Nexans Switches Basic Configuration

FTTO Switch Configuration

Version 1

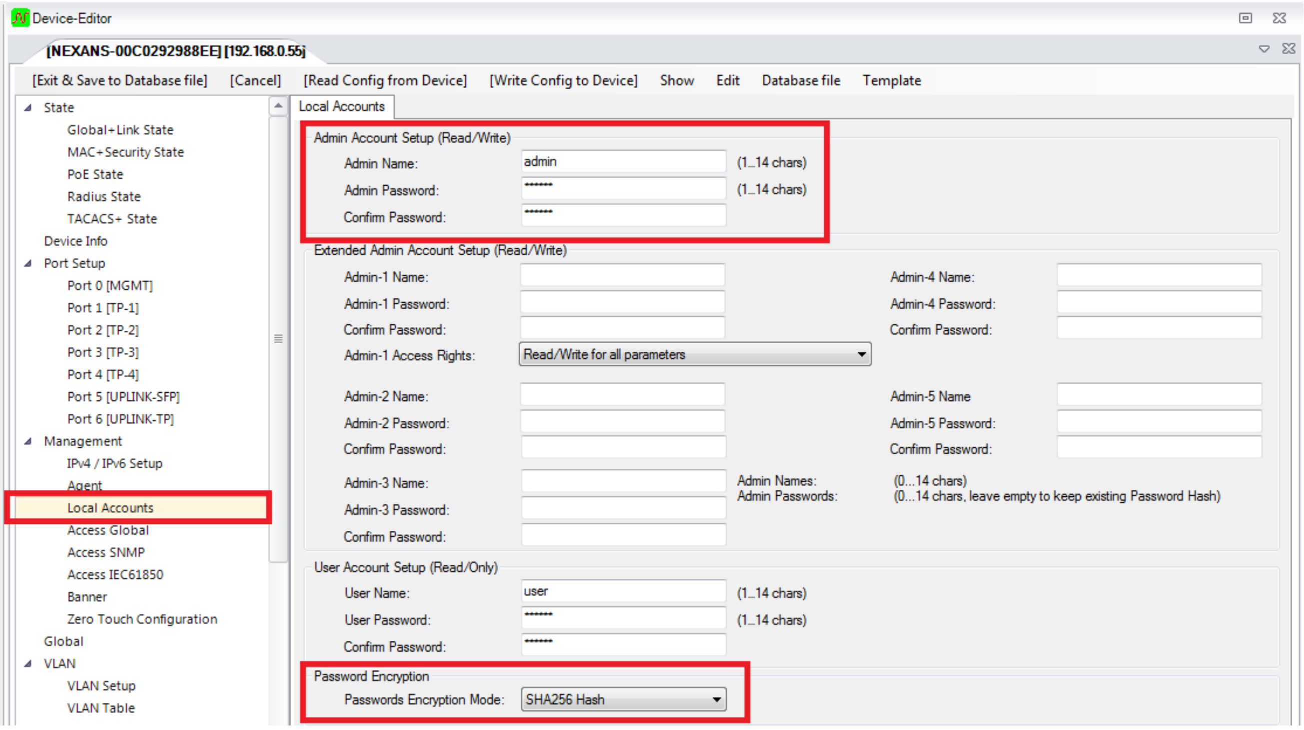
This instruction deals with the recommended basic switch configuration of Nexans FTTO switches

Content

1. Local Accounts

It is mandatory to change the login credentials from username: admin and password nexans to a secure combination. In addition, the Password Encryption Mode should be set to SHA256 Hash.

NEXMAN configuration: Local Accounts -> Admin Account Setup
NEXMAN configuration: Local Accounts -> Password Encryption



Admin Account Setup (Read/Write)

Admin Name: admin (1..14 chars)
Admin Password: ****** (1..14 chars)
Confirm Password: ******

Extended Admin Account Setup (Read/Write)

Admin-1 Name:
Admin-1 Password:
Confirm Password:
Admin-1 Access Rights: Read/Write for all parameters

Admin-2 Name:
Admin-2 Password:
Confirm Password:

Admin-3 Name:
Admin-3 Password:
Confirm Password:

Admin-4 Name:
Admin-4 Password:
Confirm Password:

Admin-5 Name
Admin-5 Password:
Confirm Password:

Admin Names: (0...14 chars)
Admin Passwords: (0...14 chars, leave empty to keep existing Password Hash)

User Account Setup (Read/Only)

User Name: user (1..14 chars)
User Password: ****** (1..14 chars)
Confirm Password: ******

Password Encryption

Passwords Encryption Mode: SHA256 Hash

CLI configuration:

```
se:t {admin|admin-x|u:ser} {n:ame|p:assword} <string 1...14 chars>
   Set local name and password for admin or user access level.
   Allowed admin-x accounts are {admin-1|admin-2|admin-3|admin-4|admin-5}
   The admin(-x) accounts have full access rights (marked with '#' or '>')
   The user account has read-only access rights (marked with '>')
   Allowed characters for name and password are (NO Umlauts):
   a-z A-Z 0-9 . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ | ( ) [ ] { } < >
```

CLI configuration:

```
se:t password-e:ncryption {st:andard|m:d5-hash|sha-:hash|sha2:56-hash|d:es}
   Selects algorithm for internal storage of admin/user account passwords.
```

