GE
Grid Solutions

GE Reason S20

Промислові керовані Ethernet-комутатори

Технічне керівництво

Версія платформи апаратних засобів S20: C
Версія платформи програмного забезпечення S20 : 07
Посилання на публікацію: GE_Reason_S20_TM_EN_4.6_HWC

imagination at work

ЗМІСТ

Список рисунків

Список таблиць

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 1: Вступ

Цей розділ містить загальну інформацію про технічне керівництво та вступну частину до пристрою, що описується у цьому технічному керівництві.

1 Передмова

Це технічне керівництво містить функціональний та технічний опис пристрою GE Reason S20, а також повний набір інструкцій щодо використання пристрою. Рівень викладення матеріалу у даному керівництві передбачає, що користувач вже є обізнаним з апаратурою захисту та має досвід роботи у цій сфері. Опис принципів і теорії обмежується обсягом, що є необхідним для розуміння даного виробу.
Ми намагалися зробити це керівництво точним, всеосяжним та максимально зручним для користувача. Проте ми не можемо гарантувати, що воно не містить помилок. Ми також не можемо заявити, що його не можна покращити. Тому ми будемо дуже вдячні за надану інформацію, якщо ви виявите будь-які помилки або маєте будь-які пропозиції щодо вдосконалення. Наша політика полягає в тому, щоб надати вам необхідну інформацію для безпечного визначення, проектування, монтажу, налагодження та введення в експлуатацію, обслуговування та, зрештою, утилізації цього виробу. Ми вважаємо, що це керівництво містить усю необхідну інформацію, але якщо ви вважаєте, що вам потрібні додаткові відомості, будь ласка, зв'яжіться з нами.
Усі відгуки слід надсилати в наш контактний центр за наступною URL-адресою:
http://www.gegridsolutions.com/contact.htm

1.1 Цільова аудиторія

Це керівництво призначене для всіх спеціалістів, відповідальних за монтаж, налагодження та введення в експлуатацію, обслуговування, виявлення та усунення несправностей або експлуатацію будь-якого з виробів у межах зазначеного асортименту. Цільова аудиторія включає в себе персонал з монтажу та налагодження, відповідальний за роботу виробу. Рівень викладення матеріалу у цьому керівництві передбачає, що персонал з виконання монтажу та пусконалагоджувальних робіт має відповідні знання щодо поводження з електронним обладнанням та поглиблені знання у сфері комутаторів Ethernet та пов’язаного обладнання.

1.2 Акроніми та абревіатури

BC	Граничний годинник (Boundary Clock)
BPDU	Блок протокольних даних моста

CSMA/CD	Множинний доступ з контролем несучої і виявленням конфліктів
CIST	Протокол єдиного кістякового дерева
CPU	Центральний процесор (ЦП)
CoS	Клас обслуговування
CLI	Інтерфейс командного рядка
МЕК (IEC) TR 61850-90-4	Комунікаційні мережі та системи для автоматизації електроенергетичних підприємств. Частина 90-4. Настанови щодо мережних технологій.
UTC	Всесвітній (універсальний) скоординований час
DDM	Контроль цифрової діагностики
DEI	Індикатор допустимості видалення
DST	Перехід на літній час
DSCP	Точка коду диференційованих послуг
DNS	Сервер доменних імен
DHCP	Протокол динамічної конфігурації вузла
DPL	Рівень пріоритету відкидання
EMC	Електромагнітна сумісність
E2E	Наскрізний механізм вимірювання затримок (End-to-end)
ECN	Явне повідомлення про перевантаження
FCS	Послідовність перевірки кадра
FDDI	Волоконно-оптичний розподілений інтерфейс передачі даних
FE	Швидкий Ethernet
Гбіт/с (Гбіт/с)	Гігабіт на секунду
GE	General Electrics (якщо йдеться про Reason S20) або Гігабітний Ethernet (якщо йдеться про Ethernet-порт RJ45)
GPS	Глобальна система навігації і визначення положення
GMC	"Гросмейстерський" (головний) годинник (Grandmaster Clock)
HRC	Висока вимикальна здатність
HMI	Людино-машинний інтерфейс
HTTP	Протокол передачі гіпертекстових даних
HTTPS	Протокол захищеної передачі гіпертекстової інформації
GOOSE	МЕК 61850 - Загальна об'єктно-орієнтована подія на підстанції
SV	МЕК 61850 - Вибіркові величини
МЕК (IEC) 61850-9-2LE	Настанова з впровадження цифрового інтерфейсу для вимірювальних трансформаторів з використанням МЕК 61850-9-2
IEEE	Інститут інженерів з електротехніки та електроніки

IED	Інтелектуальний електронний пристрій
IEC	Міжнародна електротехнічна комісія
ICMP	Міжмережевий протокол керуючих повідомлень
IGMP	Протокол керування груповою передачею даних в мережах
IP	Інтернет-протокол
IPMC	Багатоадресна IP-передача
LACP	Протокол керування агрегуванням каналів
LED	Світловипромінювальний діод (світлодіод)
LLDP	Протокол виявлення топології канального рівня
LAN	Локальна комп'ютерна мережа
LVD	Директива ЕС щодо низьковольтного обладнання
MIB	База керуючої інформації, яка використовується протоколом SNMP
MMS	Специфікація виробничих повідомлень
MAC	Керування доступом до середовища передачі даних
Мбіт/с (Мбіт/с)	Мегабіт на секунду
MCB	Малогабаритний автоматичний вимикач
MLD	Виявлення слухачів багатоадресної передачі
MSTI	Екземпляр Протоколу кістякового дерева (STP)
MSTP	Протокол множинних кістякових дерев (IEEE 802.1Q)
NTP	Мережевий протокол часу
NC	Нормально замкнений
NO	Нормально розімкнений
OSI	Модель взаємодії відкритих систем
OSPF	Протокол вибору доступного найкоротшого маршруту
P2P	Механізм вимірювання затримок між рівноправними вузлами (Peer-to-peer)
PPE	Засоби індивідуального захисту
PDC	Концентратор синхрофазорних даних
PDU	Блоки даних протоколу
PMU	Пристрій синхронізованих векторних вимірювань
PVID	VLAN-ідентифікатор порту
PTP	Протокол точного часу (IEEE 1588)
PCP	Кодова точка пріоритету
PCT	Клема захисного провідника
PPS	Імпульсів на секунду

QCE	Запис керування QoS
QCL	Список керування QoS
QoS	Якість обслуговування (якість послуг з передачі даних, що надаються)
R&TTE	Радіо- та телекомунікаційне термінальне обладнання
RSTP	Високошвидкісний протокол кістякового дерева (IEEE 802.1D)
RADIUS	Сервіс віддаленої автентифікації користувачів
RMON	Віддалений мережевий моніторинг
RIP	Протокол інформації маршрутизації
RFC	Запит коментарів (документ із серії специфікацій та стандартів "Request for Comments")
SFP	Компактний модульний трансивер
SSH	Мережевий протокол типу SSH ("безпечна оболонка")
SSL	Рівень захищених сокетів (криптографічний протокол)
VLAN ID	Див. VID
VRRP	Протокол резервування віртуальних маршрутизаторів
SNMP	Простий протокол мережевого керування
STP	Протокол кістякового дерева (IEEE 802.1D)
TACACS+	Система керування доступом для контролера доступу до терміналу "плюс"
TCP	Протокол керування передачею
TC	Прозорий годинник (Transparent Clock)
ToS	Тип обслуговування
USB	Універсальна послідовна шина
UTP	Неекранована вита пара
UDP	Протокол датаграм користувача
VLAN	Віртуальна локальна комп'ютерна мережа (IEEE 802.1Q)
VID	VLAN-ідентифікатор
WRED	Виважене довільне раннє виявлення
WAMS	Система моніторингу перехідних режимів

2 Функціонал виробу

Лінійка комутаторів Ethernet GE Reason S20 розроблена для роботи у несприятливих умовах навколишнього середовища, таких як енергосистеми та промислове застосування, забезпечуючи всі елементи, необхідні в мережі цифрових підстанцій згідно з МЕК 61850, включаючи обов'язковий IEEE 1588v2 (PTP). Завдяки використанню пристрою Reason S20, комутація пакетів між інтелектуальними електронними пристроями (IED) є гнучкою, надійною та стійкою, навіть у ситуаціях, коли потребується маршрутизація.

Reason S20 може забезпечувати відокремлення трафіку Вибіркових величин (МЕК 61850-9-2LE), передачу повідомлень GOOSE, реалізацію протоколу синхронізації PTP та інших повідомлень з використанням віртуальних локальних мереж (VLAN). Моніторинг трафіку і портів комутатора здійснюється за допомогою протоколу SNMP, а топології на основі петель (шлейфів), такі як кільцева топологія, можуть контролюватися і переналаштовуватися за допомогою протоколу RSTP (IEEE 802.1D).

Передача даних з комутацією пакетів в комутаторах повністю виконується апаратними засобами, що забезпечує швидкість реагування і максимальну надійність навіть при взаємодії пристроїв IED з використанням різних інтерфейсів і швидкостей передачі даних.

Налаштування комутаторів може здійснюватися за допомогою інтерактивного режиму текстових команд (SSH та Telnet) або у зручному для користувача графічному середовищі (HTTP або HTTPS) з власною або віддаленою автентифікацією (RADIUS та TACACS +). Збір статистичних даних можна виконувати за допомогою протоколу SNMP v2/v3, з можливістю інтеграції PulseNet у якості програмного забезпечення для керування мережею (NMS). Інтерфейсами зв'язку є порт Ethernet або виділений порт USB-2.0.

Для критично важливих варіантів застосування існує можливість забезпечення додаткового (опційного) резервного джерела живлення для ще більшої тривалості роботи та підвищеної надійності. Пристрій Reason S20 обладнано реле з сухими контактами для сигналізації про перехід у безпечний режим (failsafe) для системи диспетчерського керування у випадку втрати зв’язку з інтерфейсом або втрати джерел живлення обладнання.

3 Функціональний опис

Модель S2020

S2020 – це найбільш економічно ефективне рішення, що пропонує високу щільність портів Ethernet у форм-факторі 1U для зручності монтажу у стійці. Ця модель підтримує до 5 модулів з 4 портами для кожного і дозволяє реалізувати конфігурації до 20 швидких портів Ethernet (100 Мбіт/с) або до 4 гігабітних портів плюс 16 швидких портів Ethernet.

- До 5 модулів по 4 порти Ethernet на кожен;
- 1 модуль може бути гігабітним або швидким Ethernet, решта 4 повинні бути швидкими Ethernet.
- Гігабітні/швидкі Ethernet-модулі доступні з мідними портами RJ45 або SFP;
- Мідні інтерфейсні модулі мають роз'єми RJ45 (Cat5e) для 10/ 100BASE-TX або 10/100/1000BASE-TX з автоматичним узгодженням та автоматичною обробкою при інверсії полярності (HP Auto-MDIX);
- Оптичні інтерфейси SFP з роз'ємами LC, багатомодові для коротких відстаней та одномодові для відстані до 120 км;
- Інтерфейси SFP RJ45 10/100BASE-TX/1000BASE-T;
- Функції рівня 3 та IEEE 1588v2 PTP можуть бути оновлені за допомогою файлу ліцензії.

Модель S2024

S2024 – це преміальна модель, яка забезпечує повну функціональність гігабітного Ethernet-комутатора. Ця модель підтримує до 24 портів, реалізованих 6 інтерфейсними модулями по 4 порти на кожен. Механічна конструкція 1U ідентична моделі S2020.

- До 6 гігабітних модулів по 4 порти Ethernet на кожен;
- Гігабітні/швидкі Ethernet-модулі доступні з мідними портами RJ45 або SFP;
- Мідні інтерфейсні модулі мають роз'єми RJ45 (Cat5e) для 10/ 100BASE-TX або 10/100 / 1000BASE-TX з автоматичним узгодженням та автоматичною обробкою при інверсії полярності (HP Auto-MDIX);
- Оптичні інтерфейси SFP з роз'ємами LC, багатомодові для коротких відстаней та одномодові для відстані до 120 км;
- Інтерфейси SFP RJ45 10/100BASE-TX/1000BASE-T;
- Функції рівня 3 та IEEE 1588v2 PTP можуть бути оновлені за допомогою файлу ліцензії.

Синхронізація часу

- Комутатори S20 відповідають стандарту IEEE 1588 v2, за ліцензуванням, на всіх портах;
- Функціонування в якості IEEE 1588v2 прозорого (TC) або граничного (BC) годинника;
- Функціонування в якості клієнта NTP;
- Функціонування в якості NTP-сервера з використанням джерела часу на основі IEEE 1588v2 PTP, NTP або внутрішнього годинника.

Висока стійкість до зовнішніх завад (EMI)

- Відповідність стандарту МЕК 61000-4;
- Відповідність стандарту МЕК 60255-5;
- Відповідність стандарту МЕК 60068-2.

Передача даних з комутацією пакетів

- Передача даних з комутацією пакетів здійснюється повністю апаратними засобами;
- Автоматичне самонавчання з автоматичним узгодженням та виявленням/ обробкою інверсії полярності на мідних портах;
- Формування та автоматичне керування топологіями на основі петель за допомогою протоколів STP (IEEE 802.1D): STP, RSTP та MSTP;
- Передача тільки достовірних пакетів (режим передачі даних з проміжним накопиченням);
- Надання підтримки VLAN (IEEE 802.1Q) з незалежним (IVL) або спільним (SVL) навчанням за допомогою апаратних засобів до 4.095 VLAN та 32.000 MAC-адрес;
- Класифікація якості обслуговування (QoS) з 512 входами та 8 лініями пріоритету на порт, із суворим або зваженим пріоритетом;
- Робота в режимі маршрутизації, статичної або динамічної, з використанням RIP v1/2 або OSPF;
- Підтримка IPv4 та IPv6 у режимах широкомовної, багатоадресної та одноадресної передачі;
- Підтримує IGMP v2/v3 та MLD v1/v2;
- Виявлення та контроль "лавини" у режимах широкомовної, багатоадресної та одноадресної передачі.

Керування

- Інтеграція мережевого керування (NMS) із програмним забезпеченням PulseNet;
- Налаштування в текстовому режимі по безпечному з'єднанню (SSH);
- Налаштування в графічному режимі по безпечному з'єднанню (HTTPS);

- Автентифікація та власна або віддалена авторизація (RADIUS та TACACS+);
- Віддалений моніторинг за допомогою RMON;
- Виділений порт налаштувань конфігурації - це USB 2.0;
- Збір статистичних даних про використання за допомогою внутрішнього агента.

SNMP v3

- Дзеркальне відображення трафіку для моніторингу.

Реле сигналізації безпечного режиму

- Нормально розімкнений (NO) і нормально замкнений (NC) сухі контакти;
- Кілька налаштовуваних аварійних сигналів.

Варіанти монтажу

- Знімний фіксатор для стандартної 19-дюймової стійки та висота 1U обладнання;
- Роз'єми інтерфейсу на задній панелі корпусу.

Блоки живлення

- Внутрішні блоки живлення;
- Доступне резервне живлення.

Робоча температура

- від -40 °C до +85 °C (16 годин) з природною конвекцією повітря (без вентилятора).

4 Основні характеристики

- Комутаційна здатність 68 Гбіт/с;
- Автоматичне навчання, автоматичне узгодження та автоматичне виявлення/усунення полярності на мідних портах (роз'єми RJ45);
- Комутація пакетів у режимі передачі з проміжним накопиченням;
- Функціональні можливості IP-маршрутизації: Статична, RIP та OSPF;
- VRRP для усунення єдиної точки відмови в статичних маршрутизованих середовищах;
- Підтримка протоколів IPv4 та IPv6 (багатоадресна, одноадресна та широкомовна передачі);
- Виявлення та керування штормами (багатоадресні, одноадресні та широкомовні типи штормів);
- Функції кібербезпеки, готові до вимог NERC CIP v5;
- Налаштування текстового режиму SSH по безпечному з'єднанню;
- Налаштування графічного режиму HTTPS по безпечному з'єднанню;
- Власна та віддалена автентифікація та авторизація за допомогою RADIUS та TACACS+;
- Віддалений моніторинг за допомогою RMON;
- SNMP v1/v2c/v3;
- Керування багатоадресною IP-передачею через IGMP v2/v3 (для застосувань IPv4) та MLD v1/v2 (для застосувань IPv6);
- Розділення трафіку VLAN (IEEE 802.1Q), допускається до 4095 VLAN;
- Таблиця MAC-адрес до 8192 записів (динамічні та статичні);
- Призначення пріоритетів трафіку (до 8 рівнів Класу обслуговування) з використанням QoS (IEEE 802.1Q);

- Виявлення та захист від петель за допомогою протоколів кістякового дерева: STP, RSTP (IEEE 802.1D) та MSTP (IEEE 802.1Q);
- Захист і фільтрація Блоку даних протоколу мосту (BPDU) для запобігання зовнішнім завадам у мережах кістякового дерева;
- UltraRSTP забезпечує час відновлення після помилок менше 5 мс на один хоп (перехід), що відповідає вимогам МЕК 61850-90-4;
- Функція виявлення та захисту від петель без протоколів кістякового дерева;
- Внутрішня синхронізація годинника за допомогою головного (grandmaster) годинника 1588v2 або до 5 серверів часу NTP;
- Апаратна сумісність з IEEE 1588v2 (Протокол точного часу – PTP) на всіх портах;
- Робота в якості NTP-сервера з використанням IEEE 1588v2 як джерела часу;
- Порт зв'язку USB 2.0 для локальної конфігурації;
- Реле з сухими контактами для зовнішньої сигналізації переходу у безпечний режим.

5 Відповідність

Пристрій пройшов серію комплексних випробувань та процедур сертифікації, щоб забезпечити та підтвердити його сумісність на усіх цільових ринках. Детальний опис цих критеріїв міститься у розділі "Технічні характеристики".

5.1 Відповідність стандартам

Відповідність Директиві ЄС щодо електромагнітної сумісності та Директиві ЕС щодо низьковольтного обладнання продемонстрована шляхом самостійної сертифікації на відповідність міжнародним стандартам.

CE

Визнання UL 60950-1 продемонстроване сертифікатом UL та ярликом.

c UL us

Крім цього, S20 відповідає:

- МЕК 60255-27: 2013 щодо вимог безпеки, продемонстрованих лабораторними типовими випробуваннями;
- МЕК 60255-26: 2013 щодо вимог до електромагнітної сумісності (EMC), продемонстрованих лабораторними типовими випробуваннями;
- МЕК 61850-3, видання 2: 2013 щодо вимог до електромагнітної сумісності, захисту навколишнього середовища та безпеки, продемонстрованих лабораторними типовими випробуваннями;
- IEEE 1613 та IEEE 1613.1 щодо вимог до електромагнітної сумісності, продемонстрованих лабораторними типовими випробуваннями;
- Директиві RoHS 2011/65/ЄС зі змінами, внесеними згідно з Директивою (ЄС) 2015/863;

- R&TTE – Директива 99/5/ЕС щодо радіо- та телекомунікаційного термінального обладнання. Відповідність демонструється дотриманням як Директиви щодо електромагнітної сумісності (EMC), так і Директиви щодо низьковольтного обладнання, до рівня нульової напруги.

5.2 Безпечність пристрою

Для визначення відповідності використовували стандарт МЕК 60255-27: 2013.

Клас захисту

Клас захисту I згідно з МЕК 60255-27: 2013.

Категорія встановлення

Категорія встановлення III (Категорія перенапруги III) згідно з МЕК 60255-27: 2013.

6 Попередження щодо інформаційної безпеки

S20 являє собою цифровий пристрій, призначений для встановлення та експлуатації у промислових середовищах і на енергетичних підстанціях, та підключення до захищених приватних мереж. S20 не слід підключати до загальнодоступного Інтернету. Компанія GE наполегливо рекомендує користувачам захищати свої цифрові пристрої за допомогою стратегії глибокоешелонованого захисту своїх пристроїв, мережі, систем та інтерфейсів від загроз у сфері кібербезпеки. Це включає, але не обмежується цим, розміщення цифрових пристроїв у межах периметра системи мережевої безпеки, розгортання та підтримку засобів керування доступом, моніторинг виявлення мережевих атак, інструктаж щодо заходів і правил безпеки, політику у сфері безпеки, сегментацію мережі та брандмауери, надійне та активне керування паролями, шифрування даних, антивіруси та інші застосовні технології зниження ризиків. GE Grid Solution може також час від часу надавати користувачам додаткові вказівки і рекомендації щодо S20 та загроз або вразливостей у сфері кібербезпеки. Користувачі несуть виключну відповідальність за встановлення та експлуатацію пристрою S20 з урахуванням можливостей щодо його кібербезпеки, контексту безпеки, а також інструкцій та рекомендацій, що надаються користувачеві стосовно S20. Користувачі беруть на себе всі ризики та відповідальність, пов'язані з пошкодженнями або збитками, понесеними у зв'язку з будь-якими випадками порушення інформаційної безпеки.

7 Коди замовлення S20

Варіанти	Номер замовлення																
	1-3	4-5	6	7	8	9	10	11	12	13	14	15	16	17-18	19
Тип моделі															
Промисловий керований Ethernet-комутатор S20															
Кількість портів															
До 20 портів (4х гігабітних)		20													
До 24 гігабітних портів		24													
Джерело живлення 1															
24-48 В пост. струму**			1												
125-250 В пост. струму / 110-240 В змін. струму			3												
Джерело живлення 2															
24-48 В пост. струму**				1											
125-250 В пост. струму / 110-240 В змін. струму				3											
Не встановлено				X											
Варіанти монтажу															
19" Монтаж у стійці / Монтаж на задній панелі					P										
Функціональні можливості програмного забезпечення (Ліцензування)															
Стандартна комутація пакетів Рівня 2 (на основі MAC-адресації)						2									
Поліпшена комутація пакетів Рівня 2 і Рівня 3 (на основі MAC-адресації та IP-адресації)						3									
Підтримка PTP (Ліцензування)															
З підтримкою PTP (IEEE 1588v2)							P								
Без підтримки PTP (IEEE 1588v2)							X								
Інтерфейсний модуль 1															
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти								A							
Чотири слоти для SFP-трансиверів (до 1 Гбіт/с)								B							
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км								C							
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км								D							
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км								E							
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км								F							
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км								H							
Чотири RJ45 мідних 10/100BASE-TX								I							
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T 10/100BASE-TX/1000BASE-								J							
Два 1 Гбіт/с RJ45 SFP-трансивери 10/100BASE-TX/1000BASE-T Ethernet-порти + Два 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км								K							
Два 1 Гбіт/с RJ45 SFP-трансивери 10/100BASE-TX/1000BASE-T Ethernet-порти + Два 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км								L							
Два 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км + Два 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км								M							
Інтерфейсний модуль 2															
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти*									A						
Чотири слоти для SFP-трансиверів (До 1 Гбіт/с у моделі з 24 портами / До 100 Мбіт/с у моделі з 20 портами)									B						
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км*									C						
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км*									D						
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км*									E						
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км*									F						
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км									H						
Чотири RJ45 мідних 10/100BASE-TX									I						
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T*									J						
Не встановлено									X						
Інтерфейсний модуль 3															
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти*										A					
Чотири слоти для SFP-трансиверів (До 1 Гбіт/с у моделі з 24 портами / До 100 Мбіт/с у моделі з 20 портами)										B					
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км*										C					
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км*										D					
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км*										E					
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км*										F					
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км										H					
Чотири RJ45 мідних 10/100BASE-TX										I					
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T*										J					
Не встановлено										X					
Інтерфейсний модуль 4											A				
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти*											B				
Чотири слоти для SFP-трансиверів (До 1 Гбіт/с у моделі з 24 портами / До 100 Мбіт/с у моделі з 20 портами)											C				
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км*											D				
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км*											E				
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км*											F				
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км*											H				
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км											I				
Чотири RJ45 мідних 10/100BASE-TX											J				
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T*											X				
Не встановлено															
Інтерфейсний модуль 5												A			
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти*												B			
Чотири слоти для SFP-трансиверів (До 1 Гбіт/с у моделі з 24 портами / До 100 Мбіт/с у моделі з 20 портами)												C			
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км*												D			
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км*												E			
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км*												F			
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км*												H			
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км												I			
Чотири RJ45 мідних 10/100BASE-TX												J			
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T*												X			
Не встановлено															
Інтерфейсний модуль 6 (Доступно тільки у моделі з 24 портами)													A		
Чотири 1 Гбіт/с RJ45 мідних 10/100BASE-TX/1000BASE-T Ethernet-порти*													B		
Чотири слоти для SFP-трансиверів (до 1 Гбіт/с)*													C		
Чотири 1 Гбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 1000BASE-SX Ethernet до 0,5 км*													D		
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-LX Ethernet до 20 км*													E		
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 40 км*													F		
Чотири 1 Гбіт/с SFP-трансивери LC-типу з одномодовим оптоволокном 1000BASE-ZX Ethernet до 80 км*													H		
Чотири 100 Мбіт/с SFP-трансивери LC-типу з багатомодовим оптоволокном 100BASE-FX Ethernet до 2 км*													I		
Чотири RJ45 мідних 10/100BASE-TX 10/100BASE-TX/1000BASE-T*													J		
Чотири 1 Гбіт/с RJ45 SFP-трансивери Ethernet 10/100BASE-TX/1000BASE-T*													J		
Не встановлено													X		
Версія вбудованого ПЗ ("прошивки")															
Номер версії Вбудованого ПЗ 07														07	
Суфікс апаратних засобів															
Версія апаратних засобів C															C
Версія апаратних засобів B															B

* Доступно тільки у моделі з 24 портами

** На даний час доступно тільки у Версії апаратних засобів B

Випуск I

Розділ 2: Інформація про техніку безпеки

Цей розділ містить інформацію про безпечне поводження з обладнанням. Обладнання потребує належного монтажу та поводження, щоб підтримувати його в безпечному стані та завжди забезпечувати безпеку персоналу. Ви повинні ознайомитися з інформацією, що міститься в цьому розділі, перед розпакуванням, монтажем, налагодженням і введенням в експлуатацію або обслуговуванням обладнання.

