SNMP Menu

Select Main Menu ▸ [P]rotocols & IP Filtering ▸ [S]NMP to access this screen.

This menu can be used to:

- Enable or disable SNMP handling
- Set the SNMP T:LAN Listening Port
- Set the SNMP Read-Only community string

- Set the SNMP Read-Write community string
- Limit the originator IP address of SNMP requests
- Enable or disable the SNMP trap generation
- Enable or disable the SNMP Proxy Trap Mode
- Define up to four NMS trap receivers
- Clear the SNMP statistics
- View the SNMP statistics
- Reset the SNMP configuration to defaults

SNMP Handling

No SNMP requests will be processed and no traps will be sent if this parameter is set to disabled.

Complete the following procedure to change the SNMP Handling:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [S]NMP Handling.

   RESULT: The unit will prompt for the SNMP Handling Configuration.

   Select 0, disabled to turn SNMP handling off or 1, enabled to turn it on.

The following is not available prior to BN7378.

After the SNMP Handling Mode query, the T:LAN will ask for the SNMP T:LAN Listening Port. It selects the port on which a T:LAN listens for incoming SNMP requests. This user configurable field has been added to support SNMP monitoring deployments that rely on the use of port forwarding rules at remote sites. To be backwards compatible, the SNMP T:LAN Listening Port setting defaults to UDP Port 161.

Enter a UDP Port number in the range of 1 to 65535.

These reserved selections will not be accepted:

UDP Port	Reserved for use by
162	SNMP Server Trap Destination Port
123	NTP Protocol
68	DHCP Client
67	DHCP Server
11346	T:LAN DNS Queries

UDP Port	Reserved for use by
53501	T:LAN/RCC Communications

Read-Only Community

Complete the following procedure to change the SNMP read-only community string:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [R]ead-Only Community.
2. Enter a string of 20 alphanumeric characters. The default is "public."

Read-Write Community

Complete the following procedure to change the SNMP read-write community string:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ Read-[W]rite Community.
2. Enter a string of 20 alphanumeric characters. The default is "private."

Originator IP

Complete the following procedure to define a trusted host or range of hosts for SNMP requests:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [O]riginator IP.

   RESULT: The unit will prompt for an IP Address.
2. Enter the IP address of the host to trust.

   RESULT: The unit will prompt for an IP Mask.
3. Enter the IP mask that defines the host or range of hosts to trust.

To limit the access rights to a single originating IP address, enter 255.255.255.255 as the IP mask. Any other mask value can be used to cover a range of IP addresses.

Trap Generation

Complete the following procedure to enable or disable SNMP trap generation:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [T]rap Generation.

   RESULT: The unit will prompt for the SNMP Trap Generation Configuration.

   Select 0, disabled to turn trap generation off or 1, enabled to turn it on.

Proxy Trap Mode

This option is not available prior to BN7378.

This mode has been added to support SNMP monitoring deployments that rely on the SNMP trap originator MAC address to be embedded as one of the essential OID bindings inside the SNMP traps. Once enabled, the T:LAN acts as an SNMP trap proxy, embedding the originator MAC address before forwarding the received SNMP trap on to the user defined NMS destinations.

Complete the following procedure to enable or disable SNMP Proxy Trap Mode:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [P]roxy Trap Mode

   RESULT: The unit will prompt for the SNMP Proxy Trap Mode Configuration.

   Select 0, disabled to turn SNMP Proxy Trap Mode off or 1, enabled to turn it on.

For proper operation, configure 3rd party devices located at the remote site to forward their SNMP traps to the T:LAN's IP address. The T:LAN then forwards the updated trap to the destination NMS.

Trap Recipients

Each T:LAN can send alerts to a maximum of four NMS stations. Using the keys '1' to '4', the user can modify the details of these four trap recipients. Recipients can be defined or deleted in any order.

Defining a recipient requires the user to set the following parameters:

Parameter	Description
IP Address	Enter the IP address of the trap recipient station. Range: 0.0.0.0 to 255.255.255.254 (dotted decimal notation) Default: 0.0.0.0
Trap Destination Port	Enter the SNMP port of the trap recipient station. Range: 0 to 65535 Default: 162
SNMP Community String	Enter the community string to be used by the T:LAN when sending traps to this recipient. Range: max. 20 characters Default: -none-
Coldstart Trap Configuration	Select whether this recipient will receive any Coldstart traps. Range: 0 = disabled 1 = enabled Default: 0

Parameter	Description
Warmstart Configuration	Select whether this recipient will receive any Warmstart traps. Range: 0 = disabled 1 = enabled Default: 0
WAN1-2 Link Up/Down Trap Configuration	Select whether this recipient will receive any WAN1-2 link up/down traps. Range: 0 = disabled 1 = enabled Default: 0
Ethernet LAN1-4 Link Up/Down Trap Configuration	Select whether this recipient will receive the corresponding LAN1-4 link up/down traps generated by the port up/down events. Range: 0 = disabled 1 = enabled Default: 0
WAN Backup/PPP Link Up/Down Trap Configuration	Select whether this recipient will receive any PPP link up/down traps generated by the Optima Link:Guard. Range: 0 = disabled 1 = enabled Default: 0
Authentication Failure Trap Configuration	Select whether this recipient will receive any authentication failure traps. Range: 0 = disabled 1 = enabled Default: 0
Optima Enterprise Specific Trap/RIO Trap Configuration	Select whether this recipient will receive any Optima enterprise specific traps. Range: 0 = disabled 1 = enabled Default: 0

Enter an IP address of 0.0.0.0 to remove an existing entry.

Clear Statistics

Complete the following procedure to clear the SNMP Statistics/Counters:

1. From the Main Menu, select [P]rotocols & IP Filtering ▸ [S]NMP ▸ [C]lear Statistics.

   RESULT: The unit will prompt for confirmation.

2. Hit Y to proceed.

View Statistics

Select [V]iew Statistics to view the SNMP Statistics.

Refer to "SNMP Statistics" on page 270 for a detailed description of this screen.

Default SNMP Configuration

Select [D]efault SNMP Configuration to reset all SNMP Menu settings to defaults. These include:

- SNMP handling is disabled
- SNMP read-only community string is set to 'public'
- SNMP read-write community string is set to 'private'
- The originator IP is set to -any- and the mask to 0.0.0.0
- SNMP trap generation is disabled
- The list of trap recipients is cleared