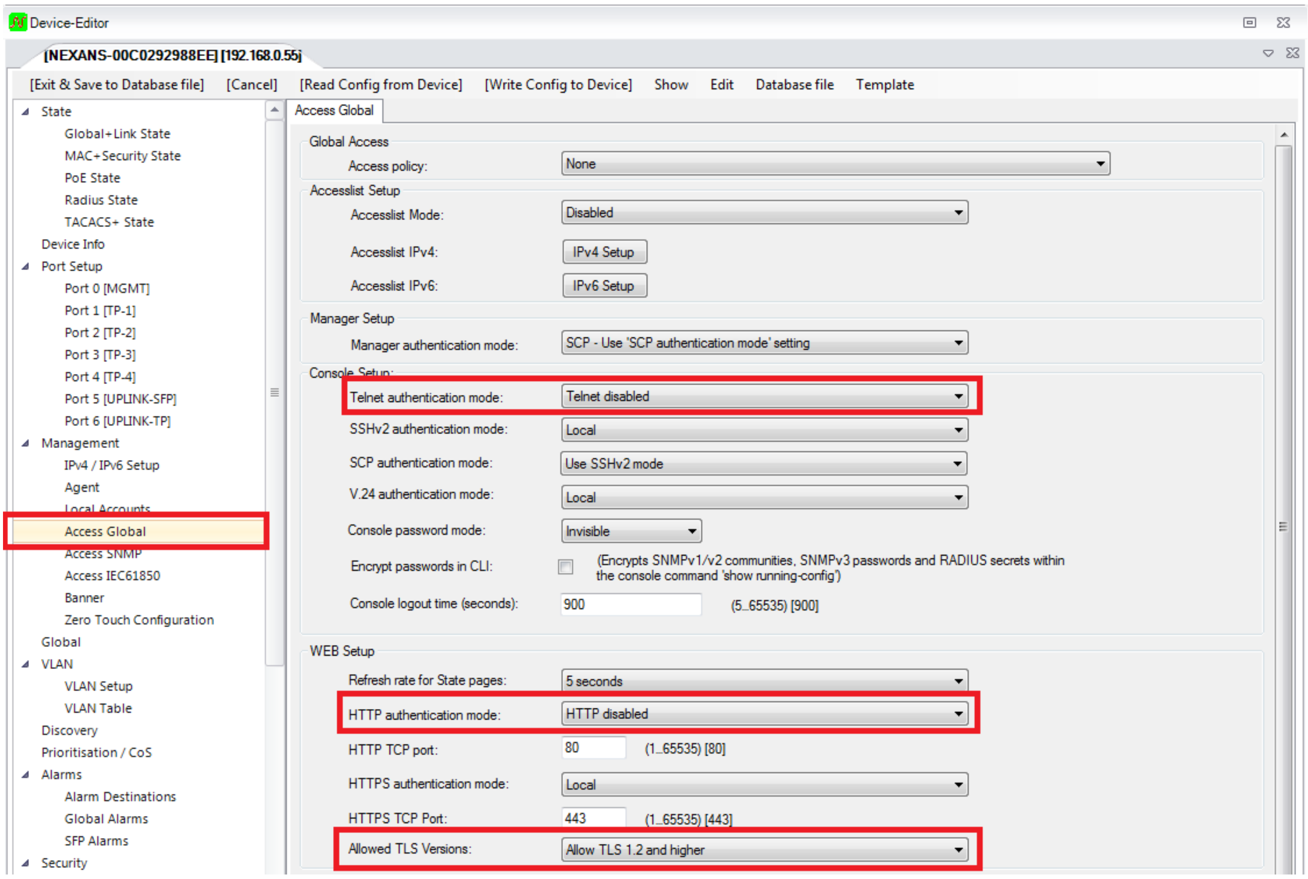
SHA256-Hash:
It is the special property of a hash value that it is practically impossible to calculate the original password from this Hash. However, the precondition is that the password has a sufficient complexity and a minimum length of 8 chars. If we have higher requirements it is useful to use at least 12 chars.

2. Device Management Access

The following configuration interfaces / protocols represent a security vulnerability and should therefore be disabled.

- Telnet
- HTTP
- TLS 1.0

NEXMAN configuration: Access Global -> Console Setup
NEXMAN configuration: Access Global -> WEB Setup



Global Access
Access policy: None

Accesslist Setup
Accesslist Mode: Disabled
Accesslist IPv4:
Accesslist IPv6:

Manager Setup
Manager authentication mode: SCP - Use 'SCP authentication mode' setting

Console Setup
Telnet authentication mode: Telnet disabled
SSHv2 authentication mode: Local
SCP authentication mode: Use SSHv2 mode
V.24 authentication mode: Local
Console password mode: Invisible
Encrypt passwords in CLI: □ (Encrypts SNMPv1/v2 communities, SNMPv3 passwords and RADIUS secrets within the console command 'show running-config')
Console logout time (seconds): 900 (5..65535) [900]

WEB Setup
Refresh rate for State pages: 5 seconds
HTTP authentication mode: HTTP disabled
HTTP TCP port: 80 (1..65535) [80]
HTTPS authentication mode: Local
HTTPS TCP Port: 443 (1..65535) [443]
Allowed TLS Versions: Allow TLS 1.2 and higher

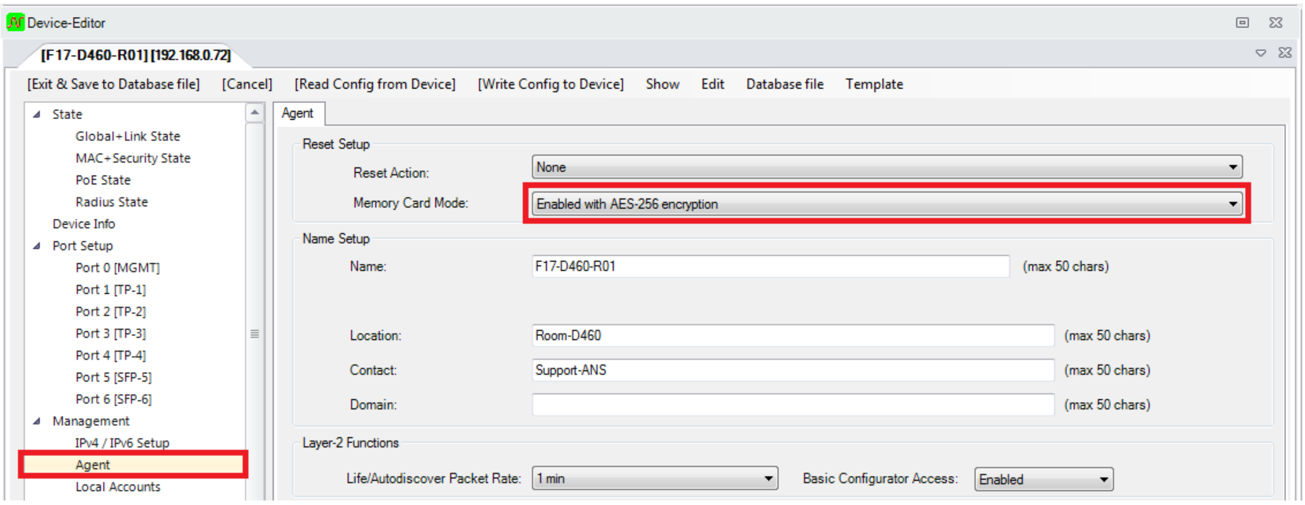
CLI configuration:

```
co:nfig tel:net-auth-mode {setup}
   Sets the Telnet authentication mode or disables the Telnet interface.
   Valid values for {setup} are:
   {l:ocal|r:adius|both-r:adius-local|t:acacs+|both-t:acacs+-local|
    d:isable-telnet}

co:nfig web-a:uth-mode {l:ocal|r:ead-only|d:isable-web}

co:nfig tls {a:ll|1.1|1.2}
   Set allowed TLS versions for HTTPS access (Default = all).
   all: allow all available TLS version
   1.1: allow 1.1 and higher version
   1.2: allow 1.2 and higher version
```

3. Memory Card Mode

To secure the configuration on the Memory Card Mode “Enabled with AES-256 encryption” or “Enabled with AES-256 encryption and Firmware storage” should be selected.

