PROFI TAP

X3-SERIES

X3-440G

X3-880G

ADVANCED NETWORK PACKET BROKERS

USER MANUAL

If you have any questions, you can contact us through our website:

www.profitap.com

or by email:

support@profitap.com

For the latest documentation and software, visit our Resource Center:

https://resources.profitap.com/

TABLE OF CONTENTS

1. Overview

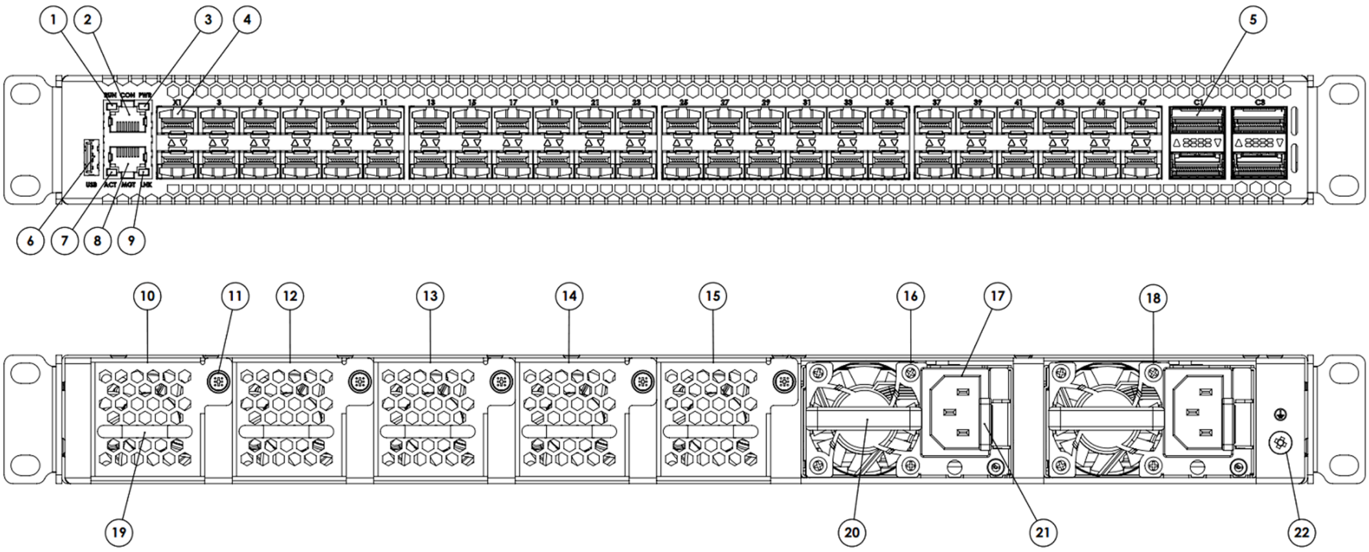
This document provides information about the configuration and operation of X3-Series Network Packet Brokers.

2. Hardware Guide

2.1 Included Accessories

- DB9 to RJ45 serial cable
- (2) Front-mounting ears with (8) screws
- (2) Rear-mounting ears
- (2) AC power cords

2.2 Physical Description



Front View		Rear View	
1	Status LED	10/12/13/14/15	(5) FAN modules
2	Console port	11	FAN module locking screw
3	Power LED	16/18	(2) modular Power Supply Units
4	(48) 1G/10G SFP+	17	PSU input connector
5	(4) 40G/100G QSFP28	19	FAN module handle
6	USB port	20	PSU handle
7	Management port Activity LED	21	PSU lock
8	Management port	22	Grounding lug
9	Management port Link LED		

2.3 Ports Description

2.3.1 Console Port

This serial port is intended to be used for local configuration and administration of the X3 device with Command Line Interface (CLI).

Port parameters: RJ45, RS232, 115200, N, 8, 1

Default username and password for serial connection:

- Username: **admin**
- Password: **admin**

2.3.2 Management Port

This port is intended to be used for local and remote configuration, administration and monitoring of the X3 device with HTTPS / SNMP / SSH.

Port parameters: RJ45, 10BASE-T/100BASE-TX, Auto negotiation, Auto MDI/MDIX

Default username and password for SSH connection:

- Username: **admin**
- Password: **admin**

2.3.3 USB Port

Port parameters: USB 2.0

2.4 Unpacking and Installing the Device

1. Unbox the X3 unit;
2. Refer to the list of included accessories and check the contents of the box;
3. Attach the (2) mounting ears to the main unit using the (8) screws;
4. Install the X3 unit in the rack;
5. Connect the ground wire to the grounding lug (#22);
6. Power up the X3 unit.

2.5 Troubleshooting and Maintenance

2.5.1 Replacing FAN Module

X3 fan tray contains five fan modules. If a fan module fails, you should replace it, however X3 will function with one failed fan module. You can remove individual fan modules using the following procedure:

1. Unscrew the FAN module locking screw (#11);
2. Remove the FAN module using the Fan module handle (#19);
3. Place the new FAN module in the empty slot;
4. Tighten the locking screw (#11).

2.5.2 Replacing PSU

X3 power tray contains two PSU modules. If a PSU module fails, you should replace it, however X3 will function with one failed PSU module. You can remove individual PSU module using the following procedure:

1. Disconnect the power cord from the PSU (#17) to be replaced;
2. Push the PSU lock (#21) on the left;
3. Pull the PSU using the handle (#20);
4. Insert the new PSU until the lock (#21) is in its locked position;
5. Connect the power cord to the new PSU (#17).

3. Initial Setup

3.1 Initial IP Settings

- IP: 192.168.2.100
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.2.1

3.2 Initial Setup

Initial setup can be done via the management port or the serial console port.

Using any terminal software, connect to the device through SSH or serial connection.

Login, using the following credentials:

- Username: **admin**
- Password: **admin**

After logging in, the user can access the system shell and administrate the device using the canonical GNU/Linux OS facilities.

The IP and subnet mask of the device can be changed using the following command:

```
ip addr add [ip_addr/mask] dev eth1
```

With **`ip_addr`** being the IP address and **`mask`** being the CIDR prefix. For example:

```
ip addr add 10.10.10.180/16 dev eth1
```

The user password can be changed using the following command:

```
passwd
```

4. Web UI

This chapter describes method to connect to the Web UI.

Use a supported browser and go to **https://192.168.2.100**

Depending on the browser you might need to accept the self-signed certificate and/or type “thisisunsafe”.

Default username and password for Web UI connection:

- Username: **admin**
- Password: **Passok**

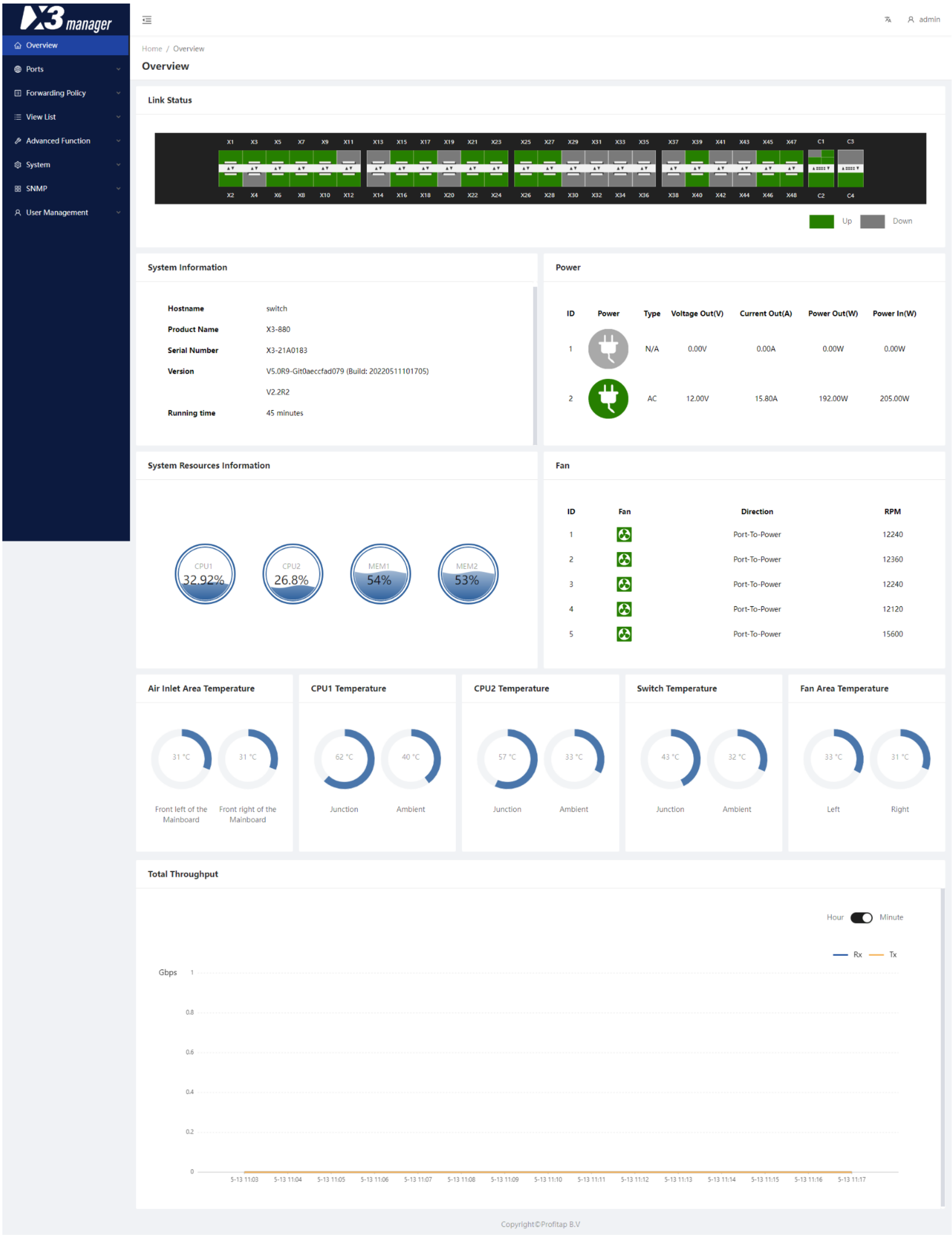
Supported browsers:

- Firefox
- Chrome

4.1 System Overview

This page provides system information about:

- PSU and FAN state;
- System temperature;
- System resource;
- Global Throughput;
- Firmware version.