1 Охорона праці та здоров'я

Персонал, який працює з обладнанням, повинен бути належним чином ознайомлений зі змістом цієї інформації про техніку безпеки.
Під час експлуатації електричного обладнання певні частини обладнання знаходяться під небезпечною напругою. Неправильне використання обладнання та невиконання вимог попереджувальних надписів створюють небезпеку для персоналу.
Тільки кваліфікований персонал може працювати з обладнанням або здійснювати його експлуатацію. До кваліфікованого персоналу належать особи, які:

- є обізнаними з монтажем, налагодженням та експлуатацією обладнання та системи, до якої воно підключене;
- є обізнаними з прийнятими правилами техніки безпеки та мають повноваження на подачу напруги та знеструмлення обладнання у належний спосіб;
- пройшли навчання з догляду та використання захисних засобів відповідно до правил техніки безпеки;
- пройшли навчання щодо порядку дій у надзвичайних ситуаціях (надання першої невідкладної допомоги).

Документація містить інструкції з монтажу, налагодження та експлуатації обладнання. Проте, вона не може охоплювати всі ймовірні обставини. У разі виникнення запитань чи проблем, не вживайте жодних дій без належного дозволу. Будь ласка, зв'яжіться з вашим місцевим офісом з продажу та запитайте необхідну інформацію.

Користувач несе відповідальність за встановлення, експлуатацію та використання обладнання за призначенням у спосіб, визначений виробником. Будь ласка, уважно ознайомтесь із наступними розділами, щоб переконатися, що інструкції з техніки безпеки дотримуються належним чином.

2 Символи

У цьому керівництві використовуються наступні символи. Ви також побачите ці символи на частинах обладнання.

Увага: Зверніться до документації на обладнання. Невиконання цієї вимоги може призвести до пошкодження обладнання.

Ризик ураження електричним струмом

Клема захисного (заземлювального) провідника

Змінний струм

Постійний струм

Інструкції щодо вимог з утилізації

3 Монтаж, введення в експлуатацію та обслуговування

3.1 Небезпека при виконанні вантажопідіймальних робіт

Підвищений травматизм спричиняють:

- Підйом важких предметів;
- Неправильне підіймання вантажів;
- Штовхання або перетягання важких предметів;
- Постійне навантаження на ті самі м'язи.

Виконайте ретельне планування, виявіть можливі небезпеки і визначте, яким чином краще переміщувати виріб. Розгляньте інші способи переміщення вантажу, щоб уникнути ручної праці. Застосовуйте правильні методи підіймання та засоби індивідуального захисту (ЗІЗ) для зниження ризику травматизму.

3.2 Небезпека ураження електричним струмом

Увесь персонал, залучений до монтажу, налагодження та введення в експлуатацію або обслуговування цього обладнання, має бути обізнаним з процедурами належного виконання робіт.

Перед монтажем, налагодженням та введенням в експлуатацію, або обслуговуванням обладнання ознайомтеся з документацією на обладнання.

Завжди використовуйте обладнання згідно із зазначеними вимогами. Невиконання таких вимог ставить під загрозу захист, який забезпечує обладнання.

Знімання панелей або кришок обладнання може призвести до розкривання небезпечних струмопровідних частин. Не торкайтесь обладнання, поки не буде вимкнене живлення. Будьте обережними, якщо розблоковано доступ до задньої панелі обладнання.

Перед виконанням робіт на клемних колодках ізолюйте обладнання.

Використовуйте підходящий захисний бар'єр для приміщень з обмеженим простором, де існує ризик ураження електричним струмом через відкриті клеми.

Від'єднайте живлення перед розбиранням. Розбирання обладнання може призвести до оголення чутливої електронної схеми. Для запобігання пошкодженню обладнання вживайте відповідні запобіжні заходи захисту від електростатичного розряду (ESD).

НІКОЛИ не втручайтеся у оптичні волокна або оптичні вихідні з'єднання. Завжди використовуйте вимірювачі оптичної потужності, щоб визначити справний стан або рівень сигналу.

Під час тестування конденсатори можуть залишитися зарядженими до небезпечних рівнів напруги. Розрядіть конденсатори шляхом зниження випробувальної напруги до нуля перед від'єднанням випробувальних проводів.

Якщо обладнання використовується у спосіб, не передбачений виробником, захист, який забезпечується обладнанням, може бути порушений.

Експлуатуйте обладнання в межах зазначених гранично допустимих електричних параметрів та умов навколишнього середовища.

Перед очищенням обладнання, переконайтеся у відсутності приєднань під напругою. Використовуйте безворсу тканину, змочену чистою водою.

Інтегрування обладнання у системи не повинне впливати на його нормальне функціонування.

Пристрій було сертифіковано за робочих умов, описаних у стандартах, зазначених у Розділ 8: Технічні характеристики". Використання обладнання в умовах, що відрізняються від зазначених у цьому керівництві, може негативно вплинути на його нормальну цілісність.

Усі роз'єми на задній панелі обладнання та SFP повинні бути приєднані, навіть якщо вони не використовуються, для того, щоб максимально забезпечити їх рівень захисту від проникнення пилу і вологи.

Ніколи не здійснюйте жодних маніпуляцій з посудинами для рідини поблизу обладнання навіть після його вимкнення.

Уникайте здійснення будь-яких модифікацій з проводкою панелі, коли система працює.

3.3 Вимоги до застосування запобіжників

Плавкий запобіжник з високою вимикальною здатністю (запобіжник типу HRC) з максимальним струмом 10 А і мінімальним постійним струмом 250 В може використовуватися для оперативного живлення (наприклад, запобіжник "Red Spot" типу NIT або TIA). Як альтернатива, може бути використаний малогабаритний автоматичний вимикач (MCB) типу C, 10 A, що відповідає вимогам МЕК 60947-1 та МЕК 60947-3.

Пристрої Reason містять внутрішній плавкий запобіжник для ланцюга живлення, доступ до якого є можливим тільки після відкриття виробу. Це не усуває вимоги щодо застосування зовнішніх запобіжників або використання MCB як зазначено вище. Внутрішні запобіжники мають наступні характеристики:

3,15 A, тип T, номінальна напруга 250 В

Моделі з джерелом живлення з низьким постійним струмом повинні живитися від джерела постійного струму для обладнання, що подається від вторинного ланцюга, ізольованого від мережі змінного/постійного струму подвійною або посиленою ізоляцією (наприклад: сертифіковане UL живлення ITE, що забезпечує подвійну або посилену ізоляцію).

3.4 З'єднання обладнання

Клеми, відкриті під час монтажу, налагодження та введення в експлуатацію і технічного обслуговування, можуть знаходитися під небезпечною напругою, якщо обладнання не є електрично ізольованим.

Затягніть затискні гвинти M3 роз'ємів високопродуктивних клемних колодок до номінального моменту затяжки 1,0 Нм.

Затягніть невипадні гвинти знімних (Euro) клемних колодок до моменту затяжки мінімум 0,5 Нм і максимум 0,6 Нм.

Завжди використовуйте ізольовані обтискні клеми для ланцюгів напруги.

Завжди використовуйте правильні обтискні клеми та інструмент відповідно до перерізу проводу.

Для забезпечення вимог до обладнання щодо захисту від ураження електричним струмом, інші пристрої, підключені до Reason S20, повинні мати клас захисту, що відповідає або вище Класу II.

На деяких виробах передбачені контакти сторожового таймера самодіагностики (Watchdog) для індикації робочого стану пристрою. Ми наполегливо рекомендуємо завести ці контакти за допомогою дротового з'єднання в автоматизовану систему підстанції для цілей сигналізації.

Виконайте заземлення обладнання за допомогою PCT (клеми захисного провідника), що входить у комплект поставки.

Не від'єднуйте PCT.

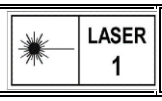
PCT іноді використовується для заземлення екранів кабелів. Завжди перевіряйте цілісність PCT після додавання або від'єднання таких заземлювальних з'єднань.

Користувач несе відповідальність за забезпечення цілісності будь-яких захисних провідникових з'єднань перед виконанням будь-яких інших дій.

З'єднання PCT повинне мати низьку індуктивність і бути максимально коротким.

Усі приєднання до обладнання повинні мати визначений потенціал. Попередньо змонтовані з'єднання, але які не використовуються, повинні бути заземлені або приєднані до загального групового потенціалу.

Перед монтажем електропроводки обладнання приділяйте особливу увагу електричним схемам. Завжди будьте впевнені, що приєднання виконані правильно, перш ніж подавати напругу на ланцюги.



Цей виріб оснащений лазерами Класу I.

3.5 Перелік контрольних перевірок перед подачею напруги

Перевірте значення напруги/полярність (паспортна табличка / документація на обладнання).

Перевірте параметри захисного плавкого запобіжника або малогабаритного автоматичного вимикача (MCB).

Перевірте цілісність з'єднання PCT.

Перевірте напругу зовнішньої проводки, переконайтеся, що вона підходить для передбаченого застосування пристрою.

3.6 Модернізація/Сервісне обслуговування

Не вставляйте або не виймайте модулі, друковані плати або плати розширення з обладнання під напругою, оскільки це може призвести до пошкодження обладнання. Також існує ризик для життя персоналу внаслідок дії небезпечних напруг.

Внутрішні модулі та вузли можуть бути важкими і мати гострі краї. Будьте обережні, коли вставляєте або витягаєте модулі з пристрою IED.

4 Виведення з експлуатації та утилізація

Перед виведенням з експлуатації, повністю ізолюйте джерела живлення обладнання (обидва полюси будь-якого джерела постійного струму). Вхід оперативного живлення може мати паралельно підключені конденсатори, які можуть залишатися зарядженими. Щоб уникнути ураження електричним струмом, розрядіть конденсатори за допомогою зовнішніх клем перед виведенням з експлуатації.

Уникайте утилізації обладнання шляхом спалення або скидання у водостоки. Утилізуйте обладнання безпечним, відповідальним та екологічно нешкідливим способом, а також, якщо це застосовно, відповідно до спеціальних норм і правил країни, в якій використовувалося обладнання.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 3: Керівництво з встановлення

1 Механічне виконання

Пристрій S20 монтується у 19-дюймовій стійці висотою 1U (44,45 мм) і глибиною 310 мм. Корпус виготовлений у вигляді безвентиляторної конструкції з попередньо обробленої сталі та пофарбований епоксидною фарбою.

Рис. 1: Механічне виконання S20

2 Розпакування

Обережно розпакуйте обладнання та переконайтесь, що все приладдя та кабелі прибрані, щоб вони не загубилися.
Перевірте вміст згідно з пакувальним листком. Якщо будь-який предмет із зазначеного вмісту відсутній, негайно зв'яжіться з компанією GE (див. контактну інформацію на початку цього керівництва).
Огляньте обладнання на наявність будь-яких пошкоджень під час транспортування. Якщо пристрій пошкоджено або він не працює, негайно повідомте транспортну компанію. Тільки вантажоодержувач (особа або компанія, яка отримує виріб) може подати позов проти перевізника щодо відшкодування випадкових збитків, пов'язаних з доставкою.
Ми рекомендуємо користувачеві зберегти оригінальні пакувальні матеріали для використання у разі необхідності перевезення або відвантаження обладнання в майбутньому.

3 Монтаж у стійці

Для підтримки цілісності обладнання, рівня захисту та забезпечення безпеки користувачів, пристрій Reason S20 повинен встановлюватися у закритій шафі із рекомендованим ступенем захисту оболонки/корпусу IP42 або вище. Під час звичайного використання пристрою повинна бути доступна тільки його передня панель.

Зовнішня шафа повинна забезпечувати безпеку з'єднань на задній панелі та бічних панелей обладнання від проникнення вологи та захищати від ударів, підтримуючи при цьому належний температурний режим та вміст вологи для пристроїв.

Пристрій Reason S20 спроектований для монтажу у стандартній 19-дюймовій стійці, і оскільки він не має вентилятора, тепло відводиться на корпус. Таким чином, рекомендується використовувати полиці стійки 1U (1,75 дюймів) незаповненими над кожним S20 для конвекції потоків повітря. Звичайний потік повітря, хоча і не є необхідним, поліпшить надійність при довгостроковій експлуатації.

Рис. 2: Виконання монтажу у стійці

4 Подача живлення

Доступні кілька варіантів джерел живлення, які можна вибрати в якості основного та/або резервного джерела живлення. Змішані джерела живлення в одному і тому ж обладнанні допускаються, тому уважно перегляньте маркувальні етикетки живлення, щоб визначити номінальний діапазон потужності кожного з них.

Для всіх підключень живлення слід використовувати ізольований вогнезахисний гнучкий кабель (типу BWF) з поперечним перерізом 1,5 мм², класу нагрівостійкості 70 °C (150 °F) та напругою ізоляції 750 В. Моделі з джерелом живлення з низьким постійним струмом повинні живитися від джерела постійного струму для обладнання, що подається від вторинного ланцюга, ізольованого від мережі змінного/постійного струму подвійною або посиленою ізоляцією (наприклад: сертифіковане UL живлення ITE, що забезпечує подвійну або посилену ізоляцію).

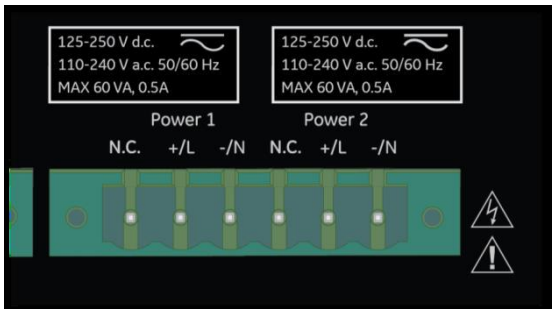


Рис. 3: Роз'єм живлення

Таблиця 1: Опис клем для приєднання до джерела живлення

Номер клеми	Опис	Використання
1	Не підключено (N.C.)	-
2	+/L	+/L підключається до плюсового провідника (+), якщо джерело живлення постійного струму, або до фазного провідника, якщо джерело живлення змінного струму.
3	-/N	-/N підключається до мінусового провідника (-), якщо джерело живлення постійного струму, або до нульового провідника, якщо джерело живлення постійного струму.
4	Не підключено (N.C.)	-
5	+/L	+/L підключається до плюсового провідника (+), якщо джерело живлення постійного струму, або до фазного провідника, якщо джерело живлення змінного струму. (Доступно тільки для обладнання, яке забезпечує резервне джерело).
6	-/N	-/N підключається до мінусового провідника (-), якщо джерело живлення постійного струму, або до нульового провідника, якщо джерело живлення постійного струму. (Доступно тільки для обладнання, яке забезпечує резервне джерело).

У цілях безпеки встановіть відповідний зовнішній вимикач або автоматичний вимикач для кожного джерела живлення S20 відповідно до його номінальної напруги, який може перервати як плюсовий (+/L), так і нульовий (-/N) проводи живлення.
В якості рекомендації розглядається зовнішній біполярний автоматичний вимикач 10 А, категорії С. Вимикач повинен мати вимикальну здатність не менше 25 кА і повинен відповідати МЕК 60947-2. Вимикач або автоматичний вимикач повинен бути встановлений у зручному і легкодоступному місці, також він не повинен переривати захисний заземлювальний провідник.

5 З’єднання заземлення

Захисний роз'єм заземлення, розташований на задній панелі обладнання, повинен бути з'єднаний з масою металевої стійки шафи, в якій повинен бути встановлений комутатор.

Тримайте заземлювальне з'єднання постійно підключеним під час звичайного використання, до увімкнення обладнання та після вимкнення обладнання.

Для захисного провідника заземлення повинна використовуватися клема кільцевого затискача з переліку UL, що підходить для проводу AWG від 10 до 12, і провідник перерізом принаймні 4 мм^2 для приєднання до гвинтового затискача зовнішнього захисного заземлення.

6 Порти зв’язку

6.1 Електричні порти Ethernet (RJ45)

Пристрій Reason S20 обладнаний портами 10/100BASE-TX та 10/100/1000BASE-TX, які мають функції автоматичного узгодження, автоматичного визначення полярності та автоматичного визначення перехрещення пар.
У середовищах з високим рівнем електричних завад виконуйте наступні дії:

- Довжина кабелю передачі даних повинна бути якомога коротшою – в ідеалі до 3 м (10'). Мідні кабелі передачі даних не слід використовувати для внутрішньостанційного зв'язку, оскільки вони можуть працювати з різною потужністю струму і можуть зазнавати впливу електромагнітних завад (EMC), що генеруються високовольтним обладнанням;
- Кабелі живлення та кабелі передачі даних не повинні проходити паралельно на великі відстані, а повинні прокладатися в окремих кабелепроводах. Кабелі живлення та передачі даних повинні перетинатися під кутами 90°, коли необхідно зменшити індуктивний вплив.

На вибір (опційно) можна використовувати захищений/екранований кабель. Екран кабелю повинен бути заземлений в одній точці, щоб уникнути утворення (паразитних) петель заземлення.

6.2 Знімний трансивер SFP

Пристрій Reason S20 може працювати з SFP-трансивером (Компактний модульний трансивер), який можна безпечно вставляти та виймати, коли на комутатор подається живлення і він знаходиться в роботі. Проте, вставляючи або виймаючи трансивер SFP, слід вживати запобіжних заходів:

- Переконайтеся, що захисні кожухи завжди встановлені на трансивері SFP, за винятком випадків, коли користувач встановлює або виймає модуль SFP;
- Переконайтеся, що користувач вжив усіх можливих запобіжних заходів щодо накопичення електростатичного заряду (ESD);
- Перед встановленням або вилученням модуля від'єднайте всі кабелі від модуля SFP;
- Використовуйте тільки трансивери, сертифіковані компанією GE Reason.

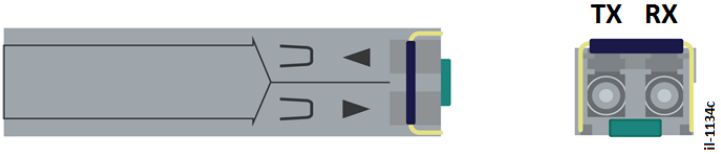


Рис. 4: SFP-трансивер

Перед тим, як зняти трансивер SFP, від'єднайте дроти та вставте захисний кожух від пилу. Трансивери SFP слід знімати, потягнувши за запобіжний фіксатор, розташований у верхній частині трансивера. Візьміться за металеву засувку та обережно потягніть назовні, щоб розблокувати та витягти модуль.

НІКОЛИ не втручайтеся в оптичні волокна або оптичні вихідні з'єднання. Завжди використовуйте вимірювачі оптичної потужності, щоб визначити справний стан або рівень сигналу.

7 Реле з сухими контактами (безпечного режиму)

Пристрій Reason S20 обладнаний реле безпечного режиму з сухими контактами (типу "form C") для сигналізації про події, які були попередньо налаштовані. За замовчуванням реле безпечного режиму вимкнено; тобто це означає, що воно не змінить свій стан.

Безпечний режим працює у комбінації з трьох штирів, з яких доступні один нормально замкнений (NC) і один нормально розімкнений (NO) контакти, де штир 2 є спільним:

- Коли в нормальному стані відсутні події, які викликали б спрацювання аварійного сигналу або, коли вимкнено безпечний режим, контакт 2-3 є нормально замкненим, а контакт 2-1 – нормально розімкненим;
- Для сигналізації стану будь-якої налаштованої події, контакт 2-3 перемикається у розімкнене положення та контакт 2-1 - у замкнене положення.

Нижче показані з'єднання для сухих контактів, і слід використовувати ізольовані гнучкі проводи з поперечним перерізом 1,5 мм².

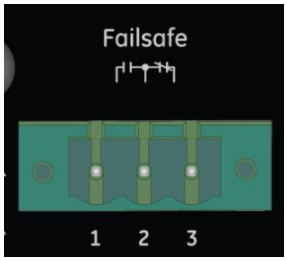


Рис. 5: Реле безпечного режиму з сухими контактами типу "form C"

8 Увімкнення живлення

Reason S20 не має кнопки увімкнення та вимкнення живлення. Після підключення джерела живлення комутатор вмикається. Після увімкнення живлення світлодіоди відображатимуть шаблон, який вказує на ініціалізацію S20. Для кожного джерела живлення передбачено світлодіодний індикатор, який вказує на те, коли пристрій знаходиться під напругою.

9 Профілактичне обслуговування

З огляду на критичний характер застосування, пристрої GE слід регулярно перевіряти, щоб підтвердити, що вони працюють належним чином. Продукція GE розрахована на строк експлуатації понад 20 років. Пристрої оснащені засобами самоконтролю і тому потребують меншого обсягу обслуговування, ніж попередні конструкції захисних пристроїв. Більшість проблем, що можуть виникнути, призводить до спрацювання аварійної сигналізації, яка вказує на необхідність вжити заходів щодо усунення несправностей. Проте, слід проводити деякі періодичні випробування, щоб переконатись, що обладнання функціонує належним чином і, що зовнішня проводка непошкоджена. Замовник несе відповідальність за визначення періодичності технічного обслуговування.

Якщо у вашій організації діє Політика профілактичного обслуговування, рекомендовані перевірки пристроїв повинні бути включені до регулярної програми. Періоди технічного обслуговування залежать від багатьох факторів, таких як:

- Робоче середовище;
- Доступність об'єкта/майданчика;
- Кількість наявної робочої сили;
- Важливість установки для енергосистеми;
- Наслідки відмови.

9.1 Попереджувальні заходи

Комутатори не часто виходять з ладу. Проте існує потреба в профілактичному обслуговуванні комутаторів. Періодично комутатори слід перевіряти на безперебійну та правильну роботу, а також на наявність фізичних пошкоджень. Будь-які виявлені проблеми слід негайно усунути. Для оптимальної роботи дотримуйтесь процедур та заходів профілактичного обслуговування:

- Підтримуйте температуру та вологість на належному рівні всередині шафи. Американське товариство інженерів з опалення, охолодження та кондиціонування повітря (ASHRAE) рекомендує експлуатувати мережеве обладнання в таких діапазонах температур та відносної вологості (див. ASHRAE TC 9.9 "Рекомендації щодо температури у середовищах обробки даних від 2011 року – Додаткові класи центрів обробки даних (ЦОД) та настанови з їх використання"):
  - Температура в межах від 18 °C до 27 °C (від 64 °F до 80,6 °F);
  - Відносна вологість менше 60%;
  - Точка роси в межах від 5,5 °C до 15 °C (від 41,9 °F до 59,0 °F).
- Робота в межах передбаченого діапазону забезпечує найвищий ступінь надійності обладнання, навіть незважаючи на те, що технічні паспорти обладнання можуть містити дані про більш широкі діапазони мінімальної та максимальної температур та вологості (наприклад, від -40 °C до 55 °C та від 5% до 95% відносної вологості). Безперервна робота обладнання на мінімальному та максимальному рівнях не рекомендується.
- Тримайте шафу щільно закритою, щоб уникнути проникнення пилу та/або тварин і комах.
- Огляньте місце монтажу на наявність вологи, вільних (незакріплених) проводів або кабелів та надмірного пилу. Переконайтеся, що потік повітря безперешкодно циркулює навколо комутатора та надходить у вентиляційні отвори.
- Перевірте звіт про стан пристрою на сервері мережевих системних журналів (syslog-сервері). Функція журналу являє собою файл, у якому записується інформація про працюючу операційну систему або програмне забезпечення на пристрої. У багатьох програмних застосунках ці дані використовуються для цілей аналізу, оскільки у журналі зберігається інформація про запущені програми або фізичні з'єднання, наприклад, активні порти Ethernet.
- Reason S20 має можливість надсилати повідомлення системного журналу на виділені сервери системних журналів. Рівень системного журналу розділений на 4 категорії: помилка (ступінь серйозності 3), попередження (ступінь серйозності 4), повідомлення (ступінь серйозності 5) та інформація (ступінь серйозності 6). При виборі більш високого рівня серйозності обладнання буде надсилати всі повідомлення з нижчих рівнів плюс вибраний рівень серйозності.

Таким чином, вибір рівня серйозності інформації дозволяє користувачеві отримувати всі повідомлення системного журналу, які обладнання може надіслати. Вибираючи рівень серйозності "помилки", користувач отримуватиме тільки повідомлення про помилки.

- Протокол SNMP може бути налаштований для контролю температури S20;
- Рекомендовані попереджувальні заходи, описані вище, допоможуть забезпечити безперебійну роботу пристрою, а також уникнути будь-яких незручностей.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 4: Інтерфейси та Конфігурація

1 Інтерфейси зв'язку

Reason S20 має локальний та віддалений інтерфейси зв'язку:

- Локальний інтерфейс:
  - Порт зв'язку USB 2.0 для локальної конфігурації (інтерфейс консолі).
- Віддалені інтерфейси:
  - Інтерфейс зв'язку Ethernet (електричний або оптичний) для віддаленого або локального моніторингу та налаштування. Доступні протоколи для цього інтерфейсу - HTTP, HTTPS, SSH та Telnet.

З міркувань безпеки за замовчуванням доступні тільки SSH та HTTPS.

1.1 Локальний інтерфейс - USB

Reason S20 має інтерфейс USB (Універсальна послідовна шина) для налаштування конфігурації обладнання та моніторингу діючих налаштувань за допомогою інтерфейсу командного рядка (CLI). Якщо використовується, для цього інтерфейсу потрібен комп’ютер із USB-портом зв'язку, програмне забезпечення для послідовного зв’язку та встановлення драйвера, який можна завантажити на веб-сайті www.gegridsolutions.com.
При доступі до Reason S20 за допомогою локального інтерфейсу USB необхідно налаштувати параметри послідовного зв'язку USB-порту на комп'ютері, щоб відповідати специфікаціям USB-порту. Слід застосовувати наступні параметри послідовного зв'язку:

- Швидкість: 115200 біт на секунду;
- Біти даних: 8;
- Стоп-біти: 1;
- Контроль парності: немає;
- Керування потоком: немає.

Роз'єм USB є розетковим ("мама") типу B, як показано на рисунку нижче.

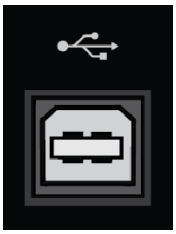


Рис. 6: USB роз’єм типу B

1.2 Віддалений інтерфейс - Ethernet

Пристрій Reason S20 можна налаштовувати, виконувати моніторинг, оновлення вбудованого програмного забезпечення та здійснювати його обслуговування за допомогою підключення Ethernet, або з використанням веб-інтерфейсу через протоколи HTTP/HTTPS, або за допомогою SSH/Telnet через інтерфейс командного рядка (CLI). Для цього інтерфейсу потрібен комп’ютер із мережевим портом та встановленим браузером. Для віддаленого інтерфейсу можуть використовуватися як електричний, так і оптичний інтерфейси Ethernet.