NEXMAN configuration: Agent -> Memory Card Mode



Reset Action: None

Memory Card Mode: Enabled with AES-256 encryption

Name: F17-D460-R01 (max 50 chars)

Location: Room-D460 (max 50 chars)

Contact: Support-ANS (max 50 chars)

Domain: (max 50 chars)

Life/Autodiscover Packet Rate: 1 min Basic Configurator Access: Enabled

CLI configuration:

```
co:nfig me:mory-card-mode {setup}
   Valid values for {setup} are:
   {e:nabled|d:isabled|permanent-disabled|a:es-256-enabled|f:w-aes256-enabled}
```

Enabled with AES-256 encryption:
The Memory Card (MC) function is active. The switch configuration is encrypted with AES-256 encryption before being stored on the MC. An encrypted configuration stored on the MC can be read, even if the Memory Card Mode is not set.

Enabled with AES-256 encryption and Firmware storage:
The Memory Card (MC) function is active. In addition to storing the configuration during a firmware update the firmware file is stored in flash memory and on the MC.

If the Memory Card is not used in the switch the mode should be set to „Disabled“

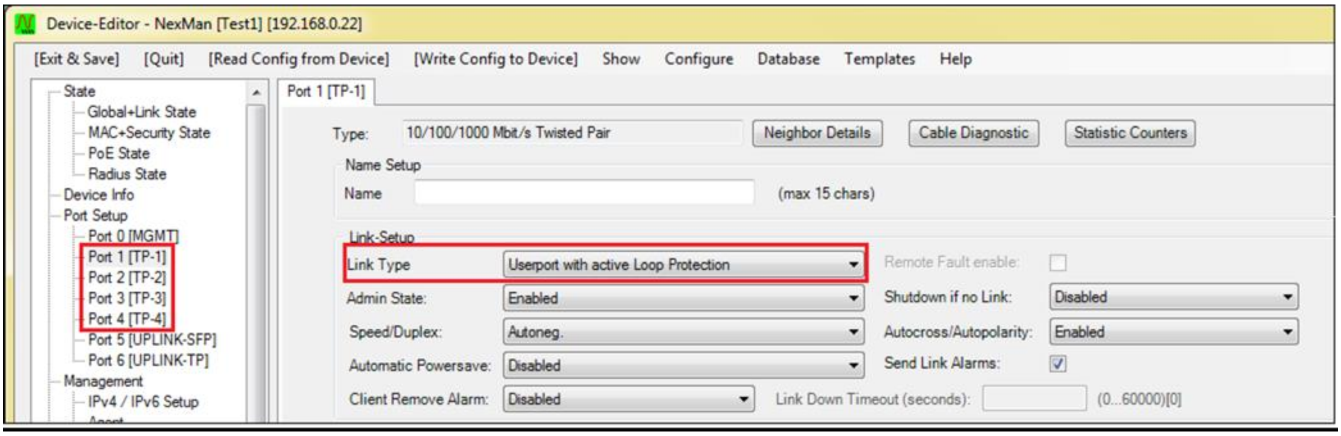
Disabled:
If the Memory Card Mode is set to „Disabled“, the memory card function is disabled.

4. Userport with active Loop Protection

To prevent a loop occurrence in the network such as short-circuiting two user ports, the Link Type “Userport with active Loop Protection” should be enabled on all user ports. With this function, the respective ports will automatically be disabled before a loop occurs.

The “Userport with active Loop Protection” function can be enabled on the Port Tabs in the Manager or via CLI.

NEXMAN configuration: Port {id} -> Link-Setup



Device-Editor - NexMan [Test1] [192.168.0.22]

Port 1 [TP-1]

Type: 10/100/1000 Mbit/s Twisted Pair

Name Setup

Name: (max 15 chars)

Link-Setup

Link Type: Userport with active Loop Protection

Remote Fault enable: ☐

Admin State: Enabled

Shutdown if no Link: Disabled

Speed/Duplex: Autoneg.

Autocross/Autopolarity: Enabled

Automatic Powersave: Disabled

Send Link Alarms: ☑

Client Remove Alarm: Disabled

Link Down Timeout (seconds): (0...60000)[0]

CLI configuration:

```
in:terface <if-no> link-t:ype {us:erport|lo:op-protect|up:link-downlink}
```

Description:
This configuration will prevent from a switching loop to crash the network. Loops can be caused by short-circuiting two ports or downstream hubs and switches.
When a loop occurs, specific Loop Protection packets will be sent over to this port and verified whether these packets are received on the same port or on another port, which also needs to be set to the corresponding link type. If so, the port is disabled and Loop Disabled will be displayed in the Admin State.

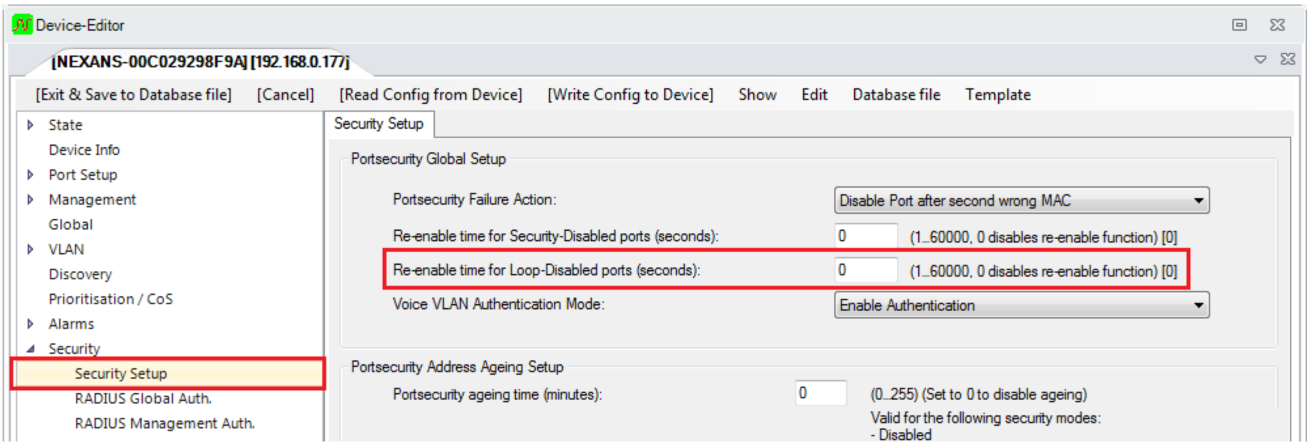
IMPORTANT:
In order to detect loops reliably, the management VLAN should not be enabled on the corresponding ports.

