Navijin

CONFIGURATION MANUAL

NAVIJIN SNMP MANAGED SWITCHES

SNMP Managed Switch CLI Manual

Configure Navijin SNMP managed switches from the command line: access and users, VLANs, IP management, MAC table, ports, PoE, link aggregation, time, mirroring, spanning tree and ERPS ring protection, with worked examples.

CLI basics | Users | VLANs | IP | Ports & PoE | LACP | NTP | Mirroring | STP/MSTP | ERPS

Applies to
Navijin SNMP managed (L2+) switches, 8 to 28 ports, PoE and non-PoE models

Document
NJ-CM-SW-001 · Rev. 2.0

Published
November 2026

ABOUT THIS GUIDE

About this manual

Navijin SNMP managed switches serve access and aggregation roles in offices, hotels, campuses, CCTV systems and carrier access networks. They can be managed through the web interface, SNMP or the command-line interface (CLI). This manual covers the CLI: every chapter explains the feature, lists the commands step by step and ends with a complete, tested example. Commands are shown in `code`; replace the values in italics or angle brackets with your own. Save your work with `copy running-config startup-config`, otherwise changes are lost at the next restart.

Conventions: menu paths are shown in **bold** (for example **Network** → **VLAN**); commands and values in `monospace`. Screenshots may differ slightly by firmware version.

Who this guide is for

- Network engineers and integrators deploying Navijin switches
- Carrier and ISP engineers building access and ring networks
- IT administrators who prefer scripting and the CLI

What you need

- A Navijin SNMP managed switch
- A console cable (RJ45 or DB9 to USB) and a terminal program such as PuTTY or Tera Term, or SSH access
- Your network plan: VLANs, IP addresses, uplinks and ring topology

Factory defaults

Setting	Default
Management IP	`192.168.1.1` / 255.255.255.0
User name / password	`admin` / `admin` (change it at first login)
Console	115200 bit/s, 8 data bits, no parity, 1 stop bit, no flow control
VLAN	All ports in VLAN 1
Port link type	Trunk
PoE	On for all PoE ports; PoE watchdog off
Storm control	Off
Time zone	UTC

Contents

01 Product overview and typical designs

02 Connect to the switch

03	CLI basics
04	System commands
05	Users and privilege levels
06	VLANs
07	Management IP address
08	MAC address table
09	Ports
10	Power over Ethernet
11	Link aggregation (LACP)
12	Time and NTP
13	Port mirroring
14	Spanning tree (STP, RSTP, MSTP)
15	ERPS ring protection (G.8032)
16	Configuration examples
17	Troubleshooting

SECTION 01

Product overview and typical designs

Navijin SNMP managed switches combine full Layer 2 features with ring protection, PoE and SNMP management, in compact and rack-mount models.



Figure 1. Navijin SNMP managed switch family.

Design	How the switch is used
Enterprise access	Access ports for PCs, phones, cameras and access points, with VLANs per service and a LACP uplink to the core
Metro / ISP access (MAN)	Switches in a G.8032 ERPS ring between buildings; each customer or service in its own VLAN
Education campus	Separate VLANs for staff, students, labs and Wi-Fi; storm control and rate limits on student ports
Multi-service carrier VLAN	Hybrid ports deliver data, voice and IPTV VLANs to the same subscriber line
CCTV and PoE	PoE ports power cameras and access points; PoE watchdog restarts devices that stop responding

TIP

Design VLANs, IP plan and uplinks on paper first. Ring and spanning-tree mistakes are much easier to fix before cables are connected.

SECTION 02

Connect to the switch

Use the console port for the first configuration. After the switch has a management address, use SSH, the web interface or SNMP.

