

Comutator Ethernet (Comutator gestionat)

Manual de utilizare



V1.0.0

Prefață

General

Acest manual prezintă operațiunile pe interfața web a comutatorului RTL (denumit în continuare „comutatorul”). Puteți accesa comutatorul dintr-un browser web, îl puteți configura și gestiona.

Instrucțiuni de siguranță

Următoarele cuvinte de semnalizare clasificate cu semnificație definită ar putea apărea în manual.

Cuvinte de semnalizare	Semnificație
 DANGER	Indică un pericol potențial ridicat care, dacă nu este evitat, va duce la deces sau vătămări grave.
 WARNING	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, poate duce la vătămări corporale ușoare sau moderate.
 CAUTION	Indică un risc potențial care, dacă nu este evitat, ar putea duce la daune materiale, pierderi de date, performanțe mai scăzute sau rezultate imprevizibile.
 TIPS	Oferă metode care te ajută să rezolvi o problemă sau să economisești timp.
 NOTE	Oferă informații suplimentare ca punct de accent și supliment la text.

Funcții utilizate frecvent

Pictogramă/Parametru	Descriere
	Editează un element.
 sau Șterge	Ștergeți elementele unul câte unul sau în loturi.
 sau 	Activați sau dezactivați elementele unul câte unul sau în loturi.
Reîmprospătare sau Reîmprospătare automată	Reîmprospătați sau reîmprospătați automat conținutul.

Istoricul reviziilor

Versiune	Conținutul revizuirii	Timp de eliberare
V1.0.0	Prima lansare.	August 2024

Despre Manual

- Manualul este doar pentru referință. Pot exista mici diferențe între manual și produs.
- Nu suntem răspunzători pentru pierderile suferite din cauza utilizării produsului în moduri care nu sunt conforme cu manualul.

- Manualul va fi actualizat în conformitate cu cele mai recente legi și reglementări ale jurisdicțiilor relevante. Pentru informații detaliate, consultați manualul de utilizare pe hârtie, utilizați CD-ROM-ul nostru, scanați codul QR sau vizitați site-ul nostru oficial. Manualul este doar pentru referință. Pot exista mici diferențe între versiunea electronică și versiunea pe hârtie.
- Toate proiectele și software-ul pot fi modificate fără notificare prealabilă scrisă. Actualizările produsului pot duce la apariția unor diferențe între produsul real și manual. Vă rugăm să contactați serviciul clienți pentru cel mai recent program și documentația suplimentară.
- Pot exista erori de tipar sau abateri în descrierea funcțiilor, operațiunilor și datelor tehnice. În caz de îndoială sau dispută, ne rezervăm dreptul de a oferi o explicație finală.
- Actualizați software-ul cititorului sau încercați un alt software de citire obișnuit dacă manualul (în format PDF) nu poate fi deschis.
- Toate mărcile comerciale, mărcile comerciale înregistrate și numele companiilor din manual sunt proprietatea deținătorilor respectivi.
- Vă rugăm să vizitați site-ul nostru web, să contactați furnizorul sau serviciul de asistență pentru clienți dacă apar probleme în timpul utilizării dispozitivului.
- În cazul în care există incertitudini sau controverse, ne rezervăm dreptul de a oferi o explicație finală.

Cuprins

Prefață.....	I
1 Autentificare	1
1.1 Inițializarea comutatorului.....	1
1.2 Conectare.....	2
2 Configurare rapidă.....	4
2.1 Configurarea informațiilor generale.....	4
2.2 Informații despre port.....	5
2.3 ONVIF	6
2.4 Vizualizarea IPC și NVR	7
3 Setări de rețea.....	8
3.1 Configurarea porturilor	8
3.2 Configurarea EEE.....	9
3.3 Configurarea VLAN-ului.....	10
3.3.1 Definiția VLAN-ului	10
3.3.2 Funcția VLAN.....	10
3.3.3 VLAN bazat pe porturi	10
3.3.4 Adăugarea VLAN-ului.....	11
3.3.5 Configurarea VLAN-ului portului.....	12
3.4 Configurarea VLANIF	13
3.5 Configurarea IP-ului și a rutării.....	14
3.6 Configurarea ERPS	15
3.6.1 Setări ERPS.....	16
3.6.2 Setări MEP	16
3.7 Configurarea supravegherii IGMP.....	17
3.8 Configurarea STP	18
3.8.1 STP	18
3.8.2 Instanța portului.....	19
3.9 Configurarea agregării linkurilor.....	20
3.10 Configurarea protocolului SNMP	22
3.10.1 Configurarea SNMP V1 și V2	22
3.10.2 Configurarea SNMP V3.....	23
3.11 Configurarea tabelului MAC	25
3.11.1 Adăugarea tabelului MAC	25
3.11.2 Adresa MAC a portului de filtrare.....	26

3.12 Configurarea LLDP	26
4 Management PoE	28
4.1 Configurarea setărilor PoE.....	28
4.2 Configurarea PoE perpetuu.....	29
4.3 Configurarea PoE pe distanțe lungi.....	29
4.4 Vizualizarea statisticilor evenimentelor PoE	30
4.5 Configurarea Green PoE	30
4.6 Configurarea Force PoE	31
4.7 Configurarea dispozitivului de supraveghere PoE.....	31
5 Securitate	33
5.1 Servicii de bază	33
5.1.1 Configurarea serviciilor de bază	33
5.1.2 Configurarea HTTPS	33
5.2 Configurarea Certificat CA	34
5.2.1 Instalarea certificatului dispozitivului.....	34
5.2.2 Instalarea certificatelor CA de încredere	35
5.3 Configurarea apărării împotriva atacurilor	36
5.3.1 Configurarea firewall-ului	36
5.3.2 Configurarea atacului Anti-DoS	38
5.4 Configurarea izolării porturilor	38
6 Politica de control	39
6.1 Configurarea priorității portului	39
6.2 Configurarea tabelului de mapare a priorităților	39
6.3 Configurarea programării cozii.....	40
6.4 Configurarea limitei de viteză a portului	41
6.5 Configurarea controlului furtunilor	41
7 Autentificare	43
7.1 Configurarea 802.1x	43
7.2 Configurarea razei.....	43

1 Autentificare

1.1 Inițializarea comutatorului

Cerințe preliminare

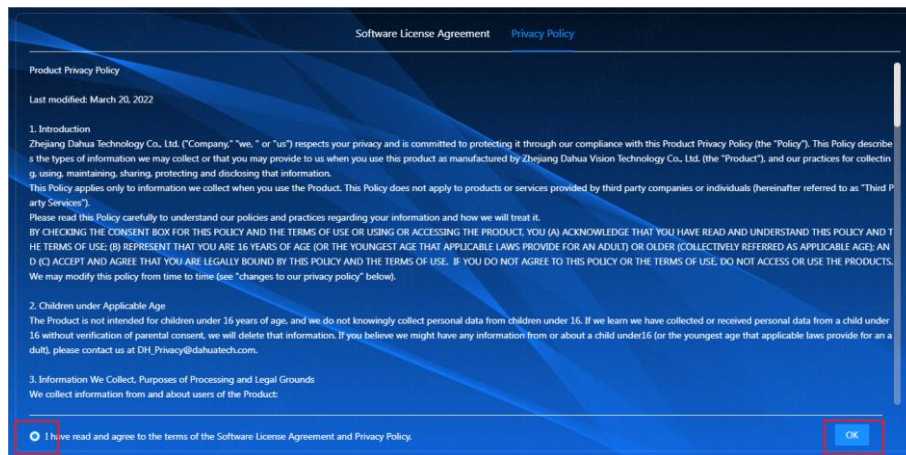
Înainte de autentificare, asigurați-vă că switch-ul și dispozitivul de configurare sunt conectate și pornite.

Procedură

Pasul 1 Deschideți browserul IE, introduceți adresa IP (192.168.1.110 în mod implicit) a switch-ului în bara de adrese a browserului web, apoi apăsați tasta Enter.

Pasul 2 Citiți Acordul de licență software și Politica de confidențialitate, faceți clic pe Am citit și sunt de acord cu termenii Acordului de licență software și ai Politicii de confidențialitate, apoi faceți clic pe OK.

Figura 1-1 Politica de citire

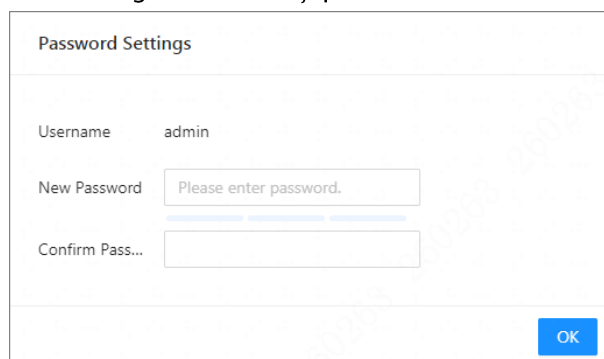


Pasul 3 Setări parola.



Numele de utilizator este admin.

Figura 1-2 Setări parola



Pasul 4. Faceți clic pe OK.

1.2 Conectare

Cerințe preliminare

Înainte de autentificare, asigurați-vă că:

- Ați configurat deja adresa IP a switch-ului. Adresa IP a VLAN 1 este 192.168.1.110 în mod implicit.
- Calculatorul este conectat la rețea și poate da ping switch-ului.

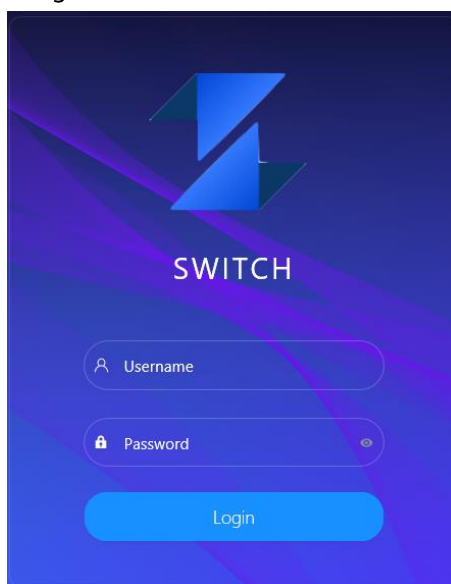
Procedură

Pasul 1 Introduceți adresa IP (192.168.1.110 în mod implicit) a switch-ului în bara de adrese a browserului web, apoi apăsați tasta Enter.

Pasul 2 Introduceți numele de utilizator și parola.