Note:
This function will cause an additional quiet time of approximately 5 seconds after a Link-Up. During this time the switch is already sending Loop Protection packets, however, any other traffic will be blocked, in order to prevent a temporary loop in case of a short-circuit.

4.1. Re-Enable Time for Loop-Disabled ports

Loop disabled Ports can be automatically re-enabled after time period of 1 to 60000 seconds by using the parameter “Re-Enable time for Loop-Disabled ports”. If the time is set to “0”, the port has to be re-enabled manually.

NEXMAN configuration: Security Setup -> Portsecurity Global Setup



Portsecurity Global Setup

Portsecurity Failure Action: Disable Port after second wrong MAC

Re-enable time for Security-Disabled ports (seconds): 0 (1..60000, 0 disables re-enable function) [0]

Re-enable time for Loop-Disabled ports (seconds): 0 (1..60000, 0 disables re-enable function) [0]

Voice VLAN Authentication Mode: Enable Authentication

Portsecurity Address Ageing Setup

Portsecurity ageing time (minutes): 0 (0..255) (Set to 0 to disable ageing)
Valid for the following security modes:
- Disabled

CLI configuration: `co:nfig r:e-enable l:oop-disable (0...60000)`

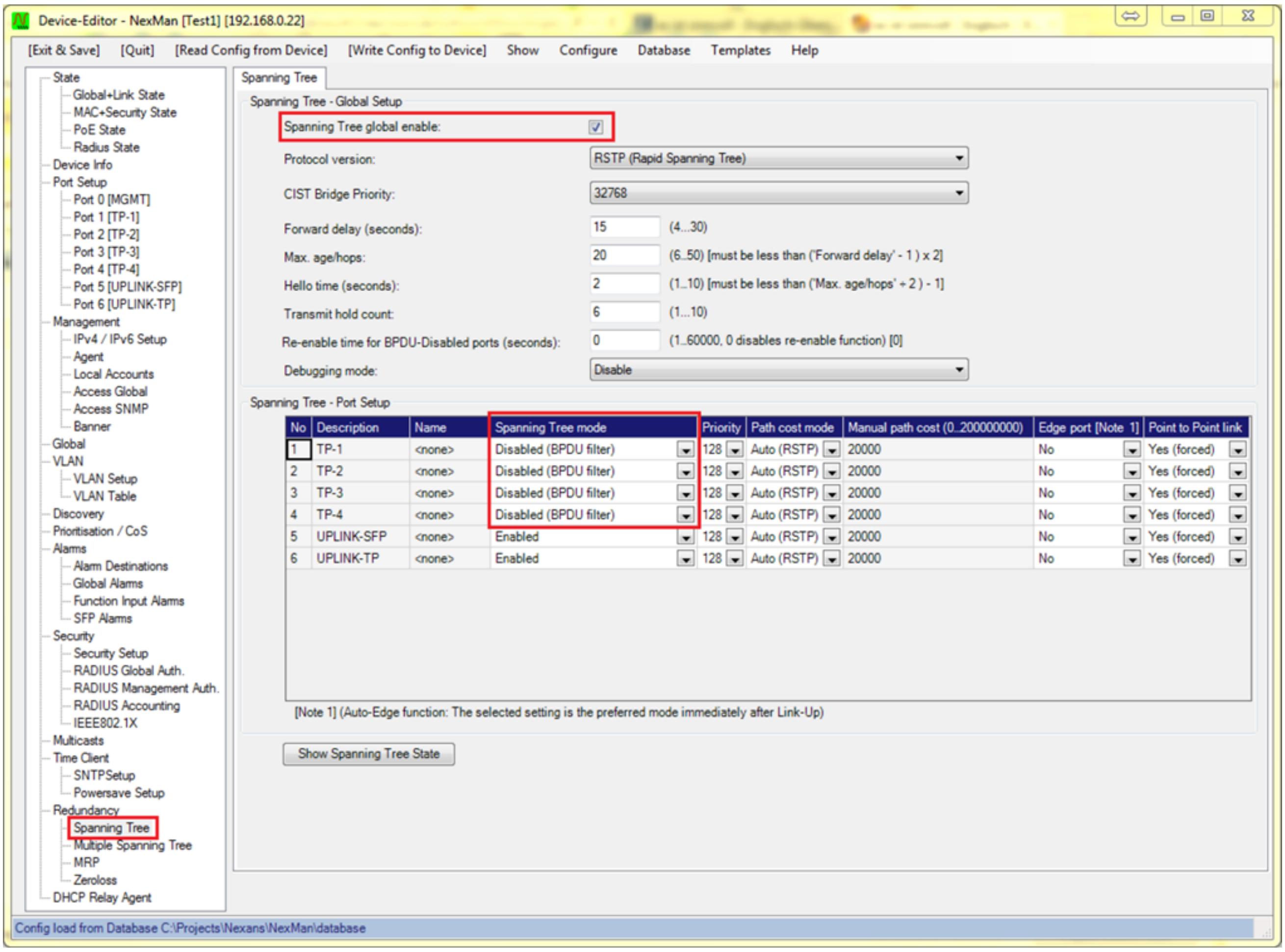
Description:
Disabled ports can automatically be re-enabled after “Re-Enable time for Loop-Disabled Ports” has been configured. The time value can be set in the range from 1 to 60000 seconds.

5. BPDU (Bridge Protocol Data Unit) Guard

To protect the networks against undesired Spanning-Tree devices the BPDU Guard can be enabled on the Userports.

The BPDU Guard can be enabled on the “Spanning Tree” tab. There are two modes available: “Disabled BPDU filter)” and “Disabled (BPDU disables Port)”.