Overview

Link Status

🟩 Up ▨ Down

System Information

Hostname	switch
Product Name	X3-880
Serial Number	X3-21A0183
Version	V5.0R9-Git0aeccfad079 (Build: 20220511101705)
	V2.2R2
Running time	45 minutes

Power

ID	Power	Type	Voltage Out(V)	Current Out(A)	Power Out(W)	Power In(W)
1		N/A	0.00V	0.00A	0.00W	0.00W
2		AC	12.00V	15.80A	192.00W	205.00W

System Resources Information

Fan

ID	Fan	Direction	RPM
1		Port-To-Power	12240
2		Port-To-Power	12360
3		Port-To-Power	12240
4		Port-To-Power	12120
5		Port-To-Power	15600

Air Inlet Area Temperature

CPU1 Temperature

CPU2 Temperature

Switch Temperature

Fan Area Temperature

Total Throughput

Copyright©Profitap B.V

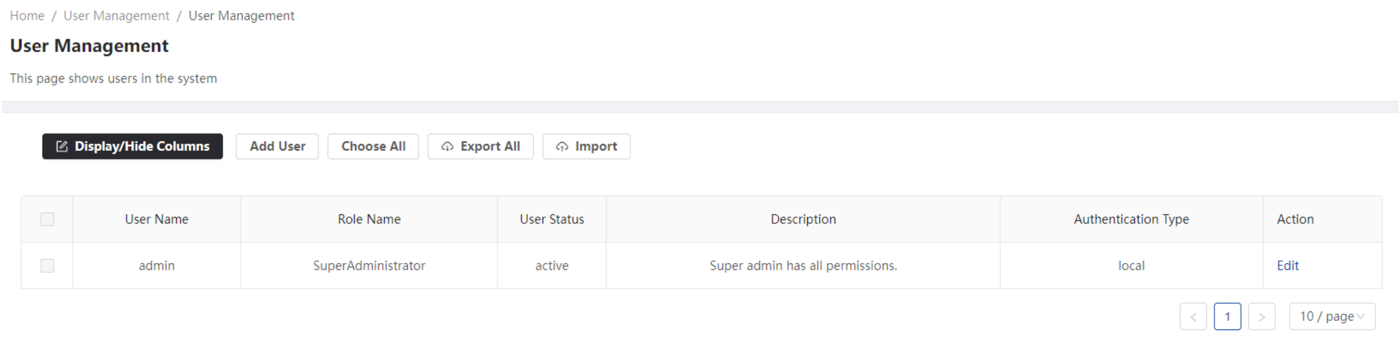
4.2 Device Administration

4.2.1 Network Configuration

Navigate to **System > Network Config** to modify the network settings of the management interface. The device supports IPv4 and IPv6.

4.2.2 Local Users

Navigate to **User Management > User Management** to add or edit users. Local and remote user accounts and type of account must be specified in this configuration panel. At least one super administrator local account is required on the unit. A super administrator may change password of any account in this panel. Current account password can also be changed on the top right user menu.



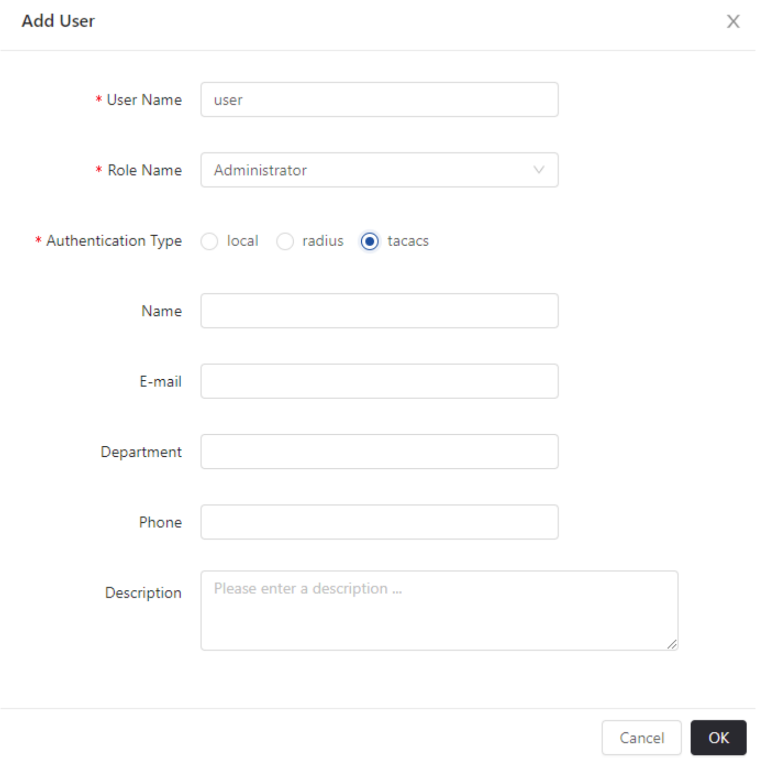
User Management

This page shows users in the system

□	User Name	Role Name	User Status	Description	Authentication Type	Action
□	admin	SuperAdministrator	active	Super admin has all permissions.	local	Edit

4.2.3 TACACS+/RADIUS

Authentication can be managed remotely by a TACACS+ or RADIUS server. The user account and its role (authorization) must be defined on the unit, the authentication will be provided by the server.


Add User

* User Name: user

* Role Name: Administrator

* Authentication Type: ○ local ○ radius ● tacacs

Name:

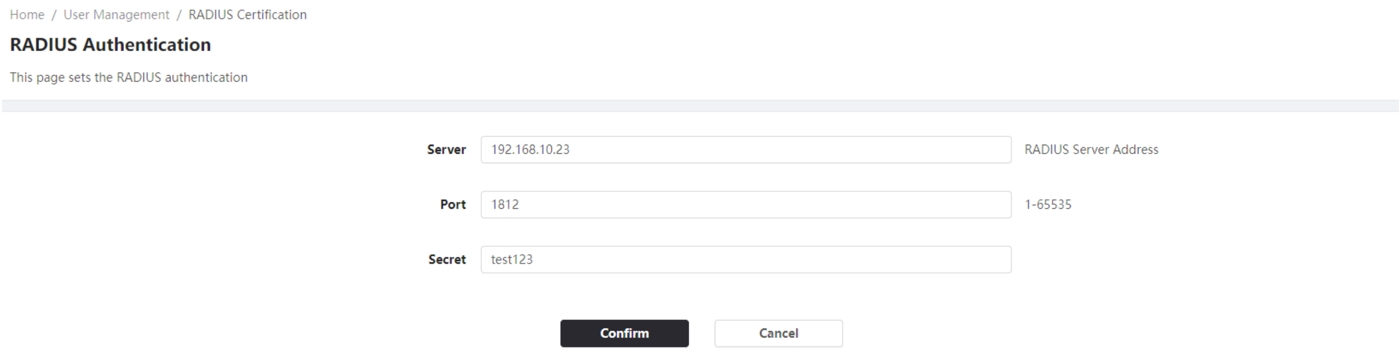
E-mail:

Department:

Phone:

Description: Please enter a description ...

The TACACS+ and RADIUS server information can be provided respectively on the **User Management > TACACS+ Certification** and **User Management > RADIUS Certification** pages. You must provide the server IP address/port and server secret.



Home / User Management / RADIUS Certification

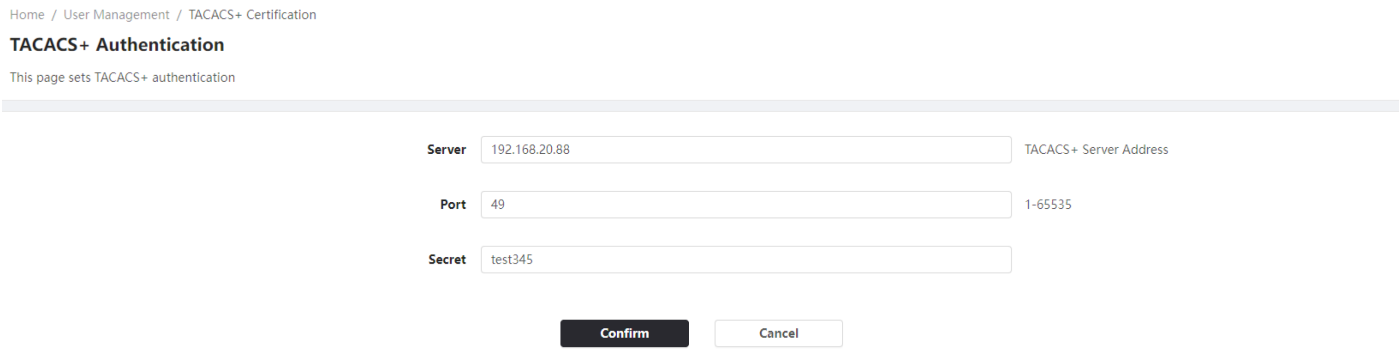
RADIUS Authentication

This page sets the RADIUS authentication

Server: 192.168.10.23 — RADIUS Server Address

Port: 1812 — 1-65535

Secret: test123



Home / User Management / TACACS+ Certification

TACACS+ Authentication

This page sets TACACS+ authentication

Server: 192.168.20.88 — TACACS+ Server Address

Port: 49 — 1-65535

Secret: test345

4.2.4 SNMP

SNMP Config

The **SNMP > SNMP Config** page can be used to control the device's SNMP(v2c/v3) service. The **SNMP Server Config** tab allows the configuration of SNMP server settings, the **SNMP V3 Users** tab allows the configuration of SNMPv3 user settings, and the **SNMP Trap Config** allows the configuration of SNMP *Traps* and *InformRequests*.