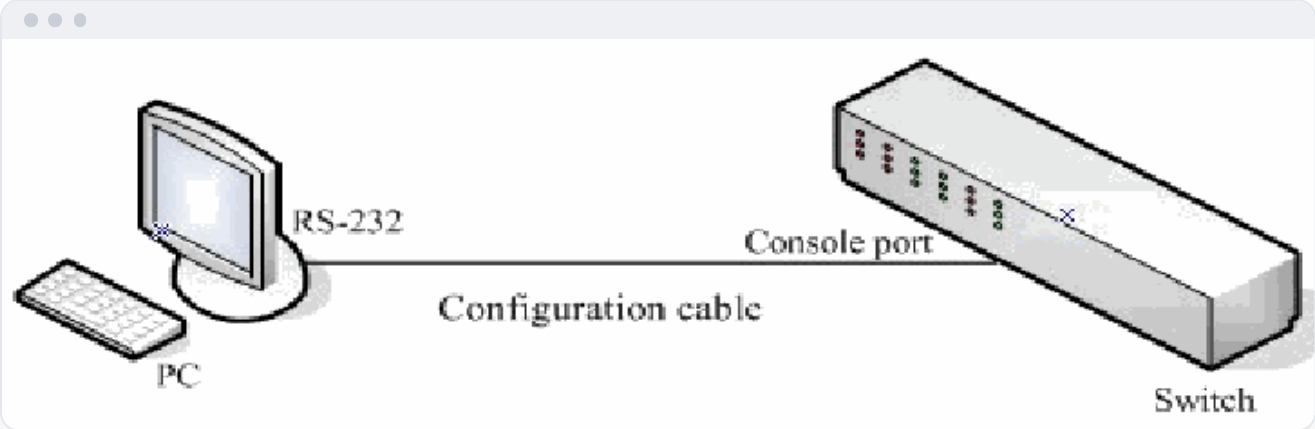


Figure 2. Console connection between a computer and the switch console port.

1 Connect the console cable

Connect the console port of the switch to your computer with the console cable (use a USB-to-serial adapter if the computer has no serial port).

2 Open a terminal

Start PuTTY, Tera Term or `screen`, select the serial port and set **115200 bit/s, 8 data bits, no parity, 1 stop bit, no flow control**.

3 Power on

Turn on the switch. After the power-on self-test, press **Enter** when you see `Press RETURN to get started`.

4 Sign in

Sign in with `admin` / `admin`, then change the password (see **Users and privilege levels**).

Access method	Use for
Console	First setup and recovery; works without IP
SSH	Secure remote CLI; preferred for daily work
Telnet	Legacy only; sends passwords in clear text
Web interface	Graphical configuration and monitoring
SNMP / NMS	Monitoring and bulk management from a network management system

IMPORTANT

Use SSH instead of Telnet on production networks, and limit management access to a dedicated management VLAN.

SECTION 03

CLI basics

The CLI is organised in modes. The prompt shows where you are.

Mode	Prompt	How to enter	Use
Privileged EXEC	`Switch#`	After login	All show commands, save, reboot
Global configuration	`Switch(config)#`	`configure`	Settings for the whole switch
Interface configuration	`Switch(config-if)#`	`interface gigabitethernet 3`	Settings for one port
Interface range	`Switch(config-if-range)#`	`interface range gigabitethernet 1-6`	Same settings on many ports
VLAN configuration	`Switch(config-vlan)#`	`vlan 10`	VLAN settings

- Type `?` to list the commands available in the current mode, or after a command to list its options: `show ?`.
- Abbreviate commands to any unique prefix: `sho int` = `show interface`.
- Most commands have a `no` form that disables or undoes them: `no shutdown`, `no description`.
- `exit` goes back one level; repeat it to return to `Switch#`.
- Select ports with `interface gigabitethernet 6` or ranges such as `interface range gigabitethernet 1-5,7`.

Convention	Meaning
`[ ]`	Optional element
`{ a | b }`	Choose one of the alternatives
italic / `<value>`	A value you provide

SECTION 04

System commands

Save, restart, restore and inspect the switch.

Command	Purpose

`copy running-config startup-config`	Save the current configuration so it survives a restart
`reboot`	Restart the switch
`restore-defaults`	Restore factory settings (asks for confirmation and restarts)
`restore-defaults interfaces GigabitEthernet 1-28`	Restore the default settings of ports only
`show info`	System name, IP, MAC address and uptime
`show cpu utilization`	CPU load
`show memory statistics`	Memory use
`show running-config`	The complete active configuration
`show running-config interfaces GigabitEthernet 1-28`	Configuration of selected ports

```
Switch# copy running-config startup-config
Success
Switch# restore-defaults
System: restore factory defaults. Do you want to reboot now? (y/n) y
```

IMPORTANT

`restore-defaults` erases the whole configuration, including the management IP and users. Run it from the console, not over the network.