HTTP та HTTPS – найбільш зручні для використання інтерфейси, оскільки вони працюють в інтерфейсі веб-браузера. На рисунку нижче проілюстровано приклад інтерфейсу початкового (першого) екрана після отримання доступу.

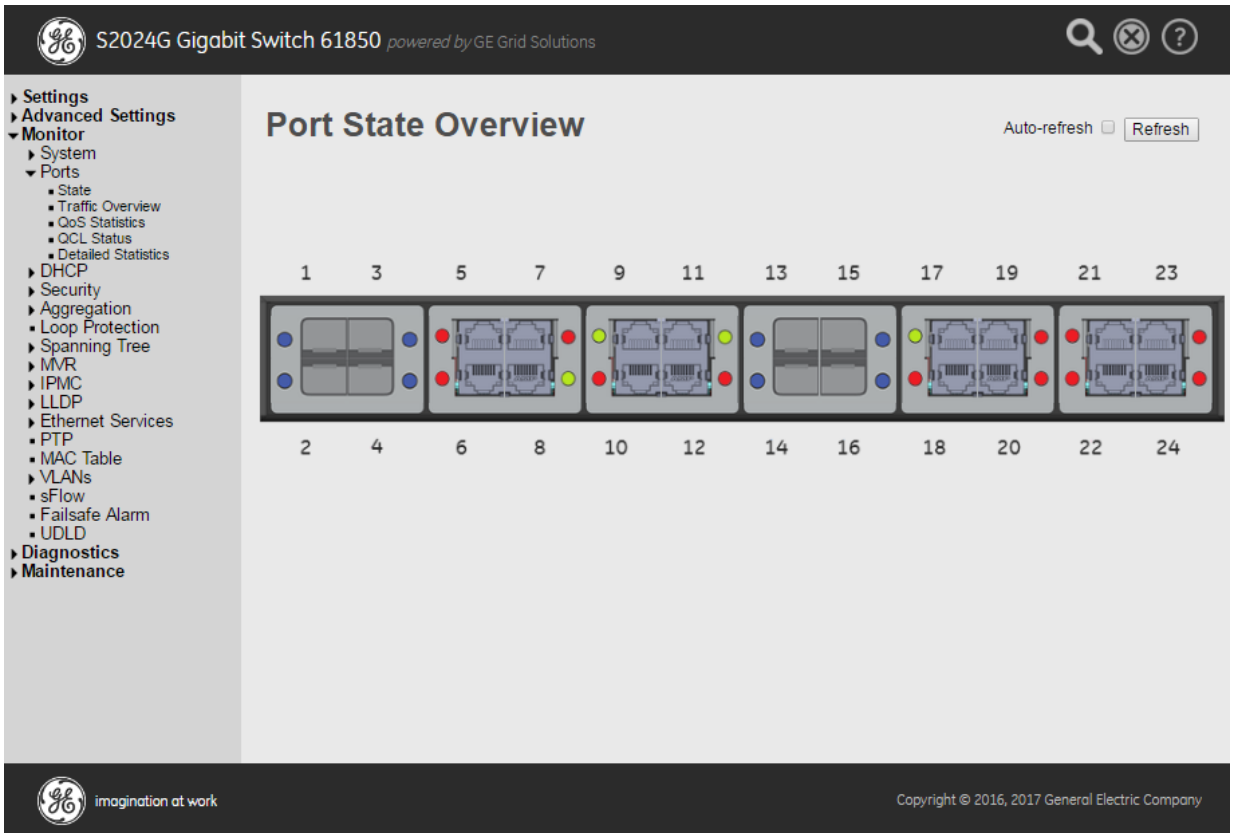


Рис. 7: Приклад початкового екрана HTTP або HTTPS

Для використання протоколу HTTPS, обов’язково введіть ***https://*** перед IP-адресою у веб-браузері. Може з’явитися повідомлення про незахищене з’єднання, оскільки браузер не може знайти дійсну сертифікацію веб-сайту. Це не впливає на функції та конфігурацію обладнання, користувач може продовжувати з'єднання, щоб нормально отримати доступ до веб-інтерфейсу обладнання.

Наявні три кнопки у верхньому правому куті веб-інтерфейсу для наступного призначення:

- **Рядок пошуку (Search Bar)**: користувач може здійснювати пошук будь-якого типу налаштувань, моніторингу, діагностики або інформації про технічне обслуговування. Наприклад, для пошуку IEEE 1588 PTP користувач може ввести "PTP" або "IEEE 1588".
- **Кнопка виходу (Logout button)**: натисніть, щоб закінчити поточний сеанс роботи користувача;
- **Інформація (Info):** натисніть на цю кнопку, щоб дізнатись більше про поточну відображену веб-сторінку. Це онлайн-вказівки щодо взаємодії при використанні HTTP або HTTPS.

Рис. 8: Панель пошуку, виходу та інформації веб-інтерфейсу

2 Доступ до Reason S20

Як зазначалося раніше, отримати доступ до Reason S20 можна за допомогою:

- Веб-інтерфейсу через протоколи HTTP/HTTPS, використовуючи інтерфейс Ethernet, або;
- Інтерфейсу командного рядка (CLI), або через SSH/Telnet Ethernet, або через консольний інтерфейс USB.

Повідомлення про застереження може бути налаштовано як спливаюче вікно при доступі до S20 або за допомогою веб-інтерфейсу, або CLI, якщо потрібно. За замовчуванням повідомлення про застереження порожнє і не відображається.

Для першого доступу до Reason S20 нижче зазначені заводські параметри за замовчуванням.

2.1 Заводські параметри за замовчуванням

IP-адреса (з усіх портів) та маска мережі

IP-адреса: 192.168.4.88
Маска мережі: 255.255.255.0

Логін і пароль

Логін: admin
Пароль: {серійний номер Reason S20}
Серійний номер можна знайти на етикетці, прикріпленій до корпусу обладнання.

2.2 Перший доступ

Налаштування терміналу

Щоб уперше отримати доступ до конфігурації програмного забезпечення через Ethernet-зв'язок, налаштуйте термінал на будь-яку адресу від 192.168.4.1 до 192.168.4.254 (крім 192.168.4.88, що є заводською IP-адресою). Маска 255.255.255.0 для локального підключення.

В ОС Windows виконайте наступні дії, щоб змінити IP-адресу терміналу:

- Увійдіть до панелі керування;
- Виберіть варіант підключення до мережі;
- У "Стані локального підключення" (Local Connection Status) виберіть параметр "Властивості" (Properties);
- У меню "Властивості підключення до локальної мережі" (Local Area Connection Properties) виберіть протокол IP версії 4;
- Після вибору IPv4 оберіть "Властивості";
- На вкладці "Загальне" (General) виберіть параметр "Використовувати наступну IP-адресу" (Use the Following IP address) та введіть:
  - IP-адресу: будь-яке значення від 192.168.4.1 до 192.168.4.254, крім IP-адреси за замовчуванням Reason S20 192.168.4.88;
  - Маску підмережі: 255.255.255.0;
  - Шлюз за замовчуванням: залиште його порожнім.
- На вкладці "Загальне" можна вибрати "Автоматично отримати адресу DNS-сервера" (Obtain DNS server address automatically).

Веб-інтерфейс

Після налаштування терміналу відкрийте веб-браузер і:

- Введіть адресу: https://192.168.4.88 та натисніть клавішу Вводу (Enter);
- Якщо з’являється попереджувальне повідомлення, клацніть, щоб продовжити доступ;
- Введіть логін та пароль за замовчуванням;

Інтерфейс командного рядка (CLI)

- Щоб отримати доступ до Reason S20 за допомогою інтерфейсу командного рядка (CLI), використовуйте інструмент налаштування Telnet/SSH, такий як PuTTY, і виберіть тип з'єднання. У наведеному нижче прикладі пристрій підключається через SSH за допомогою IP-адреси 192.168.4.88.

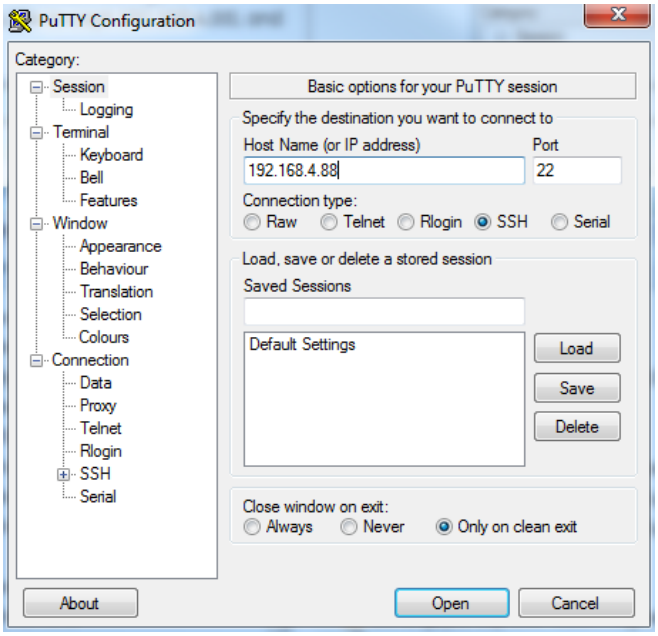


Рис. 9: Налаштування PuTTY для SSH доступу

- Коли ви натискаєте кнопку ВІДКРИТИ (OPEN), відкриється вікно та буде запропоноване введення логіну/пароля за замовчуванням.

Зміна пароля за замовчуванням

Виконавши зазначені кроки, ви вже повинні отримати доступ до веб-інтерфейсу. При першому доступі слід змінити пароль за замовчуванням.
Новий пароль повинен містити щонайменше 8 символів, включаючи малі/великі букви, цифрові та спеціальні неалфавітні символи (наприклад, #, $, @, &). Зверніть увагу, що строк дії пароля увімкнено за замовчуванням, і якщо його вирішено зберегти (як рекомендується), новий пароль буде вважатися збереженим 1 січня 1970 року, оскільки внутрішній час ще не було налаштовано.
Не забудьте зберегти новий пароль у конфігурації запуску, інакше пароль буде повернуто до значення серійного номеру після перезапуску обладнання, і користувач повинен буде ще раз пройти через той самий процес.
Щоб зберегти новий пароль у конфігурації запуску за допомогою веб-інтерфейсу:

- Перейдіть до Технічне обслуговування> Конфігурація> Зберегти конфігурацію запуску (Maintenance > Configuration > Save startup-config);
- Клацніть на "Зберегти конфігурацію" (Save Configuration).

Щоб зберегти новий пароль у конфігурації запуску за допомогою CLI, введіть наступний командний рядок: ***copy running-config startup-config***

Строк дії пароля та налаштування внутрішнього часу

Відтепер користувач повинен використовувати новий створений пароль і продовжувати виконувати решту налаштувань за потреби. Якщо строк дії пароля увімкнено, а внутрішній годинник оновлено до поточної дати та часу (за допомогою NTP або PTP), строк дії пароля користувача закінчується, і його доведеться ще раз змінити в наступному розділі.

2.3 Команди, що вводяться за допомогою Інтерфейсу командного рядка (CLI)

Представлені тут команди можуть бути використані для Telnet, SSH або локального зв'язку USB.

Кожна команда має всередині меню зі своїми підкомандами, і це можна побачити, набравши символ "?". Найпоширенішими командами головного меню є наступні:

- *clear (Очистити)* функції скидання;
- *configure terminal (Налаштувати термінал)* увійти в режим конфігурації;
- *copy (Копіювати)* копіювати від джерела до місця призначення;
- *delete (Видалити)* видалити один файл у флеш-пам'яті: файлова система;
- *dir* каталог усіх файлів у флеш-пам'яті: файлова система;
- *disable (Вимкнути)* вимкнути привілейовані команди;
- *do (Виконати)* запускати команди виконання ("exec") в режимі конфігурації;
- *dot1x* стандарт IEEE для контролю доступу на базі портів;
- *enable (Увімкнути)* увімкнути привілейовані команди;
- *erps* захисне перемикання для кільця Ethernet
- *exit (Вихід)* вихід з режиму виконання "EXEC";
- *failsafe (Безпечний режим)* налаштувати реле безпечного режиму;
- *firmware (Вбудоване ПЗ ("прошивка"))* оновлення або завантаження прошивки;
- *help (Довідка)* опис інтерактивної довідкової системи;
- ipv4 команди IPv4;
- ipv6 команди Ipv6;
- *link-oam* конфігурація OAM-каналу;
- *logout* (Вийти з облікового запису); вихід з режиму виконання "EXEC";
- *more (Більше)* відобразити файл;
- no (Ні) заперечити команду або встановити її за замовчуванням;
- *ping* надсилати ехо-повідомлення ICMP;
- *platform* (Платформа) конфігурація платформи;
- *ptp* різні непостійні налаштування 1588;
- *reload (Перезавантажити)* перезавантажити систему;
- *send* (Надіслати) надіслати повідомлення на інші tty-рядки;
- *show* (Показати) показати інформацію про діючу систему;
- *terminal (Термінал)* встановити параметри лінії терміналу;
- *Veriphy ()* ключове слово veriphy.

Як увімкнути/вимкнути SSH або Telnet

Спочатку необхідно увійти в термінал конфігурації S20. Для цього введіть наступну команду:

configure terminal (налаштувати термінал)

А потім введіть наступну команду, щоб увімкнути SSH:

ip ssh

Щоб вимкнути SSH, введіть протилежну команду:

no ip ssh

Щоб увімкнути/вимкнути протокол Telnet, просто використовуйте ті самі команди, але замінюючи ***ssh*** на ***telnet***.

Як увімкнути/вимкнути HTTP або HTTPS

Як зазвичай, необхідно увійти в термінал конфігурації S20. Для цього введіть наступну команду:

configure terminal

А потім введіть наступну команду, щоб увімкнути HTTPS:

ip http secure-server

Щоб вимкнути HTTPS, введіть протилежну команду:

no ip http secure-server

Щоб увімкнути/вимкнути протокол HHTP, просто використовуйте ті самі команди, але замінюючи ***secure-server*** на ***server***.

3 Світлодіоди сигналізації

Світлодіоди сигналізації розміщені на передній панелі обладнання, та вказують стан портів. Номер зліва від кожного світлодіода означає номер порту, пов'язаний з ним.

- Світлодіод з'єднання: Вказує стан порту. Вимкнений світлодіод означає, що порт не працює. Увімкнений світлодіод означає активне підключення до обладнання;
  - Зелений колір означає швидкість гігабітного порту;
  - Помаранчевий колір означає швидкість порту 100 Мбіт/с.
- Світлодіод живлення 1: Вказує на те, що блок живлення №1 знаходиться під напругою;
- Світлодіод живлення 2: Вказує на те, що блок живлення №2 знаходиться під напругою;
- Світлодіод синхронізації: Вказує на синхронізацію внутрішнього годинника PTP (коли увімкнено коригування системного часу з PTP або в режимі граничного PTP);
- Світлодіод безпечного режиму: Вказує на те, що стан реле безпечного режиму змінено, тобто нормально розімкнений контакт замкнувся, а нормально замкнений контакт розімкнувся.

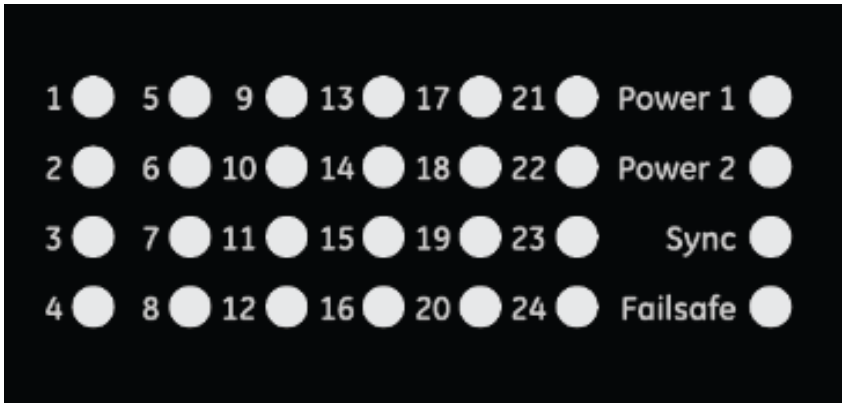


Рис. 10: Місцеві світлодіодні індикатори HMI

Таблиця 2: Опис кольорів світлодіодів

Світлодіод (LED))	Колір	Опис
З'єднання	Вимкнено	Немає з'єднання
	Оранжевий	10/100 Мбіт/с з'єднання
	Зелений	1000 Мбіт/с з'єднання
Синхронізації	Вимкнено	Внутрішній PTP годинник не синхронізовано
	Зелений	Внутрішній PTP годинник синхронізовано
Живлення (1 і 2)	Вимкнено	Живлення вимкнено
	Зелений	Живлення підключено
Безпечного режиму	Вимкнено	Реле безпечного режиму не в роботі
	Зелений	Реле безпечного режиму в роботі

4 Кнопка перезапуску

S20 має кнопку перезапуску, яка дозволяє користувачеві виконати ручне перезавантаження без необхідності підключення через інтерфейс конфігурації або відключення та повторного підключення джерела живлення. При натисканні система перезавантажується, а Reason S20 буде працювати в нормальному режимі після ініціалізації.

Якщо конфігурація на даному комутаторі не збережена у конфігурації запуску, перезавантаження відхилить цю конфігурацію (робочу конфігурацію). Після перезавантаження конфігурація запуску буде працювати.

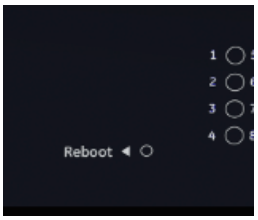


Рис. 11: Кнопка перезапуску

5 Скидання до заводських налаштувань

Щоб відновити заводські налаштування за замовчуванням у Reason S20, користувач має два варіанти: перший – увійти в обліковий запис пристрою та виконати скидання до заводських налаштувань через веб-інтерфейс (Технічне обслуговування> Заводські налаштування (Maintenance > Factory Defaults)) або за допомогою CLI. Другий варіант виконується апаратними засобами, як описано нижче.

Якщо комутатор увімкнено:
1. Підключіть порти 1 і 2, створюючи петлю на комутаторі;
2. Перезавантажте пристрій із підключеними один до одного портами 1 і 2. Перезавантаження можна виконати у веб-інтерфейсі або за допомогою кнопки перезапуску;
3. Зачекайте близько 60 секунд і перевірте, чи повернулись налаштування до значень за замовчуванням;
4. Від'єднайте петлю від портів 1 і 2.

Якщо комутатор вимкнено:
1. Підключіть порти 1 і 2, створюючи петлю на комутаторі;
2. Увімкніть пристрій;
3. Зачекайте близько 60 секунд і перевірте, чи повернулись налаштування до значень за замовчуванням;
4. Від'єднайте петлю від портів 1 і 2.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 5: Функції та конфігурація

Різні топології, підключення пристроїв IED та протоколи синхронізації можуть бути реалізовані за допомогою Reason S20, і розуміння основних принципів застосування є належною стратегією для визначення проекту мережі.
Для варіантів застосування в енергосистемах набір функцій реалізований при використанні технічної підтримки МЕК 61850-90-4 як керівної настанови для проектування та конфігурації мереж МЕК 61850. Крім того, у пристроях Reason S20 враховано ряд функцій, пов'язаних із кібербезпекою, розроблених на виконання вимог NERC CIP v5.
У цьому розділі представлений огляд загальних функцій і протоколів, а також міститься інформація про те, як налаштувати обладнання.
Після зміни будь-якої конфігурації користувач може зберегти або скасувати зміни, натиснувши:

- Зберегти (Save): зберегти конфігурацію в Робочій конфігурації (Running Config);
- Скинути (Reset): скасувати внесені локально зміни у Робочій конфігурації.

1 Опис конфігурації

Reason S20 запускає три внутрішні файли конфігурацій, які користувач може вільно вибрати.

Робоча конфігурація (Running Config)

Цей файл представляє фактичну конфігурацію комутатора. Якщо в будь-якому меню налаштувань натиснути кнопку збереження, зміни, внесені в конфігурацію, будуть збережені в цьому файлі. Якщо комутатор перезавантажується, ця конфігурація відкидається, і після перезавантаження комутатор завантажить файл Конфігурації запуску (Startup Config).

Конфігурація запуску (Start-up Config)

Цей файл представляє конфігурацію, яку комутатор запускатиме після його увімкнення або перезапуску. Якщо були внесені зміни у Робочій конфігурації, і Робочу конфігурацію необхідно використовувати під час запуску конфігурації, користувач повинен зберегти її у налаштуванні "Зберегти Робочу конфігурацію" (Save Running Configuration) як конфігурацію запуску в меню Технічне обслуговування (Maintenance).

Конфігурація за замовчуванням (Default Config)

Цей файл представляє заводську конфігурацію комутатора за замовчуванням. За необхідності його можна завантажити за допомогою програмного забезпечення для заміни фактичної робочої конфігурації або файлу конфігурації запуску.

2 Налаштування системи

2.1 Інформація про систему

У меню інформації про систему (System Information) користувач може налаштувати інтуїтивно зрозумілі та зручні дані ідентифікації з використанням імен персоналу, відповідального за комутатор, імені комутатора (або системи), де знаходиться пристрій, та повідомлення про застереження, яке з'являється під час отримання доступу до пристрою. Інформація про систему корисна при використанні протоколів керування, таких як SNMP або LLDP, оскільки система надсилатиме ім'я комутатора у своїх повідомленнях, щоб значно полегшити керування мережею та діагностику.
Меню конфігурації системної інформації знаходиться в меню Налаштування > Система > Інформація (Settings > System > Information).

Контактні дані системи

У полі Контактна інформація (Contact information) слід вказати персонал, відповідальний за цей комутатор. Дозволена довжина рядка – до 255, а дозволеними символами є символи ASCII від 32 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_").

Ім'я системи

Адміністративне ім'я комутатора. Це поле, згідно з правилами, являє собою повне доменне ім'я (FQDN). Перший символ повинен бути альфа-символом, а пробіл заборонено. Дозволена довжина рядка – до 255, а дозволеними символами є рядки, взяті з алфавіту (літери), цифри та знак мінусу ("-").

Розташування системи

Визначення місця встановлення цього комутатора. Дозволена довжина рядка - до 255, а дозволеними символами є символи ASCII від 32 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_").

Застереження

Повідомлення про застереження, яке буде показано під час доступу до S20 за допомогою веб-інтерфейсу або CLI. Максимальна довжина – до 255 символів відповідно до ASCII (в основному букви, цифри та інші символи, такі як "-" або "_").
Щоб налаштувати застереження за допомогою CLI, використовуйте таку команду "*banner [login] <text>*".

2.2 IP (Інтернет-протокол)

У цьому пункті визначені основні характеристики служб IP (Інтернету-протоколу) від S20 в мережах Ethernet. IP-конфігурація DNS серверів, IP-інтерфейси від VLAN (які можна співвідносити з портами інтерфейсу) та статичні IP-маршрутизації.
Меню IP знаходиться в меню Налаштування > Система > IP (Settings > System > IP).

DNS-сервер

Якщо для доступу до інтерфейсів потрібно використовувати доменні імена замість прямої IP-адреси, можна визначити DNS-сервери та DNS-проксі для перетворення адрес. DNS-сервери також можуть використовуватися для керування доступом.
При використанні більше одного DNS-сервера, перевага використовуваного сервера визначатиметься Індексним номером DNS-сервера. Менше число індексу означає вищий пріоритет. Якщо сервер вищого рівня пріоритету не відповідає після 5 спроб, запит надсилається на сервер з наступним індексом. За замовчуванням не налаштовано жодного DNS-сервера.

- З будь-яких інтерфейсів DHCPv4 (From any DHCPv4 interfaces): використовуватиметься перший сервер, запропонований в інтерфейсі DHCPv4;
- Немає DNS-сервера (No DNS server): сервери для перетворення імен не використовуються;
- Налаштований IPv4 (Configured IPv4): сервер повинен мати зрозумілу конфігурацію з дійсною адресою IPv4. Формат IP-адреси – десяткове позначення з крапками;
- З цього інтерфейсу DHCPv4 (From this DHCPv4 interface): використовуваний сервер буде сервером, налаштованим на заданий інтерфейс DHCPv4. Поле повинне бути налаштоване з ідентифікаційним номером VLAN бажаного інтерфейсу DHCPv4. Допустимі значення ідентифікатора VLAN становлять від 1 до 4095;
- Налаштований IPv6: сервер повинен мати зрозумілу конфігурацію з дійсною адресою IPv6. Формат IP-адреси шістнадцятковий, двокрапка (":") розділяє кожне поле;
- З цього інтерфейсу DHCPv6: використовуваний сервер буде сервером, налаштованим на заданий інтерфейс DHCPv6. Поле повинне бути налаштоване з ідентифікатором VLAN (1 – 4095) номера бажаного інтерфейсу DHCPv6;
- З будь-яких інтерфейсів DHCPv6: використовуватиметься перший сервер, запропонований в інтерфейсі DHCPv6;
- DNS-проксі: ця функція дозволена лише в мережах IPv4. Якщо увімкнено, запити DNS перенаправляються на налаштовані DNS-сервери, і відповідь буде надана до DNS-перетворювача для клієнтських пристроїв в мережі.

IP-інтерфейси

Цей пункт використовується для визначення IP-адреси для кожної VLAN. За замовчуванням усі порти налаштовані на VLAN 1, використовуючи однакову IP-адресу за замовчуванням. Проте можна створити VLAN для кожного інтерфейсу, наприклад, і налаштувати різні IP-адреси для кожного з них.
IP-адреса для VLAN може бути статичною або динамічно отримуватися конфігурацією сервера DHCP. Дозволені адреси IPv4 та IPv6.