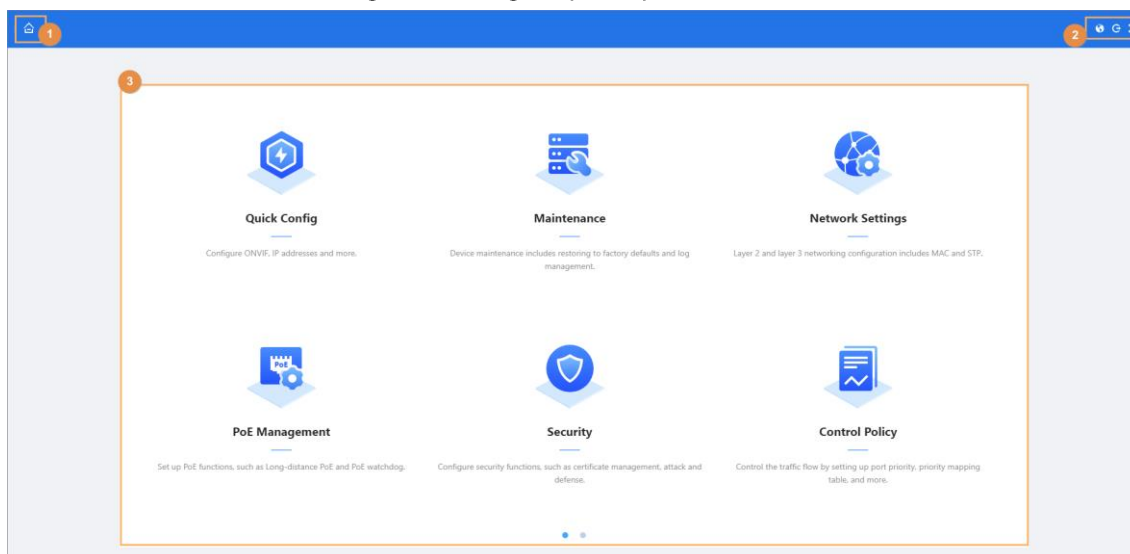
Pasul 3. Faceți clic pe Autentificare.

Figura 1-3 Autentificare



- Schimbați parola după prima conectare. Parola trebuie să fie formată din 8 până la 32 de caractere, toate acestea fiind spații libere, și să conțină cel puțin două tipuri de caractere: majuscule, minuscule, cifre și caractere speciale (cu excepția ' " ; : &).

Figura 1-4 Pagina principală



Tabelul 1-1 Descrierea paginii principale

Nu.	Nume	Descriere
1		Reveniți la pagina principală.
2		Schimbați limbile sistemului. Acceptă mai multe limbi.
		Deconectați utilizatorul, apoi reveniți la pagina de conectare.
		Pagina web se afișează pe tot ecranul.
3	Afișaj de stare	Vizualizare live a stării actuale a comutatorului.
	Configurare rapidă	Configurați setări rapide, inclusiv ONVIF, adresa IP și multe altele.
	Întreținere	Configurați setările de întreținere, inclusiv restaurarea la setările implicite din fabrică și gestionarea jurnalelor.
	Setări de rețea	Configurați setările de rețea, inclusiv setările MAC și STP.
	Management PoE	Configurați setările PoE, inclusiv PoE la distanță lungă și watchdog-ul PoE.
	Securitate	Configurați setările de securitate, inclusiv gestionarea certificatelor, atacul și apărarea.
	Politica de control	Configurați setările fluxului de trafic, inclusiv setarea priorității porturilor, tabelul de mapare a priorităților și multe altele.
	Autentificare	Configurați gestionarea autentificării, inclusiv 802.1x și RADIUS.

2 Configurare rapidă

Puteți vizualiza informațiile despre sistem și configura parametrii comutatorului, inclusiv ONVIF, adresa IP și multe altele. Paginile din manual sunt doar pentru referință și pot diferi de paginile reale.

2.1 Configurarea informațiilor generale

Puteți vizualiza și configura informațiile generale, inclusiv numele, adresa IP, masca de subrețea și gateway-ul implicit.

Procedură

Pasul 1 Selectați Configurare rapidă > General.

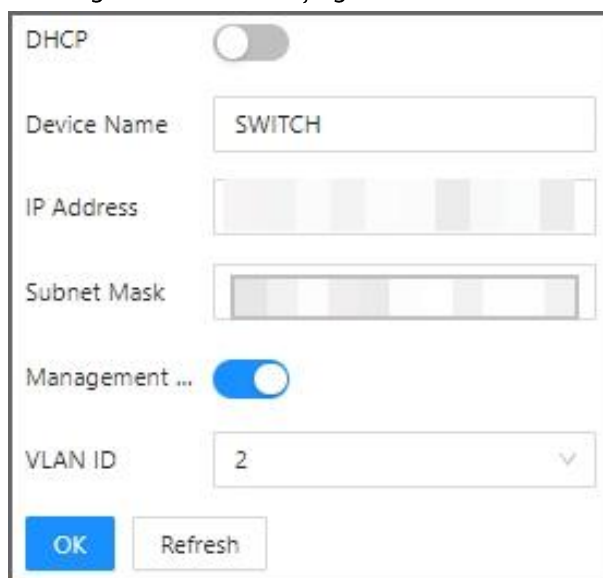
Pasul 2 Puteți vizualiza și configura informațiile generale ale comutatorului.

Pasul 3 (Optional) Faceți clic pentru a activa funcția DHCP. 



Vă rugăm să rețineți această funcție. Odată ce DHCP este activat, routerul sau serverul DHCP conectat la switch va atribui automat o adresă IP switch-ului. Adresa IP originală nu va putea accesa pagina web.

Figura 2-1 Informații generale



Tabelul 2-1 Descrierea informațiilor generale

Parametru	Descriere
DHCP	Acceptă activarea DHCP. După activarea DHCP, noua adresă IP va fi achiziționată și atribuită automat. Înainte de atribuirea noii adrese IP, se adoptă adresa IP implicită 192.168.1.110.
Nume dispozitiv	Afișează numele curent al dispozitivului. Acceptă schimbarea numelui.
Adresă IP	Afișează adresa IP curentă. Acceptă configurare manuală.

Parametru	Descriere
Mască de subrețea	Acceptă introducerea măștii de subrețea.
VLAN gestionat	După ce este activat VLAN-ul gestionat, puteți accesa pagina web doar prin adresa IP din VLAN-ul gestionat.
ID VLAN	Afișează ID-ul VLAN gestionat curent.

2.2 Informații despre port

Puteți vizualiza informații precum portul, tipul, starea legăturii, viteza/duplexarea, VLAN-ul, utilizarea RX, utilizarea TX și tipul de mediu al switch-ului.

Procedură

Pasul 1 Selectați Configurare rapidă > Informații port.

Pasul 2 Vizualizați informațiile despre port ale switch-ului.

Figura 2-2 Informații despre port

Refresh

Auto Refresh

Port	Type	Link Status	Speed/Duplexing	VLAN	RX Usage	TX Usage	Media Type
1	Access	Down	Down	4094	0	0	Copper
2	Access	Down	Down	1	0	0	Copper
3	Access	UP	100M_Full	1	0	0	Copper
4	Access	Down	Down	1	0	0	Copper
5	Access	Down	Down	1	0	0	Fiber
6	Access	Down	Down	1	0	0	Fiber
7	Access	Down	Down	1	0	0	Fiber

Tabelul 2-2 Descrierea informațiilor despre port

Parametru	Descriere
Port	Afișează toate porturile switch-ului.
Descriere	Setați descrierea portului. Acceptați introducerea numerelor, literelor, caracterelor speciale, indiferent dacă există majuscule sau minuscule. Se pot utiliza până la 16 caractere diferite de spațiile libere. În mod implicit, nu există nicio descriere.
Tip	Include trei tipuri: Acces, Hibrid și Portbagaj.
Starea legăturii	Include două stări: Sus și Jos. ● Sus: Portul este conectat. ● Nefuncțional: Portul nu este conectat sau conexiunea eșuează.
Viteză/Imprimare față-verso	● Online: Afișează rata portului și modul duplex. ● Offline: Se afișează în jos.
VLAN	Port VLAN. VLAN 1 în mod implicit.

Parametru	Descriere
Utilizarea RX	Afișează utilizarea la recepție.
Utilizarea TX-ului	Afișează utilizarea trimiterilor.
Tip de suport media	Include două tipuri: cupru și fibră. ● Cupru: port RJ-45. ● Fibră: Port de fibră.

Operațiuni conexe

- Faceți clic pe Reîmprospătare pentru a reîmprospăta manual informațiile despre port.
- Faceți clic pe lângă Reîmprospătare automată pentru a activa reîmprospătarea automată.



2.3 ONVIF

Selectați Configurare rapidă > Informații port, puteți vizualiza informațiile despre port ale switch-ului.

Faceți clic pentru a activa funcția de afișare ONVIF. După activare, pagina afișează toate porturile și starea conexiunii switch-ului.

- Port verde: Indică o conexiune reușită.
- Port albastru deschis: Indică lipsa conexiunii sau eroarea conexiunii.



Diferite modele sunt echipate cu un număr diferit de porturi. Următoarea figură este doar pentru referință. Vă rugăm să consultați produsul real.

Figura 2-3 Informații ONVIF



Tabelul 2-3 Descrierile porturilor

Nume	Descriere
Port	Afișează numărul portului.
Descriere	Afișează descrierea portului.
Tip de port	Include trei tipuri: Acces, Hibrid și Portbagaj.
Starea legăturii	Include două stări: Sus și Jos. ● Sus: Portul este conectat. ● Nefuncțional: Portul nu este conectat sau conexiunea eșuează.

Nume	Descriere
Stare control flux	Verificați starea funcției de control al fluxului.
Viteză/Imprimare față-verso	● Online: Afișează rata portului și modul duplex. ● Offline: Se afișează în jos.
VLAN	Port VLAN. VLAN 1 în mod implicit.
PoE	Afișează consumul de energie PoE.  ● Switch-urile non-PoE nu acceptă această funcție. ● Modelele diferite sunt echipate cu un număr diferit de porturi PoE. Vă rugăm să consultați produsul propriu-zis.
Utilizarea RX	Tariful curent de recepție împărțit la tariful negociat efectiv pentru o perioadă de timp (de obicei 5 minute).
Utilizare TX	Tariful curent de trimitere împărțit la tariful negociat efectiv pentru o perioadă de timp (de obicei 5 minute).
Tip de suport media	Include două tipuri: cupru și fibră. ● Cupru: port RJ-45. ● Fibră: Port de fibră.

2.4 Vizualizarea IPC și NVR

Selectați Configurare rapidă > IPC și NVR, puteți vizualiza informațiile despre IPC, NVR și alte dispozitive conectate la switch.

3 Setări de rețea

3.1 Configurarea porturilor

Informații generale

Puteți configura parametrii portului, inclusiv viteza/duplexarea, controlul fluxului și alți parametri. Parametrii portului vor afecta direct modul de funcționare al portului. Faceți configurațiile în funcție de cerințele practice.



Pagina web poate diferi în funcție de dispozitiv. Consultați paginile reale.

Procedură

Pasul 1 Selectați Setări rețea > Port.

Pasul 2 Puteți vizualiza și configura parametrii.

Figura 3-1 Setări port

Port	Description	Type	Link Stat...	Speed/D...	Speed/Duplexing	Flow Co...	RX Usage	TX Usage	Details
1		Ethernet...	Down	Down	Auto ▾	☐	0	0	
2		Ethernet...	Down	Down	Auto ▾	☐	0	0	
3		Ethernet...	Down	Down	Auto ▾	☐	0	0	
4		Ethernet...	UP	100M Full	Auto ▾	☐	0	0	
5		Optical...	Down	Down	Auto ▾	☐	0	0	
6		Optical...	Down	Down	Auto ▾	☐	0	0	
7		Optical...	Down	Down	Auto ▾	☐	0	0	
OK Refresh									

Tabelul 3-1 Descrierea parametrilor portului

Parametru	Descriere
Port	Afișează toate porturile switch-ului.
Descriere	Introduceți descrierea portului. Descrierea nu poate depăși 16 caractere. Sunt permise doar numere, litere și următoarele caractere speciale: . _ -. Primul caracter trebuie să fie o literă, iar ultimul caracter nu trebuie să fie un caracter special.
Tip de suport media	Afișează două tipuri de suporturi, inclusiv două tipuri: cupru și fibră. ● Cupru: Port Ethernet. ● Fibră: Port optic.