TIP

Before any major change, copy the output of `show running-config` into your site documentation. It is the quickest way to roll back.

SECTION 05

Users and privilege levels

Create personal accounts with the right privilege level, and replace the default password.

Privilege level	CLI	Web interface
15 (admin)	View and configure	View and configure all functions
2–14	View only	View and configure all functions
0–1 (user)	View only	View a limited set of functions

Command	Purpose
`username <name> password <password>`	Create a user with a password
`username <name> privilege {<0-15> | admin | user}`	Set the privilege level
`username <name> secret <password>`	Store the password encrypted in the configuration
`username <name> nopassword`	Create a user without password (not recommended)
`no username <name>`	Delete a user
`show username`	List users

```
Switch# configure
Switch(config)# username netadmin privilege 15 secret Str0ng-Passw0rd!
Switch(config)# username noc privilege 1 secret View-Only-2026
Switch(config)# exit
Switch# show username
Switch# copy running-config startup-config
```

IMPORTANT

Change the password of `admin` or create your own level-15 account and disable the default one. Always use `secret` so passwords are not readable in configuration backups.

SECTION 06

VLANs

VLANs split one switch into separate networks: staff, guests, voice, CCTV and management each get their own broadcast domain.

Without VLANs, every broadcast reaches every port, and any device can see the traffic and services of all others. VLANs confine broadcasts, isolate user groups at Layer 2 and let you group users by role instead of by location. Traffic between VLANs needs a router or Layer 3 switch.

Port mode	Carries	Typical use
Access	One VLAN, untagged	PCs, printers, cameras
Trunk	Many VLANs, tagged, plus one untagged native VLAN	Uplinks to switches, routers and access points
Hybrid	Many VLANs, each tagged or untagged as you choose	Carrier lines with data, voice and IPTV; special devices

1 Access port

Create the VLAN, set the port to access mode and assign it.

```
Switch# configure
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# exit
Switch# copy running-config startup-config
```

2 Trunk port

Set the port to trunk mode, define the native (untagged) VLAN and add the allowed VLANs.

```
Switch(config)# vlan 4
Switch(config-vlan)# exit
Switch(config)# interface gi 4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 4
Switch(config-if)# switchport trunk allowed vlan add 1
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# switchport trunk allowed vlan add 3
Switch(config-if)# switchport trunk allowed vlan remove 1
```

3 Hybrid port

Set the port to hybrid, choose the PVID (VLAN for untagged incoming traffic) and add VLANs as tagged or untagged.

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 3
Switch(config-if)# switchport hybrid allowed vlan add 1 tag
Switch(config-if)# switchport hybrid allowed vlan add 2 untag
Switch(config-if)# switchport hybrid allowed vlan remove 2
```

Verify	Shows
`show vlan`	All VLANs and member ports
`show vlan <id>`	One VLAN
`show interfaces switchport GigabitEthernet <n>`	Mode, PVID and allowed VLANs of a port

NOTE

A frame whose VLAN equals the native VLAN of the outgoing trunk port leaves untagged; all other VLANs leave tagged. The native VLAN must match on both ends of a trunk.

TIP

Keep VLAN 1 for nothing but defaults, put management in its own VLAN (for example 100) and allow only the VLANs each trunk really needs.

SECTION 07

Management IP address

The switch is managed through an IP address on its management interface.

Command	Purpose
`ip address <ip> mask <mask>`	Set a static address
`ip address <ip> mask <mask> secondary`	Add a second address
`ip default-gateway <ip>`	Set the default gateway
`no ip default-gateway`	Remove the gateway
`ip dhcp`	Get the address from a DHCP server
`show ip` / `show ip dhcp`	Verify