Port Trap Config

The **SNMP > Port Trap Config** page can be used to modify, reset, and query port traps.

Explanation of the fields:

FCS	Error packet with check code error.
Error	Error packet with abnormality in structure or MAC.
Speed Max	Maximum allowable port usage rate.
Speed Min	Minimum allowable port usage rate.
Mutation	Maximum allowable port speed rate (Mbps) of mutation.
Link Status	Interface link status.

System Trap Config

The **SNMP > System Trap Config** page allows the user to turn specific traps on or off, and modify trap thresholds.

MIB File Management

The **SNMP > MIB File Management** page allows the import and export of MIB files.

4.2.5 Update

Navigate to **System > Device Upgrade** to update the device software by uploading the software update file.

Navigate to **System > License Upgrade** to update the device license by uploading the license update file.

4.3 Features Overview

Features depend on the type of firmware running on the X3 device. You can change the running firmware in *System > License Upgrade*. License must be provided to enable the desired firmware. Available firmware options are:

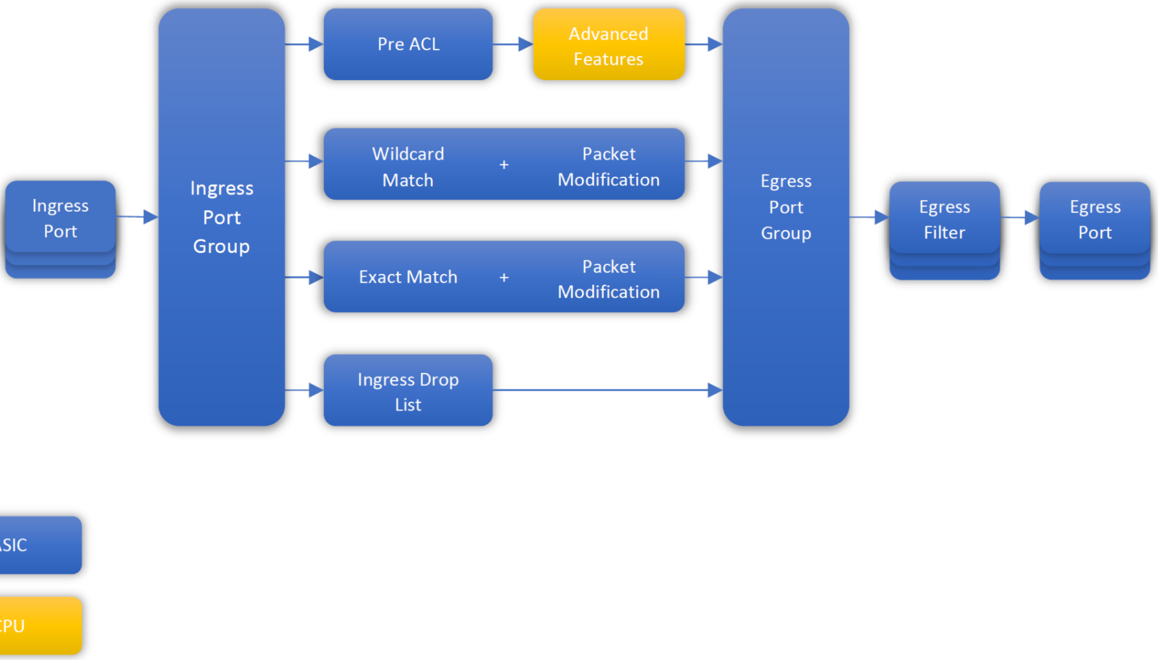
- Normal
- All SSL
- Normal + SSL

Please note that even if a feature is available for multiple firmware, performance will vary depending on the type of firmware used.

FEATURE	NORMAL FIRMWARE	SSL FIRMWARE	NORMAL + SSL FIRMWARE	PROCESSED BY
NetFlow	✔	✘	✔	CPU
SSL	✘	✔	✔	CPU
Deduplication	✔	✔	✔	CPU
IP Reassembly	✔	✘	✔	CPU
TCP Reassembly	✔	✔	✔	CPU
Wildcard Match	✔	✔	✔	ASIC
Exact Match	✔	✔	✔	ASIC
Tunnel Stripping	✔	✔	✔	ASIC
Slicing	✔	✔	✔	ASIC
Timestamping	✔	✔	✔	ASIC
*Advanced Rules**	✔	✘	✔	CPU
Load Balancing	✔	✔	✔	ASIC
*Advanced Load Balancing***	✔	✘	✔	CPU
*Encapsulation/Tunnel****	✔	✔	✔	ASIC
Traffic Management	✔	✘	✔	CPU

** Filter by: Tuple-4, Tuple-6, L2, Regex, Packet Type, URL, IMSI filtering, TCP Flag*
*** Round-Robin, Weighted Round-Robin, Inner Layer, Outer Layer*
**** Stripping/Termination VLAN, GRE, GTP, VXLAN, MPLS, ERSPAN, Cisco FabricPath*

4.4 Traffic Flow Overview



4.4.1 Functional Blocks Description

FUNCTIONAL BLOCK	FUNCTION
Ingress Port	Strip Tunnels: GRE, GTP, VXLAN, MPLS, ERSPAN, Cisco FabricPath Per port inner/outer filtering option
Ingress Port Group	Form a logical group of port(s)
Wildcard Match	Forward traffic based on: IPv4/6 addresses, L4 Ports, VNI, MPLS (3 labels), outer VLAN, inner VLAN, Protocol, EtherType, DSCP, VNI, IP Fragment, Packet Type, Packet Size, TCP Flag, HTTP method Additional action: Add/remove/modify VLAN, modify MAC addresses, slice packets
Exact Match	Forward traffic based on: IPv4/6 addresses, Protocol, L4 Ports Additional action: Add VLAN, delete double VLAN
Pre ACL	Forward traffic to CPU based on: IPv4/6 addresses, Protocol, L4 Ports
Ingress Drop List	Discard traffic based on: IPv4/6 addresses, L4 Ports, VNI, MPLS (3 labels), outer VLAN, inner VLAN, Protocol, EtherType, DSCP, VNI, IP Fragment, Packet Type, Packet Size, TCP Flag, HTTP method
Egress Port Group	Form a logical group of port(s)
Egress Filter	Drop or permit traffic based on: MAC addresses, IPv4/6 addresses, L4 Ports, outer VLAN, inner VLAN, Protocol, EtherType, DSCP, Packet Type, TCP Flag Additional action: Add/remove/modify VLAN
Egress Port	Enable Timestamp output
Advanced Features	Filter: IPv4/6 Tuple, IPv4/6 IP list, L2, Regex, packet type, packet length, URL, IMSI, TCP Flag, Combined filters

4.4.2 Theory of Operation

Ingress rules priority is managed by the rule number ID. User can define the rule ID at rule creation, but rule ID can’t be modified when the rule is applied. For this reason, it is highly recommended to partition the rule table IDs by filter type, that way it is easy to insert rules before or after the applied rules.

Example 1:

This first example describes the rule priority. It is possible to form complex rules by allowing and/or dropping part of the traffic.

ID	INGRESS	EGRESS	TYPE OF RULE	PARAMETER	EFFECT
99	X1		Ingress Drop List / Wildcard	Source IP = 10.0.0.0/8	Drop all traffic coming from X1 matching the masked IP
100	X1	X2	Policy / Wildcard	Protocol = tcp	All TCP traffic coming from X1, not dropped by rule 99, will output on X2
101	X1	X2	Policy / Pre ACL	-	All traffic coming from X1, not dropped by rule 99, not matched by rule 100, will be sent to CPU and output on X2

Example 2:

In this example, only HTTPS traffic is sent to the CPU for decryption, decrypted traffic egresses on port X2, all other traffic egresses on port X2 directly.

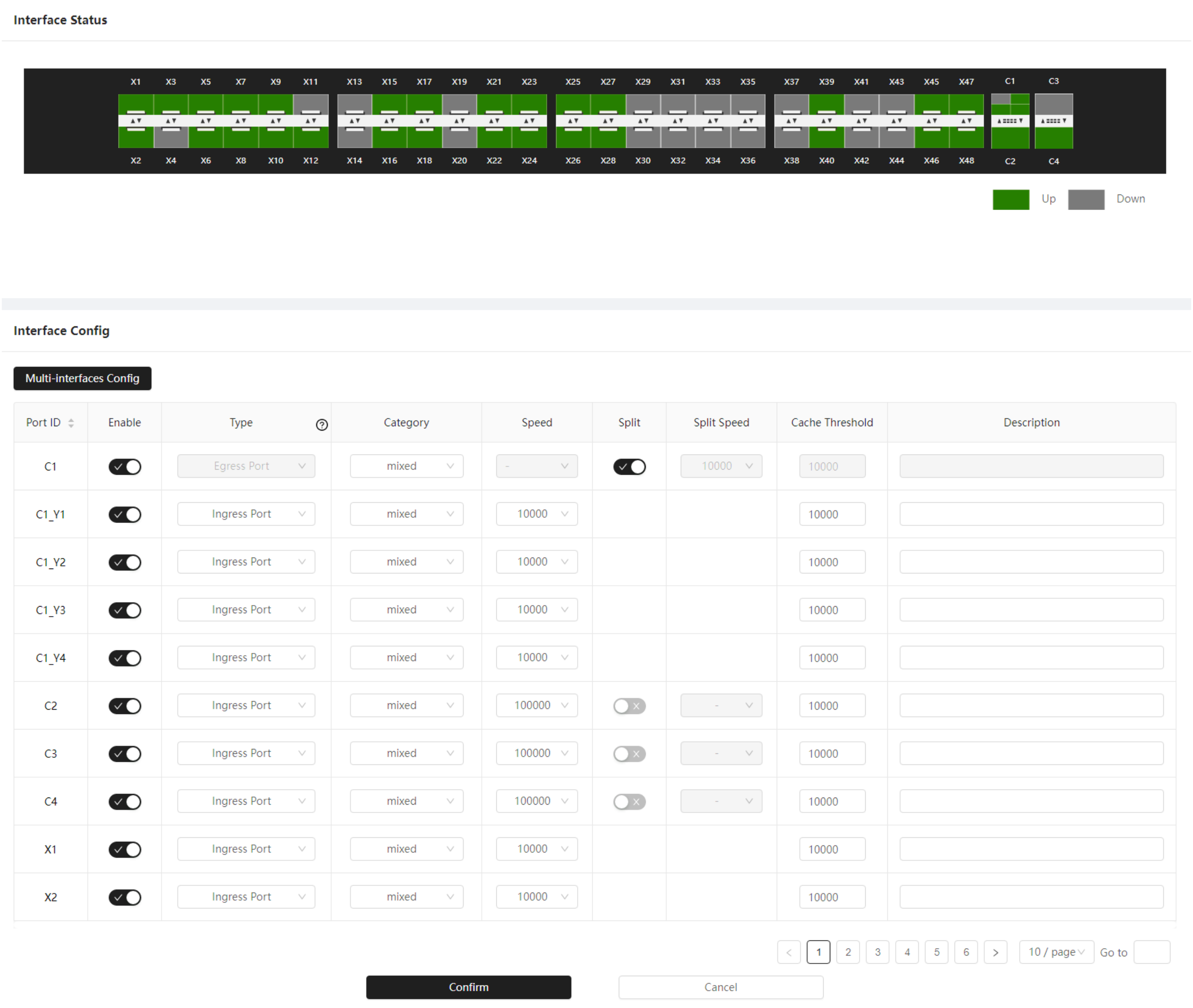
ID	INGRESS	EGRESS	TYPE OF RULE	PARAMETER	EFFECT
98	X1	X2	Policy / Pre ACL	Source Port = 443	All traffic coming from X1 and matching the rule is sent to CPU and output on X2
99	X1	X2	Policy / Pre ACL	Dest. Port = 443	All traffic coming from X1 and matching the rule, not matching rule 98 is sent to CPU and output on X2
100	X1	X2	Policy / Wildcard	-	All traffic coming from X1 and not matching rules 98 or 99 will output on X2