Parametru	Descriere
Starea legăturii	Include două staturi: Sus și Jos. ● Sus: Portul este conectat. ● Nefuncțional: Portul nu este conectat sau conexiunea eșuează.
Viteză/Stare duplexare	● Online: Afișează rata portului și modul duplex. ● Offline: Se afișează în jos.
Viteză/Imprimare față-verso	Setați viteza și modul duplex dintre Jos, Auto, 10M Jumătate, 10M Complet, 100M Jumătate, 100M Complet și 1000M Complet.  Viteza/imprimarea față-verso este setată la Automat pentru portul combo.
Controlul fluxului	Faceți clic pentru a activa sau dezactiva funcția. 
Utilizarea RX	Afișează utilizarea la recepție.
Utilizarea TX-ului	Afișează utilizarea trimiterilor.
Detalii	● Vizualizați numărul total de RX și numărul total de TX ale fiecărui port. Puteți reîmprospăta sau șterge informațiile detaliate ale fiecărui port. ● Vizualizați numărul de octeți de eroare.

Pasul 3. Faceți clic pe OK.

3.2 Configurarea EEE

Activați funcția EEE (Ethernet eficient energetic).

Procedură

Pasul 1. Selectați Setări rețea > EEE.

Pasul 2. Bifați caseta de selectare a portului pentru a activa funcția Ethernet cu eficiență energetică, apoi faceți clic pe OK pentru a salva configurația.

Figura 3-2 Funcția EEE

Port	Energy-Efficient Ethernet
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐

OK Refresh

3.3 Configurarea VLAN-ului

3.3.1 Definiția VLAN-ului

Logic, o rețea locală (LAN) poate fi împărțită în mai multe subseturi. Fiecare subset are propria zonă de difuzare: o rețea locală virtuală (VLAN). O VLAN este separată de o rețea locală pe o bază logică, mai degrabă decât fizică, pentru a realiza zona de difuzare izolată în cadrul VLAN-ului.

3.3.2 Funcția VLAN

- Îmbunătățește performanța rețelei. Pachetele de difuzare se află în VLAN, ceea ce poate controla eficient furtuna de difuzare a rețelei, reduce lățimea de bandă a rețelei și îmbunătățește capacitatea de procesare a rețelei.
- Îmbunătățește securitatea rețelei. Switch-urile din VLAN-uri diferite nu se pot accesa reciproc, iar gazdele din VLAN-uri diferite nu pot comunica între ele. Au nevoie de un router sau de un switch cu trei niveluri pentru a transmite mesajul.
- Simplifică gestionarea rețelei. Gazda aceluiași grup de lucru virtual nu este limitată la o singură zonă fizică, ceea ce poate simplifica gestionarea rețelei și facilita crearea de grupuri de lucru pentru utilizatorii din diferite zone.

3.3.3 VLAN bazat pe porturi

Tipurile de porturi includ Acces, Trunk și Hibrid.

- Acces: Portul aparține unei rețele VLAN și este utilizat pentru conectarea la portul computerului.
- Trunk: Portul permite trecerea mai multor VLAN-uri, primirea și trimiterea de mesaje de la mai multe VLAN-uri și este utilizat pentru conectarea între switch-uri.
- Hibrid: Portul permite trecerea mai multor VLAN-uri, primirea și trimiterea de mesaje de la mai multe VLAN-uri și este utilizat pentru conectarea între switch-uri și conectarea computerului.

3.3.4 Adăugarea VLAN-ului

Informații generale

Puteți adăuga portul la VLAN. VLAN-ul este VLAN1 în mod implicit.



Izolarea porturilor și VLAN-ul nu pot fi activate simultan. Dacă una dintre ele este activată, cealaltă va fi dezactivată automat. Vă rugăm să rețineți.

Procedură

Pasul 1 Selectați Setări rețea > VLAN.

Figura 3-3 Configurarea VLAN

Port	Mode	PVID	Tagged VLAN(s)	Untagged VLAN(s)
9	Hybrid	6	1-4094	6
10	Access	6		6
11	Access	7		7
12	Access	7		7
13	Access	8		8
14	Access	8		8
15	Access	9		9

Pasul 2. Pe pagina Adăugare VLAN, faceți clic pe Adăugare, introduceți ID-ul VLAN și descrierea.

Figura 3-4 Adăugați VLAN

Add VLAN

VLAN ID: (1-4094)

Description:

It can contain up to 64 characters, and can only consist of numbers, letters and underscores.

Cancel OK

Pasul 3. Faceți clic pe OK.



VLAN1 nu poate fi șters.

Operațiuni conexe

- Faceți clic pentru a edita VLAN-ul.
- Faceți clic pentru a șterge VLAN-ul.

3.3.5 Configurarea portului VLAN

Puteți configura parametrii VLAN ai portului.

Figura 3-5 Configurarea VLAN-ului

Tabelul 3-2 Parametrul de configurare a portului VLAN

Parametru	Descriere
Port	Afișează toate porturile switch-ului.
	Include trei moduri: Acces, Hibrid și Portbagaj. ● Acces: Aparține unui singur VLAN. Folosit în mod obișnuit pentru conectarea porturilor computerului. ● Trunk: Permite trecerea mai multor VLAN-uri. Primește și trimite mai multe pachete VLAN. De obicei, este utilizat pentru conexiunea între switch-uri. ● Hibrid: Permite trecerea mai multor VLAN-uri. Primește și trimite mai multe pachete VLAN. Folosit pentru conexiunea dintre switch-uri sau între switch și computer.
VLAN-uri etichetate	Setați ID-ul VLAN pentru portul care poate fi etichetat la trimiterea de pachete.
VLAN-uri neetichetate	Setați ID-ul VLAN pentru portul care poate fi detașat la trimiterea de pachete.

Tabelul 3-3 Comparație procesare cadre

Tipul de port	Procesarea cadrelor neetichetate	Prelucrarea cadrelor etichetate	Transmisie cadru
	Primește un cadru neetichetat și adaugă o etichetă cu ID-ul VLAN implicit la cadru.	● Acceptă cadrul etichetat dacă ID-ul VLAN al cadrului corespunde cu ID-ul VLAN implicit. ● Elimină cadrul etichetat dacă ID-ul VLAN al cadrului diferă de ID-ul VLAN implicit.	După ce eticheta PVID este îndepărtată, cadrul este transmis.
Trunchi	● Adaugă o etichetă cu ID-ul VLAN implicit la un cadru neetichetat și acceptă cadrul dacă interfața permite ID-ul VLAN implicit. ● Adaugă o etichetă cu ID-ul VLAN implicit la un cadru neetichetat și elimină cadrul dacă interfața respinge ID-ul VLAN implicit.	● Acceptă un cadru etichetat dacă ID-ul VLAN transportat în cadru este permis de interfață. ● Elimină un cadru etichetat dacă ID-ul VLAN transportat în cadru este refuzat de interfață.	● Dacă ID-ul VLAN al cadrului corespunde cu ID-ul VLAN implicit și ID-ul VLAN este permis de interfață, dispozitivul elimină eticheta și transmite cadrul. ● Dacă ID-ul VLAN al cadrului diferă de ID-ul VLAN implicit, dar ID-ul VLAN este încă permis de interfață, dispozitivul va transmite direct cadrul.
Hibrid			Dacă ID-ul VLAN al cadrului este permis de interfață, cadrul este transmis. Interfața poate fi configurată pentru a transmite cadre cu etichete.

3.4 Configurarea VLANIF

Informații generale

O interfață VLANIF este o interfață logică de nivel 3, utilizată cel mai frecvent pentru a implementa comunicarea de nivel 3 între gazde din diferite VLAN-uri pe diferite segmente de rețea.

Fiecare interfață VLANIF corespunde unui VLAN. După ce o adresă IP este configurată pentru o interfață VLANIF, interfața VLANIF devine gateway-ul gazdelor utilizator din cadrul acelui

VLAN și redirecționează pachete prin segmentele de rețea de la nivelul 3.

Procedură

Pasul 1 Selectați Setări rețea > VLANIF.

Pasul 2. Faceți clic pe Adăugare, introduceți numărul VLAN, apoi activați DHCP pentru port cu modul Dinamic.



Când DHCP este dezactivat, trebuie să introduceți adresa IP și lungimea măștii.

Figura 3-6 Adăugați VLANIF

The screenshot shows a dialog box titled "Add" with a close button "X" in the top right corner. The dialog contains the following fields and controls:

- VLAN:** A text input field with a range indicator "(1-4094)" to its right.
- DHCP:** A toggle switch, currently in the "off" position.
- IP Address:** A text input field containing three dashes "- - -".
- Mask Length:** A text input field with a range indicator "(1-30)" to its right.
- Buttons:** "Cancel" and "OK" buttons are located at the bottom right of the dialog.

Operațiuni conexe

- Ștergeți VLANIF: Selectați VLAN-ul, apoi faceți clic pe Ștergere sau . 
- Reîmprospătați parametrul: Faceți clic pe Reîmprospătare pentru a reîmprospăta parametrii VLAN.

3.5 Configurarea IP-ului și a rutării

Prezintă setările IP și setările de rutare ale switch-ului.

Procedură

Pasul 1 Selectați Setări rețea > IP și rutare.

Pasul 2. În fila Setări de rutare, faceți clic pe Adăugare, apoi configurați parametrii.



Unele modele acceptă doar rutarea implicită. Consultați produsul propriu-zis.

Figura 3-7 Setări de rutare

The image shows a dialog box titled 'Add' with a close button (X) in the top right corner. Inside the dialog, there are three input fields: 'Network' with a placeholder '...', 'Mask Length' with a placeholder '...' and a range '(1-30)', and 'Next Hop' with a placeholder '...'. At the bottom right of the dialog are two buttons: 'Cancel' and 'OK'.

Tabelul 3-4 Descrierea parametrilor de rutare

Parametru	Descriere
Rețea	Introduceți adresa de destinație sau rețeaua de destinație pentru a identifica pachetul IP.
Lungimea măștii	Setați segmentul pentru a identifica switch-ul sau routerul de destinație cu adresa de destinație.
Următorul salt	Setați adresa următorului hop a routerului.

Operațiuni conexe

- Ștergeți rutarea: Selectați VLAN-ul și rutarea, apoi faceți clic pe Ștergeți sau .
- Reîmprospătați parametrul: Faceți clic pe Reîmprospătare pentru a reîmprospăta parametrul rutării.