- VLAN: визначає ідентифікатор (ID) VLAN інтерфейсу;
- Увімкнути DHCPv4 (DHCPv4 Enable): увімкнути конфігурацію IP-адреси DHCPv4. Якщо увімкнено, комутатори працюватимуть як клієнти DHCPv4, а його IP-адреси та адреси мережевих масок визначатимуться сервером DHCPv4, доступним у VLAN цього інтерфейсу;
- Резервний варіант DHCPv4 (DHCPv4 fallback): визначте кількість секунд для спроби отримати IP-адреси від сервера DHCPv4 у VLAN цього інтерфейсу. Якщо жодної адреси не отримано, використовуваною IP-адресою буде IP-адреса, налаштована в полі Адреса IPv4. Значення "0" вимикає це поле, а допустимі значення становлять від 0 до 4.294.967.295 секунд;
- Поточна оренда DHCPv4 (DHCPv4 Current Lease): для інтерфейсів з увімкненим DHCPv4 у цьому полі відображається IP-адреса, отримана сервером DHCPv4 у VLAN цього інтерфейсу;
- IPv4-адреса (IPv4 Address): визначте статичну IP-адресу, яка використовуватиметься на цьому інтерфейсі. Значення потрібно вставляти в десяткове позначення з крапками. Якщо DHCPv4 увімкнено, ця адреса буде використана, якщо сервер DHCPv4 не відповідає на запити комутатора;
- Довжина маски IPv4 (IPv4 Mask Length): визначте кількість бітів, які використовуватимуться як маска для IP-адреси, від найбільш значущого біта до найменшого значущого біта. Доступні значення – від 0 до 30;

- Увімкнути DHCPv6 (DHCPv6 Enable): увімкнути конфігурацію IP-адреси DHCPv6. Якщо увімкнено, комутатори працюватимуть як клієнти DHCPv6, а його IP-адреса буде визначатися сервером DHCPv6, доступним у VLAN цього інтерфейсу;
- Швидка фіксація DHCPv6 (DHCPv6 Rapid Commit): увімкніть функцію швидкої фіксації для визначення своєї адреси IPv6. Якщо сервер DHCPv6 дозволив швидку фіксацію DHCPv6, цей прапорець дозволяє комутатору завершити процес очікування при отриманні повідомлення-відповіді з інформацією швидкої фіксації;
- Поточна оренда DHCPv6: для інтерфейсів з увімкненим DHCPv6 у цьому полі відображається IP-адреса, отримана сервером DHCPv6 у VLAN цього інтерфейсу;
- IPv6-адреса: визначте статичну IP-адресу, яка використовуватиметься на цьому інтерфейсі. Значення слід вставляти з шістнадцятковими значеннями, при цьому кожне поле адреси відокремлюється маркером двокрапки (":") Коли DHCPv6 увімкнено, ця адреса буде використана, якщо сервер DHCPv6 не відповідає на запити комутатора;
- Довжина маски IPv6: визначте кількість бітів, які використовуватимуться як маска для IP-адреси, від найбільш значущого біта до найменшого значущого біта. Доступні значення – від 0 до 128.

IP-маршрути (Статична маршрутизація)

Функціонал статичної маршрутизації не є протоколом маршрутизації, натомість вона керується адміністратором мережі вручну для визначення мережевих IP-маршрутів. Зверніть увагу що IP-маршрути, введені вручну, не оновлюються автоматично, адміністратор повинен заново їх реконфігурувати після прийняття змін у мережі. Статична IP-маршрутизація працює по-різному, залежно від активації ліцензії L3. Якщо ліцензія неактивна, S20 буде направляти пакети лише на шлюзи в тій самій VLAN. Якщо ліцензія активна, пристрій також може виконувати маршрутизацію між VLAN.

IP-маршрути (статична маршрутизація) корисні для керованої мережі, для якої IP-адреса з терміналів є фіксованою та добре відомою. Наступні параметри повинні бути налаштовані для встановлення IP-маршруту вручну.

- Мережа (Network): визначте IP-адресу мережі маршруту призначення. Значення IPv4 потрібно вставляти як десяткове позначення з крапками, а значення IPv6 – із шістнадцятковими значеннями, при цьому кожне поле адреси відокремлюється маркером двокрапки (":");
- Довжина маски (Mask Length): визначте кількість бітів, які будуть використовуватися як маска для IP-адреси, від найбільш значущого біта до найменшого значущого біта;
- Шлюз (Gateway): визначте IP-адресу шлюзу/маршрутизатора. Значення IPv4 потрібно вставляти як десяткове позначення з крапками, а значення IPv6 – із шістнадцятковими значеннями, при цьому кожне поле адреси відокремлюється маркером двокрапки (":"). Адреси шлюзу та мережі повинні мати однакову версію IP;
- Наступна транзитна ділянка VLAN (Next Hop VLAN): використовується лише за запитом маршруту IPv6. Визначте ідентифікатор VLAN інтерфейсу, пов’язаного зі шлюзом. Допустимі ідентифікатори VLAN становлять від 1 до 4095.

Для прикладу конфігурації IP-маршруту, коли активовано ліцензування Рівня 3, на рисунку нижче проілюстровано топологію мережі з обома S20, що працюють як маршрутизатор, де бажано встановити зв'язок між двома пристроями IED.

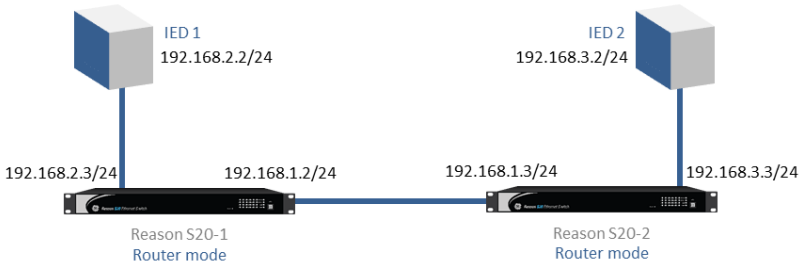


Рис. 12: Приклад IP-маршрутизації

Щоб переконатися, що повідомлення від пристрою IED 1 доставляються до IED 2 із використанням статичної маршрутизації, адміністратор мережі повинен ввести наступний маршрут до Reason S20-1:

- Мережа: 192.168.3.0
- Довжина маски: 24
- Шлюз: 192.168.1.3

З іншого боку, щоб переконатися, що повідомлення від пристрою IED 2 доставляються до IED 1, у Reason S20-2 слід налаштувати наступний маршрут:

- Мережа: 192.168.2.0
- Довжина маски: 24
- Шлюз: 192.168.1.2

Зверніть увагу, що параметр Мережі для адрес IPv4 повинен закінчуватися на 0, як показано вище.

2.3 Синхронізація NTP

NTP (Мережевий протокол часу) – це мережевий протокол, який може використовуватися для синхронізації внутрішнього годинника S20 через мережі передачі даних із комутацією пакетів, на додаток до IEEE 1588v2. NTP працює в режимі клієнт-сервер, а точність часу знаходиться в межах декількох мілісекунд, що відповідає часу UTC. Поточна версія (версія NTP 4) стандартизована згідно з RFC 5905. Деякі функції, такі як системний журнал та строк дії пароля, використовують час для встановлення позначок часу повідомлень.

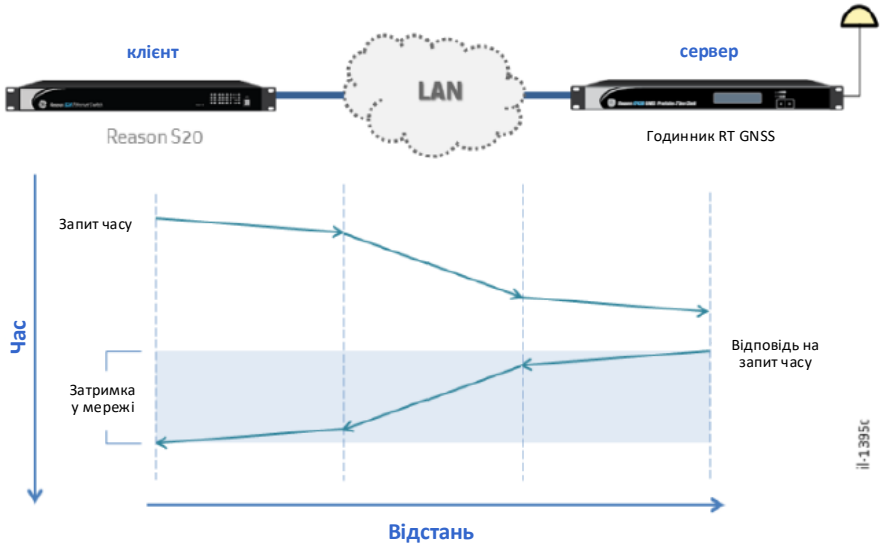


Рис. 13: Механізм протоколу часу NTP

У меню NTP користувач може налаштувати до п'яти серверів часу NTP, які будуть використовуватися як джерело часу для синхронізації внутрішнього годинника комутатора. Менший індекс сервера означає вищий пріоритет використання. Якщо сервер вищого пріоритету не відповідає, запит надсилається на сервер з наступним індексом.

Крім того, користувач може вибрати ввімкнення/вимкнення роботи сервера NTP та обрати часовий шар (рівень) NTP відповідно до умов джерела часу.

Меню конфігурації NTP знаходиться в меню Налаштування > Система > NTP (Settings > System > NTP).

Конфігурація NTP

Конфігурація, пов'язана з роботою клієнта NTP, де може бути налаштовано до п'яти серверів часу NTP:

- Режим (Mode): це поле використовується для ввімкнення/вимкнення функції синхронізації часу NTP. За замовчуванням цей режим вимкнений. Щоб увімкнути, виберіть Увімкнено (Enabled) у списку режимів, а потім налаштуйте дійсну IP-адресу сервера. Зверніть увагу, якщо увімкнено NTP, системний час PTP буде примусово вимкнено, навіть якщо він раніше був увімкнений. Системний час PTP може бути знову увімкнений (вручну), якщо режим NTP буде вимкнено.
- Сервер (Server): У цих полях (Сервер від 1 до 5) вказується, яким серверам NTP комутатор повинен надсилати запити часу NTP у режимі клієнт-сервер. Значення IPv4 повинні бути вставлені як десяткове позначення з крапками, а значення IPv6 мають бути записані з шістнадцятковими значеннями, при цьому кожне поле адреси відокремлене маркером двокрапки (":").

При використанні синхронізації NTP, переконайтесь, що комутатор доступний для сервера NTP. Команда PING, виконана комутатором, може бути використана для перевірки зв'язку.

Конфігурація Ведучого вузла (Master) NTP

Конфігурація, пов'язана з роботою S20 як NTP-сервера. S20 може працювати як повноважний NTP-сервер на основі IEEE1588, NTP-клієнт або без жодного джерела часу (на основі ручних налаштувань, не синхронізованих з іншим джерелом часу). NTP-сервер приймає до 50 запитів NTP на секунду (зазвичай представляє 50 NTP-клієнтів), відповідаючи на запити з будь-якої VLAN, що має відомий IP, зареєстрований на IP-інтерфейсах комутатора.

- Режим: увімкнення/вимкнення комутатора як NTP-сервера. NTP-сервер може базуватися на трьох різних джерелах часу, які розташовані в порядку пріоритету: NTP-клієнт, PTP-налаштування системного часу або налаштовані вручну параметри. Підсумовуючи:
  - Якщо увімкнено NTP-клієнт, NTP буде джерелом часу для NTP-сервера.
  - Якщо NTP-клієнт вимкнений, перевірте, чи використовується PTP для налаштування системного часу, перейшовши до PTP> Налаштування системного часу (PTP > Adjust System Time). Якщо увімкнено налаштування системного часу PTP, PTP є джерелом часу для NTP-сервера.
  - У разі вимкнення налаштування системного часу як NTP, так і PTP, вручну налаштовані дата/час будуть використані як джерело часу для NTP-сервера.
- Часовий шар (Stratum): Встановлює найнижче допустиме значення вихідного часового шару. Можливі значення від 1 до 15, з урахуванням наступних умов:

- Коли PTP увімкнено як джерело синхронізації часу, вихідний часовий шар відповідає налаштованому значенню.
- Коли NTP увімкнено як джерело синхронізації часу, значення вихідного часового шару буде найбільшим між вхідним часовим шаром + 1 та налаштованим значенням.
- Коли джерело синхронізації часу недоступне (NTP-клієнт та налаштування часу PTP вимкнені, або якщо вони увімкнені, але обладнання не заблоковано), вихідний часовий шар встановлюється на 16 (несинхронізований).

Користувач також може налаштувати параметри NTP-сервера за допомогою CLI, як показано нижче:

S2024# configure terminal

S2024(config)# ntp ?

master Configure the switch to act as an authoritative NTP server

server Configure NTP server

S2024(config)# ntp master ?

stratum distance from the clock source

Для моніторингу стану NTP, включаючи сервери та клієнти за допомогою CLI, використовуйте наступну команду:

S2024# show ntp status

2.4 Налаштування часу

Внутрішній годинник Reason S20 може бути синхронізований, у порядку пріоритету, протоколами часу NTP, IEEE 1588v2 або конфігурацією налаштувань дати/часу вручну. Крім того, при використанні обладнання в інших регіонах для часового поясу та переходу на літній час (DST) може бути встановлено коригування внутрішнього годинника.

Меню Конфігурація часу (Time Configuration) знаходиться в меню Налаштування > Система > Час (Settings > System > Time).

Конфігурація дати/часу

Це поле дозволяє користувачеві вручну налаштувати дату/час системи. Можливі налаштування місяця, дати, року, годин та хвилин. Кнопка "синхронізувати" (synchronize) імпортує дату/час із веб-браузера та застосовує їх до системного часу S20. Зверніть увагу, що кнопку "синхронізувати" слід використовувати лише в тих випадках, коли NTP і PTP не використовуються для синхронізації системного часу.

Конфігурація часового поясу

Це поле дозволяє налаштувати часовий пояс, який має список із усіма дозволеними часовими поясами, та Акронім, який можна використовувати для його визначення. Можливі наступні конфігурації.

- Часовий пояс(Time Zone) : визначте часовий пояс, який використовуватиметься у внутрішньому годиннику. Дозволені значення відображаються у списку;
- Акронім (Acronym): визначте акронім для вибраного часового поясу. Дозволений розмір акроніма - до 16 символів.

Конфігурація переходу на літній час

Це поле дозволяє налаштувати перехід на літній час. При використанні внутрішній годинник враховуватиме часовий пояс плюс зміщення, налаштоване у хвилинах. Можна вибрати, чи використовуватиметься перехід на літній час лише один раз або буде повторюватися протягом усіх років. За замовчуванням перехід на літній час вимкнено. Можливі наступні конфігурації.

- Перехід на літній час (Daylight Saving Time): увімкніть або вимкніть функцію переходу на літній час (DST). Якщо увімкнено, потрібно налаштувати наступне:
  - Повторювана конфігурація літнього часу (DST):
    - Тиждень (Week): виберіть тиждень місяця, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - День (Day): виберіть день тижня, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Місяць (Month): виберіть місяць, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Години (Hours): виберіть годину доби, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Хвилини (Minutes): виберіть хвилину години, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення).
  - Неповторювана конфігурація літнього часу:
    - Місяць: виберіть місяць, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Дата: виберіть день місяця, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Рік (Year): виберіть рік, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Години: виберіть годину доби, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення);
    - Хвилини: виберіть хвилину години, коли має початися перехід на літній час (якщо в налаштуваннях часу початку) або закінчитися (якщо в налаштуваннях часу закінчення).
  - Зміщення (Offset): встановіть зміщення, яке застосовуватиметься до внутрішнього годинника при переході на літній час, у хвилинах. Це значення буде додано до внутрішнього годинника під час переходу на літній час.

2.5 Журнал реєстрації

Функція журналу реєстрації забезпечує, щоб усі події операційної системи записувались в енергонезалежну пам’ять, або самим комутатором, або виділеними серверами журналів. У багатьох випадках такі журнали потрібні для цілей аналізу, оскільки вони містять збережені запущені (робочі) програми, зміни конфігурації або інформацію про фізичні з'єднання, такі як активні порти Ethernet.

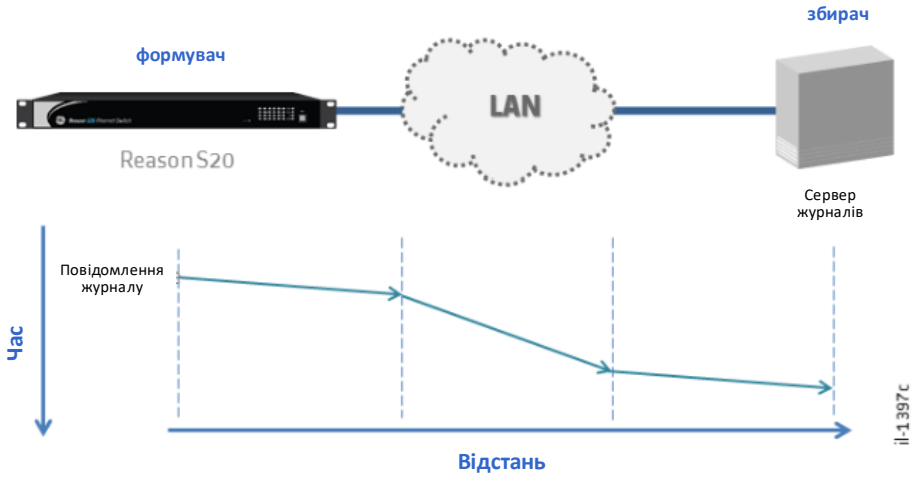


Рис. 14: Основні принципи повідомлень системного журналу NTP

Для використання на комп’ютері, формат файлу журналу (відомий як syslog) стандартизований відповідно до RFC 5424. Цей RFC не визначає протокол транспортного рівня. Використання протоколу UDP для програмних застосунків syslog визначене у RFC 5426, і цей документ визначає, що для програмних застосунків syslog потрібно використовувати принаймні порт 514 UDP. Інші порти, якщо застосовні, повинні бути налаштовані.
Reason S20 може зберігати журнальні повідомлення у внутрішній енергонезалежній пам'яті та надсилати їх на два виділені сервери системних журналів. Використовуючи внутрішню пам’ять, S20 може зберігати понад 2048 повідомлень журналу (кільцевий буфер) та всі зареєстровані типи категорій. Щоб завантажити або візуалізувати повідомлення, що зберігаються у внутрішній пам'яті, зверніться до розділу моніторингу.
Щоб налаштувати до двох віддалених серверів системних журналів, використовуйте наступні налаштування.

Меню конфігурації системного журналу знаходиться в меню Налаштування > Система > Журнал (Settings > System > Log). Наступні інструкції застосовуються як до Сервера 1, так і до Сервера 2.

Режим сервера

Це поле використовується для увімкнення/вимкнення надсилання повідомлень системного журналу на віддалений сервер. За замовчуванням цей режим вимкнений. Щоб увімкнути, виберіть "Увімкнено" (Enabled) у списку "Режим" (Mode), а потім налаштуйте дійсну IP-адресу сервера.

Адреса сервера

Це поле визначає мережеву IP-адресу сервера системних журналів, який буде отримувати повідомлення журналу. Підтримуються тільки значення IPv4, і IP-адреса повинна бути вставлена як десяткове позначення з крапками.

Якщо на комутаторі налаштовано сервер системних журналів, переконайтеся, що IP-адреса Reason S20 налаштована на сервері системних журналів, і він здатний отримувати повідомлення журналу через порт UDP 514.

Рівень системного журналу

Цей список дозволяє користувачеві вибрати, який рівень серйозності повідомлень журналу буде використовуватися як фільтр. Рівень системного журналу Reason S20 розділений на 4 категорії: помилка (серйозність 3), попередження (серйозність 4), повідомлення (серйозність 5) та інформація (серйозність 6). Рівні серйозності визначені в документі RFC 5424. При виборі більш високих рівнів серйозності, Reason S20 надсилатиме всі повідомлення нижчих рівнів плюс вибраний рівень серйозності.

Таким чином, вибір рівня серйозності інформації означає, що всі повідомлення журналу будуть надіслані на віддалений сервер системних журналів. З іншого боку, якщо вибрати рівень серйозності "помилка", віддалений сервер системних журналів отримуватиме тільки повідомлення про помилки.

3 Налаштування портів

Порти Ethernet – це з'єднання між Фізичним рівнем та Рівнем каналу (передачі) даних. Функції Рівня 2 в основному виконуються на Рівні каналу даних.

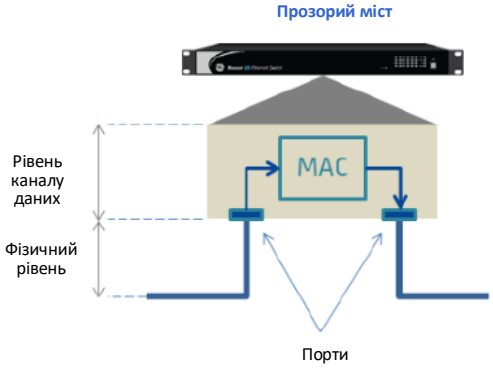


Рис. 15: Порти на прозорому мосту

Оскільки робота Ethernet-комутатора повинна бути реалізована в якості прозорого мосту, він має справу з фізичним середовищем, в якому знаходяться всі потоки пакетів даних і кінцеві вузли мережі Ethernet, що є клієнтами передачі даних.

Для мідних з'єднань Reason S20 може бути налаштований на автоматичне узгодження або швидкість порту може бути встановлена вручну. Навіть використовуючи автоматичний режим швидкості та передачі, можна визначити, яка швидкість та режим будуть кращими при підключенні до обладнання. За замовчуванням комутатор налаштований на автоматичне узгодження і надає перевагу повній пропускній здатності (тобто, 1 Гбіт/с для гігабітних портів у повнодуплексному режимі або 100 Мбіт/с для швидкісних портів Ethernet у повнодуплексному режимі), проте, він може бути налаштований користувачем. Для оптичних з'єднань швидкість попередньо визначена апаратним забезпеченням SFP, отже, вона може становити 100 Мбіт/с або 1 Гбіт/с. Крім того, оптичні порти не можуть працювати у напівдуплексному режимі. З цієї причини оптичні порти можуть бути налаштовані тільки як вимкнені або працювати із заданою швидкістю, у повнодуплексному режимі.

Меню конфігурації портів знаходиться в меню Налаштування > Порти (Settings > Ports).

У першому стовпці "Порт" (Port) перераховані всі порти комутатора. Другий стовпець доступний для визначення "опису" (description) для кожного порту, якщо це необхідно. У третьому стовпці "Канал" (Link) відображається статус даного каналу. Червоний колір означає неактивний канал, а зелений колір означає активне підключення каналу. У четвертому стовпці відображається поточна швидкість для тих портів, які мають підключення.

Налаштована швидкість

Це поле дозволяє налаштувати швидкість на даному порту. Конфігурація швидкості порту буде залежати від типу порту (електричного або оптичного), і можливі наступні варіанти.

- **Вимкнено (Disabled)**: вимкніть порт, тобто вимкніть зв’язок на цьому порту;

Щоб відповідати стандартам кібербезпеки, порти, які не використовувались, повинні бути відключені.

- **Авто (Auto)**: увімкнути автоматичне узгодження швидкості порту;
- **10 Мбіт/с HDX**: увімкнути швидкість порту до 10 Мбіт/с у напівдуплексному режимі;
- **10 Мбіт/с FDX**: увімкнути швидкість порту до 10 Мбіт/с у повнодуплексному режимі;
- **100 Мбіт/с HDX**: увімкнути швидкість порту до 100 Мбіт/с у напівдуплексному режимі;
- **100 Мбіт/с FDX**: увімкнути швидкість порту до 100 Мбіт/с у повнодуплексному режимі;
- **1 Гбіт/с FDX**: увімкнути швидкість порту до 1 Гбіт/с у повнодуплексному режимі;

Оголошення Дуплексного режиму (Adv Duplex)

Налаштувати оголошення режиму зв'язку каналу-партнера з кожного порту, коли налаштування швидкості визначається як **Автоматичне (Auto)**. За замовчуванням усі виявлені порти в дуплексному режимі будуть виконувати оголошення для своїх партнерів з дуплексною пропускною здатністю.

- **Прапорець Fdx**: увімкнути оголошення підтримки повнодуплексного режиму каналу;
- **Прапорець HDX**: увімкнути оголошення підтримки напівдуплексного режиму каналу;

Оголошення Швидкості (Adv speed)

Це поле дозволяє налаштувати оголошення швидкості зв'язку каналу-партнера, коли налаштування швидкості визначається як **Автоматичне (Auto)**. За замовчуванням вся пропускна здатність порту (10/100/1000 Мбіт/с) буде оголошуватися для своїх партнерів з повною пропускною здатністю (до 1 Гбіт/с).

- **Прапорець Швидкість 10**: увімкнути оголошення підтримки швидкості 10 Мбіт/с;
- **Прапорець Швидкість 100**: увімкнути оголошення підтримки швидкості 100 Мбіт/с;
- **Прапорець Швидкість 1000**: увімкнути оголошення підтримки швидкості 1 Гбіт/с;

Максимальний блок передачі (MTU)

Це поле надає можливість налаштувати максимальний блок передачі (MTU), іншими словами, це розмір найбільшого блоку даних протоколу мережевого рівня, який може передаватися через один порт Ethernet. Передачі із розмірами, що перевищують зазначені в цьому полі, відкидаються. Розмір повинен бути налаштований для пакетів від 1518 до 10056 байт.

Режим надмірного зіткнення

Зіткнення (колізії) можуть статися, коли порт працює в напівдуплексному режимі, коли існує можливість того, що два хости одночасно надсилають кадри передачі, генеруючи колізії на фізичному рівні та рівні каналу даних. Після 16 зіткнень Reason S20 вмикає Режим надмірного зіткнення, який за замовчуванням відкидає кадри, але передбачено наступні варіанти:

- **Відкинути (Discard):** відкинути кадр після 16 зіткнень на порту;
- **Перезапуск (Restart):** перезапустити алгоритм відмови після 16 зіткнень на порту.

Перевірка довжини кадру

Налаштовує, чи кадри з неправильною довжиною кадру в полі EtherType/Length повинні бути скинуті. Кадр Ethernet містить поле EtherType, яке можна використовувати для позначення розміру корисних даних кадру (у байтах) для значень 1535 і нижче. Якщо увімкнено функцію "Перевірка довжини кадру" (frame length check), обчислюються кадри з розміром корисних даних менше 1536 байт, і якщо поле EtherType/Length не відповідає фактичній довжині корисних даних, вони скидаються.

Якщо поле EtherType/Length перевищує 1535, це вказує на те, що поле використовується як тип EtherType (вказуючи на те, який протокол інкапсульований у корисні дані кадру).

