Title

Simple Network Management Protocol

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

To the certification exam

SNMP is a protocol that operates at the Application layer of the OSI reference model and enables the exchange of management information between various networking devices. It has the following advantages:

Simple design

The SNMP implementation in any large scale network can be performed quickly and easily.

Scalability

It is very easy to extend its capabilities and include new information in its structure in order to support any type of device.

Wide spread

Nowadays, almost all vendors have implemented into their devices the support for SNMP by configuring them as SNMP agents. This translates into a great deal of interoperability in terms of management. It doesn't matter if different types of devices are present in a network, as they can be easily integrated in the same NMS and managed in a centralized manner based on SNMP.

Security

SNMPv3 supports enhanced security features:

- Authentication is ensured by using a shared key, due to which the SNMP message is only available to the intended recipient.
- Privacy is achieved by message encryption that allows only authorized users to read the SNMP information.

A network managed based on SNMP includes a management station and the network devices to be monitored. The management station will be running the NMS application based on SNMP.

There are 3 important components characterizing the functionality of SNMP:

Management Information Base (MIB)

MIB represents a set of objects that store the information about the managed network elements.

Structure of Management Information (SMI)

SMI is a standard that describes the object syntax, specifying how MIB data is referenced and stored.

SNMP Agent

All network devices need to have an SNMP agent activated in order to allow the remote management via SNMP. The SNMP agent is responsible for sending the information stored in the MIB when requested by the NMS and to report changes in its state using traps.

InfiNet Wireless SNMP implemmentation

InfiNet Wireless units come with built-in support for SNMP. The SNMP agent can be configured from the Web interface or from CLI.

SNMP access

Support for SNMPv3 is included and a SNMPv3 user can be created in order to benefit of the security features.

Enable SNMP v1 and v2c

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 always work in read-only mode. By default, it is enabled.

Community

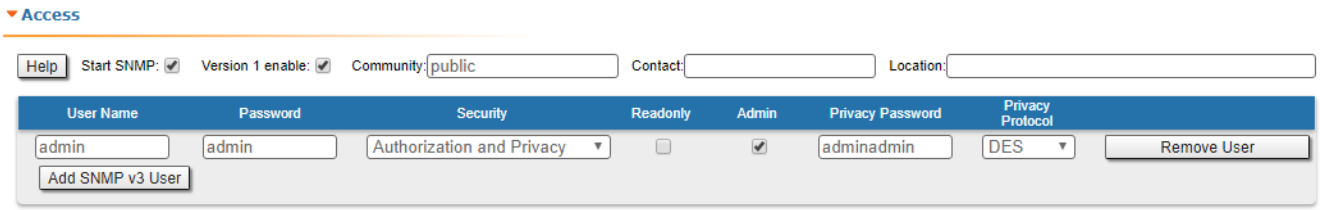
Set the community name for read-only mode (SNMP v.1 and v.2c only). The default SNMP v.1 and v.2c community name is "public". It is a security method for SNMP v.1 and v.2c, as agents can be set to reply only to queries received by accepted community names. In SNMP v.1 and v.2c the community name passes along with the data packet in clear text.