3.6 Configurarea ERPS

ERPS este un protocol definit de Uniunea Internațională a Telecomunicațiilor - Sectorul de Standardizare a Telecomunicațiilor (ITU-T) pentru a elimina bucele la nivelul 2. În general, legăturile redundante sunt utilizate într-o rețea de comutare Ethernet, cum ar fi o rețea inelară, pentru a oferi backup la legături și a spori fiabilitatea rețelei. Utilizarea legăturilor redundante, însă, poate produce bucle, provocând furtuni de broadcast și făcând tabelul de adrese MAC instabil. Drept urmare, calitatea comunicării se deteriorează, iar serviciile de comunicație pot fi chiar întrerupte. ERPS previne furtunile de broadcast și implementează comutarea rapidă a traficului într-o rețea în care există bucle, oferă convergență rapidă și fiabilitate de clasă purtătoare și permite tuturor dispozitivelor compatibile ERPS dintr-o rețea inelară să comunice.



Este posibil ca unele modele să nu fie compatibile cu funcția ERPS. Vă rugăm să consultați produsele reale.

3.6.1 Setări ERPS

Procedură

Pasul 1 Selectați Setări rețea > ERPS.

Pasul 2. În fila ERPS, faceți clic pe Adăugare pentru a adăuga ERPS.

Pasul 3 Configurați parametrii, apoi faceți clic pe OK.

Figura 3-8 Adăugați ERPS

The 'Add' dialog box for ERPS configuration contains the following fields:

- ERPS ID: (1-64)
- Port 0: (1-52)
- Port 1: (1-52)
- Port 0 APS MEP: (1-100)
- Port 1 APS MEP: (1-100)
- Port 0 SF MEP: (1-100)
- Port 1 SF MEP: (1-100)

Buttons: Cancel, OK

Tabelul 3-5 Descrierea parametrilor

Parametru	Descriere
ID-ul ERPS	Numărul de identificare al ERPS.
Portul 0	Două porturi ale switch-ului care vor fi adăugate în ERPS.
Portul 1	
Portul 0 APS MEP	● BPDU MEP al portului ERPS. ● Monitorizarea legăturii MEP a portului ERPS. Portul 0 APS MEP rămâne la fel ca Portul 0 SF MEP. Portul 1 APS MEP rămâne la fel ca Portul 1 SF MEP.
Portul 1 APS MEP	
Portul 0 SF MEP	
Portul 1 SF MEP	

3.6.2 Setări MEP

MEP (Maintenance Entity Group Endpoint Point - Punct final al grupului de entități de întreținere) face parte din inelul ERPS. Un nod se referă la un dispozitiv de comutare de nivel 2 adăugat la un inel ERPS. La același inel ERPS se pot adăuga maximum două porturi pe fiecare nod.

Procedură

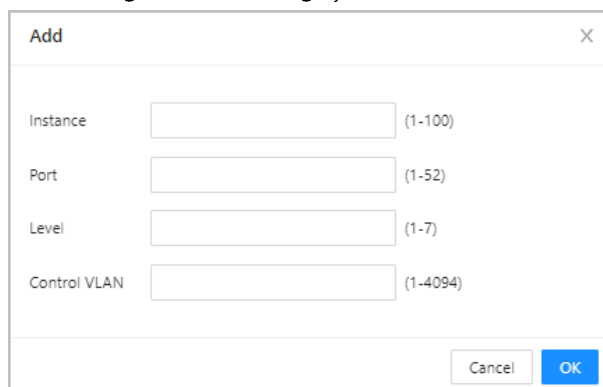
Pasul 1 Selectați Setări rețea > ERPS.

Pasul 2. În fila MEP, faceți clic pe Adăugare pentru a adăuga MEP.

Pasul 3 Configurați parametrii MEP.

Pasul 4. Faceți clic pe OK.

Figura 3-9 Adăugați MEP



Tabelul 3-6 Descrierea parametrilor MEP

Parametru	Descriere
Instanță	Numărul instanței MEP.
Port	Numărul de port al MEP.
Nivel	Nivel de întreținere. Recomandăm setarea la 0.
Control VLAN	ID-ul VLAN-ului de control într-un segment SEP.

3.7 Configurarea supravegherii IGMP

IGMP Snooping (Internet Group Management Protocol Snooping) este mecanismul de constrângere multicast care rulează pe dispozitivul de nivel 2, pentru gestionarea și controlul multicast-ului. Prin analizarea pachetului IGMP primit, dispozitivul de nivel 2, care execută IGMP Snooping, creează maparea între port și adresa MAC multicast și transmite datele multicast conform mapării.

Procedură

Pasul 1 Selectați Setări rețea > Monitorizare IGMP.

Pasul 2. Faceți clic pe lângă IGMP Snooping pentru a activa funcția.

Pasul 3. Faceți clic pe lângă Mesaje IGMP Leave Group pentru a activa funcția.

- Activați funcția: Odată ce funcția este activată, dacă switch-ul primește mesaje de grup care nu sunt înregistrate, le lasă. Lățimea de bandă va fi salvată, iar rata de redirectionare va fi crescută.
- Dezactivați funcția: Dacă mesajele de grup nu sunt înregistrate, mesajele vor fi transmise în VLAN. Lățimea de bandă va fi ocupată, iar rata de redirectionare va scădea.



Vă rugăm să rețineți că activarea mesajelor IGMP Leave Group este recomandată, altfel multicast-ul ar putea eșua.

Pasul 4. Faceți clic pe OK.

3.8 Configurarea STP

Protocolul Spanning Tree (STP) construiește o topologie logică fără bucle pentru rețelele LAN. Acesta blochează legăturile redundante dintre oricare două dispozitive de rețea și lasă o singură legătură activă între ele, astfel încât să se elimine buclele.

STP, RSTP și MSTP oferă următoarele capabilități:

- STP: Un protocol de gestionare la nivelul legăturii de date, utilizat pentru a detecta și preveni buclele într-o rețea de Nivel 2. Cu toate acestea, acesta converge lent topologia rețelei.
- RSTP: O îmbunătățire a STP, permite o convergență rapidă a topologiei rețelei. Cu toate acestea, atât RSTP, cât și STP au defectul că toate VLAN-urile de pe aceeași rețea LAN partajează același arbore de acoperire (spanning tree).
- MSTP: Un tabel virtual de mapare VLAN în care ID-urile VLAN sunt asociate cu instanțe spanning tree. Nu numai atât, MSTP împarte o rețea de comutare în mai multe regiuni, fiecare dintre acestea având mai multe instanțe spanning tree care sunt reciproc independente. Spre deosebire de STP și RSTP, MSTP oferă mai multe căi redundante pentru redirecționarea datelor. În plus, implementează echilibrarea încărcării între VLAN-uri.

3.8.1 STP

Informații generale



Când este activat spanning tree, iLinkView nu poate fi utilizat.

Procedură

Pasul 1 Selectați Setări rețea > STP.

Pasul 2. Faceți clic pe lângă STP pentru a activa funcția STP. 

Pasul 3 Selectați modul de lucru.

Pasul 4. Faceți clic pe Avansat, apoi configurați parametrii avansați.

Figura 3-10 Configurarea STP-ului

STP Port Instance

STP ☒

Working Mode RSTP

Advanced

Input Rules

Max Aging Time $\geq (\text{Hello Timer} + 1) \times 2$

Max Aging Time $\leq (\text{Forwarding Delay Time} - 1) \times 2$

Hello Timer 2 s(1~10)

Max. Aging Time 20 s(6~40)

Forwarding Delay Time 15 s(4~30)

Bridge Priority 0 (0-61440)

OK Refresh

Tabelul 3-7 Descrierea parametrilor avansați

Parametru	Descriere
STP	Protocolul de bază al arborelui de acoperire.
RSTP	O îmbunătățire a STP permite o convergență rapidă a topologiei rețelei.
Salut cronometru	Perioada de transmitere a BPDU-ului de către root bridge. Timpul variază între 1 secundă și 10 secunde.
Timp maxim de maturare	Timpul de îmbătrânire al BPDU-ului curent. Timpul variază între 6 secunde și 40 de secunde.
Timp de întârziere a redirectionării	După setarea schimbării topologice, puntea menține timpul de observare și starea de studiu. Timpul variază între 4 secunde și 30 de secunde.
Prioritate pod	Valoarea variază de la 0 la 61440.

3.8.2 Instanța portului

Procedură

Pasul 1 Selectați Setări rețea > STP > Instanță port.

Pasul 2 Introduceți Prioritatea și Costul Căii Rădăcină pentru fiecare port.



- Valoarea Priorității este cuprinsă între 0 și 240 și trebuie să fie un multiplu întreg al lui 16.
- Valoarea implicită a Priorității este 128.

Figura 3-11 Instanța portului

Port	Name	Status	Priority	Root Port Cost	Designated Port ID	Occupied Port ID
1	Designated Port	Designing	128	19	0000-0000-0000-0000	0000
2	Designated Port	Designing	128	19	0000-0000-0000-0000	0001
3	Designated Port	Designing	128	19	0000-0000-0000-0000	0002
4	Designated Port	Designing	128	19	0000-0000-0000-0000	0003
5	Designated Port	Designing	128	19	0000-0000-0000-0000	0004
6	Designated Port	Designing	128	19	0000-0000-0000-0000	0005
7	Designated Port	Designing	128	19	0000-0000-0000-0000	0006

Tabelul 3-8 Descrierea parametrilor instanței portului

Parametru	Descriere
	STP-ul de bază.
Stare	O îmbunătățire a STP permite o convergență rapidă a topologiei rețelei.
Prioritate	Prioritatea portului.
Costul căii rădăcină	Costul căii rădăcină a portului.
ID-ul podului desemnat	ID-ul podului desemnat al portului.
ID-ul portului desemnat	ID-ul de port desemnat pentru port.

3.9 Configurarea agregării linkurilor

Informații generale

Agregarea legăturilor constă în formarea mai multor porturi fizice ale switch-ului în portul logic. Legăturile multiple din același grup pot fi considerate o legătură logică cu o lățime de bandă mai mare.

Prin agregare, porturile din același grup pot partaja fluxul de comunicații, pentru a crea o lățime de bandă mai mare. În plus, porturile din același grup pot face backup reciproc și dinamic pentru a îmbunătăți fiabilitatea legăturii.



- Agregarea legăturilor se exclude reciproc cu modul STP, IGMP Snooping și modul 802.1x. Când modul STP este activat, agregarea legăturilor nu poate fi configurată. Trebuie să dezactivați modul STP înainte de a configura agregarea legăturilor.
- Nu recomandăm implementarea funcțiilor de configurare și avansate pentru porturile utilizate pentru agregarea legăturilor.
- Agregarea legăturilor poate fi împărțită în agregare statică și LACP. În general, dispozitivele peer cu agregare de legături prin comutare sunt comutatoarele și adaptoarele de rețea.
- Doar porturile cu aceeași viteză, duplex, distanță lungă și configurație VLAN pot fi în același grup de agregare.

Procedură

Pasul 1 Selectați Setări rețea > Agregare legături.

Pasul 2. Faceți clic pe Adăugare.

Pasul 3 Selectați numărul grupului de agregare.

Pasul 4 Selectați Modul grup de agregare, apoi faceți clic pe OK.

Modul grupului de agregare include static, LACP activ și LACP pasiv.