4 Безпека комутатора

Кібербезпека є актуальною темою в наш час, і оскільки технологія Ethernet широко використовується в системах автоматизації, важливість мережевої безпеки з роками зростає. Обладнання, яке використовується для вирішення завдань автоматизації мережі, розроблене з урахуванням вимог щодо кібербезпеки.
Що стосується комутаторів, необхідно оцінити безпеку керування та доступу. У цьому пункті описані основні конфігурації безпеки, пов’язані з керуванням доступом та доступними інтерфейсними протоколами.
Дотримуючись стандартів кібербезпеки, Reason S20 має набір функцій безпеки, наведених нижче. Щоб налаштувати параметри безпеки комутатора, перейдіть до Налаштування > Безпека > Комутатор (Settings > Security > Switch).

4.1 Користувачі та паролі

Можна створити кілька облікових записів користувачів, де кожен користувач має свій конкретний пароль та рівень привілеїв. Паролі зашифровані за допомогою SHA-2 і повинні мати щонайменше 8 символів, включаючи малі/великі букви, цифри та спеціальні неалфавітні символи (наприклад, #, $, @, &). Недійсними символами є:? та *пробіл*.
Згідно з заводськими параметрами, паролем Reason S20 для адміністратора є серійний номер обладнання (тільки цифри), але його потрібно змінити після першого входу до системи. Кожен користувач може змінити власний пароль, а облікові записи адміністраторів – будь-який пароль.
Спроби входу (успішні чи невдалі) зберігаються в енергонезалежній флеш-пам'яті системного журналу. Після трьох невдалих спроб входу обліковий запис блокується і потрібно зачекати 1 хвилину, щоб повторити нові три спроби.
За замовчуванням строк дії паролів також закінчується через 6 місяців. Цей параметр також може бути налаштований користувачем, і він може бути вимкнений або його період дії змінений. Строк дії пароля використовує як опорне значення дату внутрішнього годинника на момент збереження конфігурації. Таким чином, рекомендується налаштувати системний час перед створенням нових облікових записів користувачів.

- **Строк дії пароля (Password Expiration)**: увімкнено/вимкнено. За замовчуванням він увімкнений, і період дії повинен бути налаштований.
- **Період дії (Expiration Period)**: визначає період дії пароля в місяцях. Значення за замовчуванням - 6 місяців, а допустимі значення – від 1 до 120 місяців.

Під час налаштування нового користувача необхідно вказати ім’я, пароль та рівень привілеїв. Можливо налаштувати до 15 рівнів привілеїв, як описано в наступному підпункті.

- **Ім'я користувача (User Name)**: ім'я користувача, яке буде використовувати цей користувач. Дозволеними значеннями є букви, цифри та підкреслення. Максимальний розмір імені користувача – 31 символ;
- **Пароль (Password)**: пароль, який буде використовуватися для ідентифікації цього користувача. Пароль повинен містити щонайменше 8 символів, включаючи малі / великі букви, цифрові та спеціальні неалфавітні символи (наприклад, #, $, @, &). Максимальна довжина пароля – 31 символ;
- **Пароль (знову)**: повторіть пароль, введений раніше.

- **Рівень привілеїв (Privilege Level)**: виберіть рівень привілеїв для облікового запису користувача. Можливі значення – від 0 до 15. Для кожного користувача допускається тільки один рівень привілеїв.

Користувачем за замовчуванням для доступу та налаштування обладнання є користувач-адміністратор із рівнем привілеїв 15. Заводським паролем користувача адміністратора є серійний номер обладнання (тільки цифри), але його потрібно змінити після першого входу.

Нарешті, за замовчуванням недіючі користувачі виходять з системи автоматично, що налаштовується за допомогою протоколу, який використовується для встановлення зв'язку. За замовчуванням з'єднання SSH і Telnet мають час очікування 10-хвилин, тоді як HTTP/HTTPS – 60-хвилин.

4.2 Рівень привілеїв користувача

Reason S20 може мати різні рівні привілеїв для кожного обраного користувача. Доступні до 16 рівнів привілеїв, 0 – найнижчий рівень привілеїв і 15 – найвищий. Кожен користувач має один привілей, закріплений за його обліковим записом, і будь-який користувач може бачити рівні привілеїв інших користувачів. Щоб визначити, які функції користувач може читати/записувати, доступний перелік функцій, і кожна функціональна можливість може бути класифікована за бажанням адміністратора. За замовчуванням встановлено три рівні привілеїв:

- Рівень 5: користувач з доступом тільки для читання (гість);
- Рівень 10: користувач, з доступом для читання та записування (звичайний користувач);
- Рівень 15: користувач з доступом для читання, записування та керування програмним забезпеченням (адміністратор).

Для наступних описів цього керівництва рівень привілеїв 15 розглядається як обліковий запис адміністратора.

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
EVC	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
JSON_RPC	5	10	5	10
JSON_RPC_Notification	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UDLD	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
XXRP	5	10	5	10

Рис. 16: Список груп для класифікації за рівнями привілеїв (конфігурація за замовчуванням)

Стовпець "Ім'я групи" (Group Name) показує всі групи функцій, дозволених для використання в налаштуваннях рівня привілеїв.

- **Тільки для читання Конфігурації (Configuration Read-only)**: виберіть номер рівня привілеїв, який дозволить тільки читати параметри конфігурації.
- **Здійснювати читання/записування Конфігурації (Configuration/Execute Read/write)**: виберіть номер рівня привілеїв, який дозволить читати та записувати параметри конфігурації.
- **Тільки для читання Стану/Статистики (Status/Statistics Read-only)**: виберіть номер рівня привілеїв, який дозволить тільки читати параметри стану та статистики.
- **Для читання/записування Стану/Статистики (Status/Statistics Read/write)**: виберіть номер рівня привілеїв, який дозволить читати та записувати параметри стану та статистики.

Рівень привілеїв користувача повинен бути однаковим або вищим за Рівень привілеїв, призначений функції, щоб мати доступ у цій групі.

4.3 Методи автентифікації

Для доступу до S20 доступні три способи автентифікації: локальний, RADIUS або TACACS+, останні два є методами віддаленої автентифікації. Можна вибрати тип автентифікації для кожного з протоколів доступу: консольний інтерфейс (USB), Telnet, SSH та HTTP можуть мати різні методи автентифікації.
Коли вибрано локальну автентифікацію база даних користувачів (ім'я користувача, пароль та рівні привілеїв) буде зберігатися у внутрішній пам'яті комутатора, і до неї можна отримати доступ та керувати нею під час налаштування комутатора. У цьому випадку адміністратор повинен мати доступ до доступних інтерфейсів, наприклад, підключення Ethernet або USB-інтерфейс.
При використанні методу віддаленої автентифікації, або серверів RADIUS, або TACACS+, потрібен сервер, який зберігає та керує обліковими записами користувачів. Для підключення до віддаленого сервера в розділі AAA необхідно правильно налаштувати ім’я хоста та пароль (ключ).

Можливі конфігурації методу автентифікації є наступними.

- **Конфігурація методу автентифікації (Authentication Method Configuration)**: визначте спосіб автентифікації користувача під час отримання доступу через кожен інтерфейс (консоль, SSH, Telnet або HTTPS). Перший стовпець – основний метод. Після закінчення часу очікування основного методу автентифікації буде зроблена спроба використати метод, вибраний у другому стовпці. Нарешті, після закінчення часу очікування другої спроби, відбудеться спроба автентифікувати користувача за допомогою методу, вибраного у третьому стовпці.
  - **Методи (Methods)**: виберіть три методи автентифікації:
    - **Локальний (Local)**: автентифікація цього клієнта буде здійснюватися локально через базу даних обладнання;
    - **Radius**: автентифікація цього клієнта буде здійснюватися віддалено через сервер Radius;
    - **Tacacs**: автентифікація цього клієнта здійснюватиметься віддалено через сервер TACACS+;
    - **Немає (No)**: автентифікація у цьому клієнті вимкнена, і вхід в систему неможливий.
- **Конфігурація методу авторизації команд (Command Authorization Method Configuration)**: визначте спосіб автентифікації користувача під час використання CLI (інтерфейсу командного рядка) при отриманні доступу з консолі, SSH або Telnet.

- **Метод**: виберіть метод автентифікації цього клієнта. Дозволеними методами є:
  - **Tacacs**: автентифікація цього клієнта здійснюватиметься віддалено через сервер TACACS +;
  - **Немає**: автентифікація у цьому клієнті вимкнена, і вхід в систему неможливий.
- **Рівень команд (Cmd Lvl)**: дозволити всі команди цього клієнта з рівнем привілеїв вищим, ніж значення Рівня команд. Тобто це значення буде найнижчим Рівнем привілеїв, необхідним для використання інтерфейсу CLI. Допустимі значення – від 0 до 15;
- **Команди конфігурації (Cfg Cmd)**: увімкнути команди конфігурації на цьому інтерфейсі.

- **Конфігурація методу обліку (Accounting Method Configuration)**: визначте спосіб автентифікації користувача під час ведення обліку користувачів (консоль, SSH або Telnet).
  - **Метод**: виберіть метод автентифікації цього клієнта. Дозволеними методами є:
    - **Tacacs**: автентифікація цього клієнта здійснюватиметься віддалено через сервер TACACS +;
    - **Немає**: автентифікація у цьому клієнті вимкнена, і вхід в систему неможливий.
  - **Рівень команд**: увімкнути облік усіх команд цього клієнта з рівнем привілеїв вищим, ніж значення Рівня команд. Тобто це значення буде найнижчим Рівнем привілеїв, необхідним для ведення обліку. Допустимі значення - від 0 до 15;
  - **Exec**: увімкнути виконання (exec) обліку (логін) на цьому інтерфейсі.

4.4 Протоколи Telnet/SSH

Для доступу до Reason S20 доступні протоколи Telnet та SSH (Secure Shell ("безпечна оболонка")). За замовчуванням Telnet вимкнено, а SSH увімкнено, але їх можна увімкнути/ вимкнути за бажанням. Застосовуючи засоби безпеки, слід уникати використання Telnet і віддавати перевагу SSH, якщо потрібен CLI через Ethernet. Можливі конфігурації наведені нижче:

Конфігурація SSH/Telnet

- **Режим SSH (SSH Mode)**: увімкнення / вимкнення протоколу SSH.
- **Максимум з'єднань SSH (SSH Max Connections)**: визначає максимальну кількість одночасних з'єднань клієнтів SSH (від 1 до 20). Команда CLI – це "*ip ssh max-connections*".
- **Час очікування SSH (хвилин) (SSH Timeout)**: Час очікування SSH визначає інтервал очікування від неактивного сеансу для з'єднань USB/SSH. Коли інтервал проходить без активності клавіатури, час очікування спливає, і користувач повинен повторно автентифікуватися. Допустимі значення знаходяться в діапазоні від 0 до 1440, за замовчуванням 10. Значення 0 вимикає час очікування сеансу. Команда CLI - "*ip ssh timeout*".
- **Режим Telnet (Telnet Mode)**: увімкнення/вимкнення протоколу Telnet.
- **Максимум з'єднань Telnet (Telnet Max Connections)**: визначає максимальну кількість одночасних підключень клієнта Telnet (від 1 до 20). Команда CLI – це "*ip telnet max-connections*".
- **Час очікування Telnet (хвилин) (Telnet Timeout)**: Час очікування Telnet визначає інтервал очікування від неактивного сеансу для з'єднань Telnet. Коли інтервал проходить без активності клавіатури, час очікування спливає, і користувач повинен повторно автентифікуватися.

Допустимі значення знаходяться в діапазоні від 0 до 1440, за замовчуванням 10. Значення 0 вимикає час очікування сеансу. Команда CLI – "*ip telnet timeout*".

У разі використання налаштування "Максимум з'єднань" (Max Connections), адміністратори завжди повинні мати можливість підключення або через зарезервований сеанс, або шляхом відключення іншого користувача. У цьому останньому випадку перший сеанс не-адміністратора вимикається, а якщо такий відсутній, то вимикається найстаріший сеанс адміністратора.

Авторизовані ключі SSH

Авторизовані ключі SSH визначають ключі SSH, які можна використовувати для входу в обліковий запис користувача без пароля.

4.5 Протоколи HTTP/HTTPS

Оскільки веб-інтерфейс – це простий та інтуїтивно зрозумілий спосіб отримати доступ до налаштувань комутатора, протокол HTTPS є доступним і ввімкнений за замовчуванням. HTTP також доступний, але за замовчуванням вимкнений, оскільки його слід уникати і надавати перевагу HTTPS. Якщо HTTP увімкнено, рекомендується також увімкнути заголовок HSTS (автоматичне перенаправлення), щоб браузер міг визначити, чи безпечне з'єднання може бути встановлено автоматично.
Як би там не було, наполегливо рекомендується тримати протоколи HTTP і HTTPS вимкненими, як тільки пристрій S20 буде правильно налаштований і готовий до введення в роботу. Оскільки SSH і Telnet також рекомендується вимкнути, локальний інтерфейс USB (за допомогою команд CLI) може бути використаний для відновлення зв'язку через веб-інтерфейс.

Конфігурація HTTP/HTTPS є наступною:

- **HTTPS**: виберіть, чи слід увімкнути HTTPS чи ні, за замовчуванням він увімкнений. Автоматичне перенаправлення можна ввімкнути, тільки якщо увімкнено HTTPS.
- **HTTP**: виберіть, чи слід увімкнути HTTP чи ні. За замовчуванням він вимкнений.
- **Максимум з'єднань (Max Connections)**: визначає максимальну кількість одночасних підключень клієнта HTTP/HTTPS (від 1 до 20). Команда CLI – це "*ip http max-connections*".
- **Автоматичне перенаправлення (Automatic Redirect)**: виберіть, чи слід автоматично перенаправляти з'єднання HTTP на з'єднання HTTPS, використовуючи заголовок HSTS.
  - **Увімкнено**: заголовок HSTS увімкнено;
  - **Вимкнено**: заголовок HSTS вимкнено.
- **Час очікування HTTP/S (хвилини) (HTTP/S Timeout)**: Час очікування HTTP/S визначає інтервал очікування від неактивного сеансу для з'єднань веб-інтерфейсу. Коли інтервал проходить без активності клавіатури, час очікування спливає, і користувач повинен повторно автентифікуватися. Допустимі значення знаходяться в діапазоні від 0 до 1440, за замовчуванням 60. Значення 0 вимикає час очікування сеансу. Команда CLI – "*ip http secure-timeout*".
- **Конфігурація SSL (SSL Configuration)**: вкажіть конфігурацію SSL, яка використовується для узгодження з'єднання з віддаленим клієнтом.
  - **Спеціальна (Custom)**: для служб, які потребують індивідуальних наборів шифрів.
  - **Безпечна (Secure)**: для служб, які не потребують зворотної сумісності, забезпечує більш високий рівень безпеки.

Ця конфігурація сумісна з Firefox 27, Chrome 30, IE 11 у Windows 7, Edge, Opera 17, Safari 9, Android 5.0 та Java8.
Протокол: TLS v1.2
Набір шифрів (Cipher suite): ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256

- **За замовчуванням (Default)**: для служб, які не потребують сумісності із застарілими клієнтами (здебільшого WinXP), але все одно мають підтримувати широкий діапазон клієнтів. Сумісна з Firefox 1, Chrome 1, IE 7, Opera 5 та Safari 1. Це варіант за замовчуванням.
  Протоколи: TLS v1.2, TLS v1.1, TLS v1
  Набір шифрів: ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
- **Сумісність (Compatible)**: Це старий набір шифрів, який працює з усіма клієнтами часів Windows XP /IE6. Його слід використовувати лише в крайньому випадку.
  Протоколи: TLS v1.2, TLS v1.1, TLS v1, SSL v3
  Набір шифрів: ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:DES-CBC3-SHA:HIGH:SEED:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!RSAPSK:!aDH:!aECDH:!EDH-DSS-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA:!SRP

- **Підтримка сертифікатів (Certificate Maintain)**: виберіть, який режим використовувати для підтримки сертифікації HTTPS. Дозволено лише тоді, коли Режим вимкнено.

- **Немає (None)**: жодних дій щодо підтримки сертифікації не буде здійснено;
- **Видалити (Delete)**: видалити сертифікацію;
- **Завантажити (Upload)**: завантажити сертифікат. Якщо дозволено, з'являться поля "Кодова фраза", "Завантаження сертифіката" та "Завантаження файлу". Можливі наступні значення:
  - **Кодова фраза (PassPhrase)**: введіть кодову комбінацію, що буде використовуватися для шифрування сертифіката;
  - **Завантаження сертифіката (Certificate Upload)**: виберіть спосіб завантаження сертифіката. Можливі режими – веб-браузер та URL. Можливі наступні конфігурації:
    - **Веб-браузер (Web Browser)**: завантаження сертифікатів здійснюється через Веб-браузер. При використанні цього методу необхідно завантажити дійсний файл веб-браузера, щоб виконати завантаження сертифіката в рядку Завантаження файлу (File Upload);
    - **URL**: завантаження сертифіката здійснюється за вказаною адресою. При використанні цього методу необхідно ввести URL-адресу, яка буде використовуватися в рядку URL-адреси, використовуючи наступну методологію:
      <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>];
- **Створити (Generate)**: створити сертифікат. Якщо дозволено, з'явиться поле Алгоритм сертифіката (Certificate Algorithm). Можливі наступні значення:

- **Стан сертифіката (Certificate Status)**: відображає інформацію про стан фактичної сертифікації HTTPS на комутаторі. Можливі наступні значення:
  - **Сертифікат захищеного HTTP комутатора представлений**: сертифікація зберігається в базі даних HTTPS;
  - **Сертифікат захищеного HTTP комутатора відсутній**: сертифікація не зберігається в базі даних HTTPS;
  - **Сертифікат захищеного HTTP комутатора генерується ...:** комутатор генерує сертифікацію, яка зберігатиметься в базі даних HTTPS.

4.6 Керування доступом

Доступ може бути обмежений визначеною VLAN або діапазоном IP-адрес. Для кожної групи VLAN та діапазонів IP-адрес може бути обраний тип увімкненого протоколу зв'язку: HTTP/HTTPS, TELNET/SSH та протокол SNMP для віддаленого моніторингу.
За замовчуванням він вимкнений, тобто будь-який користувач з будь-якої IP-адреси або VLAN за допомогою будь-якого протоколу доступу може отримати доступ до обладнання. Якщо увімкнено, це меню дозволяє керувати VLAN, діапазоном IP-адрес та протоколами. Максимальна кількість фільтрів, що застосовуються в системі Керування доступом, - 16.
Якщо керування доступом **увімкнено**, у пункті **Додати новий запис (Add New Entry)** надається можливість вставити новий фільтр, який буде застосовуватися до інтерфейсів доступу.

- **Видалити (Delete)**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Ідентифікатор VLAN (VLAN ID)**: вкажіть ідентифікатор VLAN, який дозволяє отримати доступ до інтерфейсів керування. Дозволені значення – це дозволені значення VLAN (від 1 до 4095);

- **Початкова IP-адреса (Start IP Address)**: вкажіть найнижчу IP-адресу, дозволену для доступу до інтерфейсів керування. IP-адреса повинна бути вставлена як десяткове позначення з крапками;
- **Кінцева IP-адреса (End IP Address)**: вкажіть найвищу IP-адресу, дозволену для доступу до інтерфейсів керування. IP-адреса повинна бути вставлена як десяткове позначення з крапками;
- **HTTP/HTTPS**: дозволяє, якщо обрано, хосту отримувати доступ до комутатора через протокол HTTP і HTTPS у налаштованій VLAN та в межах вказаного діапазону IP-адрес;
- **SNMP**: дозволяє, якщо обрано, хосту отримувати доступ до комутатора через протокол SNMP у налаштованій VLAN та в межах вказаного діапазону IP-адрес;
- **Telnet/SSH**: дозволяє, якщо обрано, хосту отримувати доступ до комутатора через інтерфейс Telnet або SSH у налаштованій VLAN та в межах вказаного діапазону IP-адрес.

5 Простий протокол мережевого керування (SNMP)

Протокол SNMP був створений в середині 1990-х років для розширення обсягів керівної інформації, яку мережеві пристрої дозволяють надсилати на робочі станції. Створення протоколу для надсилання на сервер стандартизованої інформації через IP-мережі збільшило можливості обслуговування та діагностики мережі. Існують десятки керівних документів RFC, що стосуються SNMP, наприклад, RFC 1157 (Простий протокол мережевого керування) або RFC 3418 (База керуючої інформації (MIB) для Простого протоколу мережевого керування). При використанні цього протоколу важливо вказати перелік відповідної документації RFC до застосування.

5.1 Основні принципи SNMP

Reason S20 підтримує три версії SNMP v1, v2c і v3, а згідно зі стандартом RFC 3584 визначено, що всі версії можуть співіснувати в мережі. Хоча мережі SNMPv1 можуть включати протоколи SNMPv3 або SNMPv2c, можливості агентів SNMPv1 неоднакові. При використанні різних версій SNMP, переконайтеся, що SNMP-адміністратор розуміє всі використовувані версії протоколу. Серед іншого, загальна інформація та керування, доступні через SNMP, включають в себе:

- Швидкість та використання інтерфейсів;
- Серійний номер обладнання та його місцезнаходження;
- Використання процесора та пам'яті;
- Внутрішня температура;
- Помилки канального рівня (з'єднання);
- Час з моменту останнього завантаження системи;
- Стан сигналізації;
- Увімкнення / вимкнення протоколів керування зв’язком: HTTP/HTTPS, SSH та Telnet;
- Завантаження та встановлення файлу конфігурації;
- Оновлення вбудованого ПЗ ("прошивки").

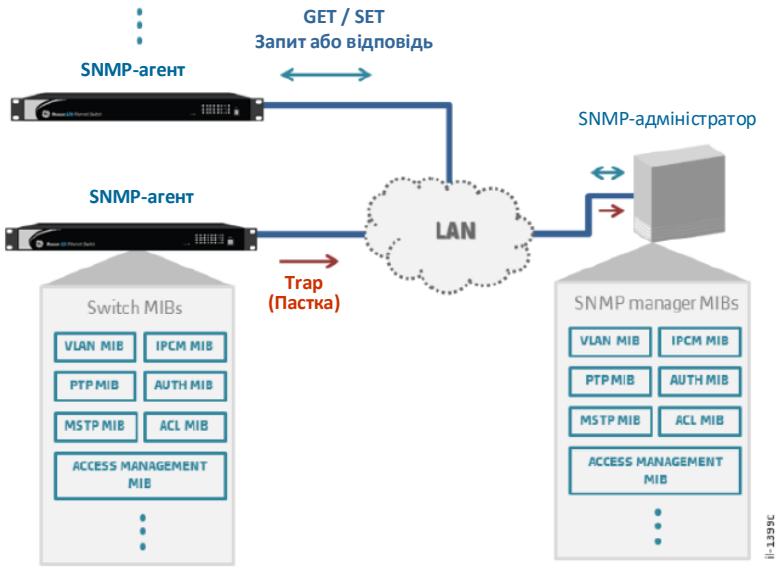


Рис. 17: Приклад архітектури керування SNMP

Загальний принцип роботи базується на запитах GET та SET, які SNMP-адміністратор надсилає агентам. Під час роботи адміністратор буде періодично запитувати інформацію від агентів, незалежно від інформації, отриманої на момент її виникнення. Такі приклади, як приєднання (Link up), інформація протоколу STP або "холодний" запуск (Cold Start) комутатора, можуть надсилатися SNMP-агентами без запиту від сервера. Останній тип операції називається Trap ("Пастка"), а асинхронне повідомлення, отримане від агента, - Trap-повідомлення.
Коли інформація SNMP повинна надсилатися через мережу, агент здійснюватиме пошук у власній бібліотеці інформації протоколу SNMP, щоб з'ясувати, чи може бути задоволений запит, зроблений адміністратором. Інформаційна бібліотека називається Базою керуючої інформації (MIB). Як адміністратор, так і агент повинні мати бібліотеки MIB на власному обладнанні, щоб розуміти інформацію, якою обмінюються між собою. Що стосується Trap-повідомлень, існує кілька бібліотек MIB, які можна налаштувати на розсилку без запиту адміністратора.

5.2 Конфігурація SNMP

Обмін повідомленнями SNMP відбувається в IP-мережі, як правило, за допомогою транспортного протоколу UDP. UDP-порт 161 використовується для надсилання повідомлень-запитів, а UDP-порт 162 – для Trap-повідомлень.
За замовчуванням SNMP вимкнено на комутаторах Reason S20, і щоб змінити його конфігурацію, перейдіть до Налаштування > Безпека > Комутатор > SNMP (Settings > Security > Switch > SNMP).

Система

Меню "Система" (System) дозволяє виконувати конфігурацію основних налаштувань SNMP і ввімкнути протокол. Дозволена конфігурація показана нижче.

- **Режим (Mode)**: виберіть, чи потрібно увімкнути SNMP. Дозволені значення **Увімкнено (Enabled)**, щоб увімкнути використання протоколу SNMP або **Вимкнено (Disabled)**, щоб вимкнути використання протоколу SNMP.

- **Версія (Version)**: виберіть, яку версію SNMP слід використовувати. Допустимими значеннями є **SNMPv1, SNMPv2c** та **SNMPv3**;
- **Читати Рядок спільноти (Read Community)**: вказує доступ до рядка спільноти для читання, який дозволяє доступ SNMP-агента. Використовується лише у версіях SNMPv1 та SNMPv2c. Інформацію про спільноту версії SNMPv3 можна отримати в таблиці спільнот. Дозволена довжина рядка – до 255, а дозволеними символами є символи ASCII від 32 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Редагувати Рядок спільноти (Write Community)**: вказує доступ до рядка спільноти для редагування, який дозволяє доступ SNMP-агента. Використовується лише у версіях SNMPv1 та SNMPv2c. Інформацію про спільноту версії SNMPv3 можна отримати в таблиці спільнот. Дозволена довжина рядка – до 255, а дозволеними символами є символи ASCII від 32 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Ідентифікатор механізму (Engine ID)**: вказує ідентифікатор механізму (агента) SNMPv3. Використовується тільки у версії SNMPv3.

Trap

Меню "Trap" ("Пастки")дозволяє здійснювати конфігурацію розсилки trap-повідомлень в рамках протоколу SNMP. Тоді як загальні SNMP-повідомлення повинні запитуватися SNMP-сервером, Trap-повідомлення надсилаються автоматично, коли відбувається подія (Trap-повідомлення) або циклічно (повідомлення-сповіщення про відправку, на SNMPv3). Дозволена конфігурація показана нижче.