4.4.3 Benchmarks

Performance of features are evaluated with the latest released firmware. Performance of features processed in CPU depend on the type of traffic, packet rate and concurrent features enabled. Concurrent use of multiple features may affect the overall performance of all features processed in CPU. ASIC features are processed at wire speed and are not subject to any performance degradation.

4.5 Port Configuration and Statistics

4.5.1 Port Configuration



Interface Config

Multi-interfaces Config

Port ID	Enable	Type	Category	Speed	Split	Split Speed	Cache Threshold	Description
C1	✓	Egress Port	mixed	-	✓	10000	10000	
C1_Y1	✓	Ingress Port	mixed	10000			10000	
C1_Y2	✓	Ingress Port	mixed	10000			10000	
C1_Y3	✓	Ingress Port	mixed	10000			10000	
C1_Y4	✓	Ingress Port	mixed	10000			10000	
C2	✓	Ingress Port	mixed	100000	✗	-	10000	
C3	✓	Ingress Port	mixed	100000	✗	-	10000	
C4	✓	Ingress Port	mixed	100000	✗	-	10000	
X1	✓	Ingress Port	mixed	10000			10000	
X2	✓	Ingress Port	mixed	10000			10000	

Ports can be configured on the **Ports > Config** page.

Enable

Individual ports can be enabled or disabled via the *Enable* button. All ports are enabled by default.

Port Type

By default, all ports are set to Egress. To accept traffic, a port must be set to Ingress.

Port type configuration details:

- Egress Port: packets are allowed to be sent;
- Ingress Port: packets are allowed to be received and sent;
- Egress Port (Force Tx): packets are allowed to be sent, packets can output without valid link;
- Loopback: packets egressing a loopback interface will be available on its ingress interface, without the need for external physical loopback.

Port Category

The *Category* option is purely informative, and can be used to describe the function of the port (e.g. *mixed* for mixed traffic source, *mirror* for SPAN port, *monitor* for TAP).

Port Speed

The port speed can be set depending on the type of port:

- SFP+: 1G/10G
- QSFP28: 40G/100G/100G FEC

Port Split

QSFP28 ports can be split into 4 x 1G, 4 x 10G, 4 x 25G, or 4 x 25G FEC logical ports by enabling the *Split* option and selecting a *Split Speed*.

Packet Buffer

Packet buffer (*Cache Threshold* option) can be defined for each port. The value represents the number of 256B memory blocks allocated for the port, with a maximum of 90,000 per port.

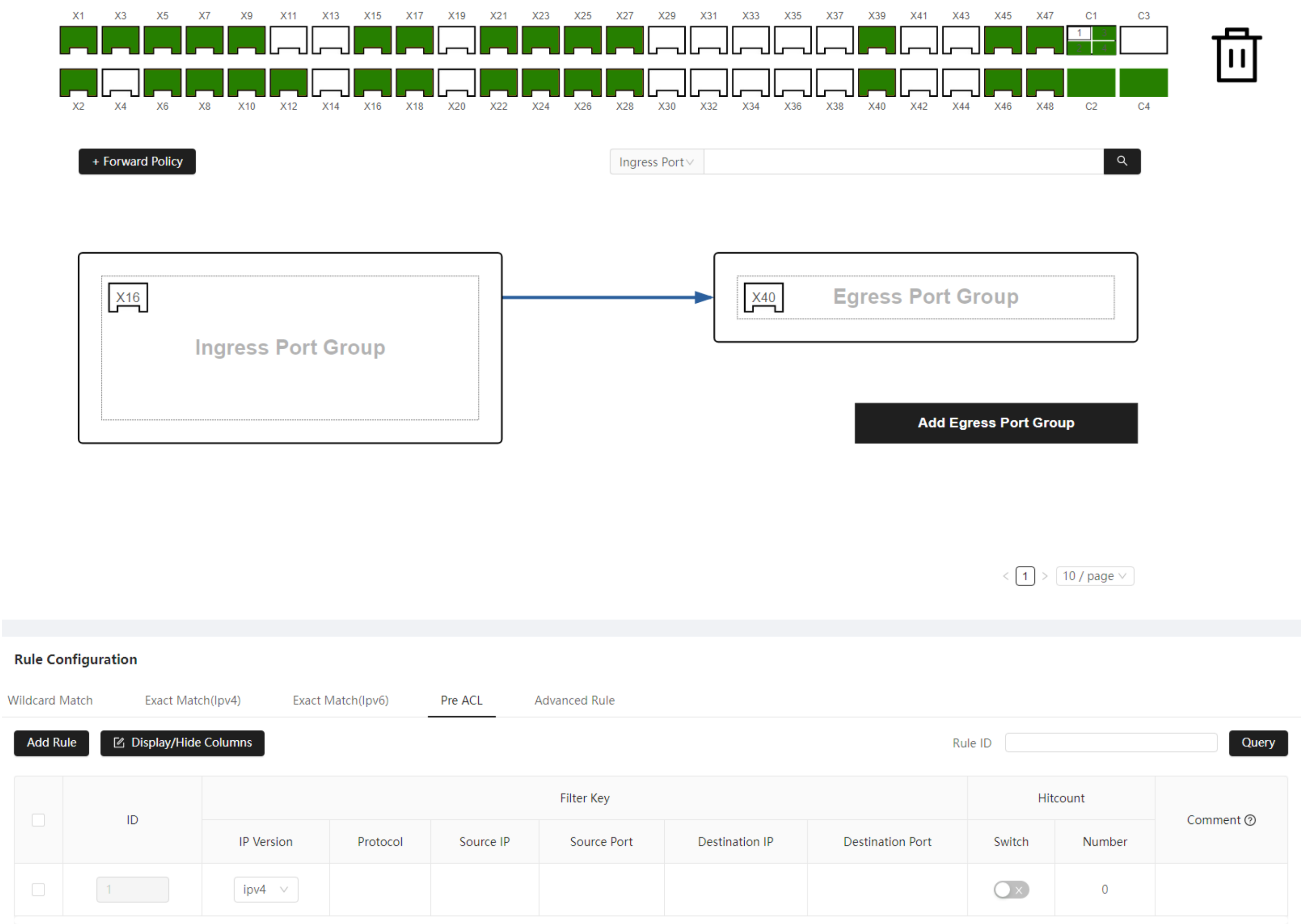
Port Description

A description can be input for each port.

4.5.2 Statistics

The **Ports > Statistics** page displays statistics for each port. Statistics columns can be displayed or hidden via the *Display/Hide Columns* button.