- Static: Staticul este cunoscut și sub denumirea de mod manual. Interfața Eth-Trunk trebuie creată manual, iar interfețele membre trebuie adăugate manual. Protocolul LACP este dezactivat.
- LACP activ: Interfața Eth-Trunk trebuie creată manual, iar interfețele membre trebuie adăugate manual. Comparativ cu modul static, selecția interfeței este configurată prin protocolul LACP. Acest mod plasează o interfață într-o stare de negociere activă. În acest mod, interfața inițiază negocierile cu alte interfețe prin trimiterea de LACPDU-uri.
- LACP pasiv: Interfețele Eth-Trunk sunt create, iar interfețele membre sunt adăugate prin protocolul LACP. Acest mod plasează o interfață într-o stare de negociere pasivă. În acest mod, interfața răspunde la LACPDU-urile pe care le primește, dar nu inițiază negocierea LACPDU.

Pasul 5 Selectați porturile care vor fi adăugate, apoi faceți clic pe OK.

Pasul 6 Setati cheia operațională.

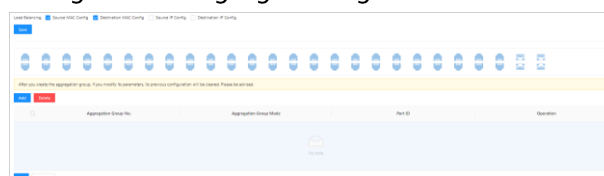


- Puteți configura agregarea linkurilor numai atunci când Modul grup de agregare este setat ca LACP.
- Valoarea este cuprinsă între 1 și 65535.

Pasul 7 Selectați Timeout-ul dintre Timeout lung sau Timeout scurt.

Pasul 8 Faceți clic pe OK.

Figura 3-12 Agregarea legăturilor



3.10 Configurarea protocolului SNMP

SNMP (Simple Network Management Protocol) este protocolul standard pentru gestionarea rețelelor pe Internet și este utilizat pe scară largă pentru accesarea și gestionarea dispozitivelor gestionate. SNMP are următoarele caracteristici:

- Acceptă management inteligent pentru dispozitivele de rețea. Prin utilizarea platformei de management al rețelei bazate pe SNMP, administratorul de rețea poate interoga starea de funcționare și parametrii dispozitivului de rețea, poate configura parametrii, poate identifica erorile, poate efectua diagnosticarea defecțiunilor, apoi poate planifica capacitatea și poate crea raportul.
- SNMP permite gestionarea dispozitivelor cu diferite caracteristici fizice. SNMP oferă doar cea mai simplă bibliotecă de funcții. Face ca sarcina de gestionare, caracteristicile fizice și tehnologia de rețea a dispozitivului gestionat să fie independente, pentru a gestiona dispozitive de la diferiți producători.

Rețeaua SNMP oferă 2 elemente, NMS și Agent.

- NMS (Network Management System) este managerul în rețeaua SNMP și oferă o interfață om-mașină prietenoasă pentru a ajuta administratorul de rețea să finalizeze majoritatea activităților de gestionare a rețelei.
- Agentul este rolul gestionat în rețeaua SNMP și primește și gestionează pachetul de solicitare de la NMS. În anumite circumstanțe de urgență, de exemplu, dacă starea portului se modifică, Agentul poate trimite pachete de alarmă către NMS în mod proactiv.

3.10.1 Configurarea SNMP V1 și V2

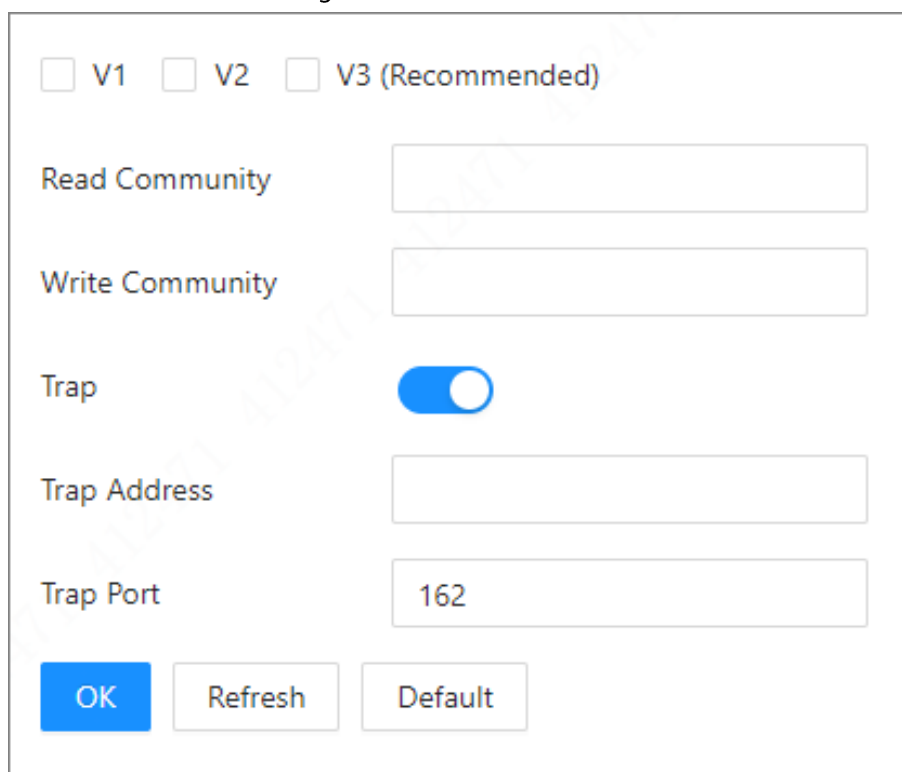
Procedură

Pasul 1 Selectați Setări rețea > SNMP.

Pasul 2 Selectați versiunea V1 sau V2.

Pasul 3 Configurați parametrii, inclusiv Comunitatea de citire, Comunitatea de scriere, Adresa trap-ului și Portul trap-ului.

Figura 3-13 SNMP



☐ V1 ☐ V2 ☒ V3 (Recommended)

Read Community

Write Community

Trap ☒

Trap Address

Trap Port

Pasul 4. Faceți clic pe OK.

3.10.2 Configurarea SNMP V3

Procedură

Pasul 1 Selectați Setări rețea > SNMP.

Pasul 2 Selectați V3.

Pasul 3 Configurați parametrii.

Figura 3-14 SNMP V3

☐ V1
 ☐ V2
 ☒ V3 (Recommended)

Read Community:

Write Community:

Trap: ☐

Read-Only Username:

Authentication Type: ☒ MD5 ☐ SHA

Authentication Password:

Encryption Type: ☒ CBC-DES ☐ CFB-AES

Encryption Password:

Read/Write Username:

Authentication Type: ☒ MD5 ☐ SHA

Authentication Password:

Encryption Type: ☒ CBC-DES ☐ CFB-AES

Encryption Password:

Tabelul 3-9 Descrierea parametrilor SNMP

Parametru	Descriere
Comunitatea de lectură	Comunitatea de citire susținută de programele agenților.
Comunitatea de scriere	Comunitatea de scriere este susținută de programele de agenți.
Adresă capcană	Adresa de destinație a informațiilor despre capcane trimise de programul agent.
Port capcană	Portul de destinație al informațiilor despre capcane trimise de programul agent.
Nume de utilizator doar pentru citire	Setați numele de utilizator doar pentru citire. Este valabil doar pentru versiunea 3.
Tip de autentificare	Setați modul de autentificare când nivelul de securitate este Autentificare fără criptare sau Autentificare și criptare. Modul de autentificare include MD5 și SHA.
Parolă de autentificare	Setați parola de autentificare.
Tip de criptare	Setați modul de criptare când modul de autentificare este Autentificare și criptare.
Parolă de criptare	Setați parola de criptare când modul de autentificare este Autentificare și criptare.

Parametru	Descriere
Nume utilizator cu permisiuni de citire/scriere	Setează utilizatorul pentru citire și scriere.

Pasul 4. Faceți clic pe OK.

3.11 Configurarea tabelului MAC

Tabelul MAC (Media Access Control) înregistrează relația dintre adresa MAC și port, precum și informațiile, inclusiv VLAN-ul căruia îi aparține portul. Când dispozitivul transmite pachetul, acesta interoghează în tabelul de adrese MAC adresa MAC de destinație a pachetului. Dacă adresa MAC de destinație a pachetului este conținută în tabelul de adrese MAC, pachetul este transmis direct prin portul din tabel. Și dacă adresa MAC de destinație a pachetului nu este conținută în tabelul de adrese MAC, dispozitivul adoptă broadcasting-ul pentru a transmite pachetul către toate porturile, cu excepția portului receptor din VLAN.

3.11.1 Adăugarea tabelului MAC

Procedură

Pasul 1 Selectați Setări rețea > Tabel MAC.

Pasul 2. În fila Tabel MAC, faceți clic pe Adăugare.

Pasul 3. Setati adresa MAC, VLAN-ul și portul.

De exemplu, asociați adresa MAC 00:00:00:00:00:01 cu portul 3 din VLAN 2.

Pasul 4. Faceți clic pe OK.

Figura 3-15 Adăugați tabelul MAC

Operațiuni conexe

Figura 3-16 operațiuni conexe

- Ștergeți adresa MAC statică: Selectați o adresă MAC, apoi faceți clic pe Ștergere.
- Reîmprospătați lista de adrese MAC: Faceți clic pe Reîmprospătare sau activați Reîmprospătare automată.
- Ștergeți adresa MAC dinamică: Faceți clic pe Ștergeți adresa MAC dinamică.
- Căutați adresa MAC și portul: Introduceți adresa MAC sau numărul portului în colțul din dreapta sus, apoi faceți clic pe Căutare.

3.11.2 Filtrarea portului MAC

Informații generale

După activarea filtrării MAC a porturilor, următoarele dispozitive MAC pot comunica cu portul.

- Dispozitive în lista MAC permisă.
- Dispozitivele MAC statice se schimbă față de dispozitivele MAC dinamice.



După activarea filtrării MAC a portului, portul nu poate accesa adresa de administrare sau datele de autentificare.

Procedură

Pasul 1 Selectați Setări rețea > Tabel MAC.

Pasul 2. În fila Filtrare MAC, selectați portul, apoi faceți clic pe pentru a activa funcția de filtrare. 

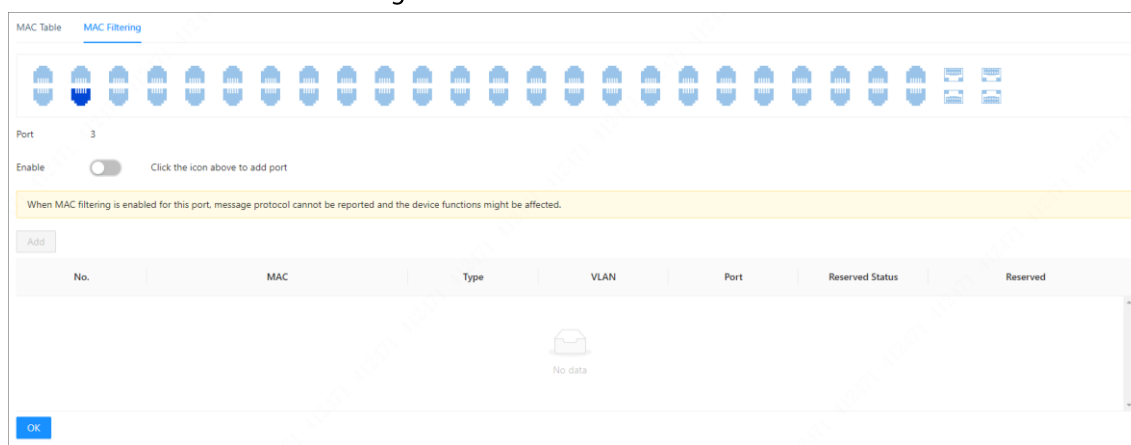
Pasul 3 Configurați filtrarea MAC a portului.

