole, as well as of each component.

SNMP section contains a set of parameters to exchange data about network activity of the device.

The SNMP Protocol has two sides, the agent and the management stations:

- The agent sends data to the management station
- The management station collects data from all the agents on the network. You can set several destinations of traps with individual set of traps as well as several users with individual access rights.
- The agent sends alerts called traps (see Traps zone) and answers requests that were sent by the management station
- The management station captures and decodes the traps. The management station also requests specific information from the agent.
- The information is passed through requests and replies with the use of the MIB
- The management station is responsible for decoding the SNMP packets and providing an interface to the administrator. The interface can be a GUI or a command line.

Access

In the "Access" section, you can view and edit the current SNMP access settings; you can delete the current SNMP v.3 users by clicking the "Remove User" button or create new ones by clicking the "Add SNMP v.3 User" button:

SNMP access parameter	Description
Start SNMP	• Enable/disable SNMP daemon in the device
Version 1 enable	• Enable/disable SNMP v.1 and v.2c support • The first version of the SNMP protocol lacks security in the operation of the protocol itself, which hinders its use for network management, so SNMP v.1 and v.2c works only in read-only mode • By default, it is enabled
Community	• Set the community name for read-only mode (SNMP v.1 and v.2c only) • The default SNMP v.1 and v.2c community name is "public" • It is a security method for SNMP v.1 and v.2c, as Agents can be set to reply only to queries received by accepted community names • In SNMP v.1 and v.2c the community name passes along with the data packet in clear text
Contact	• Set the contact information • Used as a reference information about the device owner
Location	• Set the geographical location where the unit is installed • Used as a reference information about physical device's location
User Name	• Set the authorization user name of SNMP v.3
Password	• Set the authorization password of SNMP v.3

Security	• Set the security level:
	  • the lowest level means no authentication or privacy (No Authorization No Privacy), you have to set the User Name only
	  • the medium level means authorization and no privacy (Authorization No Privacy), you have to set User Name and Password
	  • the highest level means authorization and privacy (Authorization and Privacy), you have to set the User Name, Password and Privacy Password

Read only	• Enable/disable the read-only permission • Read/Write is the default value
Admin	• Enable/disable the full access to the variables • For example: ability to reboot the device • Limited access is the default value
Privacy Password	• Set the privacy password • It is necessary when privacy is enabled for the required security level

Table - SNMP Access

Traps

SNMP protocol operation requires a network agent instance to send asynchronous messages (traps) whenever a specific event occurs on the controlled device (object). Infinet Wireless units have a built-in "*SNMP Traps*" support module (which acts as an agent) that performs a centralized information delivery from unit internal subsystems to the SNMP server. This zone focuses on "*SNMP Traps*" agent configuration.

In this section, you can view and edit the current "SNMP traps" settings. You can clone, remove and clear target and traps by clicking the corresponding buttons:

SNMP traps parameter	Description
Enable SNMP Traps	• Enable/disable to send "*SNMP traps*"
Agent IP	• Set the IP address of the device which sends traps

Transport	• Set the transport method
	• Two options are available:
	  • “IP” - all SNMP traps are sent to the server specified in the “Destination” field below
	  • “MINT Gateway” - this option should be used when the SNMP server is located beyond a gateway that acts as an SNMP agent for the whole MINT network

Gateway MAC	• Set the MAC address of the gateway in your MINT network (relay device) if you selected “*MINT Gateway*” option • If there's no MAC address specified, all "*SNMP traps"* are sent to the MINT SNMP relay • The relay can be specified by checking the "*Trap Gateway"* check-box in the "Link Settings" section
Destination	• Set the IP address of the server and the UDP port (162 port is commonly used)

Table - SNMP Traps

SNMP trap types

The check boxes below specify traps or trap groups that are sent to the server:

SNMP trap types	Description
topoGroup	• Events about topology changes in MINT network
topoEvent	• Number of neighbors or their status has changed (full neighbor list)
newNeighborEvent	• The new Neighbor has appeared
lostNeighborEvent	• The Neighbor has been lost
radioGroup	• Events which are related to changes of radio link parameters
radioFreqChanged	• The Frequency has changed
radioBandChanged	• The Band has changed
mintGroup	• Events about link quality changes in MINT network
mintRetries	• Retries has changed by more than 10%
mintBitrate	• The Bitrate has changed
mintSignalLevel	• Signal Level has changed by more than 10%
ospfGroup	• Events about OSPF table changes in MINT network
ospfNBRState	• The State of the relationship with this Neighbor has changed
ospfVirtNBRState	• The State of the relationship with this Virtual Neighbor has changed
ospfIFState	• The State of the OSPF Interface has changed
ospfVirtIFState	• The State of the Virtual OSPF Interface has changed
ospfConfigError	• Parameters conflict in the configuration of 2 routers
others	• Other changes in MINT network

linkEvent	• One of the communication links represented in the agent's configuration has come up or come down
trapdColdStartEvent	• Cold Start event has occurred
snmpdAuthenticationFailureEvent	• Not properly authenticated SNMP protocol message has been received
syslog	• Events about messages recorded in a system log

Table - SNMP Trap Types

Click the "Clone" button if you need to setup multiple SNMP servers. Each server can have an individual set of traps directed toward it. Click the "Clear" button in order to clear all check-boxes for the current server.