4.6 Traffic Policy



	ID	Filter Key						Hitcount		Comment ⓘ
		IP Version	Protocol	Source IP	Source Port	Destination IP	Destination Port	Switch	Number	
□	1	ipv4							0	

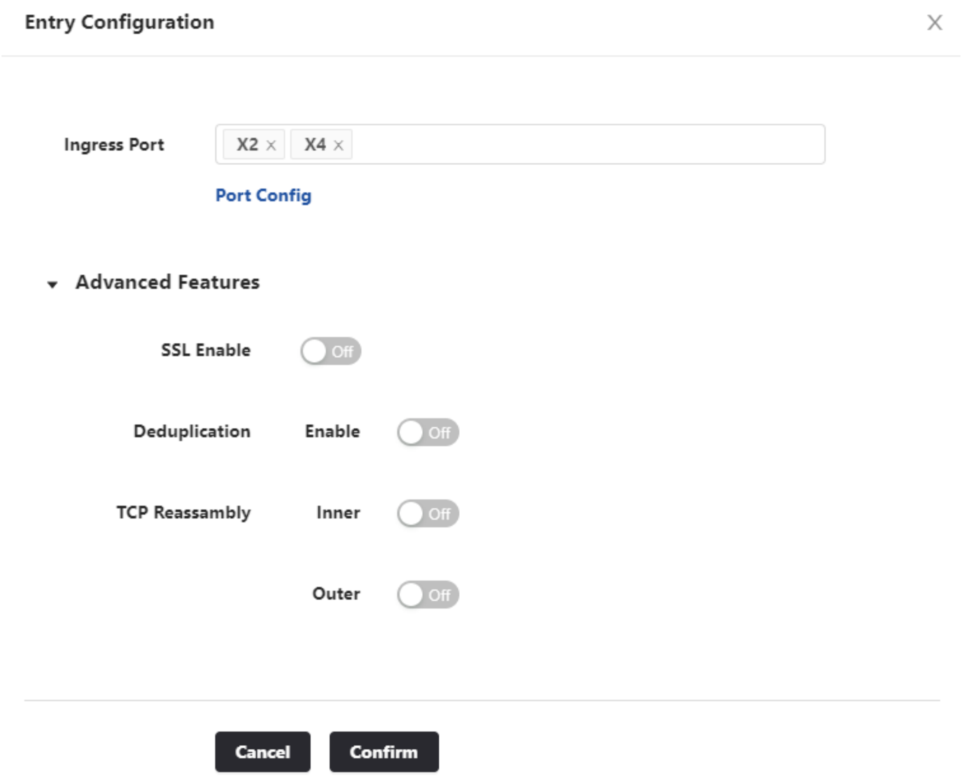
Traffic Policy can be configured on the **Forwarding Policy > Policy** page. It defines the routing between Ingress and Egress ports, the filters, and the traffic manipulation.

A typical workflow is as follows:

1. Add a new Forward Policy by pressing the **+ Forward Policy** button.
2. Drag and drop one or more ports into the **Ingress Port Group** block.
   Note: ingress port and port group options can be defined by clicking on the Ingress Port Group block (see 4.6.1 and 4.6.2).
3. Drag and drop one or more ports into the **Egress Port Group** block.
   Note: egress port and port group options can be defined by clicking on the Egress Port Group block (see 4.6.3 and 4.6.4).
4. Click the **arrow** connecting the Ingress Port Group and Egress Port Group.
   The page will scroll at the bottom of the page, where you can then define the traffic rules for these port groups.
5. Define the traffic rules.
   Note: depending on the ingress and egress port and port group options defined previously, you may need to define a *Pre ACL* rule to direct traffic to the CPU (see Features Overview for the list of features processed by the CPU).
6. Press the *Confirm All* button at the bottom of the page.

Note: An Ingress port can only be part of one Ingress Port Group at a time. An Egress Port can be part of multiple Egress Port Groups.

4.6.1 Ingress Port Group Options



Entry Configuration

Ingress Port: X2 × X4 ×

Port Config

Advanced Features

SSL Enable: Off

Deduplication Enable: Off

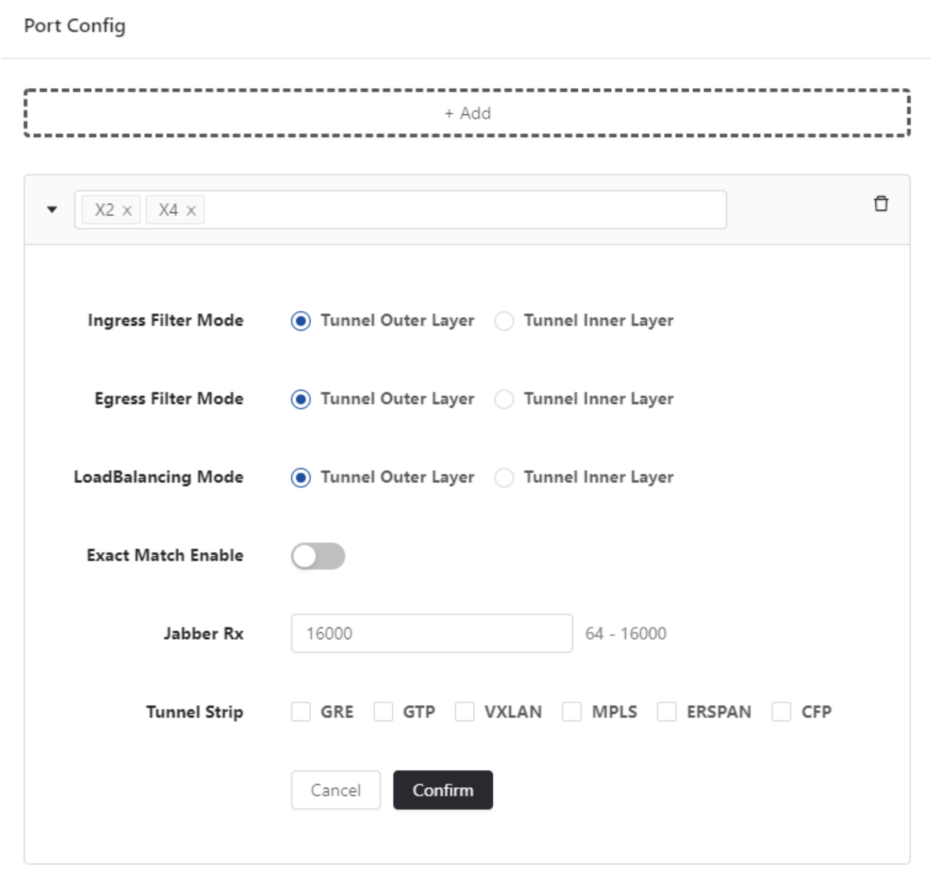
TCP Reassambly Inner: Off

Outer: Off

On the **Forwarding Policy > Policy** page, click an *Ingress Port Group* to open its configuration. Some *Ingress Port Group* features may not be available with the running firmware. The list of available features for each firmware is described in the following table. To change the Firmware, see the Update section.

SETTING	NORMAL FIRMWARE	SSL FIRMWARE	NORMAL + SSL FIRMWARE	DESCRIPTION
NetFlow	✔	✘	✔	Enable NetFlow generation
SSL Enable	✘	✔	✔	Enable SSL decryption on the traffic
Deduplication	✔	✔	✔	Enable packet deduplication
IP Reassembly	✔	✘	✔	Enable IP fragment reassembly
TCP Reassembly	✔	✔	✔	Enable TCP packet reordering
Tuple Mode	✔	✘	✔	Define the tuple mode (Outer, Sub-Outer, Inner)
Match Mode	✔	✘	✔	Define the filtering mode (First match: only the first match is executed, Full match: all filters are ANDed)
Priority	✔	✘	✔	When filtering mode = First match, define the filter priority
Regex Rule Priority	✔	✘	✔	When filtering mode = First match, define the regex priority

4.6.2 Ingress Port Options



Port Config

+ Add

X2 × X4 ×

Ingress Filter Mode ● Tunnel Outer Layer ○ Tunnel Inner Layer

Egress Filter Mode ● Tunnel Outer Layer ○ Tunnel Inner Layer

LoadBalancing Mode ● Tunnel Outer Layer ○ Tunnel Inner Layer

Exact Match Enable

Jabber Rx 16000 64 - 16000

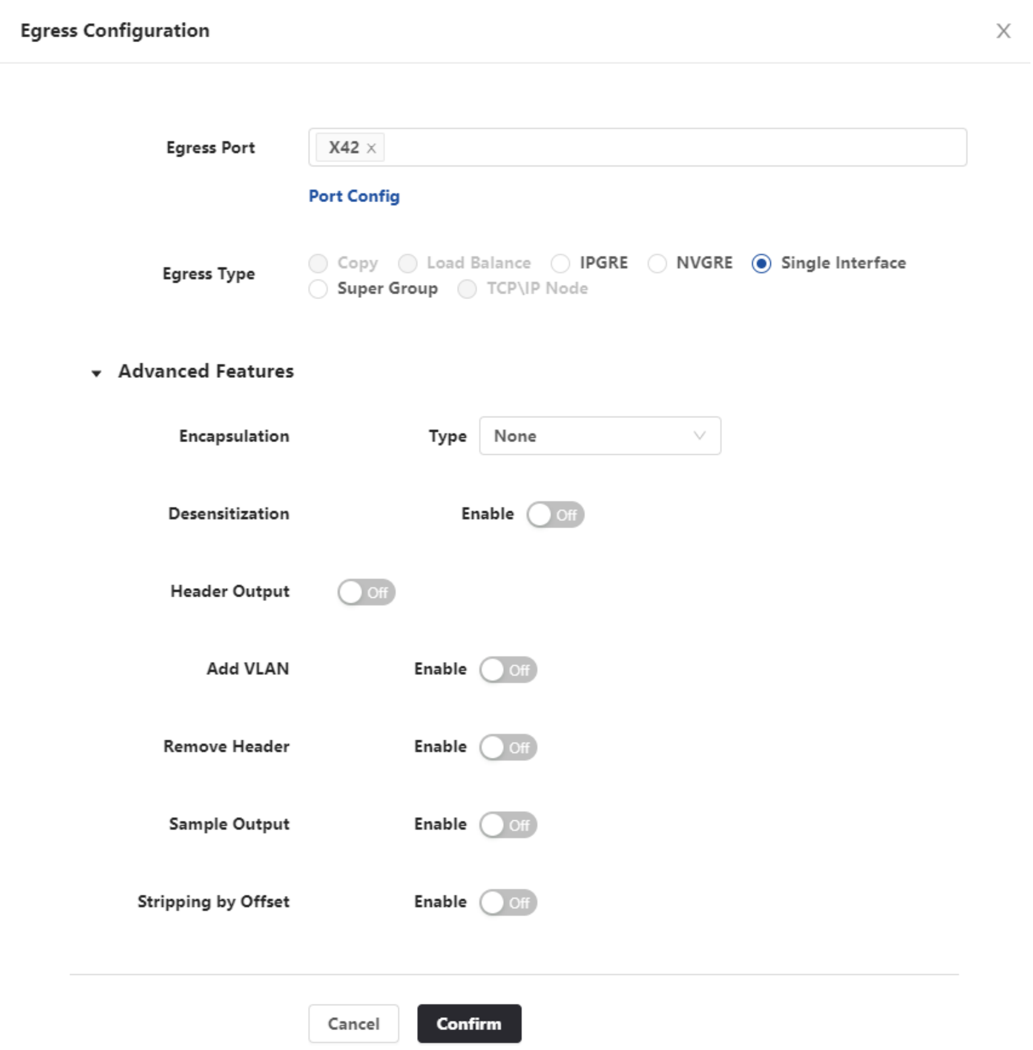
Tunnel Strip □ GRE □ GTP □ VXLAN □ MPLS □ ERSPAN □ CFP