- Trecerea de la dinamic la static.
 1. Selectați o înregistrare, apoi faceți clic pe Selectare lângă Rezervat. 
 2. Faceți clic pe OK.

Tipul se schimbă de la Dinamic la Static.

Dispozitivele MAC statice pot comunica normal cu portul.
- Creați o listă de adrese MAC permise.
 1. Faceți clic pe Adăugare.
 2. Setați adresa MAC și VLAN-ul.
 3. Faceți clic pe OK.

Figura 3-17 Filtrare MAC



3.12 Configurarea LLDP

LLDP (Link Layer Discovery Protocol) este o metodă standard de descoperire a nivelului de legătură. Acesta își poate forma principalele capabilități, adresa de gestionare, numărul dispozitivului și numărul portului ca TLV (Type Length Value), le poate încapsula în LLDPDU (Link Layer Discovery Protocol Data Unit) și le poate elibera vecinului său. Vecinul va păstra

informațiile primite sub forma unui MIB (Management Information Base) standard, astfel încât managementul rețelei să poată interoga și evalua starea comunicației legăturii.

Procedură

Pasul 1 Selectați Setări rețea > LLDP.

Pasul 2. În fila Dispozitiv LLDP la distanță, vizualizați informațiile despre Dispozitivul LLDP la distanță.

Figura 3-18 Dispozitiv la distanță LLDP



The screenshot shows a network management interface for LLDP. At the top, there are controls for 'Global Enable' (a toggle switch that is turned on) and 'Auto Refresh' (a toggle switch that is turned off). Below these controls is a table with the following columns: 'Local Port', 'Port ID', 'Port Description', 'System Name', 'System Capacity', and 'Address Management'. The table contains one row of data representing a discovered device.

Local Port	Port ID	Port Description	System Name	System Capacity	Address Management
GigabitEthernet1/0/48	eth-0-36	eth-0-36	qwert	Bridge(+), Router(+)	View Details

4 Management PoE

PoE se referă la faptul că dispozitivul folosește cabluri de rețea pentru a conecta extern PD (Powered Device) pentru alimentare de la distanță prin porturi electrice Ethernet. Funcția PoE permite alimentarea centralizată și backup-ul convenabil. Terminalele de rețea nu necesită o sursă de alimentare externă, ci doar un cablu de rețea. Respectând standardele IEEE 802.3af, IEEE 802.3at și IEEE 802.3bt, dispozitivul utilizează un port de alimentare unificat la nivel global. Poate fi utilizat în telefoane IP, puncte de acces wireless (AP), încărcătoare portabile, terminale de carduri de credit, camere de rețea, colectare de date.

- Switch-urile non-PoE nu acceptă această funcție.
- Doar unele modele de switch-uri PoE sunt conforme cu standardul IEEE 802.3at. Un singur port BT suportă până la 90 W. Vă rugăm să consultați produsele reale.

4.1 Configurarea setărilor PoE

Selectați Gestionare PoE > Setări PoE. Puteți configura setările de alimentare, starea alimentării, starea portului și controlul.

Procedură

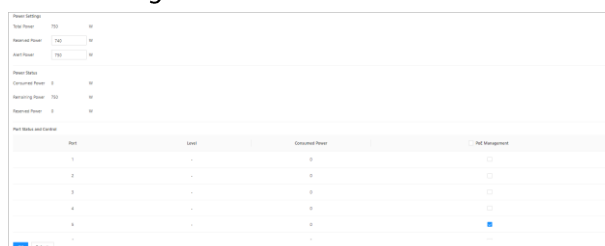
Pasul 1 În Setări de alimentare, puteți vizualiza puterea totală a celor 4 porturi și puteți configura puterea rezervată și puterea de alertă.

Pasul 2 În secțiunea Stare alimentare, puteți vizualiza energia consumată, energia rămasă și energia rezervată.

Pasul 3. În Port Status and Control, selectați din lista de sub PoE Management pentru a activa sau dezactiva PoE-ul portului corespunzător.

Pasul 4. Faceți clic pe OK.

Figura 4-1 Setări PoE



Tabelul 4-1 Descrierea parametrilor PoE

Parametru		Descriere
Setări de alimentare	Putere totală	Afișează puterea totală PoE.
	Putere rezervată	Configurați alimentarea PoE rezervată.
	Putere de alertă	Configurează alimentarea PoE pentru alerte.
Starea alimentării	Putere consumată	Afișează consumul curent de energie PoE de către toate porturile.
	Putere rămasă	Afișează puterea PoE rămasă în prezent.

Parametru		Descriere
	Putere rezervată	Alimentare PoE inutilizabilă. Alimentare rezervată = alimentare totală – alimentare de supraîncărcare.
Starea și controlul porturilor	Nivel	Afișează nivelul alimentării cu energie a dispozitivelor terminale. Nivelul alimentării cu energie variază de la 0 la 8, iar nivelul standard al alimentării Hi-PoE este afișat ca 5+.
	Putere consumată	Afișează consumul actual de energie PoE de către portul individual corespunzător.
	Gestionarea PoE	Selectați dintre Activare și Dezactivare. ● Când se selectează Dezactivare, sistemul nu furnizează energie PD-ului și nu rezervă energie pentru PD. ● Când selectați Activare, portul PoE nu va duce la o supraîncărcare a alimentării PoE. În caz contrar, nu aveți voie să activați PoE pentru portul PoE.  ● În mod implicit, PoE este dezactivat pe un port PoE. ● Supraîncărcare energie PSE: Când consumul total de energie al tuturor porturilor depășește puterea maximă a PSE, sistemul consideră că PSE este supraîncărcat.

4.2 Configurarea PoE perpetuu

Procedură

Pasul 1 Selectați Gestionare PoE > PoE perpetuu.

Pasul 2. Faceți clic pentru a activa Activare globală. 

Pasul 3. Faceți clic pe OK pentru a salva configurația.

4.3 Configurarea PoE pe distanțe lungi

Informații generale

După ce activați PoE pe distanțe lungi, distanța maximă de transmisie se va schimba de la 100 m la 250 m, iar viteza de transmisie va fi redusă de la 100 Mbps la 10 Mbps.



În modul Extins, distanța de transmisie a portului PoE este de până la 250 m, dar rata de transmisie scade la 10 Mbps. Distanța reală de transmisie poate varia în funcție de consumul de energie al dispozitivelor conectate sau de tipul și starea cablului.

Procedură

Pasul 1 Selectați Gestionare PoE > PoE pe distanță lungă.

Pasul 2. Faceți clic pe portul corespunzător pentru a activa PoE la distanță lungă.

Pasul 3. Faceți clic pe OK.

Figura 4-2 PoE la distanță lungă

After long distance PoE is enabled, the maximum transmission distance will be increased from 100 meters to 250 meters, but the transmission speed will be reduced from 100 Mbps to 10 Mbps.

Port	☐ Long Distance PoE
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐

4.4 Vizualizarea statisticilor evenimentelor PoE

Selectați Gestionare PoE > Statistici evenimente PoE pentru a vizualiza statisticile evenimentelor PoE.

Tabelul 4-2 Descrierea statisticilor evenimentelor PoE

Parametru	Descriere
Suprasarcină	Portul unic pornește atunci când curentul de alimentare a depășit pragul de curent.
Scurtcircuit	Când cipul de alimentare trimite curent către port, acesta intră în scurtcircuit.
Deconectare CC	Alimentarea de la un singur port este oprită.
Scurtcircuit în timpul pornirii	Puterea este scurtcircuitată atunci când cipul de alimentare emite curent.
Protecție la supraîncălzire	Portul unic pornește atunci când temperatura cipului de alimentare a depășit pragul.

4.5 Configurarea Green PoE

Green PoE poate reduce consumul de energie, menținând în același timp compatibilitatea

deplină cu echipamentele existente.

Procedură

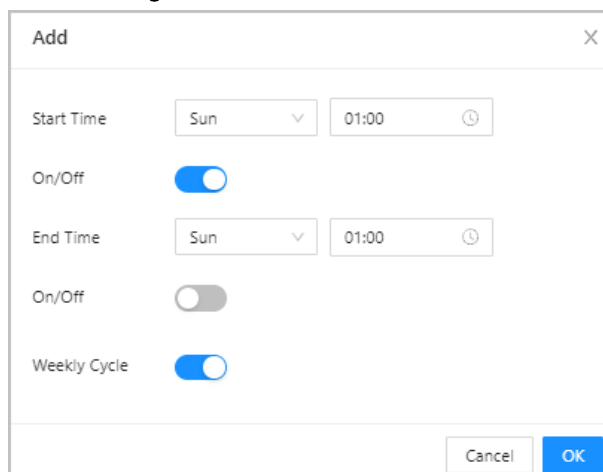
Pasul 1 Selectați Gestionare PoE > PoE verde.

Pasul 2 Adăugați ora de început și ora de sfârșit.

Pasul 3 Selectați portul, apoi faceți clic pe pentru a activa PoE-ul verde. 

Pasul 4. Faceți clic pe OK.

Figura 4-3 PoE verde



4.6 Configurarea Force PoE

Informații generale



După activarea forțată a PoE, portul va forța alimentarea dispozitivului alimentat, indiferent dacă dispozitivul conectat la port îndeplinește sau nu cerințele. Vă rugăm să rețineți acest lucru.

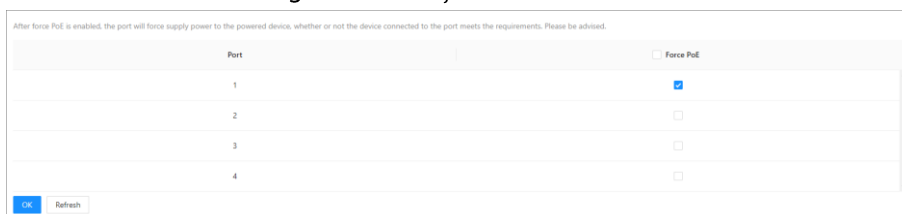
Procedură

Pasul 1 Selectați Gestionare PoE > Forțare PoE.

Pasul 2. Faceți clic pe portul corespunzător pentru a activa PoE forțat. 

Pasul 3. Faceți clic pe OK.

Figura 4-4 Forțare PoE



Port	Force PoE
1	☒
2	☐
3	☐
4	☐

4.7 Configurarea dispozitivului de supraveghere PoE

Informații generale

Cu funcția de supraveghere PoE activată, puteți monitoriza PD-ul și îl puteți menține online,

verificând starea dispozitivelor PD la fiecare 60 de secunde. Dacă nu există transmisie de date, portul PoE se va opri automat și va reporni.