NEXMAN configuration: Spanning Tree -> Spanning Tree – Port Setup



Spanning Tree - Global Setup

Spanning Tree global enable: ☑

Protocol version: RSTP (Rapid Spanning Tree)

CIST Bridge Priority: 32768

Forward delay (seconds): 15 (4...30)

Max. age/hops: 20 (6..50) [must be less than ('Forward delay' - 1) x 2]

Hello time (seconds): 2 (1..10) [must be less than ('Max. age/hops' + 2) - 1]

Transmit hold count: 6 (1...10)

Re-enable time for BPDU-Disabled ports (seconds): 0 (1..60000, 0 disables re-enable function) [0]

Debugging mode: Disable

Spanning Tree - Port Setup

No	Description	Name	Spanning Tree mode	Priority	Path cost mode	Manual path cost (0..200000000)	Edge port [Note 1]	Point to Point link
1	TP-1	<none>	Disabled (BPDU filter)	128	Auto (RSTP)	20000	No	Yes (forced)
2	TP-2	<none>	Disabled (BPDU filter)	128	Auto (RSTP)	20000	No	Yes (forced)
3	TP-3	<none>	Disabled (BPDU filter)	128	Auto (RSTP)	20000	No	Yes (forced)
4	TP-4	<none>	Disabled (BPDU filter)	128	Auto (RSTP)	20000	No	Yes (forced)
5	UPLINK-SFP	<none>	Enabled	128	Auto (RSTP)	20000	No	Yes (forced)
6	UPLINK-TP	<none>	Enabled	128	Auto (RSTP)	20000	No	Yes (forced)

[Note 1] (Auto-Edge function: The selected setting is the preferred mode immediately after Link-Up)

Config load from Database C:\Projects\Nexans\NexMan\database

CLI configuration:

```
rs:tp mo:de {e:nabled|d:isabled}
   Valid values for {setup} are:
   {e:nable|l:oop-protect-enable|d:isable|b:pdu-disable}
```

Description:

Disabled (BPDU filter):

The port does not send any BPDU packets and the received BPDU packet are ignored.

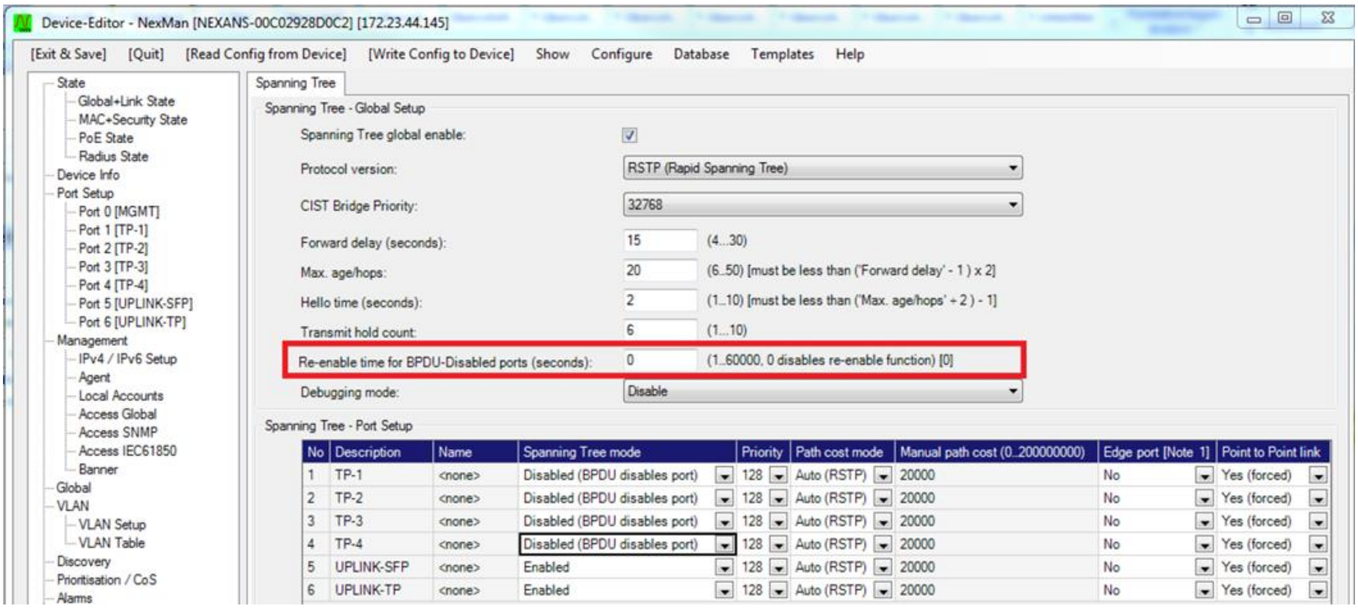
Disabled (BPDU disables Port):

The port does not send any BPDU packets and the received BPDU packets will disable the port. In this case BPDU-DISABLED will be indicated as the port’s link status and a Port Error Disable alarm will be sent.

5.1. Re-Enable Time for BPDU-DISABLED ports

BPDU disabled Ports can be automatically Re-Enabled after a time period of 1 to 60000 seconds by using the parameter “Re-Enable time for BPDU-Disabled ports”. If the time is set to “0”, the port has to be re-enabled manually.

NEXMAN configuration: Spanning Tree -> Spanning Tree – Global Setup



Spanning Tree - Global Setup

Spanning Tree global enable:	☑	
Protocol version:	RSTP (Rapid Spanning Tree)	
CIST Bridge Priority:	32768	
Forward delay (seconds):	15	(4...30)
Max. age/hops:	20	(6..50) [must be less than ('Forward delay' - 1) x 2]
Hello time (seconds):	2	(1..10) [must be less than ('Max. age/hops' + 2) - 1]
Transmit hold count:	6	(1...10)
Re-enable time for BPDU-Disabled ports (seconds):	0	(1..60000, 0 disables re-enable function) [0]
Debugging mode:	Disable	

Spanning Tree - Port Setup

No	Description	Name	Spanning Tree mode	Priority	Path cost mode	Manual path cost (0..200000000)	Edge port [Note 1]	Point to Point link
1	TP-1	<none>	Disabled (BPDU disables port)	128	Auto (RSTP)	20000	No	Yes (forced)
2	TP-2	<none>	Disabled (BPDU disables port)	128	Auto (RSTP)	20000	No	Yes (forced)
3	TP-3	<none>	Disabled (BPDU disables port)	128	Auto (RSTP)	20000	No	Yes (forced)
4	TP-4	<none>	Disabled (BPDU disables port)	128	Auto (RSTP)	20000	No	Yes (forced)
5	UPLINK-SFP	<none>	Enabled	128	Auto (RSTP)	20000	No	Yes (forced)
6	UPLINK-TP	<none>	Enabled	128	Auto (RSTP)	20000	No	Yes (forced)