```
Switch# configure
Switch(config)# ip address 192.168.1.2 mask 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.253
Switch(config)# exit
Switch# show ip
IP Address: 192.168.1.2
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.253
```

IMPORTANT

Changing the address over SSH or Telnet disconnects your session. Reconnect at the new address, then save.

TIP

Use static addresses (or DHCP reservations) for switches. Monitoring and backups depend on a stable management address.

SECTION 08

MAC address table

The switch learns which device is behind which port. You can also add static and blocking entries.

Entry type	Behaviour
Dynamic	Learned automatically; removed after the aging time without traffic
Static	Added by you; never ages; pins a device to a port
Blackhole (drop)	Added by you; all frames from or to this MAC are dropped

```
Switch(config)# mac-address-table static 00:00:00:00:00:dd vlan 1 interface gi 1
Switch(config)# mac-address-table static 22:22:22:33:33:33 vlan 1 drop
Switch(config)# mac-address-table aging-time 300
Switch(config)# exit
Switch# show mac address-table
Switch# show mac address-table static
Switch# show mac address-table aging-time
```

Show command	Displays
`show mac address-table`	All entries
`show mac address-table <mac>`	Where one device is connected
`show mac address-table interface GigabitEthernet <n>`	Devices on one port
`show mac address-table vlan <id>`	Devices in one VLAN
`show mac address-table counters`	Number of entries

TIP

To find where a device is plugged in, look up its MAC address with `show mac address-table <mac>` on each switch, following the port until it is not an uplink.

NOTE

An aging time that is too short floods traffic unnecessarily; one that is too long fills the table with stale entries. A few minutes suits most networks.

SECTION 09

Ports

Speed and duplex, flow control, descriptions, storm control, rate limits and cable testing.

Command (interface mode)	Purpose
`speed {10 | 100 | 1000 | auto}`	Force or auto-negotiate speed
`duplex {auto | full | half}`	Force or auto-negotiate duplex
`flowcontrol on` / `no flowcontrol`	Enable or disable 802.3x flow control
`description <text>`	Label the port, e.g. room3 or AP-LOBBY
`shutdown` / `no shutdown`	Disable or enable the port

```
Switch(config)# interface gi 3
Switch(config-if)# description AP-LOBBY-01
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# exit
Switch# show interface gi 1-28 status
Switch# show port-description
```

1 Storm control

Limits broadcast, unknown multicast and unknown unicast floods per port. It is off by default. Choose the unit (`storm-control unit {bps | pps}`) globally, then enable it per port.

```
Switch(config)# interface gigabitethernet 1
Switch(config-if)# storm-control broadcast
Switch(config-if)# storm-control broadcast level 100
Switch(config-if)# storm-control unknown-multicast
Switch(config-if)# storm-control unknown-multicast level 100
Switch(config-if)# storm-control unknown-unicast
Switch(config-if)# storm-control unknown-unicast level 100
Switch(config-if)# exit
Switch(config)# exit
Switch# show storm-control
```

2 Rate limiting

Limit the bandwidth of a port in each direction, from QoS mode.

```
Switch(config)# qos
Switch(config)# interface gigabitethernet 1
Switch(config-if)# rate-limit ingress 1000
Switch(config-if)# rate-limit egress 5000
Switch(config-if)# exit
Switch(config)# exit
Switch# show running-config interfaces GigabitEthernet 1
```

3 Cable test

`show cable-diag interfaces gi 1-24` tests copper cables and reports faults such as open or short pairs and their distance.

TIP

Enable storm control on all access ports. A looped cable or faulty device then cannot flood the whole network.

NOTE

Leave speed and duplex on auto unless the connected device requires fixed settings, and then set both ends the same. A duplex mismatch causes slow, error-prone links.

SECTION 10

Power over Ethernet

PoE models power cameras, phones and access points over the data cable.

The switch detects PoE devices (PDs) and powers only devices that comply with IEEE 802.3af or 802.3at. The **PoE watchdog** checks a powered port every 3 minutes: if the link is down or no traffic arrives, it switches the power off and on again. This restarts hung cameras and access points in hard-to-reach places automatically.