Forțarea PoE și sistemul de supraveghere PoE nu pot fi activate simultan.

Procedură

Pasul 1 Selectați Gestionare PoE > Sistem de supraveghere PoE.

Pasul 2. Faceți clic pe portul corespunzător pentru a activa funcția de supraveghere PoE.

Pasul 3. Faceți clic pe OK.

Figura 4-5 Sistem de supraveghere PoE

Force PoE and PoE watchdog cannot be enabled at the same time.

Port	☐ PoE Watchdog
1	☐
2	☐
3	☐
4	☐

5 Securitate

5.1 Servicii de bază

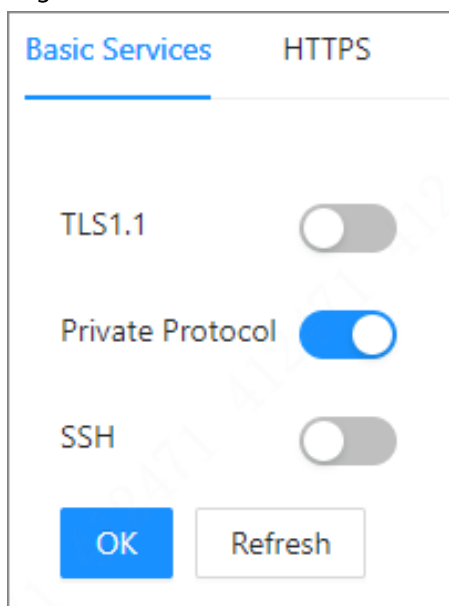
5.1.1 Configurarea serviciilor de bază

Protocolul TLS (Secure Transport Layer Protocol) este utilizat pentru a garanta confidențialitatea și integritatea datelor între două aplicații de comunicare. Acest protocol este format din două straturi: TLS Record și TLS Handshake. TLS1.1 utilizează un algoritm de criptare slab. Vă recomandăm să îl dezactivați.

Un protocol privat este un protocol nepublicat. Vă recomandăm să îl dezactivați.

SSH și Secure Shell sunt protocoale de securitate bazate pe nivelul aplicației. SSH este un protocol fiabil care oferă securitate pentru sesiunile de conectare la distanță și alte servicii de rețea. Utilizarea SSH poate preveni eficient scurgerile de informații în timpul administrării la distanță.

Figura 5-1 Servicii de bază



5.1.2 Configurarea HTTPS

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) este un serviciu bazat pe Transport Layer Security (TLS). HTTPS oferă servicii web, servicii de acces ONVIF și servicii de acces RTSP.

Procedură

Pasul 1 Selectați Securitate > HTTPS.

Pasul 2 (Opțional) În fila Servicii de bază, faceți clic pe pentru a activa TLS1.1 după cum este necesar, apoi faceți clic pe OK.



În mod implicit, pagina web acceptă doar TLS1.2. Dacă trebuie să utilizați TLS1.1, trebuie să activați TLS1.1 pe pagina web. Vă rugăm să rețineți că TLS1.1 prezintă riscuri de securitate. Vă recomandăm să dezactivați TLS1.1 pentru a evita riscurile neașteptate.

Pasul 3. În fila HTTPS, faceți clic pe pentru a activa HTTPS.

Pasul 4 Selectați un certificat pentru dispozitiv.

Pasul 5 Selectați Gestionare certificate și pagina va trece la pagina Certificat CA.



Pentru detalii, consultați "5.2 Configurarea certificatului CA".

Pasul 6 Faceți clic pe OK.

Figura 5-2 Configurați HTTPS

No.	Custom Name	Certificate Number	Validity Period	User	Issued by	Used by
1		38383233353635313239383...	2052-11-24 10:13:53		TS	HTTPS
2		38383233353635313239383...	2029-12-24 08:00:51	192.168.1.110	TS	

5.2 Configurarea Certificat CA

5.2.1 Instalarea certificatului dispozitivului

Un certificat de dispozitiv este o dovadă a statutului legal al dispozitivului. De exemplu, atunci când browserul accesează dispozitivul prin HTTPS, certificatul dispozitivului va fi verificat.

Procedură

Pasul 1 Selectați Securitate > Certificat CA > Certificat dispozitiv.

Pasul 2. În fila Certificat dispozitiv, faceți clic pe Instalare certificat dispozitiv.

Pasul 3 Selectați un mod de instalare, după cum este necesar.

Figura 5-3 Selectați modul de instalare

Step 1: Select installation mode.

☐ Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

☒ Apply for CA Certificate and Import (Recommended)

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

☐ Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

Next

Cancel

Pasul 4 Completați informațiile despre certificat, apoi faceți clic pe Creare și instalare certificat, Creare și descărcare și Importare și instalare.

Pasul 5 (Optional) Faceți clic pe Intrați în modul de editare pentru a edita Numele personalizat, apoi faceți clic pe Salvați configurația.

Figura 5-4 Editare certificat

No.	Custom Name	Certificate Num...	Validity Period	User	Issued by	Used by	Certificate Status	Download	Delete
1		323032313131...	2029-12-24 08:...	192.168.1.110	TS	HTTPS	Normal		

Operațiuni conexe

- Descărcați certificatul: Faceți clic pe
- Ștergeți certificatul: Faceți clic pe

5.2.2 Instalarea certificatelor CA de încredere

Informații generale

Un certificat CA de încredere este utilizat pentru a verifica statutul legal al unei gazde. De exemplu, un certificat CA de tip switch trebuie instalat pentru autentificarea 802.1x.



Acceptă doar instalarea certificatului CA subordonat.

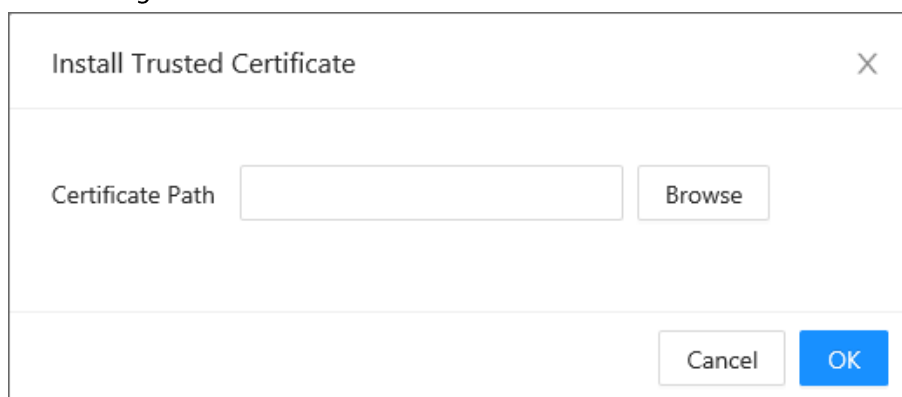
Procedură

Pasul 1 Selectați Securitate > Certificat CA.

Pasul 2. În fila Certificate CA de încredere, faceți clic pe Instalare certificat de încredere.

Pasul 3. Faceți clic pe Răsfoire, apoi pe OK.

Figura 5-5 Instalarea certificatului de încredere



Pasul 4 (Opțional) Faceți clic pe Intrare în modul de editare pentru a edita Numele personalizat, apoi faceți clic pe Salvare configurație.

Figura 5-6 Editare certificat

No.	Custom Name	Certificate N...	Validity Period	User	Issued by	Used by	Certificate St...	Download	Delete
1		6364336236...	2030-10-17...	TS	TS		Expired		

Operațiuni conexe

- Descărcați certificatul: Faceți clic pe
- Ștergeți certificatul: Faceți clic pe

5.3 Configurarea apărării împotriva atacurilor

5.3.1 Configurarea firewall-ului

Procedură

Pasul 1 Selectați Securitate > Apărare împotriva atacurilor.

Pasul 2. În fila Firewall, faceți clic pe Toate, iar toate adresele IP/MAC ale gazdelor sursă vor avea acces la toate porturile dispozitivului.

Faceți clic pe Listă permisă și numai gazdele sursă ale căror adrese IP/MAC se află în lista următoare vor avea permisiunea de a accesa porturile corespunzătoare ale dispozitivului, apoi faceți clic pe Adăugare pentru a adăuga gazde la Lista permisă.

Figura 5-7 Adăugați la lista permisă

The dialog box titled 'Add' contains the following elements:

- Add Mode:** A dropdown menu currently showing 'IP'.
- IP Address:** A text input field with three dots (.) as placeholders.
- All Device Ports:** A toggle switch that is currently turned on (blue).
- Buttons:** 'Cancel' and 'OK' buttons located at the bottom right.

Faceți clic pe Listă de blocare, iar gazda sursă corespunzătoare a adreselor IP/MAC listată nu va putea accesa porturile corespunzătoare ale dispozitivului prin conexiunea de rețea. Faceți clic pe Adăugare pentru a adăuga gazde la Lista de blocare.

Figura 5-8 Adăugați la lista de blocare

This dialog box is identical to the one in Figure 5-7, showing the 'Add' dialog for adding to the blocked list. It includes the same fields for 'Add Mode' (IP), 'IP Address' (.), and 'All Device Ports' (toggled on), with 'Cancel' and 'OK' buttons at the bottom.

Tabelul 5-1 Firewall

Parametru	Descriere
Toate	Toate adresele IP/MAC ale gazdelor sursă au permisiunea de a accesa toate porturile dispozitivului.
Listă permisă	Numai gazdele sursă ale căror adrese IP/MAC se află în lista următoare au permisiunea de a accesa porturile corespunzătoare ale dispozitivului.
Listă de blocare	Gazda sursă corespunzătoare listată pentru adresele IP/MAC nu are voie să acceseze porturile corespunzătoare ale dispozitivului.

Pasul 3. Faceți clic pe OK.

5.3.2 Configurarea atacului Anti-DoS

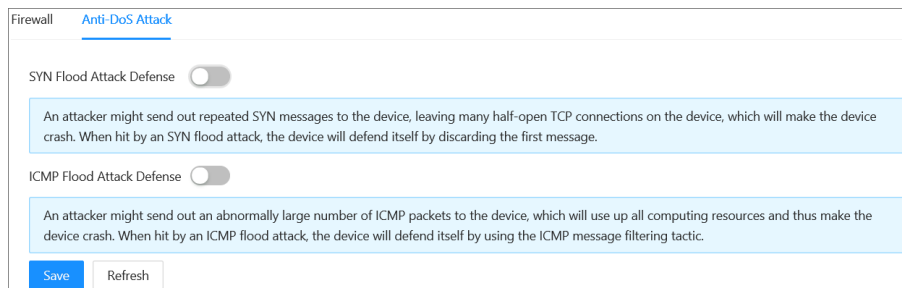
Procedură

Pasul 1 Selectați Securitate > Apărare împotriva atacurilor.

Pasul 2. În fila Anti-DoS Attack, faceți clic pe pentru a activa diferite funcții de apărare, după cum este necesar.

Pasul 3. Faceți clic pe Salvare.