CLI configuration: `co:nfig r:e-enable b:pdu-disable (0...60000)`

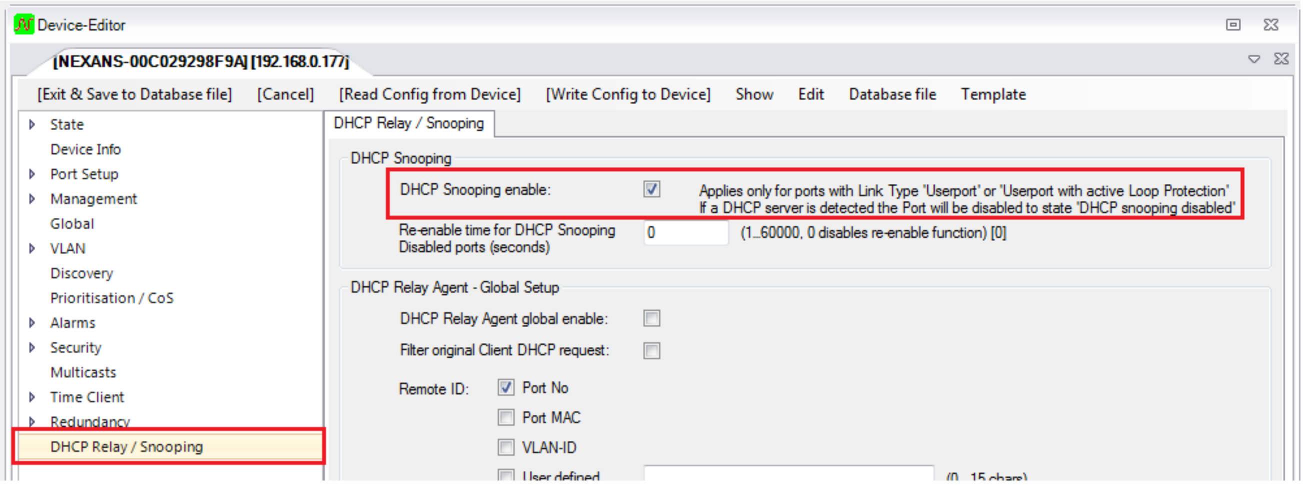
Description:
BPDU-DISABLED ports can automatically be re-enabled after “Re-Enable time for BPDU-Disabled Ports” has been configured. The time value can be set in the range from 1 to 60000 seconds.

IMPORTANT:
If Spanning Tree is globally disabled, the switch will be transparent for the BPDU packets and any received BPDU packets will be forwarded to all ports of the same VLAN.

6. DHCP Snooping

If DHCP Snooping is set to “Enable”, it will be enabled on all ports whose link type is set to “Userport” or “Userport with Active Loop Protection”. As soon as a packet from a DHCP server is received on these ports, the switch will set the respective port’s Admin State to “Disabled by DHCP Snooping”. Thus, it is possible to prevent a DHCP server from being connected to the switch’s user ports.

NEXMAN configuration: DHCP Relay / Snooping -> DHCP Snooping



DHCP Snooping

DHCP Snooping enable: ☑ Applies only for ports with Link Type 'Userport' or 'Userport with active Loop Protection'
If a DHCP server is detected the Port will be disabled to state 'DHCP snooping disabled'

Re-enable time for DHCP Snooping Disabled ports (seconds): 0 (1..60000, 0 disables re-enable function) [0]

DHCP Relay Agent - Global Setup

DHCP Relay Agent global enable: □

Filter original Client DHCP request: □

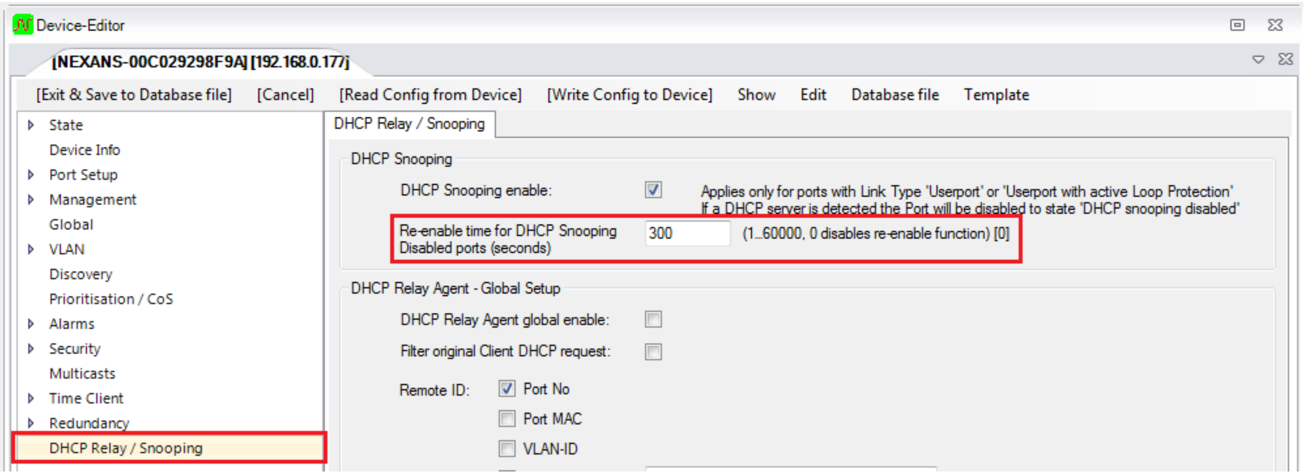
Remote ID: ☑ Port No
□ Port MAC
□ VLAN-ID
□ User defined (0...15 chars)

CLI configuration: `dh:cp s:nooping mo:de {e:nabled|d:isabled}`

6.1. Re-enable time for DHCP Snooping Disabled ports

Ports, which were disabled due to DHCP Snooping can optionally be re-enabled automatically after a time period of 1 to 60000 seconds. If the time is set to “0”, the port has to be re-enabled manually.