```
Switch(config)# interface gi 3
Switch(config-if)# no poe
Switch(config-if)# poe watchdog
Switch(config-if)# exit
Switch(config)# exit
Switch# show poe status
Switch# show poe interface GigabitEthernet 3
```

Command	Purpose
`poe` / `no poe`	Enable or disable power on a port (on by default)
`poe watchdog` / `no poe watchdog`	Enable or disable the watchdog (off by default)
`show poe status`	Power per port and total budget

TIP

Keep total PoE load below about 80% of the switch budget, so the switch can power everything at start-up and in cold weather when heaters in outdoor cameras switch on.

TIP

To reboot a frozen camera remotely, run `no poe` then `poe` on its port.

SECTION 11

Link aggregation (LACP)

Bundle several ports into one logical link for more bandwidth and redundancy.

Mode	Behaviour
`static`	Ports are bundled without negotiation; both ends must be configured identically
`active`	LACP; the port starts negotiation
`passive`	LACP; the port answers negotiation

```
Switch# configure
Switch(config)# lag load-balance src-dst-mac-ip
Switch(config)# interface gi 5
Switch(config-if)# lacp port-priority 1
Switch(config-if)# lacp timeout long
Switch(config-if)# lag 2 mode active
Switch(config-if)# exit
Switch(config)# interface gi 6
Switch(config-if)# lacp port-priority 1
Switch(config-if)# lacp timeout long
Switch(config-if)# lag 2 mode active
Switch(config-if)# exit
Switch(config)# exit
Switch# show lag
Switch# show lacp neighbor
```

Setting	Notes
`lag load-balance {src-dst-mac | src-dst-mac-ip}`	How traffic is spread over the member links
`lacp system-priority <1-65535>`	Lower value wins when switches decide which links are active
`lacp port-priority <value>`	Default 32768; lower values become active first
`lacp timeout {long | short}`	Short detects failures faster
Group numbers	1 to 8 aggregation groups

Verify	Shows
`show lag`	Groups and member ports
`show lacp counters`	LACP packets sent and received
`show lacp internal` / `show lacp neighbor`	Local and partner state

`show lacp sys-id`	System ID and priority

IMPORTANT

All member ports must have the same speed, duplex and VLAN settings. Configure the LAG on both switches before connecting the second cable, or you create a loop.

TIP

Prefer LACP (active) over static mode: LACP detects a miswired or failed member link and removes it automatically.

SECTION 12

Time and NTP

Accurate time makes logs, alarms and troubleshooting across devices consistent.

```
Switch# configure
Switch(config)# clock source sntp
Switch(config)# sntp host 192.168.1.100
Switch(config)# clock timezone CET +1
Switch(config)# clock summer-time CEST recurring eu
Switch(config)# exit
Switch# show sntp
Switch# show clock detail
```

Command	Purpose
`clock source {local | sntp}`	Use the internal clock or an NTP/SNTP server
`sntp host <ip> [port <port>]`	Time server
`clock timezone <name> <offset>`	Time zone from UTC−12 to UTC+13 (default UTC)
`clock summer-time <name> recurring {eu | usa | first | last}`	Recurring daylight saving rules
`clock summer-time <name> date <start> <end>`	Daylight saving between fixed dates
`clock set hh:mm:ss <day> <month> <year>`	Set the clock by hand

TIP

Point all switches, cameras, NVRs and gateways at the same NTP server. Navijin gateways can serve NTP to the LAN.

SECTION 13

Port mirroring

Copy traffic from one or more ports to a monitoring port for analysis with Wireshark or an IDS.

```
Switch# configure
Switch(config)# mirror session 1 destination interface gi 1 allow-ingress
Switch(config)# mirror session 1 source interfaces gi 2-3 both
Switch(config)# exit
Switch# show mirror
```

Option	Meaning
`source ... rx`	Mirror received traffic
`source ... tx`	Mirror transmitted traffic
`source ... both`	Mirror both directions
`destination ... allow-ingress`	The monitoring port can still send normal traffic
`no mirror session <id>`	Remove the session

NOTE

The destination port receives copies of all mirrored traffic. Mirroring several busy gigabit ports into one gigabit port drops packets.

SECTION 14

Spanning tree (STP, RSTP, MSTP)

Spanning tree blocks redundant paths so the network has no loops, and reopens them when a link fails.

Mode	Convergence	Use
STP (802.1D)	30–50 s	Compatibility with old switches only
RSTP (802.1w)	About 1–2 s	Recommended for most networks
MSTP (802.1s)	Fast, per instance	Several VLAN groups with different active paths