Cancel Confirm

On the **Forwarding Policy > Policy** page, click an *Ingress Port Group* to open its configuration, then click *Port Config* to open the additional port configuration options. In this section, ports can be organized into subgroups, and the following settings can be configured for each subgroup:

SETTING	OPTION	DESCRIPTION
Ingress Filter Mode	Tunnel Outer Layer	Enable Ingress Filters on the outer layer
	Tunnel Inner Layer	Enable Ingress Filters on the inner layer
Egress Filter Mode	Tunnel Outer Layer	Enable Egress Filters on the outer layer
	Tunnel Inner Layer	Enable Egress Filters on the inner layer
Load Balancing Mode	Tunnel Outer Layer	Calculate Load Balancing hash on the outer layer
	Tunnel Inner Layer	Calculate Load Balancing hash on the inner layer
Exact Match Enable	Enable/Disable	Enable accurate matching rules on this port
Jabber Rx	64 - 16000	Define the max ingress packet length in Byte
Tunnel Strip	GRE|GTP|VXLAN|MPLS|ERSPAN|CFP	Enable tunnel stripping on this port or port group

4.6.3 Egress Port Group Options



Egress Configuration

Egress Port: X42

Port Config

Egress Type: ○ Copy ○ Load Balance ○ IPGRE ○ NVGRE ● Single Interface ○ Super Group ○ TCP\IP Node

Advanced Features

Encapsulation — Type: None

Desensitization — Enable: Off

Header Output: Off

Add VLAN — Enable: Off

Remove Header — Enable: Off

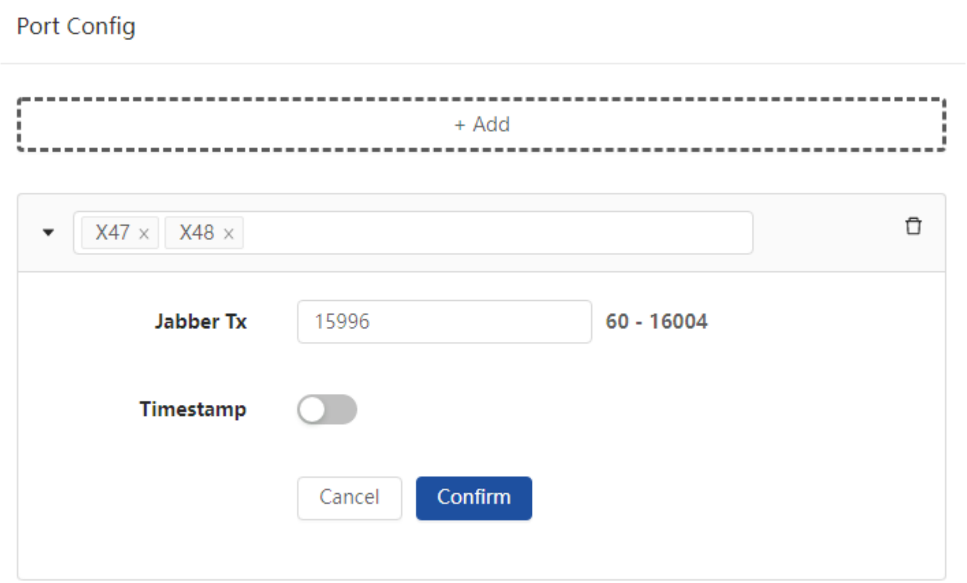
Sample Output — Enable: Off

Stripping by Offset — Enable: Off

On the **Forwarding Policy > Policy** page, click an *Egress Port Group* to open its configuration. The *Egress Port Group* type can be defined. This option defines the way traffic will egress the ports that are part of the port group. The egress type can be defined to output traffic to a single interface, multiple interfaces in replication or load balancing, replication to multiple load balancing groups, and the encapsulation method.

EGRESS TYPE	DESCRIPTION	ADDITIONAL OPTIONS
Copy	Replicate traffic to multiple interfaces	Encapsulation (ERSPAN / VXLAN) Desensitization Header out Add VLAN Remove Header (VLAN | VXLAN) Sample Output Stripping by Offset
Load Balance	Load Balance the traffic to multiple interfaces	
Single Interface	Send traffic to a single interface	
Super Group	Send traffic to multiple Load Balance groups	
IPGRE	Create an IPGRE tunnel to encapsulate the traffic	Source IP, Destination IP, Source MAC, Destination MAC
NVGRE	Create an NVGRE tunnel to encapsulate the traffic	

4.6.4 Egress Port Options



Port Config

+ Add

X47 × X48 ×

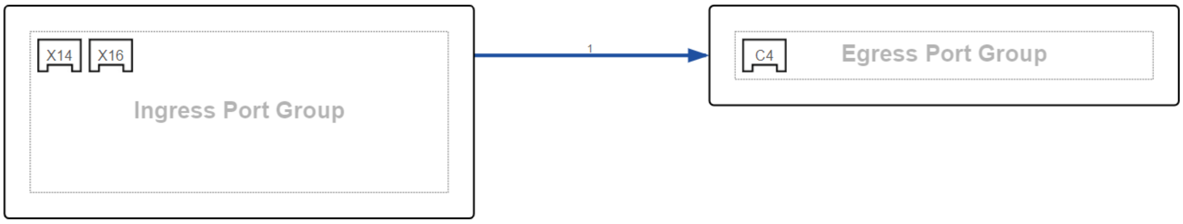
Jabber Tx 15996 60 - 16004

Timestamp

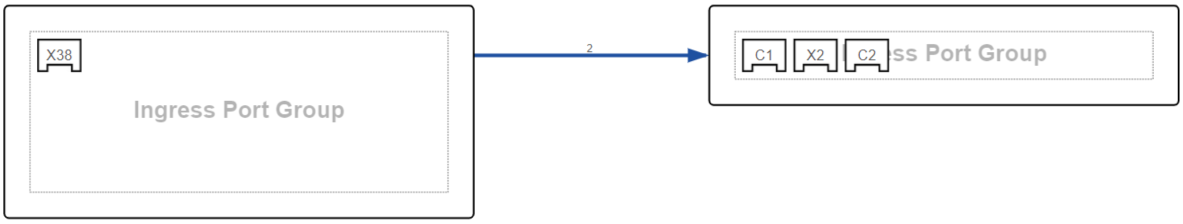
On the **Forwarding Policy > Policy** page, click an *Egress Port Group* to open its configuration, then click *Port Config* to open the additional port configuration options. In this section, ports can be organized into subgroups, and the following settings can be configured for each subgroup:

SETTING	OPTION	DESCRIPTION
Jabber Tx	60 – 16004	Define the max egress packet length in Byte
Timestamp	-	Add timestamp trailer to packets

4.6.5 Aggregation

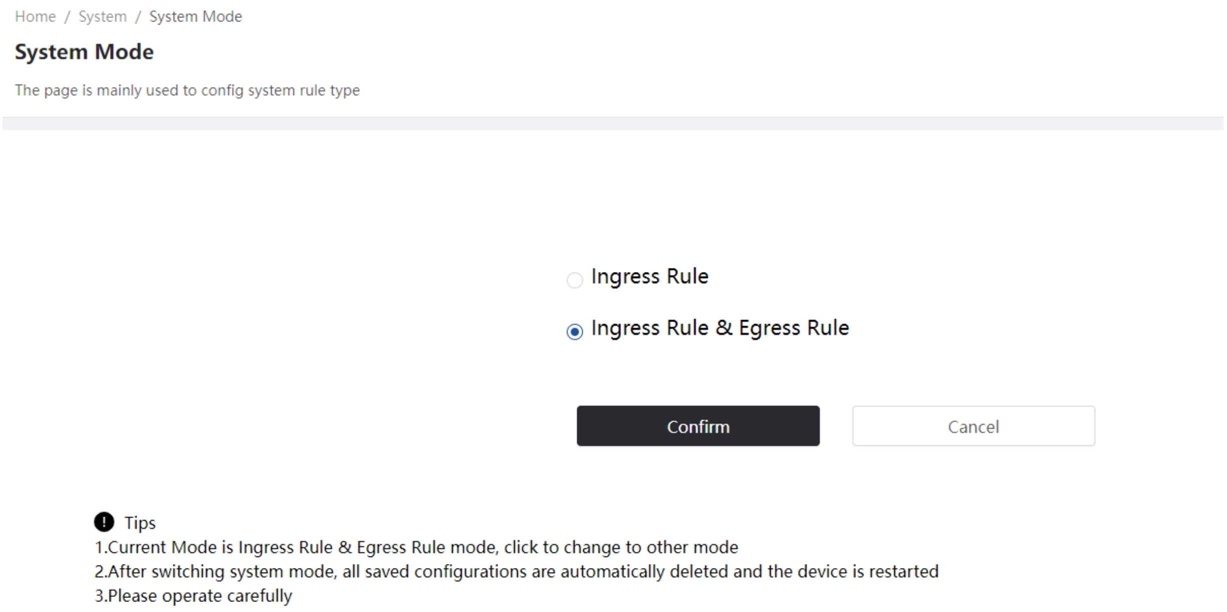


4.6.6 Replication



4.7 Filtering

4.7.1 Mode Configuration



System Mode

The page is mainly used to config system rule type

○ Ingress Rule

● Ingress Rule & Egress Rule

Tips

1.Current Mode is Ingress Rule & Egress Rule mode, click to change to other mode

2.After switching system mode, all saved configurations are automatically deleted and the device is restarted

3.Please operate carefully

The X3 system can be configured in two different rule modes:

- Ingress Rule
- Ingress Rule & Egress Rule

The configured mode has an impact on the number of configurable rules. The number of rules available for each mode is as follows:

- Ingress Rule mode: 3,000 ingress rules, no egress rules available
- Ingress Rule & Egress Rule: 2,000 ingress rules + 1,000 egress rules

4.7.2 Ingress Rule

Wildcard Match

Wildcard match rules is a flexible type of rule that can be used to match packets by several fields. One rule can contain key values for any of the listed fields.