NEXMAN configuration: DHCP Relay / Snooping -> DHCP Snooping



DHCP Snooping

DHCP Snooping enable: ☑ Applies only for ports with Link Type 'Userport' or 'Userport with active Loop Protection'
If a DHCP server is detected the Port will be disabled to state 'DHCP snooping disabled'

Re-enable time for DHCP Snooping Disabled ports (seconds): 300 (1..60000, 0 disables re-enable function) [0]

DHCP Relay Agent - Global Setup

DHCP Relay Agent global enable: □

Filter original Client DHCP request: □

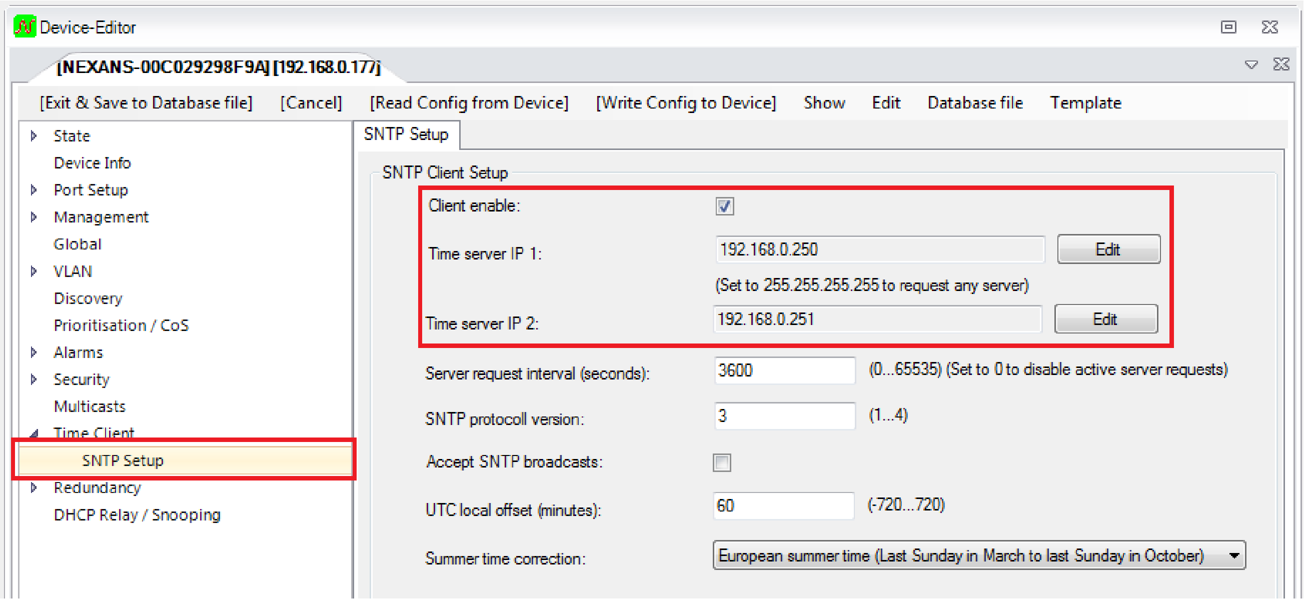
Remote ID: ☑ Port No
□ Port MAC
□ VLAN-ID

CLI configuration: `co:nfig r:e-enable d:hcp-snoop-disable (0...60000)`

7. Simple Network Time Protocol (SNTP)

If a NTP/SNTP time server is available in the network, it should also be a part of the Nexans Configuration. This allows the switch to add the local time to its internal logs. This is useful for later analyze/debug in case of a failure.

NEXMAN configuration: SNTP Setup -> SNTP Client Setup



SNTP Client Setup

Client enable: ☑

Time server IP 1: 192.168.0.250

(Set to 255.255.255.255 to request any server)

Time server IP 2: 192.168.0.251

Server request interval (seconds): 3600 (0...65535) (Set to 0 to disable active server requests)

SNTP protocoll version: 3 (1...4)

Accept SNTP broadcasts: □

UTC local offset (minutes): 60 (-720...720)

Summer time correction: European summer time (Last Sunday in March to last Sunday in October)

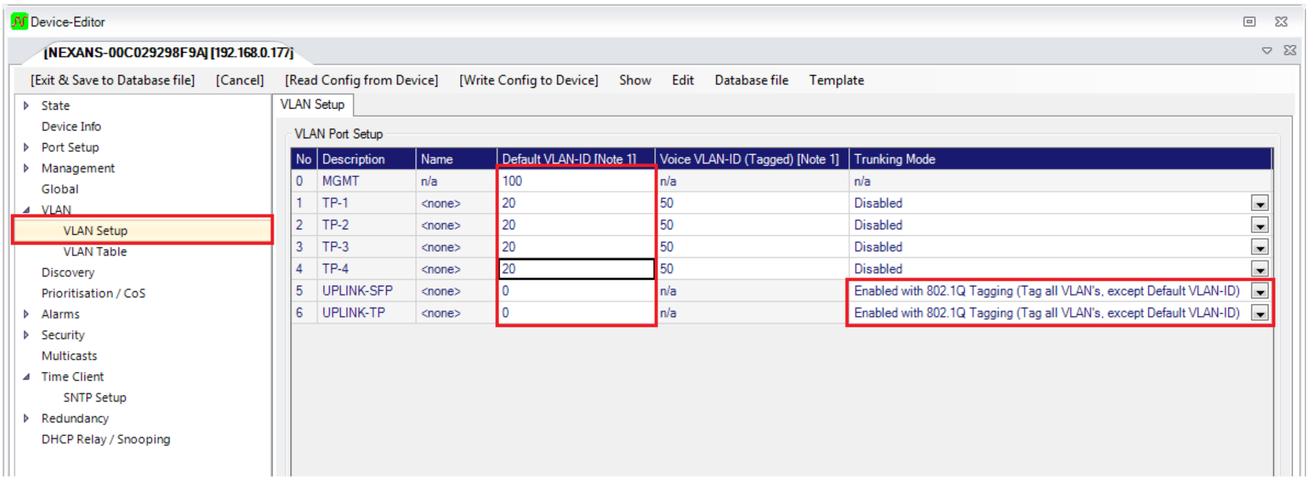
CLI configuration:

```
snt:p st:atus {e:nable|d:isable}
snt:p server-ip {<ip-address>|di:sable}
snt:p server-ip-2 {<ip-address>|di:sable}
```

8. VLAN Configuration

Of course, every Network has its own global VLAN implementation and it is therefore difficult to define a configuration that will fit into every architecture. However, this chapter will show one possibility that has been successfully implemented in many network environments. The goal of this configuration is to sperate the Management VLAN of the switches from the rest of the ports and at the same time drop all untagged packets arriving at the uplink port to achieve a fully tagged network.