```
Switch# configure
Switch(config)# spanning-tree
Switch(config)# spanning-tree mode rstp
Switch(config)# exit
Switch# show spanning-tree
```

Tuning command	Purpose
`spanning-tree mst <instance> priority <value>`	Switch priority; the lowest becomes root
`spanning-tree mst <instance> port-priority <value>`	Port priority (interface mode)
`spanning-tree mst <instance> cost <value>`	Path cost (interface mode); default from link speed
`spanning-tree mst hello-time <s>`	BPDU interval
`spanning-tree mst forward-time <s>`	Forward delay
`spanning-tree maximum-age <s>`	Maximum age of BPDU information
`spanning-tree max-hops <n>`	Hops inside an MST region

TIP

Make the core switch the root bridge with the lowest priority, and the backup core the second lowest. Never let an access switch become root by accident.

NOTE

All switches in an MST region need the same region name, revision and VLAN-to-instance mapping, otherwise they act as separate regions.

SECTION 15

ERPS ring protection (G.8032)

ERPS protects ring networks with fast switchover (typically under 50 ms), faster and more predictable than spanning tree.

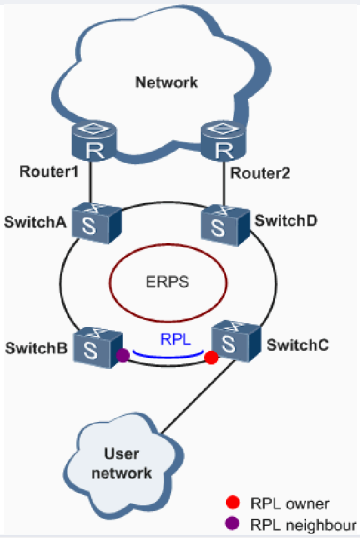


Figure 3. ERPS ring: one link (the RPL) is blocked in normal operation and opened when another link fails.

Term	Meaning
Ring	Switches connected in a closed loop, each with two ring ports
RPL (ring protection link)	The link kept blocked in normal state to prevent a loop
RPL owner	The switch port that blocks the RPL and opens it on failure
Control VLAN	VLAN that carries ERPS protocol messages (R-APS); not used for data

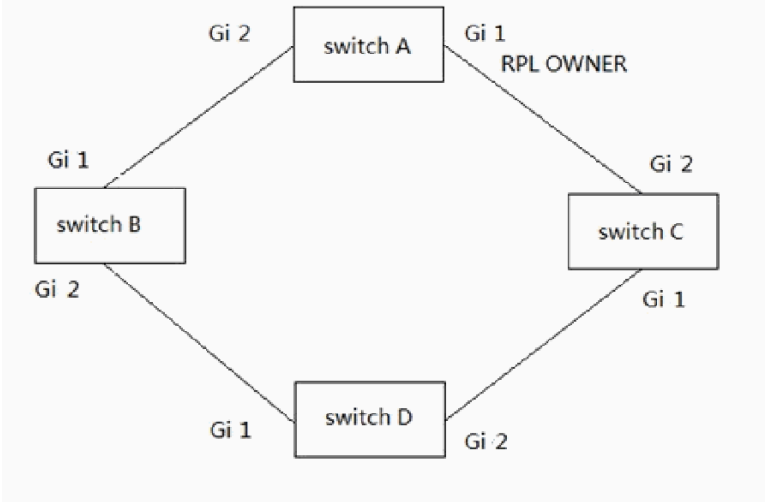


Figure 4. Example: four switches in a ring; switch A port Gi1 is the RPL owner.

1 On every switch

Create the control VLAN, set both ring ports to trunk and allow the control VLAN on them, then enable ERPS.