- **Глобальні налаштування (Global settings)**: виберіть, чи надсилання Trap-повідомлення слід Увімкнути чи Вимкнути (Enabled та Disabled). За замовчуванням воно вимкнене;

Якщо Trap увімкнено, необхідно налаштувати, які повідомлення слід надсилати без запиту SNMP-сервера. За допомогою кнопки **Додати новий запис (Add New Entry)** можна вставити новий Trap, який потрібно застосувати. При натисканні на нього з’явиться меню **Конфігурації Trap SNMP (SNMP Trap Configuration)** з наступними полями для налаштування:

- **Ім'я конфігурації Trap (Trap Config Name)**: вказує ім'я конфігурації Trap. Дозволені символи – це символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Режим Trap (Trap Mode)**: увімкніть ці налаштування для функціонування Trap-повідомлень SNMP. Дозволені значення Увімкнено або Вимкнено;
- **Версія Trap (Trap Version)**: виберіть SNMP-версію повідомлень Trap. Допустимими значеннями є SNMPv1, SNMPv2c та SNMPv3;
- **Спільнота Trap (Trap Community)**: вказує назву спільноти Trap. Дозволені символи – це символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Адреса призначення Trap (Trap Destination Address)**: вказує місце призначення Trap-повідомлень, тобто SNMP-сервер, відповідальний за цей вузол. IP-адреса повинна бути вставлена як десяткове позначення з крапками;
- **Порт призначення Trap (Trap Destination Port)**: вказує порт UDP, який використовується для транспортування Trap-повідомлень. За замовчуванням це значення – 162. Допустимі значення – від 1 до 65 535 UDP-портів;
- **Режим сповіщення Trap (Trap Inform Mode)**: увімкніть ці налаштування, щоб увімкнути функцію Trap-повідомлень в режимі сповіщення. У цьому випадку Trap-повідомлення з цією назвою конфігурації Trap будуть надсилатися циклічно у певний час. Тільки SNMPv3 підтримує цей режим роботи. Дозволені значення Увімкнено або Вимкнено;

- **Час очікування сповіщення Trap (секунди) (Trap Inform Timeout)**: вказує час очікування операції сповіщення Trap. За замовчуванням це значення становить 3 секунди. Допустимі значення – від 0 до 2147 секунд;
- **Кількість спроб сповіщення Trap (Trap Inform Retry Times)**: вказує, скільки разів операція сповіщення Trap повторить спробу надсилання повідомлення-сповіщення. За замовчуванням це значення становить 5 разів. Допустимі значення – від 0 до 255 разів;
- **Ідентифікатор механізму безпеки зонду Trap (Trap Probe Security Engine ID)**: увімкніть використання ідентифікатора механізму (engine ID) як облікових даних для зондів Trap SNMP. Дозволені значення Увімкнено або вимкнено;
- **Ідентифікатор механізму безпеки Trap (Trap Security Engine ID)**: вказує engine ID, який використовується як облікові дані для зондів Trap SNMP. Якщо ідентифікатор механізму безпеки Trap увімкнено, використовується engine ID, показаний у меню Система (System). В іншому випадку значення в цьому полі буде використовуватися як engine ID;
- **Ім'я безпеки Trap (Trap Security Name)**: вказує ім'я безпеки Trap. Якщо використовуються Trap-повідомлення та повідомлення-сповіщення, для кожного з них потрібне своє власне ім'я безпеки.

Після визначення основних конфігурацій розсилки та автентифікації Trap-повідомлень та Повідомлень-сповіщень (Inform), за даною конфігурацією Trap необхідно повідомити, яка подія призведе до надсилання цих повідомлень. Ці налаштування виконуються в полі подій Trap SNMP. Дозволена конфігурація показана нижче.

- **Система (System)**: увімкнути Trap-повідомлення "Гарячого" запуску (Warm Start) або "Холодного" запуску (Cold Start). Прапорець "*" автоматично вибирає всі можливості;
- **Інтерфейс (Interface)**: увімкнути Trap-повідомлення про з’єднання та роз’єднання портів і протокол LLDP. Варіант "Немає" (None) означає відсутність порту, налаштованого на відправлення Trap-повідомлення, вибрана опція дозволяє користувачеві вибрати, які порти будуть генерувати Trap-повідомлення, і всі комутатори вибирають усі порти для створення Trap-повідомлень. З’єднання та роз’єднання портів та порти LLDP можуть бути вільно налаштовані;
- **Автентифікація (Authentication)**: увімкнути повідомлення про помилку автентифікації SNMP, щоб генерувати Trap-повідомлення;
- **Комутатор (Switch)**: увімкніть надсилання Trap-повідомлень STP та RMON.

Спільноти

Меню "Спільноти" (Communities) дозволяє налаштувати таблицю спільнот SNMPv3. За замовчуванням створюються публічні та приватні спільноти. Щоб додати нові спільноти, натисніть кнопку Додати новий запис (Add New Entry). При натисканні з’являться наступні поля для налаштування:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Спільнота (Community)**: вказує ім'я спільноти, щоб дозволити доступ агента SNMPv3. Максимальна довжина імені спільноти – 32, а дозволеними символами є символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_"). Для SNMPv1 та SNMPv2c ім'я спільноти буде розглядатися як ім'я безпеки.
- **IP джерела (Source IP)**: вказує адресу джерела доступу до SNMP. IP-адреса повинна бути вставлена як десяткове позначення з крапками;
- **Маска джерела (Source Mask)**: вказує адресу маски джерела доступу SNMP. Адреса маски повинна бути вставлена як десяткове позначення з крапками.

Після того, як одна із описаних раніше конфігурацій змінена, є дві кнопки, які дозволяють користувачеві зберігати або скидати конфігурації.

- Зберегти (Save): зберегти конфігурацію в Робочій конфігурації (Running Config);

- Скинути (Reset): скасувати зміни, внесені локально в Робочій конфігурації.

Користувачі

Меню "Користувачі" (Users) дозволяє налаштувати конфігурацію користувача SNMPv3. Щоб додати нових користувачів, натисніть кнопку Додати новий запис. При натисканні з'являться наступні поля для налаштування:

- **Видалити**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Ідентифікатор механізму (Engine ID)**: вказує ідентифікатор engine ID, який використовує користувач. Ідентифікатор engine ID, що дорівнює ідентифікатору engine ID комутатора, означає локального користувача, а відмінний ідентифікатор engine ID означає віддаленого користувача. Номер engine ID повинен бути вставлений у шістнадцятковому форматі;
- **Ім'я користувача (User Name)**: вказує ім'я користувача, налаштованого за вказаним ідентифікатором engine ID. Максимальна довжина імені спільноти – 32, а дозволеними символами є символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Протокол автентифікації (Authentication Protocol)**: виберіть протокол, який буде використовуватися для автентифікації користувача. Можливі наступні значення:
  - **Немає (None)**: для цього користувача не використовується протокол автентифікації;
  - **MD5**: для автентифікації цього користувача використовується протокол MD5. Увімкнення цього поля дозволяє комутатору створювати прапорець, що вказує на використання цього протоколу;
  - **SHA**: для автентифікації цього користувача використовується протокол SHA. Увімкнення цього поля дозволяє комутатору створювати прапорець, що вказує на використання цього протоколу.
- **Пароль автентифікації (Authentication Password)**: пароль, який буде використовуватися для ідентифікації цього користувача. Довжина пароля для протоколу MD5 повинна становити від 8 до 32 символів, а для протоколу SHA – від 8 до 40 символів. Дозволені символи – це символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Протокол конфіденційності (Privacy Protocol)**: виберіть протокол конфіденційності, в якому братиме участь цей запис. Можливі наступні значення:
  - **Немає**: для цього користувача не використовується протокол конфіденційності;
  - **DES**: використовується протокол DES. Увімкнення цього поля дозволяє комутатору створювати прапорець, що вказує на використання цього протоколу;
  - **AES**: використовується протокол AES. Увімкнення цього поля дозволяє комутатору створювати прапорець, який вказує на використання цього протоколу.
- **Пароль конфіденційності (Privacy Password)**: пароль, який буде використовуватися для ідентифікації цього користувача. Довжина пароля повинна становити від 8 до 32 символів. Дозволені символи – це символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");

Після того, як одна із описаних раніше конфігурацій змінена, є дві кнопки, які дозволяють користувачеві зберігати або скидати конфігурації.

- Зберегти (Save): зберегти конфігурацію в Робочій конфігурації (Running Config);
- Скинути (Reset): скасувати зміни, внесені локально в Робочій конфігурації.

Групи

Меню "Групи" (Groups) дозволяє налаштувати таблицю груп SNMPv3. За замовчуванням створюються default_ro_group і default_rw_group.

Щоб додати нову групу, натисніть кнопку Додати новий запис. При натисканні з’являться наступні поля для налаштування:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Модель безпеки (Security Model)**: виберіть модель безпеки, яка буде використовуватися в даній групі. Допустимими значеннями є v1, v2c та usm. Модель безпеки USM – це модель безпеки на рівні користувачів. Моделі безпеки V1 та v2c зарезервовані для використання SNMPv1 та SNMPv2c;
- **Ім'я безпеки (Security Name)**: виберіть ім'я безпеки, до якого буде віднесена група. Можливі значення – **загальнодоступний** та **приватний (public** та **private)**, для моделей безпеки v1 та v2c, та default_user для моделі безпеки usm;
- **Ім'я групи (Group Name)**: вказує ім'я створеної групи. Максимальна довжина імені спільноти – 32, а дозволеними символами є символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_").

Представлення

Меню "Представлення" (Views) дозволяє налаштувати таблицю представлення SNMPv3 для вибору елементів, які повинні або не повинні відображатися на дереві ідентифікатора об'єкта OID SNMP. За замовчуванням створюється представлення default_view. Щоб додати нове представлення, натисніть кнопку Додати новий запис (Add New Entry), і з’явиться наступне поле:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Ім'я представлення (View Name)**: вказує ім'я створеного представлення. Максимальна довжина імені спільноти – 32, а дозволеними символами є символи ASCII від 33 до 126 (в основному букви, цифри та інші символи, такі як "-" або "_");
- **Тип представлення (View Type)**: виберіть, чи потрібно включити це представлення до піддерева SNMP OID чи ні. Можливі значення **включено** або **виключено (included** або **excluded)**. Включено означає, що це представлення відображатиметься у піддереві OID, а виключено означає, що це представлення не відображатиметься у піддереві OID;
- **Піддерево OID (OID Subtree)**: вказує OID, який визначає корінь піддерева, для додавання до названого представлення. Дозволена довжина OID становить 128, а дозволеними символами є цифри та символ "*", перед якими завжди стоїть крапка (приклади: .1, .2,. *, тощо).

Після того, як одна із описаних раніше конфігурацій була змінена, є дві кнопки, які дозволяють користувачеві зберегти або відкинути конфігурації.

- Зберегти (Save): зберегти конфігурацію в Робочій конфігурації (Running Config);
- Скинути (Reset): скасувати зміни, внесені локально в Робочій конфігурації.

Доступ

Меню "Групи" (Groups) дозволяє налаштувати таблицю доступу SNMPv3. За замовчуванням створюються default_ro_group і default_rw_group. Щоб додати нову конфігурацію доступу, натисніть кнопку Додати новий запис (Add New Entry), і з’явиться наступне поле:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити фільтр у рядку;
- **Ім'я групи (Group Name)**: виберіть ім'я групи, яку потрібно налаштувати. Перелічені імена груп можна отримати в меню "Групи";
- **Модель безпеки (Security Model)**: виберіть модель безпеки, яка буде використовуватися для доступу. Допустимими значеннями є будь-яка, v1, v2c та usm. Виберіть будь-яку (any), якщо може використовуватися будь-яка модель безпеки. Модель безпеки USM – це модель безпеки на рівні користувачів. Моделі безпеки V1 та v2c зарезервовані для використання SNMPv1 та SNMPv2c;
- **Рівень безпеки (Security Level)**: виберіть модель безпеки, що буде використовуватися для обраної групи. Можливі значення: NoAuth, NoPriv, Auth, NoPriv та Auth, Priv. "H" (No) на початку означає відсутність використання авторизації чи конфіденційності. Таким чином, можна вибрати

рівень безпеки без автентифікації та без конфіденційності, з автентифікацію але без конфіденційності і, і нарешті, з автентифікацію та конфіденційністю;

- **Ім'я представлення для читання (Read View Name)**: виберіть ім'я, яке відображатиметься у цій Базі керуючої інформації (MIB) при запиті поточних значень. Можливі значення: "Немає" (None), "Представлення за замовчуванням" (default_view) або "Ім'я даного представлення" (name of a given view). "Немає" означає відсутність імені представлення, "Представлення за замовчуванням" означає, що MIB буде відображатися як "Представлення за замовчуванням", і, якщо створюється представлення, його ім'я, введене в меню "Представлення" (Views), може використовуватися як ім'я MIB;
- **Ім'я представлення для редагування (Write View Name)**: виберіть ім'я, яке відображатиметься у цій базі MIB при потенційно встановлених нових значеннях. Можливі значення: "Немає" (None), "Представлення за замовчуванням" (default_view) або "Ім'я даного представлення" (name of a given view). "Немає" означає відсутність імені представлення, "Представлення за замовчуванням" означає, що MIB буде відображатися як "Представлення за замовчуванням", і, якщо створюється представлення, його ім'я, введене в меню "Представлення" (Views), може використовуватися як ім'я MIB;

6 Налаштування агрегування

Функція агрегування каналів визначається стандартом IEEE 802.3ad. Метою агрегування каналів є підвищення продуктивності та доступності мережевих пристроїв з кількома з'єднаннями, завдяки чому паралельні канали працюють так, ніби вони є єдиним високопродуктивним каналом зв'язку. Ця функція також відома як групування або об’єднання портів (Port Trunking або Port Bundling). Основними перевагами використання агрегування каналів є:

- Збільшена пропускна здатність;
- Баланс навантаження на канали;
- Підвищена доступність (готовність) зв'язку.

Групування може стосуватися магістрального порту (протокол RSTP), який передає дані багатьох тегованих кадрів VLAN, або, у даному контексті, магістральних з'єднань. У цьому керівництві використовується термін "агрегований канал", коли мова йдеться про канали, які працюють у рамках агрегування.

На сьогоднішній день швидкість каналу, як правило, не є основною проблемою при модернізації локальної мережі. Оскільки мережеві пристрої стають дешевшими, модернізація пристроїв на більш швидкісні пристрої, як правило, є доступною. Крім того, що стосується резервування, функція агрегування може мати переваги для даного з'єднання між двома станціями. Оскільки поведінка двох каналів буде такою, ніби вони є одним цілим, у зв'язку між цими станціями буде наявне резервування. У випадку відмови одного з каналів, швидкість мережі зменшиться, але вона буде продовжувати працювати.

При використанні цієї функції, важливо знати, що деякі функції, такі як VLAN, протокол STP або операції CoS, працюватимуть так, ніби агреговані канали є тільки одним портом. Таким чином, фізична петля, що утворюється при з'єднанні двох мостів разом, не буде виявлена протоколом STP, оскільки функція агрегування логічно об'єднає порти. На рисунку нижче наведено приклад агрегування каналів зв'язку між двома мережевими пристроями та поведінки протоколу у випадку відмови агрегованого каналу.

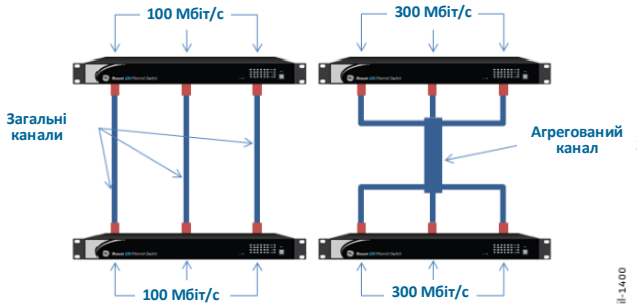


Рис. 18: Порівняння швидкості загального та агрегованого каналів

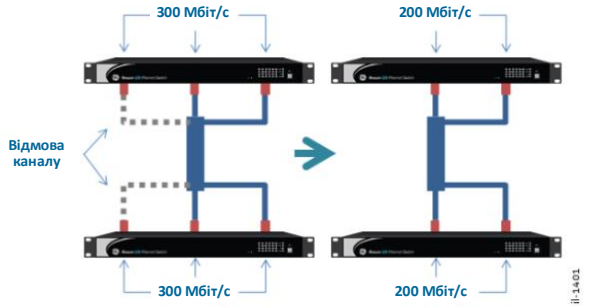


Рис. 19: Поведінка агрегованого каналу у випадку відмови каналу

В агрегованих каналах балансування навантаження не буде ідеальним через спосіб перенаправлення трафіку на каналах. Таким чином, якщо використовується три агрегованих канали по 100 Мбіт/с; можливо, що отриманий канал не буде каналом з пропускною здатністю 300 Мбіт/с.

Щоб гарантувати роботу функції агрегування, канали повинні працювати в повнодуплексному режимі з однаковою швидкістю. Таким чином, порти з різною швидкістю не повинні використовуватися як агреговані канали.

Потрібно бути обережним при налаштуванні функції агрегування на комутаторі. Оскільки фізична топологія створюватиме петлі в мережі, рекомендується налаштувати обидва комутатори перед увімкненням використовуваних портів.

Щоб використовувати цю функцію, обидва підключених мережевих пристрої повинні бути оповіщені для виконання агрегування. Крім того, агреговані порти повинні мати один і той самий ідентифікатор групи агрегування. Reason S20 може створювати до 12 груп, і максимально допустимі порти для однієї групи – це максимальна кількість портів, які має комутатор.

Балансування навантаження при агрегуванні виконується на основі деяких аспектів трафіку на портах. Reason S20 може спільно використовувати канали на основі наступних аспектів:

- MAC-адреса джерела;
- MAC-адреса призначення;
- IP-адреса;
- Номер порту TCP/UDP.

Це означає, що трафік із заданої MAC-адреси джерела буде перенаправлений через даний порт агрегованого каналу. Трафік на основі інших параметрів повинен використовувати інший канал. Таким чином, якщо між кінцевими вузлами є трафік різної пропускної здатності, буде виконано неідеальне балансування навантаження. Зрештою, видима швидкість каналу збільшиться, і з’явиться резервний тракт для трафіку кінцевих вузлів. На рисунку нижче показаний приклад такої поведінки, а використовуваний метод балансування навантаження – це MAC-адреса джерела.

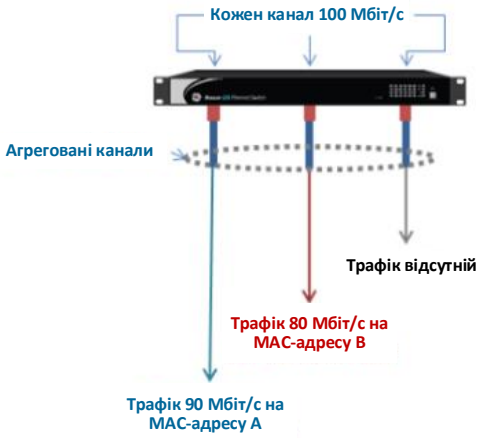


Рис. 20: Балансування навантаження на агрегованих каналах

Незважаючи на те, що загальна швидкість портів становить 300 Мбіт/с, використовується лише 170 Мбіт/с, і один з каналів не переадресовує жодного трафіку. Незважаючи на те, що доступний один порт, якщо MAC-адреса A або B потребує більшої пропускної здатності, додатковий трафік буде генеруватися на вже використовуваних портах.

6.1 Конфігурація статичного агрегування

Статичне агрегування буде агрегувати порти так, як визначає користувач, без використання автоматичних протоколів.
Меню "Статичного агрегування" (Aggregation Static) знаходиться в меню Налаштування > Агрегування > Статичне (Settings > Aggregation > Static).

Конфігурація режиму агрегування

Це меню містить налаштування, дозволені для використання в якості фільтрів у режимі статичного агрегування. У таблиці Складових хеш-коду є чотири прапорці, які можна встановити, щоб увімкнути задані параметри як фільтри статичного агрегування.

- **MAC-адреса джерела (Source MAC Address)**: для балансування трафіку використовуватиметься MAC-адресу джерела як фільтр. Поле MAC-адреси джерела в кадрі Ethernet буде використано для визначення того, на який порт групи агрегування буде перенаправлений трафік;
- **MAC-адреса призначення (Destination MAC Address)**: для балансування трафіку використовуватиметься MAC-адресу призначення як фільтр. Поле MAC-адреси призначення в кадрі Ethernet буде використано для визначення того, на який порт групи агрегування буде перенаправлений трафік;
- **IP-адреса (IP Address)**: для балансування трафіку використовуватиметься трафік IP-адреси як фільтр. IP-адреси в кадрі Ethernet будуть використані для визначення того, на який порт групи агрегування буде перенаправлений трафік;
- **Номер порту TCP/UDP (TCP/UDP Port Number)**: для балансування трафіку будуть використовуватися номери портів TCP або UDP як фільтри. Поле з номером порту TCP/UDP у кадрі Ethernet буде використане для визначення того, на який порт групи агрегування буде перенаправлений трафік.

Конфігурація групи агрегування

Це меню дозволяє визначити, які порти будуть в одній групі в режимі статичного агрегування. У таблиці є стовпець Ідентифікатора групи та стовпці Портів-членів (Group ID та Port Members). Два порти, що належать до одного ідентифікатора групи, означають, що вони будуть поводитися як один порт, і MAC-адреса, що використовується в потоці трафіку, буде MAC-адресою найменшого номера порту.

Максимальна кількість дозволених груп агрегування складатиме половину загальної кількості портів, тобто мінімальна група агрегування повинна складатися принаймні з двох портів. За замовчуванням усі порти належать до Групи зі звичайним ідентифікатором. Можливі наступні конфігурації.

- **Порти-члени (Port Members)**: виберіть, які порти будуть членами Групи з даним ідентифікаційним номером. Порти групи з однаковим ідентифікатором означають, що ці порти будуть працювати як агреговані порти.

При використанні агрегованих портів обидві сторони тракту передачі трафіку повинні бути налаштовані на роботу як Агреговані статичні порти, і обидві сторони повинні належати до Групи з однаковим ідентифікатором. Це означає, що для використання функції агрегування, обидва підключених комутатори або обидва вузли повинні підтримувати протокол агрегування. Крім того, вони повинні бути налаштовані на використання одних і тих же Складових хеш-коду, а порти, підключені для використання, повинні належати до Групи з однаковим ідентифікатором.

Після того, як одна із описаних раніше конфігурацій була змінена, є дві кнопки, які дозволяють користувачеві зберігати або скидати конфігурації.

- Зберегти (Save): зберегти конфігурацію в Робочій конфігурації (Running Config);
- Скинути (Reset): скасувати зміни, внесені локально в Робочій конфігурації.

6.2 Налаштування протоколу керування агрегуванням каналів (LACP)

Меню LACP-агрегування дозволяє налаштувати динамічне агрегування портів на комутаторі. Налаштування протоколу керування агрегуванням каналів буде автоматично агрегувати порти, коли підключено два вузли агрегування, а підключені порти дозволяють використовувати їх в режимі агрегування.
Меню LACP-агрегування знаходиться в меню Налаштування > Агрегування> LACP (Settings > Aggregation > LACP).

Конфігурація порту LACP

Усі дозволені конфігурації відображаються за замовчуванням. Перший стовпець відображає номер порту, який налаштовується в даному рядку. Інші стовпці дозволяють налаштувати порт, як показано нижче.

- **LACP увімкнено (LACP enabled)**: увімкніть використання протоколу LACP на порту. Вибраний прапорець означає, що LACP увімкнено, а порожній прапорець – вимкнено. Максимальна допустима кількість груп агрегування при використанні протоколу LACP – 32;
- **Ключ (Key)**: вказує ключ, що використовується на порту, який відображає можливості швидкості порту. Два порти можна використовувати в агрегованому режимі, лише якщо вони мають однакові швидкісні можливості, тобто той самий ключ. Якщо вибрано "Автоматична" (Auto), Reason S20 використовує значення ключа 1 для портів 10 Мбіт/с, значення ключа 2 для портів 100 Мбіт/с та значення ключа 3 для портів 1 Гбіт/с. Якщо вибрано "Визначено" (Specific), користувач може визначити ключ порту. У режимі "Визначено" дозволеними значеннями є цілі числа від 1 до 65.535.
- **Роль (Role)**: вказує правила дії LACP для використання. "Активна робота" (Active operation) означає, що порт буде передавати кадри автоматично, а "Пасивна робота" (Passive operation) означає, що порт буде передавати повідомлення тільки у відповідь на отримані повідомлення LACP з іншого боку каналу. Якщо вибрано активну роботу, порт буде передавати пакети LACP щосекунди під час роботи (порт увімкнено). Якщо вибрано пасивну роботу, порт не буде передавати пакети LACP, поки не будуть прийняті повідомлення LACP з іншого боку каналу;

- **Час очікування (Timeout)**: вказує час очікування LACP між передачами пакетів LACP. "Швидко" (Fast) дозволить передавати повідомлення LACP щосекунди, а "Повільно" (Slow) – передавати повідомлення LACP кожні 30 секунд.
- **Пріоритет (Prio)**: вказує пріоритет порту, який буде використовуватися протоколом LACP. Якщо партнер LACP намагається сформувати групу більшу, ніж підтримується пристроєм, це значення буде використано для визначення портів, які будуть використовуватися. Менші числа пріоритету означають вищий пріоритет, і група буде створена з портами з вищим пріоритетом. Допустимими значеннями є цілі числа від 1 до 65.535.

7 Захист від утворення петель

Пристрій Reason S20 підтримує виявлення та захист від мережевої петлі двома способами, використовуючи протоколи кістякового дерева (STP) або використовуючи функцію Захисту від петель (Loop Protection). У цьому пункті описано функцію захисту від петель. Зверніться до наступного пункту для опису протоколу кістякового дерева.

7.1 Основні принципи формування петель

У мережі петлю можна розуміти як більш ніж один тракт з'єднання між кінцевими точками. Типовими прикладами петлі є підключення двох комутаторів з використанням більш ніж одного порту, як це відбувається у кільцевій топології, або підключення одного порту до іншого порту того самого комутатора. На рисунку нижче показано приклад топології на основі петлі.