Figura 5-9 Atacul Anti-DoS



5.4 Configurarea izolării porturilor

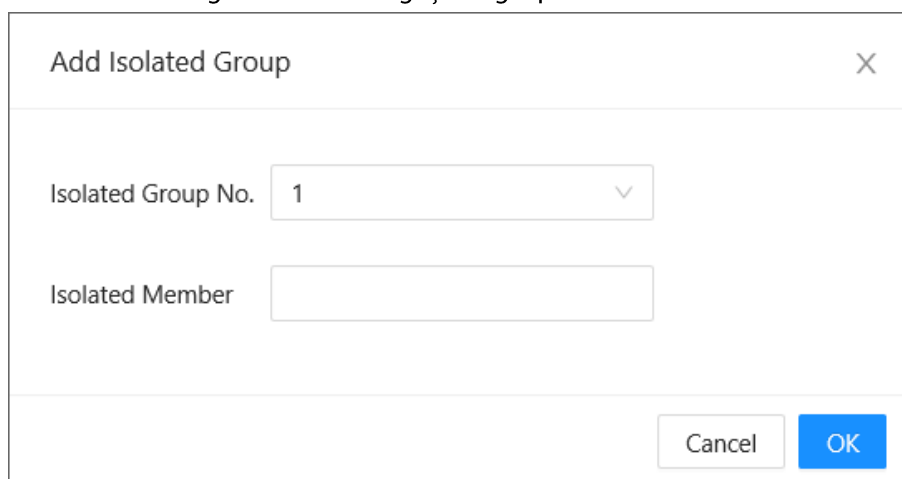
Izolarea porturilor are rolul de a realiza izolarea de nivel 2 între mesaje. Trebuie doar să adăugați Portul la grupul de izolare pentru a izola datele de nivel 2 între porturile din grupul de izolare. Funcția de izolare a porturilor oferă utilizatorilor o soluție de rețea mai sigură și mai flexibilă.

Procedură

Pasul 1 Selectați Securitate > Izolare port.

Pasul 2. Faceți clic pe Adăugare.

Figura 5-10 Adăugați un grup izolat



Pasul 3 Selectați Nr. grup izolat și Membru izolat, apoi faceți clic pe OK.

Operațiuni conexe

- Editați grupul izolat: Faceți clic pe .✎
- Ștergeți grupul izolat: Faceți clic pe .🗑

6 Politica de control

6.1 Configurarea priorității portului

Informații generale

În mod implicit, prioritatea 802.1p și prioritatea DSCP pentru o rețea VLAN vocală sunt 6, respectiv 46. Puteți configura dinamic prioritatea 802.1p și prioritatea DSCP pentru a planifica prioritățile pentru diferite servicii vocale.

- Prioritatea 802.1p este indicată de valoarea din câmpul PRI pe 3 biți din fiecare cadru VLAN 802.1Q. Acest câmp determină prioritatea de transmisie pentru pachetele de date atunci când un dispozitiv de comutare este congestionat.
- Valoarea DSCP este indicată de cei 6 biți din câmpul Tip de serviciu (ToS) din antetul pachetului IPv4. DSCP, ca semnalizare pentru DiffServ, este utilizat pentru garantarea QoS în rețelele IP. Controlerul de trafic de pe gateway-ul de rețea ia măsuri doar pe baza informațiilor transportate de cei 6 biți.

Procedură

Pasul 1 Selectați Politica de control > Prioritate port.

Pasul 2 Selectați dintre modul Prioritate și modul Încredere.



Modul de încredere include 4 tipuri de neîncredere: 802.1P, DSCP și DSCP și 802.1P.

Pasul 3. Faceți clic pe OK.

Figura 6-1 Configurați prioritatea portului

Port	Priority	Trust Mode
1	0	Untrust
2	0	Untrust
3	0	Untrust
4	0	Untrust
5	0	Untrust
6	0	Untrust
7	0	Untrust

OK Refresh

6.2 Configurarea tabelului de mapare a priorităților

Procedură

Pasul 1 Selectați Politica de control > Tabel de mapare a priorităților.

Pasul 2 Selectați DSCP > Prioritate locală sau 802.1p > Prioritate locală.

Pasul 3 Selectați Valoarea de ieșire.



Valoarea de intrare și valoarea de ieșire variază în funcție de moduri.

Pasul 4. Faceți clic pe OK.

Figura 6-2 Maparea priorităților

Input Value	Output Value
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1

6.3 Configurarea programării cozii

Informații generale

- PQ: Coadă cu prioritate. PQ programează pachetele în ordine descrescătoare a priorității. Pachetele din cozile cu o prioritate mai mică pot fi programate numai după ce toate pachetele din cozile cu o prioritate mai mare au fost programate.
- WRR: Weighted Round Robin. În planificarea WRR, dispozitivul planifică pachetele din cozi într-o manieră de interogare pe baza ponderii cozii. După o rundă de planificare, ponderile tuturor cozilor sunt reduse cu 1. Coadă a cărei pondere este redusă la 0 nu poate fi planificată.

Procedură

Pasul 1 Selectați Politica de control > Planificarea cozii.

Pasul 2 Selectați din algoritmul coadă.



În modul WRR, raportul de ponderare al cozii de prioritate este Queue0:Queue1:Queue2:Queue3=1:2:4:8.

Pasul 3. Faceți clic pe OK.

Figura 6-3 Planificarea cozii

Interface	Queue Algorithm	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Operation
		Weight	Weight	Weight	Weight	Weight	Weight	Weight	Weight	
1	SP									
2	SP									
3	SP									
4	SP									
5	SP									
6	SP									
7	SP									
8	SP									
9	SP									
10	SP									
11	SP									

Total 52 records < 1 2 3 > Go to Page

6.4 Configurarea limitei de viteză a portului

Procedură

Pasul 1 Selectați Politica de control > Limită de viteză a portului.

Pasul 2. Faceți clic pe Adăugare.

Figura 6-4 Adăugați limita de viteză a portului

Add Port Speed Limit

* Interface

* Direction

* CIR

Kbps Range: 16 - 100000

Cancel

OK

Pasul 3 Introduceți Interfața, Direcția și CIR-ul.



- Valorile Direcției includ Intrare și Ieșire.
- Regula de introducere pentru CIR: Interval de la 16 la 100000 și trebuie să fie un multiplu întreg al lui 16.

Pasul 4. Faceți clic pe OK.

6.5 Configurarea controlului furtunilor

Cadrele de difuzare din rețea sunt transmise continuu, ceea ce afectează buna comunicare și reduce considerabil performanța rețelei. Controlul furtunilor poate limita fluxurile de difuzare ale portului și poate elimina cadrele de difuzare odată ce fluxul depășește pragul specificat, ceea ce poate reduce riscul furtunilor de difuzare și poate asigura funcționarea

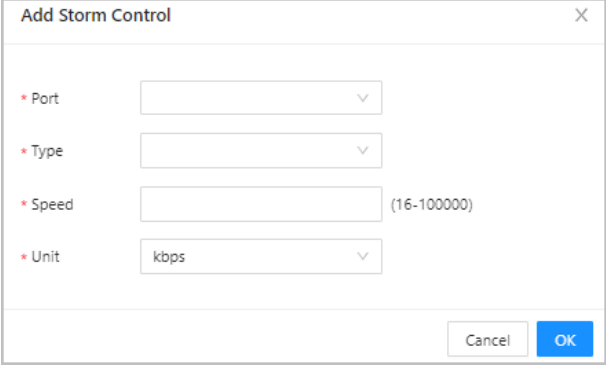
corectă a rețelei.

Procedură

Pasul 1 Selectați Politica de control > Control al furtunilor.

Pasul 2. Faceți clic pe Adăugare.

Figura 6-5 Adăugați controlul furtunilor



The screenshot shows a dialog box titled "Add Storm Control". It contains the following fields:

- Port:** A dropdown menu.
- Type:** A dropdown menu.
- Speed:** A text input field with the range "(16-100000)" displayed to its right.
- Unit:** A dropdown menu with "kbps" selected.

At the bottom right of the dialog are two buttons: "Cancel" and "OK".

Pasul 3 Introduceți portul, tipul și viteza.

Pasul 4. Faceți clic pe OK.

7 Autentificare

7.1 Configurarea 802.1x

802.1X este un protocol de autentificare a rețelei care deschide porturi pentru accesul la rețea atunci când o organizație autentifică identitatea unui utilizator și îl autorizează pentru accesul la rețea.

Procedură

Pasul 1. Faceți clic pe lângă Activare pentru a activa NAS (Network Attached Storage - Stocare conectată la rețea).

Pasul 2 Selectați din Stare port.



Starea include Automat, Forțat neautorizat și Forțat autorizat.

Figura 7-1 Configurarea 802.1x

Port	Port Status
1	Force Authorized
2	Force Authorized
3	Force Authorized
4	Force Authorized
5	Force Authorized
6	Force Authorized

Tabelul 7-1 Descrierea standardului 802.1x

Parametru	Descriere
Automat	Portul configurează automat starea în funcție de rezultatele autentificării.
Forțare neautorizată	● Portul este întotdeauna într-o stare neautorizată, iar utilizatorii nu au voie să se autentifice. ● Dispozitivul nu oferă servicii de autentificare pentru utilizatorii care accesează prin acest port.
Forțare autorizată	Portul este întotdeauna în starea autorizată, iar utilizatorii au voie să acceseze resursele rețelei fără autentificare.

Pasul 3. Faceți clic pe OK.

7.2 Configurarea razei

Informații generale

RADIUS (Remote Authentication Dial-In User Service) este un protocol comun pentru

realizarea AAA (Authentication, Authorization and Accounting).

RADIUS este un protocol de interacțiune informațională cu construcție distribuită și C/S.

Acesta poate proteja rețeaua de vizite neautorizate. Este utilizat în rețele care permit vizite la distanță, dar solicită o securitate mai mare. Definește formatul pachetului RADIUS și mecanismul de transmitere a mesajelor. Acesta stipulează utilizarea UDP ca protocol de nivel de transport pentru a încapsula pachetul RADIUS.

La început, RADIUS era protocolul AAA exclusiv pentru utilizatorii dial-up. Odată cu dezvoltarea accesului utilizatorilor, RADIUS se adaptează la diverse tipuri de acces, inclusiv acces Ethernet și acces ADSL. Accesează serverul prin autentificare și autorizare și colectează înregistrări privind utilizarea sursei de rețea prin intermediul contabilizării.

Procedură

Pasul 1 Selectați Autentificare > RADIUS.

Figura 7-2 RAZĂ



The screenshot shows a configuration window for RADIUS. At the top, there is a label 'Re-authentication Times' with a value of '3'. Below this, there is a table with four columns: 'Port', 'IP', 'Secret Key', and 'Operation'. The table is currently empty. There are 'OK' and 'Add' buttons at the top left of the table area.

Pasul 2. Faceți clic pe Adăugare.

Figura 7-3 Adăugați RADIUS



The screenshot shows a dialog box titled 'Add RADIUS'. It contains three input fields: 'IP Address' (with a placeholder 'x . x . x'), 'Port' (with a placeholder 'x' and a range '(0~65535)'), and 'Secret Key' (with a placeholder 'x'). At the bottom right, there are 'Cancel' and 'OK' buttons.

Pasul 3 Setati adresa IP, portul și cheia.

Pasul 4. Faceți clic pe OK.