```
Switch# configure
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)# interface range GigabitEthernet 1,2
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk allowed vlan add 200
Switch(config-if-range)# exit
Switch(config)# erps
Switch(config)# erps control-vlan 200
```

2 On switch A (RPL owner)

Set Gi1 as the RPL owner and Gi2 as a normal ring port.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# erps rpl owner
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# erps ring
Switch(config-if)# exit
Switch(config)# exit
```

3 On switches B, C and D

Set both ring ports as normal ring ports.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# erps ring
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# erps ring
Switch(config-if)# exit
Switch(config)# exit
Switch# show erps
Switch# copy running-config startup-config
```

4 Test

Run a continuous ping across the ring, unplug one ring link and check that only a few packets are lost; plug it back and check that the RPL is blocked again with `show erps`.

IMPORTANT

Configure ERPS on all ring switches before closing the ring, and disable spanning tree on the ring ports. Only one RPL owner per ring.

TIP

Also allow the data VLANs on the ring trunks; ERPS protects every VLAN carried on the ring ports.

SECTION 16

Configuration examples

Two complete examples you can adapt.

Office access switch: ports 1–20 for staff PCs in VLAN 10, ports 21–22 for IP phones in VLAN 20, ports 23–24 for access points (trunk with VLANs 10, 20, 40), ports 25–26 as a LACP uplink to the core, management in VLAN 100.

```
configure
vlan 10
exit
vlan 20
exit
vlan 40
exit
vlan 100
exit
interface range GigabitEthernet 1-20
switchport mode access
switchport access vlan 10
storm-control broadcast
exit
interface range GigabitEthernet 21-22
switchport mode access
switchport access vlan 20
exit
interface range GigabitEthernet 23-24
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan add 10
switchport trunk allowed vlan add 20
switchport trunk allowed vlan add 40
exit
interface range GigabitEthernet 25-26
lag 1 mode active
exit
ip address 192.168.100.21 mask 255.255.255.0
ip default-gateway 192.168.100.1
clock source sntp
sntp host 192.168.100.1
exit
copy running-config startup-config
```

CCTV PoE switch: ports 1–24 for cameras in VLAN 30 with PoE watchdog, ports 25–26 uplink to the NVR network, storm control on all camera ports.

```
configure
vlan 30
exit
interface range GigabitEthernet 1-24
switchport mode access
switchport access vlan 30
poe watchdog
storm-control broadcast
storm-control unknown-multicast
exit
exit
copy running-config startup-config
```

SECTION 17

Troubleshooting

Answers to the most common questions.

The console shows nothing or unreadable characters.

Check the cable and COM port, and set 115200 bit/s, 8N1, no flow control. Press Enter a few times.

My changes are gone after a restart.

You did not save. Run `copy running-config startup-config` after every change.

I lost access after changing the IP or VLAN.

Connect through the console and correct the management IP, gateway or management VLAN.

Devices in the same VLAN cannot reach each other across switches.

Check that the VLAN is allowed on every trunk in the path (`show interfaces switchport`) and that native VLANs match.

The network slows down or stops; LEDs blink fast.

A loop. Enable RSTP or ERPS, enable storm control on access ports and find the looped cable with `show mac address-table` and port counters.

A LAG does not come up.

Check that both ends use the same mode (LACP active/passive or static), speed and VLANs, then `show lacp neighbor` .

A PoE device does not power up.

Check `show poe status` for the port and the total budget, make sure PoE is enabled on the port, and test the cable with `show cable-diag` .

I forgot the admin password.

Contact Navijin support with the serial number for the password recovery procedure.

Navijin

Need help?
We are here for you.

TECHNICAL SUPPORT
navijin.com/en/contact/technical

DOCUMENTATION & FIRMWARE
navijin.com/en/documentation

COMMUNITY TUTORIALS
navijin.com/en/tutorials

VERIFY YOUR PRODUCT
navijin.com/en/verification

NJ-CM-SW-001 · Rev. 2.0 · November 2026. Information in this document is subject to change without notice. Screenshots are for illustration and may differ by firmware version. Navijin® is a registered trademark in the United Arab Emirates. © 2026 Navijin. All rights reserved.