FIELD	EXPECTED VALUE	EXAMPLE
Source IPv4/6	IP / Mask	10.10.10.0/255.255.255.0
Destination IPv4/6	IP / Mask	10.10.10.0/255.255.255.0
Source Port	Decimal	55397
Destination Port	Decimal	80
Outer VLAN	Decimal	10
Inner VLAN	Decimal	12
EtherType	0x0800, 0x86dd, VLAN (single, double, QinQ), VNTag, None	QinQ
Protocol	Protocol number or literal	tcp
DSCP	Decimal	46
VNI	Decimal	36
IP Fragment	Yes, No, None	No
TCP Flag	Decimal bitmap	3
MPLS #1	Decimal	1
MPLS #2	Decimal	2
MPLS #3	Decimal	3
Packet Size	=/< Decimal	< 127
Request Method	GET, POST, None	GET

One or many actions can be associated for each rule. Possible actions are:

- VLAN (add, delete outer/inner/both, modify outer/inner)
- Source MAC modifier
- Destination MAC modifier
- Slice Packet (to 128 Bytes)
- IPinIP termination
- Hit Counter

Exact Match

Exact match is another type of ingress rule. Packets are filtered according to exact match tuple rules.

FIELD	EXPECTED VALUE	EXAMPLE
Source IPv4/6	IP	10.10.10.1
Destination IPv4/6	IP	10.10.10.2
Protocol	Protocol number or literal	udp
Source Port	Decimal	55397
Destination Port	Decimal	80

One or more actions can be associated for each rule. Possible actions are:

- VLAN (add, delete double)
- Hit Counter

4.7.3 Egress Rule

Navigate to the **Forwarding Policy > Egress Filter List** page to set up egress rules.

Select a port group, then add one or more egress rules to target specific traffic. Targeted traffic can be either allowed to egress (*permit*), or dropped (*deny*).

4.7.4 Pre ACL Rule

Pre ACL rules send the targeted packets to the CPU for the processing of advanced features. See Features Overview for the list of features processed by the CPU.

To create a Pre ACL rule, navigate to the **Forwarding Policy > Policy** page, click the **arrow** connecting the *Ingress Port Group* to the *Egress Port Group*, select *Pre ACL*, add a Pre ACL rule, then confirm. If the created Pre ACL rule isn't configured to target specific traffic, all of the traffic will be sent to the CPU for processing.

4.8 Advanced Features

4.8.1 Packet Deduplication

The Packet Deduplication feature discards duplicated packets from a physical port, a port group, or across any port. As duplication may have various causes, X3 provides several options to configure the feature.

Packet fields used for deduplication:

- Layer 1: Ingress Port Group
- Layer 2: MAC addresses, EtherType, VLAN
- Layer 3: IP header
- Layer 4: TCP sequence number, TCP ACK

To set up deduplication, navigate to the **Forwarding Policy > Policy** page, click an *Ingress Port Group* to open its configuration, enable *Deduplication*, configure the options, then confirm.

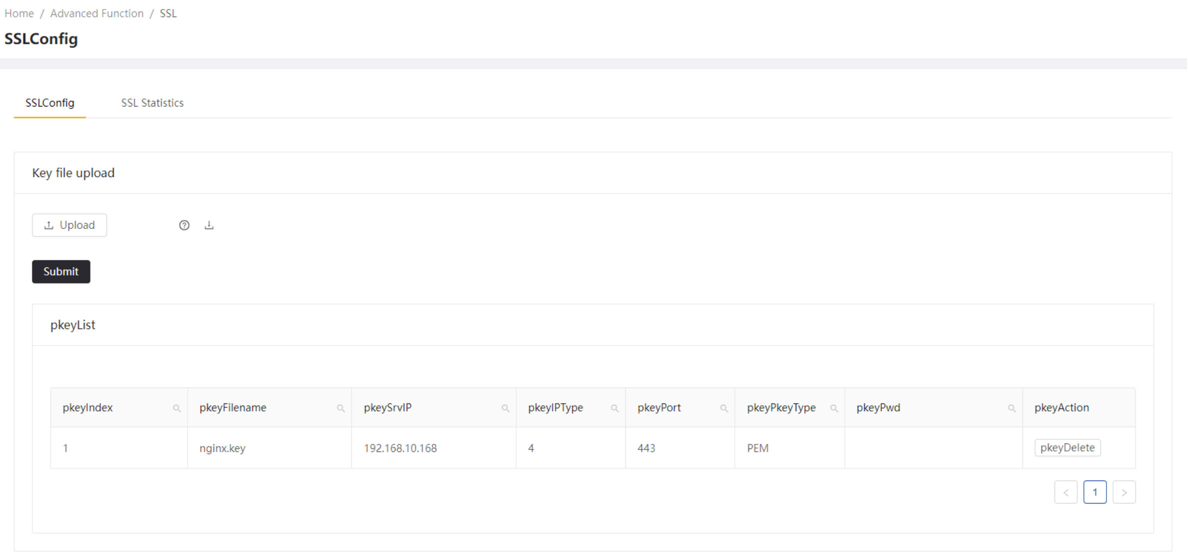
The Deduplication feature is achieved in CPU. Traffic must be routed to the CPU using a Pre ACL rule. To do so, click the **arrow** connecting the *Ingress Port Group* to the *Egress Port Group*, select *Pre ACL*, add a Pre ACL rule, then confirm.

Configurable Deduplication options:

Option	**Layer**	**Fields**
Ignore Port	1 (Port Group)	Ingress Port Group
Ignore MAC	2 (ETHERNET)	Source MAC Address Destination MAC Address
Ignore L2	2 (ETHERNET)	EtherType VLAN MPLS
Ignore DSCP	3 (IP)	DSCP
Ignore TTL	3 (IP)	TTL
Ignore IP-ID	3 (IP)	IPv4 Identification field
Ignore IP	3 (IP)	IP Header (except DSCP, IP-ID and TTL)
Ignore TCP	4 (TCP)	TCP sequence number TCP ACK Flag

Time interval
The deduplication time interval can be set per 100 ms (max. 1000 ms).

4.8.2 SSL Decryption



Home / Advanced Function / SSL

SSLConfig

SSLConfig | SSL Statistics

Key file upload

Upload

Submit

pkeyList

pkeyIndex	pkeyFilename	pkeySrvIP	pkeyIPType	pkeyPort	pkeyPkeyType	pkeyPwd	pkeyAction
1	nginx.key	192.168.10.168	4	443	PEM		pkeyDelete

To enable SSL Decryption, first upload a private key file (.key) and its associated configuration file (.json) on the **Advanced Function > SSL** page. Example files can be downloaded from this page. The files should be formatted as follows:

example.json	{"pkey_index":1,"srv_ip":"192.168.10.168","file_password":"","srv_port":443,"filename":"example.key","ip_type":4,"pkey_type":"PEM"}
example.key	-----BEGIN PRIVATE KEY----- MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQDv7pBDJgQJASPv VndDJnVhLQy3LjAnwK4/nqCx0WMhz+f2Sb/T3FQMdabf31jrEg2OFM31TBi5w+sd WIbGO4VwWPSCTGhKWWJiLOWN052cLXK8jV+9HP29JkrxJgasbN2Hhs6hue/j3pWZ ... L/4ggvQSWvefMhpslNwubzVDZpzapMnuRw5kxQClbyLTG3nWKPMe1FdjMaCuXF/V pn2FJVhtctnlhrxJHRlNLB1cd18NxPUepWDRuJhFpu2dHW4zqp/egsEzZglV47bY 1x68m081vyYjYTNhCm2w5t3aqWifaMEbHt5MwBXiN7THfs07WEva61goDP8XaZoW YKgrRnuj/WFwzciAPjBCmQYFv9V7vw== -----END PRIVATE KEY-----

Once this is done, navigate to the **Forwarding Policy > Policy** page, click an *Ingress Port Group* to open its configuration, activate *SSL Enable*, then confirm.

The SSL Decryption feature is achieved in CPU. Traffic must be routed to the CPU using a Pre ACL rule. To do so, click the **arrow** connecting the *Ingress Port Group* to the *Egress Port Group*, select *Pre ACL*, add a Pre ACL rule, then confirm.

4.8.3 Data Masking

Data Masking allows you to obfuscate specific data in egress.

To configure data masking, navigate to the **Forwarding Policy > Policy** page, click an *Egress Port Group* to open its configuration, and enable *Desensitization*. With *Desensitization* enabled, select the mode. Depending on the selected mode, the configuration options are defined below.

After configuring the *Desensitization* option, add a Pre ACL rule, and a Default Advanced Rule (*Advanced Rule > Default*).

Mode: Keyword

Range
The range in bits of the data that will be obfuscated, starting from the targeted data (regex).

Match Times
The number of times the regex can match data within each packet.

Regex
The regular expression for targeting data.

Mode
Set_Num: replaces all data bytes within the specified range with the specified value.

Value
The value that will replace the targeted data, specified as decimal ASCII value.

Mode: Customize

Offset Type
MAC_Hdr_Start: data obfuscation will start from the MAC header.
MAC_Data_Start: data obfuscation will start from the MAC payload.
IP_Hdr_Start: data obfuscation will start from the IP header.
IP_Data_Start: data obfuscation will start from the IP payload.
L4_Hdr_Start: data obfuscation will start from the L4 header.
L4_Data_Start: data obfuscation will start from the L4 payload.

Range
The range in bits of the data that will be obfuscated, starting from the selected offset type.