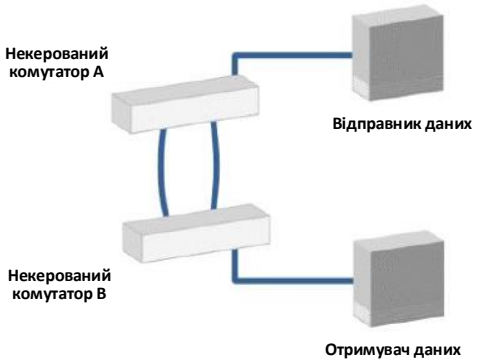


Рис. 21: Петля мосту

У наведеній петлі мосту є три основні проблеми:

- Дублювання одноадресного кадру;
- Лавинне розповсюдження багатоадресного кадру;
- Неконвергенція таблиці адрес.

Якщо Відправник даних (Data Sender) починає передавати дані до Отримувача (Data Receiver), комутатор A зрозуміє, що отримувач знаходиться на двох різних портах, і тому надішле дані на обидва порти. Комутатор B відобразить MAC-адресу отримувача на двох портах і, таким чином, надішле його з обох. Така поведінка призведе до того, що дубльовані кадри будуть вставлятися у кожні передані дані, що може спричинити небажану поведінку вузлів, наприклад, збій програми.
Якщо Відправник даних починає багатоадресну передачу, канал між комутаторами стане швидко насиченим. Оскільки комутатор працює як прозорий міст, багатоадресні кадри повинні доставлятися до всіх портів, крім вхідного порту. У наведеному прикладі комутатор A буде надсилати багатоадресну передачу комутатору B через усі порти.

Комутатор В буде виконувати алгоритм комутації і надсилатиме багатоадресний кадр на всі порти, крім порту вхідного кадру. Таким чином, багатоадресна передача, отримана на одному порту, буде відтворена на інший підключений порт і так далі. Оскільки заголовок Рівня 2 не підтримує час життя пакета (TTL), кожен кадр багатоадресної передачі буде нескінченно відтворюватися, доки не буде вичерпано ресурси або не відбудеться збій у мережі.
Нарешті, таблиця MAC-адрес не буде зіставляти фактичну топологію, оскільки порт Відправника та Отримувача буде постійно змінюватися. Якщо Відправник починає передачу даних до Отримувача, комутатори А і В спочатку бачать, що позиція отримувача – це один порт, а потім інший. Така поведінка змусить комутатор постійно перераховувати таблицю MAC-адрес, що призведе до втрати трафіку.
Резервування може бути вимогою в мережах. Резервний тракт можливий завдяки використанню протоколів резервування або визначення петлі. Для визначення петлі найпоширенішими є протоколи кістякового дерева (Spanning Tree), а для резервування каналу – Протокол агрегування каналів.

7.2 Захист від утворення петель

Функція Захисту від петель (Loop Protection) використовується для запобігання утворенню петель між одним портом та іншим портом на одному комутаторі або на портах, підключених до некерованих комутаторів, тим самим втручаючись у їх роботу. Щоб запобігти проблемам, спричиненим цими ситуаціями, функцію захисту від петель слід увімкнути на портах, де може утворитися петля.

Рис. 22: Ситуації використання захисту від петель

Функція реалізована шляхом надсилання повідомлень через усі порти, які мають можливість надсилати протокол виявлення петлі. Якщо порт, якому дозволено надсилати пакет виявлення петлі, отримує його, цей порт буде вимкнено, як тільки він виявить петлю на цьому порту.
Можна визначити час повторення передачі пакета та час, протягом якого даний порт залишатиметься вимкненим, якщо буде виявлено петлю. Крім того, для кожного порту можна вільно встановити функцію увімкненою, і визначити надсилати або не надсилати пакети виявлення петлі. Якщо виявлено петлю, дозволено три дії:

- Вимкнення порту;
- Вимкнення та здійснення запису до журналу;
- Тільки здійснення запису до журналу.

Якщо параметр Здійснення запису до журналу (Log) увімкнено, сервер журналу повинен бути налаштований для надсилання повідомлень журналу, що інформують про виявлення петлі на даному порту.

7.3 Конфігурація захисту від утворення петель

Ця функція застосовується до петлі, утвореної безпосередньо, або петлі, утвореної в некерованих комутаторах, підключених до одного порту Reason S20. Петля виявляється за допомогою повідомлень захисту від петель (повідомлення PDU). Меню "Захисту від петель" знаходиться в меню Налаштування > Захист від петель (Settings > Loop Protection).

Загальна конфігурація

У цьому меню відображаються налаштування, що стосуються увімкнення та часу, пов’язаного з цією функцією.

- **Увімкнути захист від петель (Enable Loop Protection)**: увімкнути функцію захисту від петель. "Увімкнути" (Enable) дозволить функції працювати, а "Вимкнути" (Disable) вимкне функцію захисту від утворення петель;
- **Час передачі (Transmission Time)**: вказує інтервал між кожним повідомленням захисту від петель, що надсилається до мережі. Допустимі значення становлять від 1 до 10 секунд, а значення за замовчуванням – 5 секунд;
- **Час вимкнення (Shutdown Time)**: вказує проміжок часу в секундах, протягом якого порт буде вимкнено, коли виявлено петлю, і при цьому порт налаштований на вимкнення, якщо це відбудеться. Допустимі значення становлять від 1 до 604.800 секунд, а значення за замовчуванням – 180 секунд.

Конфігурація порту

Це меню містить налаштування, дозволені для виконання при виявленні петлі. Перший стовпець відображає номер порту, який налаштовується у даному рядку, а інші стовпці дозволяють налаштувати конфігурацію цього порту. Якщо бажано застосувати одну конфігурацію до всіх портів, тоді слід використовувати рядок "*", тобто конфігурація, налаштована в рядку "*", відповідатиме всім портам. Можливі наступні конфігурації.

- **Увімкнути (Enable)**: увімкнути функцію захисту від петель на порту. Вибраний прапорець означає, що LACP увімкнено, а порожні прапорці - вимкнено;
- **Дія (Action)**: вказує на дію, яка повинна бути виконана при виявленні петлі на порту. Допустимі значення є наступними:
  - **Вимкнення порту (Shutdown Port)**: вказує, що порт буде вимкнено, коли на порту буде виявлено петлю. Період, протягом якого порт залишатиметься вимкненим, – це період, визначений у полі "Час вимкнення" (Shutdown Time);
  - **Вимкнення порту та здійснення запису до журналу (Shutdown Port and Log)**: вказує, що порт буде вимкнено при виявленні петлі, а комутатор надішле повідомлення журналу на сервер журналу, налаштований у меню "Системний журнал" (System Log). Період, протягом якого порт залишатиметься вимкненим, – це період, визначений у полі "Час вимкнення";
  - **Тільки здійснення запису до журналу (Log Only)**: вказує, що комутатор при виявленні петлі надішле повідомлення журналу на сервер журналу, налаштований у меню "Системний журнал".
- **Режим передачі (Tx Mode)**: вказує, чи порти надсилають повідомлення захисту від петель або просто чекають повідомлення PDU про утворені петлі в мережі. Якщо вибрано "Увімкнути" (Enabled), порт ефективно надсилатиме повідомлення, а якщо "Вимкнути" (Disable), порт буде тільки чекати на повідомлення PDU захисту від петель.

8 Протокол кістякового дерева (STP)

Протокол кістякового дерева – це механізм, створений для вирішення проблем, що виникають при утворенні петлі в локальній мережі. Як показано у пункті Основні принципи формування петель, мережі Ethernet не були розроблені для роботи з топологіями на основі петель. Оскільки для більшості мережевих схем зазвичай потрібні тракти резервування, для вирішення цих проблем було розроблено кілька протоколів.

Найбільш поширеним протоколом для виявлення петель є протокол кістякового дерева, визначений стандартом IEEE 802.1D-2004. Крім того, Технічний звіт МЕК 61850-90-4 визначає, що для мереж підстанцій повинен використовуватися Високошвидкісний протокол кістякового дерева (RSTP), коли на рівні підстанції потрібні топології на основі петель, такі як кільцева топологія. У цьому пункті спочатку будуть представлені основні принципи STP, а далі пояснюється, як налаштувати протокол на Reason S20.

8.1 Основні принципи кістякового дерева

У цьому пункті спочатку будуть представлені основні принципи STP, а далі увагу зосереджено на наступних конкретних протоколах:

- Протокол STP;
- Протокол RSTP;
- Протокол MSTP;
- UltraRSTP.

Потреба у протоколах для вирішення проблеми петель у мережах Ethernet виникла від початку комерційного використання. Оскільки петлі були потрібні для підвищення надійності мереж, а топології без петель важко підтримувати, автоматичне виявлення петель стало необхідністю. Тому було створено протокол кістякового дерева.

Протокол оперує відправленням та прийомом певних пакетів через мережу, щоб відобразити фактичну топологію та діяти за необхідності. Пакети являють собою пакети BPDU (Блоки протокольних даних моста), і вони структуровані, як показано нижче.

Рис. 23: Пакет BPDU

Надсилаючи ці пакети по мережі, комутатори можуть зіставити фізичну топологію для пошуку петель та їх вимкнення. Таким чином, отримана логічна топологія буде топологією дерева без петель. На наступному рисунку показані можливі тракти передачі даних від пристрою IED A до IED B.

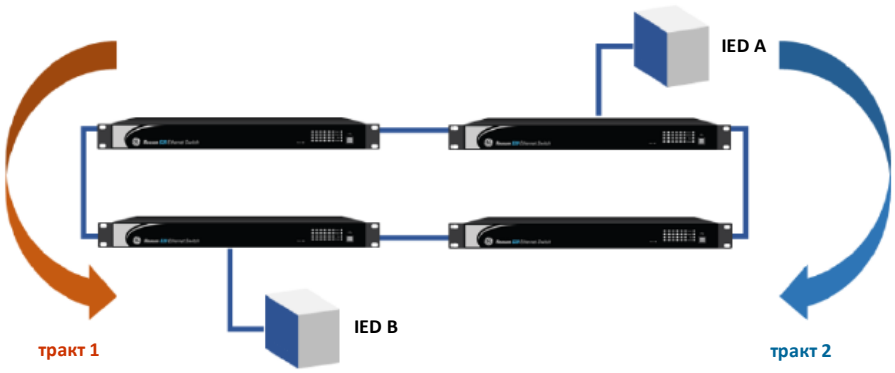


Рис. 24: Кільцева топологія LAN та можливі тракти для трафіку даних від IED A до B

Протокол працює над створенням логічної топології, яка нагадує дерево. Топологія матиме корінь; гілки, що відходять від нього до листя. Першим кроком є визначення, де знаходиться корінь дерева, іншими словами, який буде кореневим комутатором. Кореневий комутатор є логічним центром топології, а решта комутаторів будуть призначені в якості мостів.
Після призначення мостів необхідно визначити порти, які є частиною цього мосту. Вони можуть бути кореневими портами і призначеними портами. Кореневий порт – це порт призначеного мосту, який веде до кореневого комутатора, а призначені порти перенаправляють трафік від кореневого порту. Якщо порт не є призначеним портом або кореневим портом, його буде вимкнено, інакше він блокуватиме трафік. На комутаторі може бути лише один кореневий порт та кілька призначених портів.

Щоб вирішити, який комутатор буде кореневим, відбудуться вибори між усіма підтримуючими комутаторами кістякового дерева у певній локальній мережі (LAN). Кожен комутатор має ідентифікатор моста, який містить інформацію про комутатор (як правило, MAC-адресу першого порту Ethernet) та пріоритет моста. Мости з меншим числом пріоритету матимуть перевагу, коли відбудуться вибори.

Крім ідентифікатора моста, кожен порт комутатора має ідентифікатор порту, що містить номер порту та пріоритет порту. Якщо існує рівна вартість тракту, порти з меншим числом пріоритету матимуть перевагу в дереві.

Вартість тракту – це число, яке використовується для мостів, що задіяні в кістяковому дереві, щоб вирішити, який тракт слід використовувати як гілку дерева. Якщо порт має більшу швидкісну здатність, вартість тракту буде нижчою. Обраним трактом буде тракт до мосту з найменшою вартістю. Наступна таблиця ілюструє рекомендований діапазон вартості, який слід використовувати:

Рекомендований діапазон вартості трактів:

Таблиця 3: Рекомендація щодо діапазону вартості трактів STP

Швидкість передачі даних	Рекомендований діапазон вартості
10 Мбіт/с	50-600
100 Мбіт/с	10-60
1 Гбіт/с	3-10

На рисунку нижче наведено приклад цих визначень. Показане число є ідентифікатором моста, а також показано вартість тракту до всієї фізичної топології. У цьому прикладі всі пріоритети мостів і пріоритети портів вважатимуться однаковими. Таким чином, логічна топологія буде визначена тільки на основі вартості тракту та ідентифікатора моста.

Крім того, вважається, що всі комутатори надсилають і отримують пакети BPDU для відображення топології та відключення активних петель.

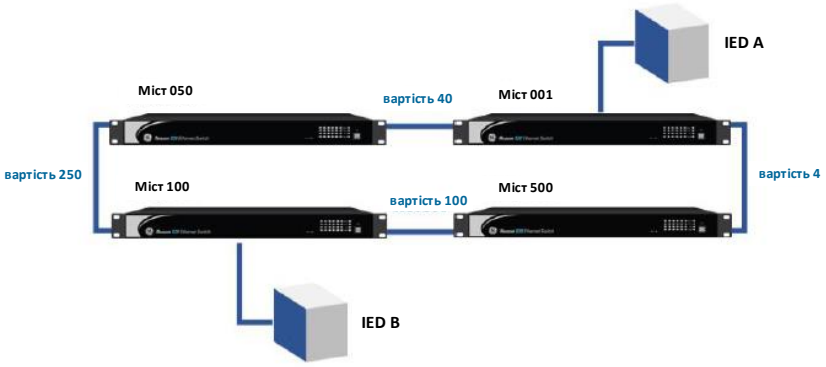


Рис. 25: Приклад петлевої топології з мостами

У прикладі найнижчим ідентифікатором моста є Міст 001 (Bridge 001). Таким чином, цей комутатор буде кореневим мостом.

Тракт, який буде використовуватися для передачі даних по мережі, буде визначений на основі вартості тракту від кореневого моста до останнього вузла. Якщо трафік від пристрою IED A до IED B проходить через мости 001 і 500, загальна вартість складе 104. Проте, якщо трафік від IED A до IED B проходить через мости 001, 050 і 100, загальна вартість складе 290. Таким чином, буде використаний перший тракт. Після виборів активна логічна топологія буде наступною.

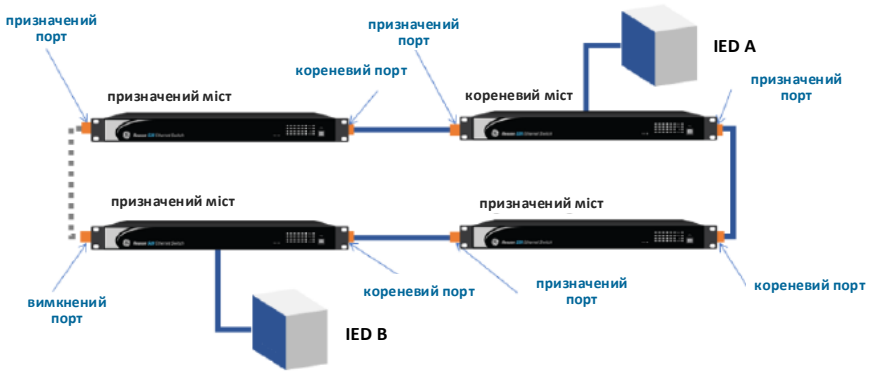


Рис. 26: Логічна топологія після реалізації Протоколу кістякового дерева

На попередньому рисунку також показано, як порти визначаються як кореневий і призначені порти. Якщо порт веде до петлі і це кінець гілки дерева, порт буде вимкнено. Якщо відбудеться зміна топології, наприклад, одна з гілок буде від'єднана або комутатор вийде з ладу, відбудуться інші вибори для пошуку кореня та гілок у мережі. Таким чином, фізична топологія мережі матиме петлі, але логічна не буде.

Коли ініціалізується міст або відбувається зміна фізичної топології, усі порти перебувають у вимкненому стані. Після ініціалізації між ними відбуватиметься трафік, щоб визначити, які порти будуть непризначеними (заблокованими), а які кореневим портом або призначеними портами. Після цього передбачено час для заповнення таблиці MAC-адрес (щоб вивчити всі адреси), і тоді порт буде пересилати трафік як загальний порт комутатора. На рисунку нижче продемонстровано такі кроки, від вимкненого стану до стану пересилання.

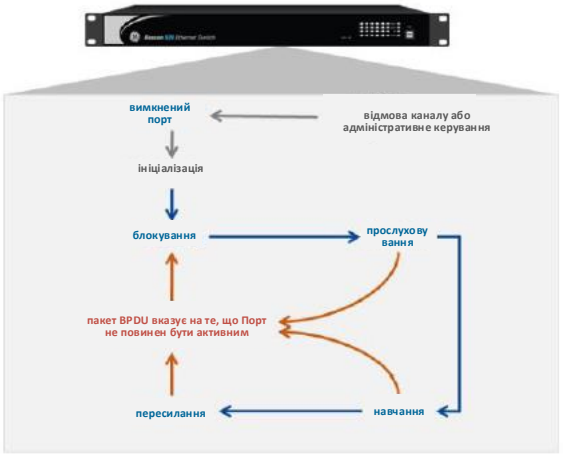


Рис. 27: Стани портів у Протоколі кістякового дерева

З роками протокол розвивався. Після першої версії Протоколу кістякового дерева (STP) був створений Високошвидкісний протокол кістякового дерева (RSTP) для покращення часу відгуку. Коли були впроваджені VLAN, було створено Протокол множинних кістякових дерев (MSTP) для ідентифікації петель всередині VLAN. У наступних пунктах будуть описані ці протоколи, які доступні для використання на пристроях Reason S20.

Протокол STP

Механізм протоколу STP був описаний у пункті Основи принципи кістякового дерева. Проте, протокол STP має деякі унікальні характеристики. Для початку, на наступному рисунку проілюстровано, як би поводились порти при обміні пакетами BPDU у мережі та максимально дозволений час зміни стану порту.

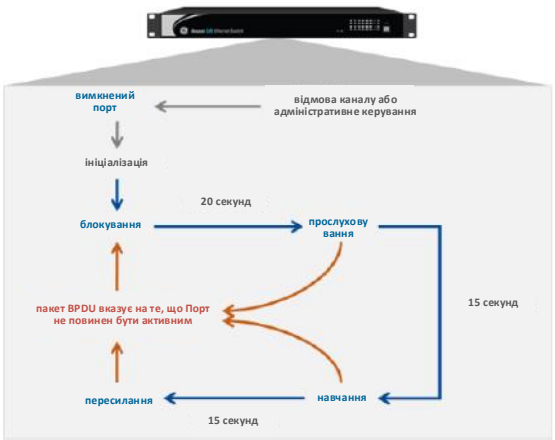


Рис. 28: Механізм протоколу STP та максимальний час зміни стану порту

У таблиці нижче показано логіку роботи при зміні стану порту згідно з протоколом STP.

Таблиця 4: Логіка роботи порту при використанні протоколу STP

Стан порту	Надіслати BPDU	Отримати BPDU	Пересилання кадрів	Вивчення MAC-адрес
Вимкнений	Ні	Ні	Ні	Ні
Блокування	Ні	Так	Ні	Ні

Стан порту	Надіслати BPDU	Отримати BPDU	Пересилання кадрів	Вивчення MAC-адрес
Прослуховування	Так	Так	Ні	Ні
Навчання	Так	Так	Ні	Так
Пересилання	Так	Так	Так	Так

Важливо зазначити, що перехід з одного стану в інший відбуватиметься лише після того, як час отримання пакетів буде перевищено. Таким чином, можливо, що перехід від стану блокування до стану пересилання займає до 50 секунд, враховуючи максимально дозволений час. Як висновок, зміна топології буде виявлена та виправлена через десятки секунд при використанні протоколу STP. Як правило, ці таймери можуть бути налаштовані користувачем, і тоді можна змінити період надсилання та отримання повідомлень, щоб підвищити його продуктивність.
За замовчуванням Reason S20 налаштовано виявляти та виправляти топологію, що змінюється, протягом 30 секунд, використовуючи протокол STP. На наступних рисунках проілюстровано, які кроки здійснюються, у випадку відмови тракту даної кільцевої топології з використанням STP. Коли відбувається збій каналу або відмова комутатора, кожен порт буде проходити через усі стани STP, поки він знову не почне надсилати пакети.

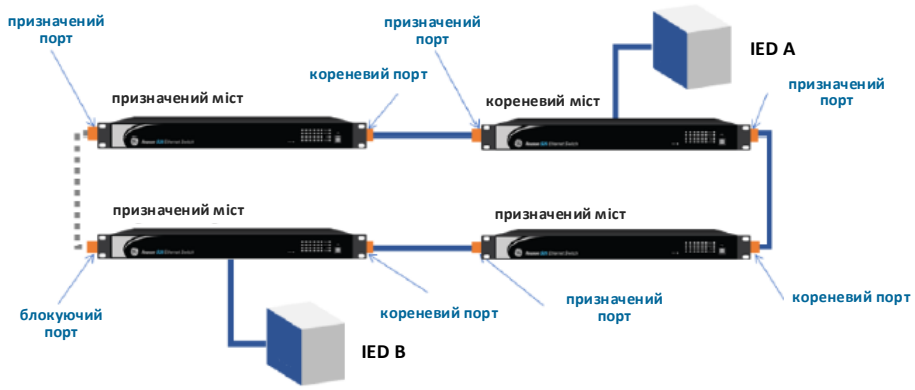


Рис. 29: Стани порту при використанні протоколу STP у кільцевій фізичній топології

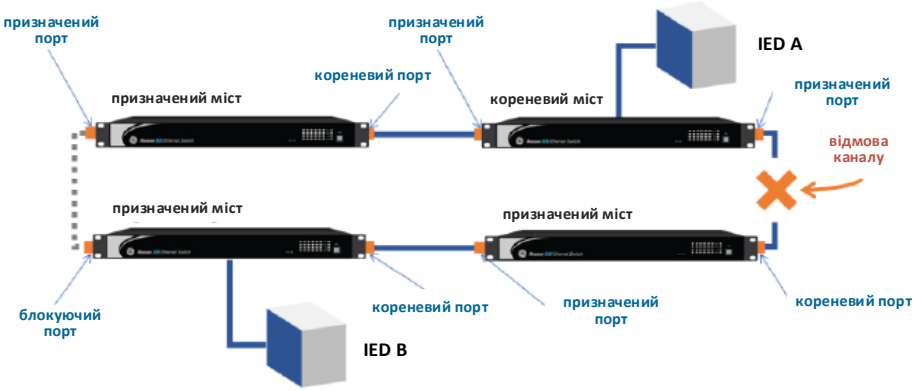


Рис. 30: Відмова на призначеному каналі Кістякового дерева

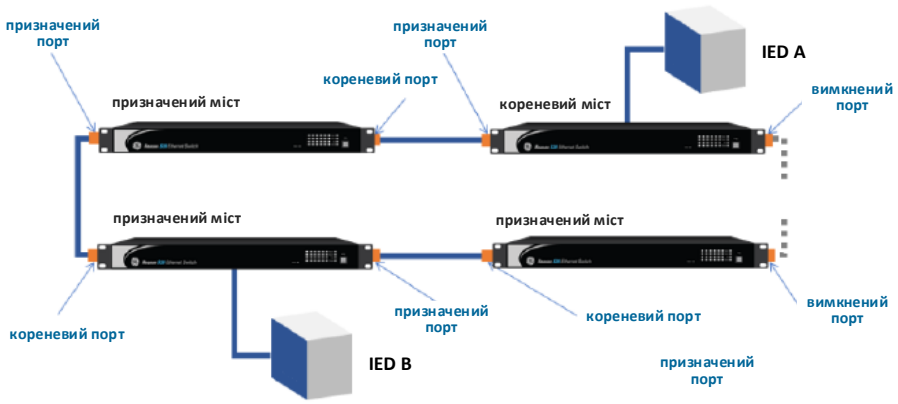


Рис. 31: Реконфігурована топологія після відмови призначеного каналу

Протокол RSTP

Протокол STP має обмеження щодо часу, необхідного для відновлення топології, коли відбувається зміна топології. Як показано в попередньому пункті, протокол очікує закінчення часу дії своїх таймерів, а потім вживає дій, потребуючи кілька секунд для переходу до нової топології. Існувала потреба в більш швидкому протоколі, що призвело до створення Високошвидкісного протоколу кістякового дерева.

Визначений стандартом IEEE 802.1w, RSTP є вдосконаленням протоколу STP. Він використовує ту саму філософію, таку як обрання кореневого моста, але також додає деякі нові характеристики та концепції до протоколу STP. На рисунку нижче показано очікувану логіку роботи портів при використанні RSTP.

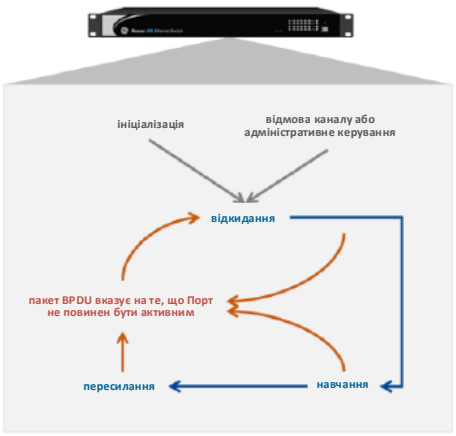


Рис. 32: Механізм протоколу RSTP

У таблиці нижче показано логіку роботи при зміні стану порту згідно з протоколом RSTP.

Таблиця 5: Логіка роботи порту при використанні протоколу RSTP

Стан порту	Надіслати BPDU	Отримати BPDU	Пересилання кадрів	Вивчення MAC-адрес
Вимкнений	Так	Так	Ні	Ні
Навчання	Так	Так	Ні	Так
Пересилання	Так	Так	Так	Так

Порівняно з протоколом STP, кількість станів порту зменшилась. У STP, якщо порт вимкнений, здійснюється блокування трафіку або прослуховування пакетів BPDU у мережі - це дорівнює стану відкидання в RSTP.