NEXMAN configuration: VLAN Setup -> VLAN Port Setup



VLAN Port Setup

No	Description	Name	Default VLAN-ID [Note 1]	Voice VLAN-ID (Tagged) [Note 1]	Trunking Mode
0	MGMT	n/a	100	n/a	n/a
1	TP-1	<none>	20	50	Disabled
2	TP-2	<none>	20	50	Disabled
3	TP-3	<none>	20	50	Disabled
4	TP-4	<none>	20	50	Disabled
5	UPLINK-SFP	<none>	0	n/a	Enabled with 802.1Q Tagging (Tag all VLAN's, except Default VLAN-ID)
6	UPLINK-TP	<none>	0	n/a	Enabled with 802.1Q Tagging (Tag all VLAN's, except Default VLAN-ID)

CLI configuration:

```
in:terface {if-no range} vl:an-id (0|1...4095)
in:terface {if-no range} t:runking-mode {di:sable|do:t1q|n:otag|h:ybrid}
```

8.1. VLAN Name configuration

In the VLAN Table a unique name can be assign to each VLAN that in most cases will represent the functionality.

NEXMAN configuration: VLAN Table -> Table

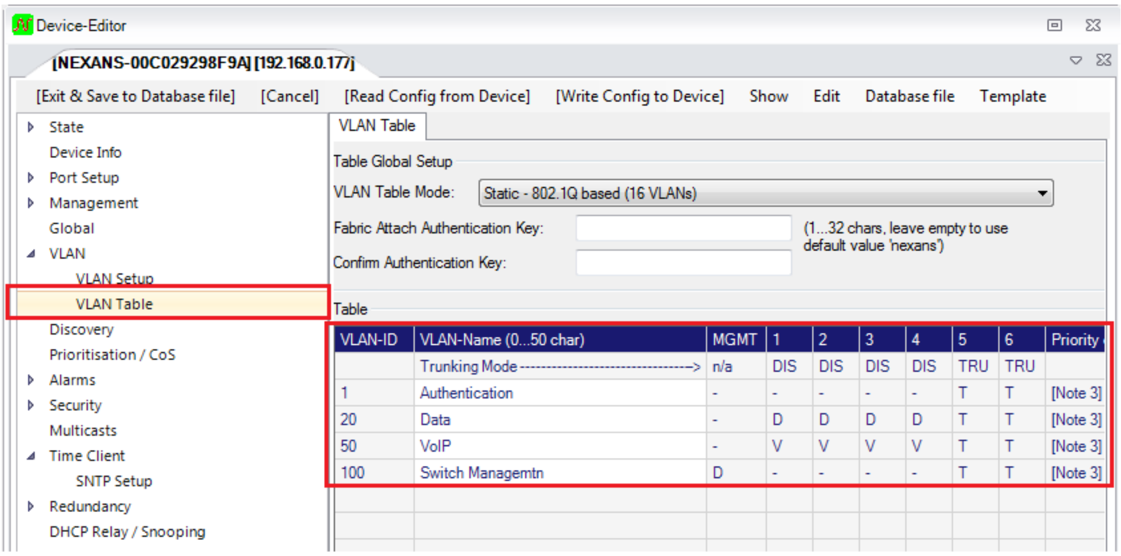


Table Global Setup

VLAN Table Mode: Static - 802.1Q based (16 VLANs)

Fabric Attach Authentication Key: (1...32 chars, leave empty to use default value 'nexans')

Confirm Authentication Key:

Table

VLAN-ID	VLAN-Name (0...50 char)	MGMT	1	2	3	4	5	6	Priority
	Trunking Mode ------------------------------>	n/a	DIS	DIS	DIS	DIS	TRU	TRU	
1	Authentication	-	-	-	-	-	T	T	[Note 3]
20	Data	-	D	D	D	D	T	T	[Note 3]
50	VoIP	-	V	V	V	V	T	T	[Note 3]
100	Switch Managemtn	D	-	-	-	-	T	T	[Note 3]

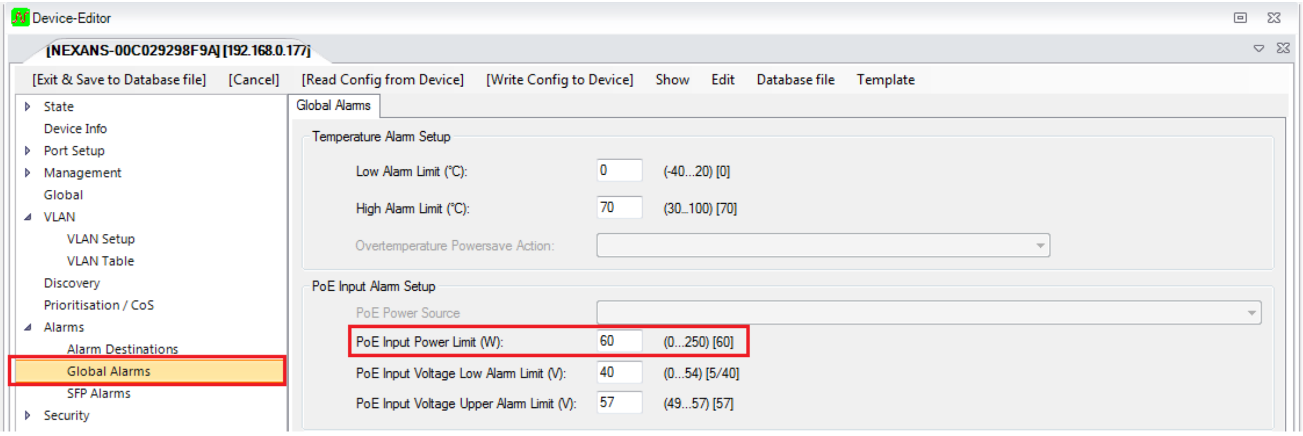
CLI configuration:

```
v:lan-table a:dd {vlan-id range} [<string max. 50 chars>]
```

9. PoE Input Power Limit

It is important to define the maximum available power that can be used for delivering PoE. The “PoE Input Power Limit” defines which maximum overall power may be taken from the power supply for the PoE. If the set power limit is exceeded, one port after the other will be switched off, starting with the highest port number, until the power consumption is within the limit again. This means that port TP-1 has highest priority and will always be the last to be disabled. However, only those ports will be switched off, which actually have a PoE load connected. Moreover, in case of an overload, the Switch will send the PoE Overload event.

NEXMAN configuration: Global Alarms -> PoE Input Power Limit (W)



Low Alarm Limit (°C): 0 (-40...20) [0]

High Alarm Limit (°C): 70 (30...100) [70]

Overtemperature Powersave Action:

PoE Power Source

PoE Input Power Limit (W): 60 (0...250) [60]

PoE Input Voltage Low Alarm Limit (V): 40 (0...54) [5/40]

PoE Input Voltage Upper Alarm Limit (V): 57 (49...57) [57]

CLI configuration:

```
co:nfig poe-li:mit (1..250)
```