Mode
Set_Num: replaces all data bytes within the specified range(s) with the specified value.
Rc4_Key: encrypts all data bytes within the specified range(s) with RC4 algorithm.

Value (*Set_Num* mode selected)
The value that will replace the specified data.

RC4 Key (*Rc4_Key* mode selected)
The RC4 key with which to encrypt the specified data.

4.8.4 NetFlow

The X3 NetFlow feature enables generation and export of NetFlow statistics.

NetFlow can be enabled and configured on the **Advanced Function > NetFlow** page.

NetFlow Version: v5 / v9

SETTING	OPTION	DESCRIPTION
NetFlow Version	v5 / v9	Select the NetFlow version to use
IP Version	IPv4 / IPv6	Select the IP version for the NetFlow packets
Dst MAC1	MAC Address	Input the MAC address of the NetFlow collector
Dst IP1	IP Address	Input the IP address of the NetFlow collector
Dst Port	UDP Port	Input the destination port
Sample Mode	None / Fixed / Random / Stream	Select the sampling mode. The sampling mode is based on packets, except for stream option
Sample Rate Interval	0 - 16000	In fixed sampling, sample one of configured number of packets In random sampling: randomly take one of configured number of packets as a sample In stream sampling: take a stream of packets from configured number of packets as a sample
NetFlow Output	Enable / Disable	Enable the NetFlow statistic output
Output ports	Port	Assign the output port of NetFlow statistic messages

Once enabled and configured, NetFlow generation can be enabled for specific ingress port groups (see Ingress Port Group Options).

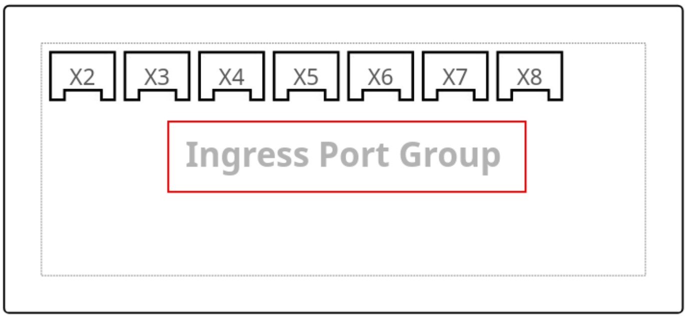
4.8.5 Tunnel Stripping

Strips tunnel headers at ingress. This functionality is performed at line rate in the data plane. The following tunneling protocols are supported: GRE, GTP, VXLAN, MPLS, ERSPAN, CFP. To enable tunnel stripping, see Ingress Port Options.

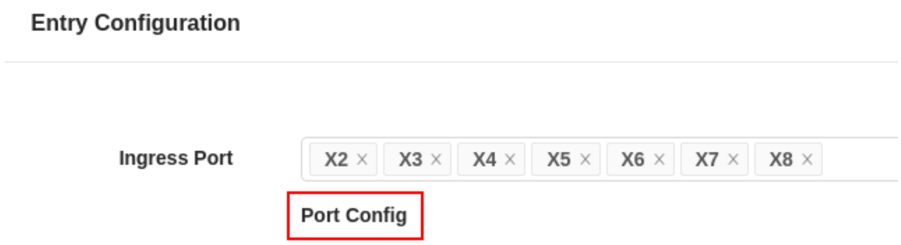
4.8.6 Tunnel Termination

In order to configure one or more input interfaces to perform tunnel termination, it is necessary to activate the tunnel stripping option on these interfaces, and to configure an IP address for ICMP response. This is possible using the following procedure:

1. In **Forwarding Policy > Policy**, click *Ingress Port Group* to open the ingress port group configuration menu.



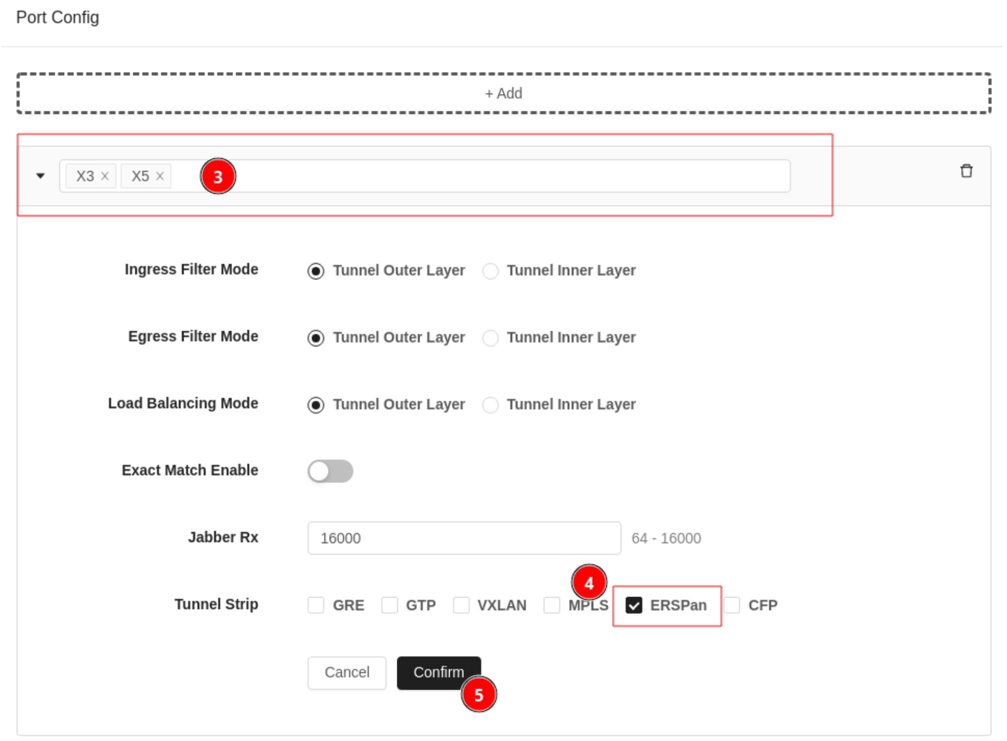
2. Click *Port Config* to open the port configuration menu.



Entry Configuration

Ingress Port: X2 × X3 × X4 × X5 × X6 × X7 × X8 ×

3. Remove all ports from the port list except for those for which you wish to activate tunnel stripping.
4. Select the type(s) of tunnel(s) to strip, for instance ERSPAN.
5. Click *Confirm*.



Port Config

X3 × X5 ×

Ingress Filter Mode: ● Tunnel Outer Layer ○ Tunnel Inner Layer

Egress Filter Mode: ● Tunnel Outer Layer ○ Tunnel Inner Layer

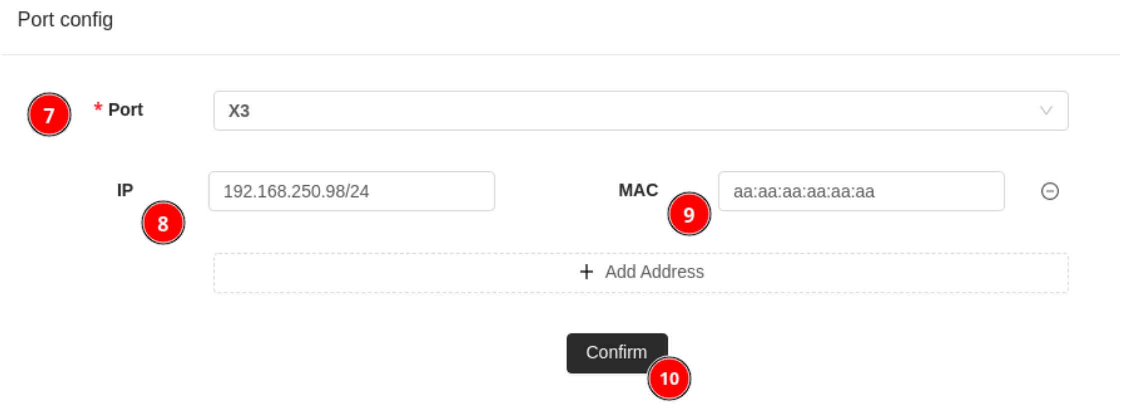
Load Balancing Mode: ● Tunnel Outer Layer ○ Tunnel Inner Layer

Exact Match Enable

Jabber Rx: 16000 64 - 16000

Tunnel Strip: □ GRE □ GTP □ VXLAN □ MPLS ☑ ERSPan □ CFP

6. Navigate to **Advanced Function > ICMP Response** and click *New config* to add a new configuration.
7. Select the port you wish to configure.
8. Set the IP address and CIDR mask.
9. Set the interface MAC address (this must be unique in your network).
10. Click *Confirm*.



Port config

* Port: X3

IP: 192.168.250.98/24

MAC: aa:aa:aa:aa:aa:aa

4.8.7 Tunnel Creation

To encapsulate the traffic in an IPGRE or NVGRE tunnel, navigate to the **Forwarding Policy > Policy** page, click an *Egress Port Group* to open its configuration, set *Egress Type* to *IPGRE* or *NVGRE*, and fill in the fields.

To encapsulate the traffic in a VXLAN or ERSPAN tunnel, navigate to the **Forwarding Policy > Policy** page, click an *Egress Port Group* to open its configuration, set *Egress Type* to *Single Interface*, set *Encapsulation Type* to *VXLAN* or *ERSPAN*, and fill in the fields.

4.8.8 Traffic Management

The **Advanced Function > Traffic Management** section allows the user to enable traffic shaping, which limits the amount of traffic sent out from the interfaces. Click *Add Group* to select the ports on which to enable shaping, and set the maximum speed in Mbps.

The *Statistics* page will display the amount of packets which are sent from the interfaces.

Note: The traffic shaping feature requires the presence of a Pre ACL rule, and will use part of the bandwidth available for other advanced features.

Legal

Disclaimer

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

Copyright

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Trademarks

The trademarks mentioned in this manual are the sole property of their owners.

Profitap HQ B.V.
High Tech Campus 84
5656AG Eindhoven
The Netherlands
sales@profitap.com
www.profitap.com