SNMP v3 settings

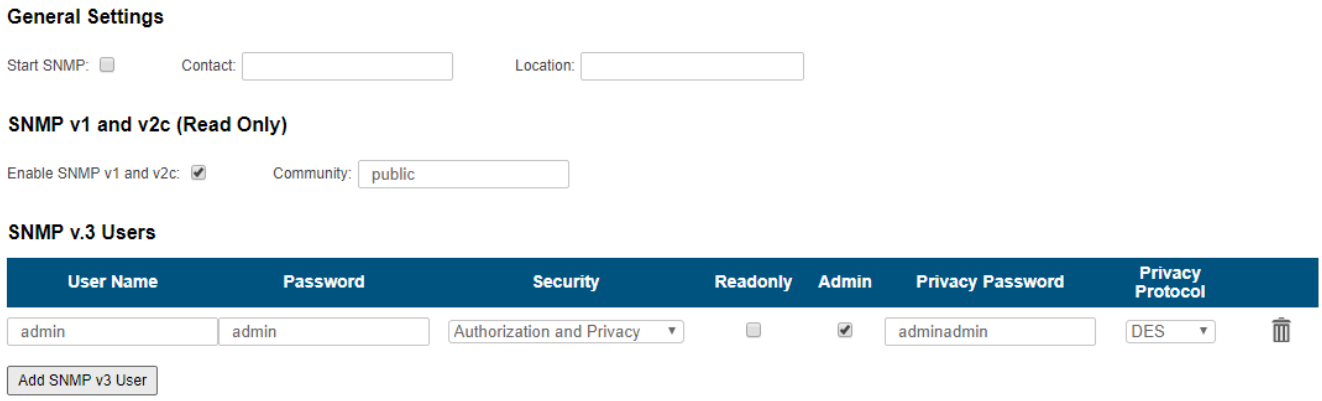
- **User Name** - sets the authorization user name of SNMP v.3.
- **Password** - sets the authorization password of SNMP v.3.
- **Security** - sets the security level:
  - "No Authorization No Privacy" - the lowest level means no authentication or privacy, you have to set the User Name only;
  - "Authorization No Privacy" - the medium level means authorization and no privacy, you have to set the User Name and Password;
  - "Authorization and Privacy" - the highest level means authorization and privacy, you have to set the User Name, Password and Privacy Password.
- **Read only** - enable/disable the read-only permission.
- **Admin** - enable/disable the full access to the variables.
- **Privacy Password** - set the privacy password, it is necessary when privacy is enabled for the required security level.

SNMP settings are similar for all InfiNet Wireless devices families.

InfiLINK 2x2 and InfiMAN 2x2 product families



InfiLINK XG and InfiLINK XG 1000 product families



SNMP traps

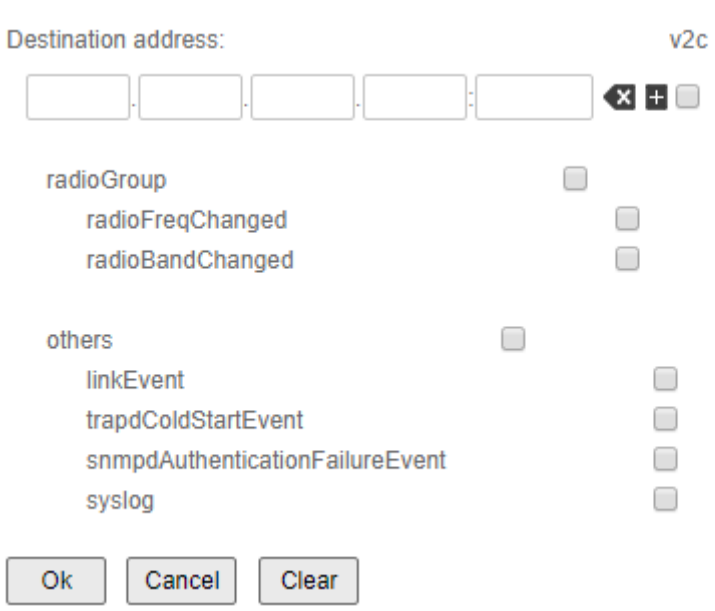
The SNMP protocol operation requires a network agent instance to send asynchronous messages (traps) whenever a specific event occurs on the controlled device (object). InfiNet Wireless units have a built-in "SNMP Traps" support module (which acts as an agent) that performs a centralized information delivery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

In the "SNMP Traps" section it is possible to enable/disable the sending of "SNMP traps" and to set the IP address of the device which sends traps; normally it is the IP address of the InfiNet Wireless unit. To select traps or trap groups to be sent to the server, it is enough to mark the check boxes. The available traps depend on the product family, the full list of possible values is below:

SNMP trap types	Description
topoGroup	Events about topology changes in the MINT network
topoEvent	Number of neighbors or their status has changed (full neighbor list)
newNeighborEvent	A new Neighbor has appeared
lostNeighborEvent	A Neighbor has been lost
radioGroup	Events which are related to changes of the radio link parameters

Title

radioFreqChanged	The Frequency has changed
radioBandChanged	The Band has changed
mintGroup	Events about link quality changes in the 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 the 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 the 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



The MIB structure and object identifiers for the InfiNet Wireless units can be obtained from https://ftp.infinet.ru/pub/Firmware/MIBS. This ensures the Integration of the InfiNet units in any monitoring system (for example a NMS may already exist and include all other network devices owned by a company).