Стани навчання та пересилання залишаються такими, як пояснювалося у пункті "Основні принципи кістякового дерева".
Що стосується визначення портів, у RSTP були змінені деякі аспекти протоколу STP. Тоді як у протоколі STP були блокуючі, вимкнені, призначені та кореневі порти, у RSTP вони визначені як альтернативні, резервні, призначені та кореневі порти.
На рисунку нижче показано топологію після того, як протокол RSTP виявив усі петлі.

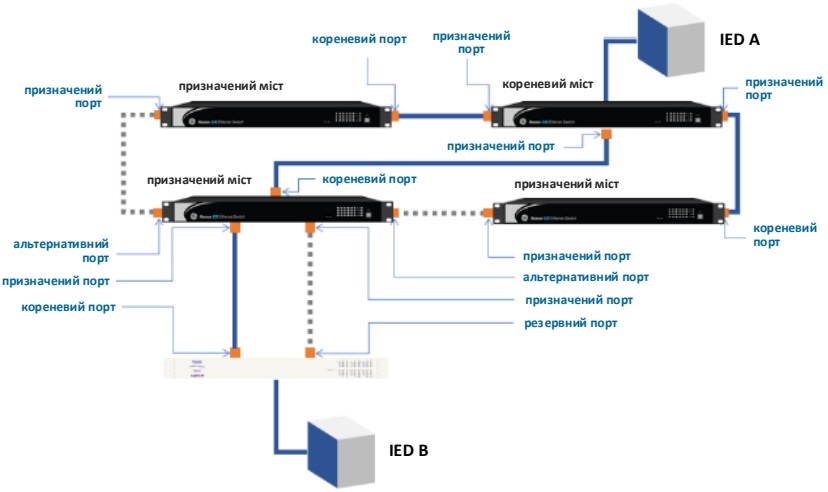


Рис. 33: Стан портів RSTP у петлевій топології

Окрім різниці між станами та визначенням портів, існує також два визначення портів, які не використовуються у протоколі STP і використовуються в RSTP, що називаються Граничні і Магістральні порти.
Граничні порти підключені до кінцевих вузлів, наприклад, до пристроїв IED або комп'ютерів. Потрібно бути обережним при використанні IED, який підтримує RSTP, оскільки він поводиться як міст, і його порти не повинні розглядатися як Граничні порти.
Магістральні порти – це порти, з'єднані між комутаторами з RSTP. На рисунку нижче показано ці типи портів.

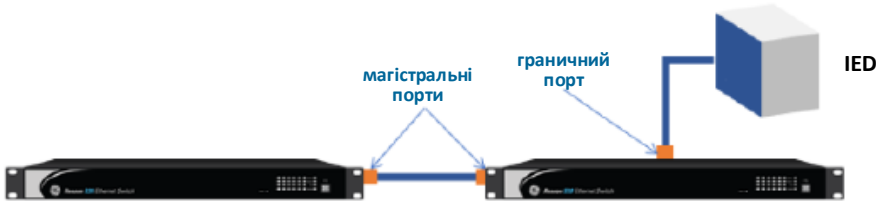


Рис. 34: Граничні та магістральні порти RSTP

Ці визначення використовуються для підвищення продуктивності RSTP, оскільки граничні порти не надсилають або не отримують пакети BPDU, вони переходять із вимкненого стану до стану пересилання, не проходячи через інші стани. Якщо граничний порт починає отримувати пакети BPDU, він переходить у стан магістрального порту та починає бути частиною протоколу RSTP.
Кожен порт також можна налаштувати як порт типу "точка-точка" або "спільний" канал передачі. Повнодуплексні порти вважаються безпосередньо каналами типу "точка-точка", що призводить до зміни їхнього стану безпосередньо на пересилання, якщо вони є призначеними портами. З іншого боку, напівдуплексні порти вважаються портами "спільного" (загального) каналу.
У протоколі RSTP змінився спосіб використання поля "прапорці" у кадрі BPDU порівняно з протоколом STP. У RSTP біти використовуються наступним чином:

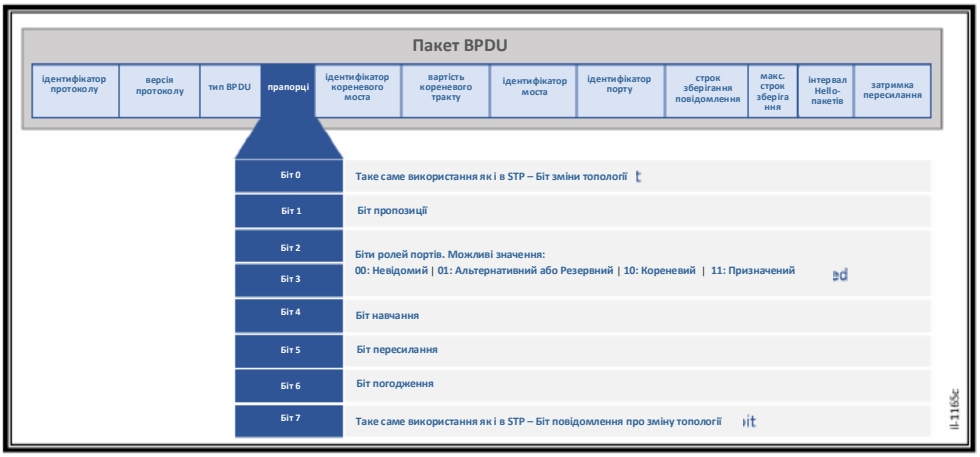


Рис. 35: Поле прапорців BPDU у протоколі RSTP

Були внесені зміни у використання бітів, оскільки змінився механізм передачі пакетів BPDU. У протоколі RSTP кожен міст у мережі може надсилати пакети BPDU, а також мости можуть отримувати пакети BPDU від "менш важливого" мосту в топології. Таким чином, оскільки всі мости можуть надсилати BPDU, виявити відмову каналу можна швидше. У разі отримання пакета BPDU від нижчого мосту, він припускає, що з'єднання з кореневим мостом втрачено, і потрібна реконфігурація топології.

Нарешті, у протоколі RSTP кожен міст, що знаходиться в топології, починає надсилати пакети BPDU на основі "hello-таймера" передачі кадру. Мости, що підтримують RSTP, можуть надсилати пакети BPDU, не отримуючи їх від кореневого мосту. Якщо міст тричі поспіль припиняє отримувати пакети BPDU від призначених або кореневих мостів, він вважатиме, що втратив з'єднання з мостом, і тоді слід запустити реконфігурацію портів. За замовчуванням пристрій Reason S20 надсилає повідомлення "hello-таймера" кожні 2 секунди.

Протокол MSTP

Протокол множинних кістякових дерев (IEEE 802.1s) – це вдосконалення протоколу RSTP, розроблене для використання в середовищах з VLAN. При використанні цього протоколу вся інформація кістякового дерева міститься в одному пакеті BPDU, таким чином зменшуючи трафік і забезпечуючи сумісність протоколу MSTP з іншими протоколами кістякових дерев.

Основним вдосконаленням, пов'язаним з RSTP, є можливість створення ділянок кістякового дерева, зіставлених із визначеними VLAN, що робить конвергенцію кістякового дерева швидшою.

Замість обчислення кістякового дерева для всіх VLAN, MSTP дозволяє групувати набір VLAN в екземплярах, і ці екземпляри можуть працювати в межах регіону. Комутатори, які налаштовані на роботу протоколу, повинні знайти сусідні комутатори, які також працюють з MSTP.

Ця концепція визначає три основні характеристики, що дозволяють мостам стати членами одного регіону:

- Ім'я конфігурації MSTI;
- Версія конфігурації MSTI;
- Прив'язка VLAN до MSTI.

Визначається, що мости знаходяться на одній ділянці, якщо вони мають однакове ім'я конфігурації, версію та зіставлені (прив'язані) з однаковими VLAN.
На рисунку нижче наведено приклад ділянок екземпляра MSTP.

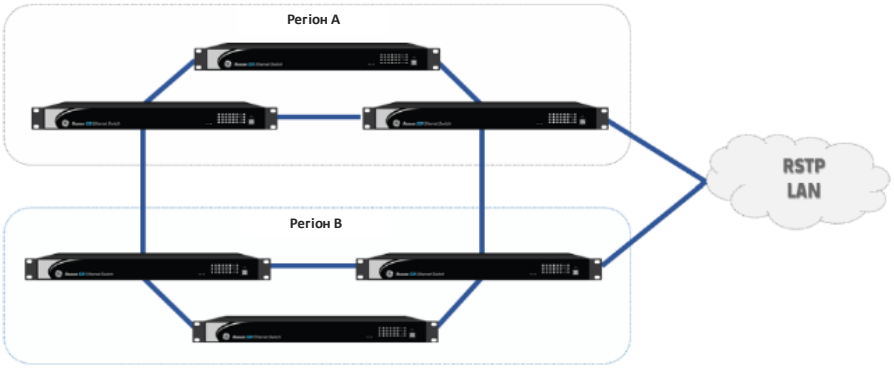


Рис. 36: Регіони MSTP та підключення до локальної мережі минулої версії RSTP

Кожен регіон матиме свій власний кореневий комутатор, оскільки він функціонує як окреме кістякове дерево для інших. Крім того, передбачено комутатор, який буде обраний як кореневий комутатор регіону, що дозволить регіонам підключатися одне до одного. Рисунок нижче ілюструє ці мости в регіонах A та B.

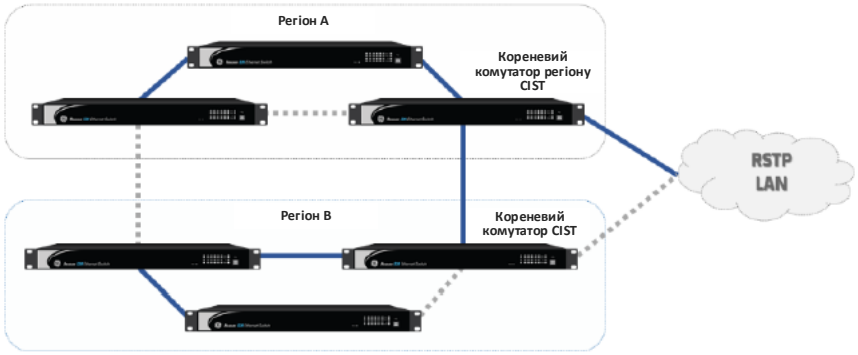


Рис. 37: Кореневі мости CIST, регіони MSTP та локальна мережа минулої версії RSTP

Кореневий міст Протоколу єдиного кістякового дерева (CIST) – це корінь внутрішнього кістякового дерева, що обмежується кожним регіоном. Кореневий комутатор регіону – головний корінь усіх взаємопов'язаних регіонів.
У макроскопічному представленні всі регіони протоколу MSTP функціонують як мости в локальній мережі єдиного кістякового дерева. Таким чином, конвергенція RSTP буде простішою, оскільки внутрішні петлі, утворені в регіонах, будуть визначатися самостійно. Крім того, зміна топології всередині регіону не вплине на всі мости, оскільки вона буде обмежена своїм регіоном. На рисунку нижче показано, як поводитимуться мости RSTP та STP при підключенні до регіонів, створених протоколом MSTP.

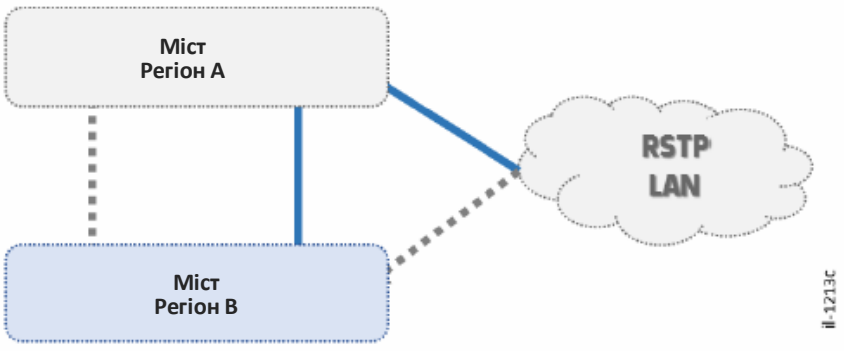


Рис. 38: Логіка роботи регіонів MSTP з використанням протоколу RSTP

UltraRSTP

UltraRSTP – це підхід GE для поліпшення показників відновлення після відмови стандартного RSTP за рахунок реалізації апаратного переривання, яке повідомляє про відмову у мережі. Будь ласка, зверніться до довідкового повідомлення GER-4848, якщо використовується Мідний SFP-трансивер RJ45, Номер деталі GLC-T-BI (код замовлення SFP1GCU01K).

Завдяки UltraRSTP, Reason S20 забезпечує час відновлення після відмови менше 5 мс на хоп (перехід), зменшуючи втрату пакетів, при цьому зберігаючи сумісність з іншими стандартними пристроями RSTP. Reason S20 підтримує UltraRSTP, і оскільки він виконується апаратними засобами, додаткова конфігурація, крім стандартної RSTP, не потрібна.

Як приклад продуктивності UltraRSTP розглянемо мережу з двадцяти пристроїв Reason S20 (SW01 – SW20) у кільцевій топології, оскільки час відновлення після відмови кращий, ніж 5 мс/хоп, збій зв'язку між будь-якими з двадцяти комутаторів повинен призвести до часу відновлення меншого ніж 100 мс.

Для підтвердження продуктивності UltraRSTP був сформований та протестований такий сценарій із двадцятьма Reason S20. Результати показали, що в найгіршому випадку час відновлення після відмови становив 49 мс.

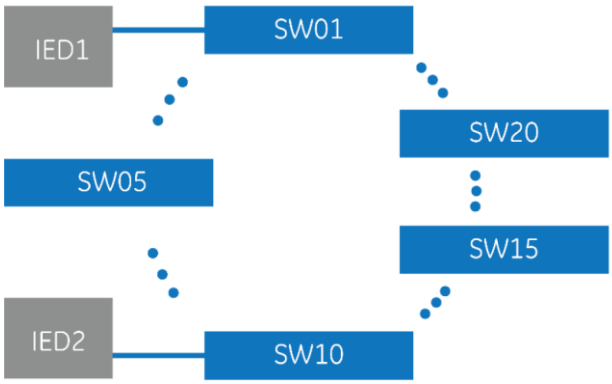


Рис. 39: Відновлення після відмови у мережі за допомогою GE Reason S20s

8.2 Налаштування мостів

Меню "Налаштувань мосту" (Bridge Settings) дозволяє налаштувати основні засоби використання STP. Воно розділене на таблиці Основних і Розширених (Basic та Advanced) налаштувань. Можливі наступні налаштування.

Основні налаштування (Basic Settings)

- **Версія протоколу (Protocol Version)**: виберіть Протокол кістякового дерева, який буде використовуватися. Можливі значення – протоколи STP, RSTP та MSTP. Протокол, налаштований у цьому полі, буде протоколом, який використовується на цьому комутаторі для розв'язування петель у заданій локальній мережі. Якщо протокол нижчого рівня є єдиним доступним у мережі, комутатор використовуватиме протокол нижчого рівня замість налаштованого в цьому полі. Протокол MSTP – це протокол найвищого рівня, RSTP – проміжний, а STP – протокол найнижчого рівня. За замовчуванням обраний протокол RSTP;
- **Пріоритет мосту (Bridge Priority)**: вказує пріоритет мосту, який буде використаний у виборах корінного мосту. Тільки один міст є кореневим мостом у протоколах кістякового дерева, і всі вузли будуть підключені до кореневого мосту. Менші числа пріоритету мостів означають мости з вищим пріоритетом, тобто більш надійний міст, який буде коренем ієрархії кістякового дерева. Нижче значення – 0, а максимальне доступне значення – 61.440;

- **Затримка пересилання (Forward Delay)**: вказує затримку часу, яка буде використана на мостах STP для зміни стану блокування на стан пересилання. Ця затримка часу використовується тільки тоді, коли використовується протокол STP. Дозволеними значеннями є цілі числа від 6 до 40 секунд, і поле Максимального строку зберігання залежить від цього значення, яке потрібно визначити;
- **Максимальний строк зберігання (Max Age)**: вказує максимальний строк зберігання інформації, що передається комутатором, коли він є кореневим мостом. Ця затримка використовується тільки тоді, коли використовується протокол STP. Дозволеними значеннями є цілі числа від 6 до 40 секунд, а поле Максимального строку зберігання залежить від Затримки пересилання наступним чином:

  Максимальний строк зберігання ≤ 2 x (Затримка пересилання - 1)
- **Максимальне число хопів (переходів) (Maximum Hop Count)**: вказує початкове значення залишкових мостів для генерування інформації про екземпляри MSTI на межі регіону MSTI. Таким чином, це значення визначає, скільки мостів може належати даному регіону, оскільки це обмежує кількість мостів, для яких кореневий міст може поширювати інформацію BPDU. Ця інформація використовується лише тоді, коли використовується протокол MSTP. Дозволеними значеннями є цілі числа від 6 до 40 хопів (мостів);
- **Кількість затримок передачі (Transmit Hold Count)**: вказує максимальну кількість пакетів BPDU, які можна надсилати за секунду на порти, яким дозволено брати участь у мережі Протоколу кістякового дерева. Дозволеними значеннями є цілі числа від 1 до 10 пакетів BPDU на секунду.

Розширені налаштування (Advanced Settings)

- **Фільтрація BPDU граничного порту (Edge Port BPDU Filtering)**: вказує, чи будуть граничні-порти (явно налаштовані як Граничні-порти в меню Портів CIST) передавати та приймати пакети BPDU. Вибраний прапорець означає, що граничні порти не будуть приймати та передавати дані BPDU, а порожній прапорець означає, що граничні порти можуть приймати та передавати інформацію BPDU;
- **Захист BPDU граничного порту (Edge Port BPDU Guard)**: вказує, чи граничні порти (явно налаштовані як Граничні порти в меню Портів CIST) змінять свій стан на магістральні порти автоматично, коли буде отриманий пакет BPDU. Вибраний прапорець означає, що граничні порти автоматично змінять свій стан на магістральні, коли на порт отримано пакет BPDU, а порожній прапорець означає, що порти не змінять свого граничного стану;
- **Відновлення після помилки порту (Port Error Recovery)**: вказує, чи буде порт у стані помилки (який буде вимкнений протоколом) автоматично ввімкнений через певний час. Вибраний прапорець означає, що порти у стані помилки чекатимуть, поки не закінчиться час очікування ("таймаут") відновлення після помилки порту, щоб увімкнутись, а порожній прапорець означає, що порт не буде автоматично активований після переходу в стан помилки;
- **Час очікування відновлення після помилки порту (Port Error Recovery Timeout)**: вказує час очікування, який буде застосовано до функції відновлення після помилки порту. Дозволеними значеннями є цілі числа від 30 до 86.400 секунд.

8.3 Конфігурація відображення MSTI

Меню "Налаштувань відображення MSTI" (MSTI Mapping Settings) дозволяє налаштувати регіони, які будуть використовуватися протоколом MSTP. Меню розділене на Ідентифікацію конфігурації (Configuration Identification) та Таблиці відображення MSTI (MSTI Mapping tables). Нижче описано можливі конфігурації.

Для створення регіону в протоколі MSTP всі мости в даному регіоні повинні мати однакове ім'я конфігурації, версію конфігурації та відображення (прив'язку) MSTI до VLAN. Це останнє поле означає, що VLAN на всіх комутаторах у даному регіоні повинні мати однаковий номер ідентифікатора MSTI.

Ідентифікація конфігурації

- **Ім'я конфігурації (Configuration Name)**: вказує ім'я, яке ідентифікує регіон MSTI. Усі мости в одному регіоні повинні мати однакове ім'я конфігурації. За замовчуванням ім'я конфігурації на даному комутаторі – це MAC-адреса комутатора. Максимальне ім'я конфігурації - 32 символи;
- **Версія конфігурації (Configuration Revision)**: вказує версію імені конфігурації, що ідентифікує регіон MSTI. Усі мости в одному регіоні повинні мати однакову версію конфігурації. За замовчуванням версія конфігурації для даного комутатора дорівнює 0. Дозволеними значеннями є цілі числа від 0 до 65.535.

Відображення MSTI

- **MSTI**: показує ідентифікатор екземпляра MSTI, заданий рядком таблиці. Екземпляр MSTI, коли він використовується, буде розумітись як регіон у протоколі MSTP. Reason S20 підтримує до 7 екземплярів;
- **Відображені VLAN (VLANs Mapped)**: вказує ідентифікатори VLAN, які зіставляються з даним екземпляром MSTI. За замовчуванням усі екземпляри порожні, що означає відсутність використання MSTI. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095). Можна вставити конкретні ідентифікатори VLAN, розділені комами (наприклад, 1,2,10,40), діапазон ідентифікаторів VLAN з використанням символу "-" (наприклад, 10-40), а також об'єднані конкретні ідентифікатори та діапазони ідентифікаторів VLAN (наприклад, 1,2,10-40).

8.4 Налаштування пріоритетів MSTI

Меню "Налаштувань пріоритетів MSTI" (MSTI Priorities Settings) дозволяє налаштувати пріоритет мосту, який буде використовуватися протоколом MSTP. У цьому полі дозволено налаштовувати пріоритет CIST та пріоритет MSTI.
Поле пріоритету CIST – це екземпляр за замовчуванням, який відповідає екземпляру, що використовується протоколами STP та RSTP. Таким чином, це значення пріоритету, що використовується в цих протоколах. Поле пріоритету CIST взаємно блокується з версією протоколу, налаштованою в меню Налаштування моста (Bridge Settings), тобто його налаштування в меню Налаштування моста змінить його значення в меню Пріоритетів MSTI і, подібним чином, відповідно змінюється, якщо воно буде змінено в меню Пріоритетів MSTI.
Поле пріоритету MSTI – це значення, яке використовується мостами, що підтримує протокол MSTP, для вибору кореневого моста в даному регіоні.

Якщо бажано застосовувати одну конфігурацію у всіх екземплярах, тоді слід використовувати рядок "*", тобто конфігурація, задана в рядку "*", буде відповідати всім екземплярам. Можливі наступні конфігурації.

- **MSTI**: показує ідентифікатор екземпляра MSTI, заданий рядком таблиці. Перший рядок відображає екземпляр CIST, який є екземпляром за замовчуванням, що використовується протоколами STP та RSTP. Екземпляр MSTI буде розумітися як регіон у протоколі MSTP. Reason S20 підтримує до 7 екземплярів;
- **Пріоритет (Priority)**: вказує пріоритет моста, який буде використовуватися протоколом MSTP. Для визначення кореня екземпляра (кореневий комутатор регіону) цей пріоритет використовується як один із параметрів.

Число пріоритету плюс число екземпляра MSTI та MAC-адреса комутатора будуть використовуватися як параметр ідентифікатора моста в мережі MSTP. Менші числа пріоритетів означають вищий пріоритет. Допустимі значення – від 0 до 61.440.

8.5 Конфігурація портів CIST

Меню "Налаштувань портів CIST" (CIST Ports Settings) дозволяє налаштувати параметри портів, які будуть використовуватися у функції кістякового дерева. Це меню розділене на дві таблиці: одна для конфігурації агрегованого порту CIST та інша для конфігурації звичайного порту CIST. Якщо функція агрегування виконується комутатором, перша таблиця буде використана для налаштування конкретних параметрів агрегованих портів. Якщо бажано застосовувати одну конфігурацію на всіх екземплярах, тоді слід використовувати рядок "*", тобто конфігурація, виконана в рядку "*", буде відповідати всім екземплярам. Можливі наступні конфігурації.

Конфігурація агрегованого порту CIST

- **Порт (Port)**: показує агреговані порти, які потрібно налаштувати в цьому рядку;
- **STP увімкнено (STP Enabled)**: увімкніть функцію STP на порту. Вибраний прапорець означає, що STP увімкнено, а порожній прапорець – вимкнено;
- **Вартість тракту (Path Cost)**: вказує значення вартості тракту, яке буде повідомлено портом на інші мости. Нижча вартість тракту означає вищу швидкість порту, і їх вибирають для пересилання трафіку за рахунок вищої вартості тракту. Дозволені значення: Автоматична та Конкретна (Auto та Specific). Якщо вибрано Автоматична, вартість тракту буде розраховуватись на основі можливостей швидкості порту, як рекомендовано стандартом 802.1D. Якщо вибрано Конкретна, використана вартість тракту буде вартістю тракту, визначеною користувачем у полі, дозволеному в стовпці Вартість тракту. Дозволеними значеннями вартості тракту є цілі числа від 1 до 200000000;
- **Пріоритет (Priority)**: вказує пріоритет порту. Якщо між мостами є два тракти з однаковою вартістю тракту, поле пріоритету буде використано для вибору, який порт повинен пересилати трафік. Менші значення означають вищий пріоритет для порту. Дозволеними значеннями є цілі числа від 0 до 240;
- **Адміністрування Граничного порту (Admin Edge)**: вказує прапорець стану для роботи у якості Граничного порту при ініціалізації порту. Допустимі значення – Не-граничний та Граничний порти. Не-граничний означає, що прапорець роботи у якості граничного порту буде ініціалізований зі значенням, що дорівнює 0, а Граничний означає, що прапорець роботи у якості граничного порту буде ініціалізований зі значенням, що дорівнює 1;
- **Автоматичне визначення Граничного порту (Auto Edge)**: увімкніть автоматичне визначення граничного порту на порту. Цей прапорець дозволяє комутатору автоматично визначати, чи є порт кістякового дерева граничним (Edge) або магістральним (Trunk). Вибраний прапорець означає увімкнене Автоматичне визначення Граничного порту, а порожній прапорець – вимкнено;
- **Обмежений (Restricted)**: вмикає функції захисту кореня. Якщо бажано контролювати порти, щоб не поширювати зміни топології або не бути кореневими портами, щоб гарантувати, що порти не знаходяться в головній мережі логічної топології, слід увімкнути функції захисту кореня. Можливі значення:
    - **Обмежена роль (Restricted Role)**: увімкнути функцію захисту Кореня. Цей прапорець дозволяє порту гарантувати, що порт не буде кореневим портом, навіть якщо це найкращий тракт до кореня. Вибраний прапорець означає, що порт не буде працювати в якості кореневого порту, а порожній прапорець означає, що порт може бути обраний як кореневий порт;

- **Обмежений TCN (Restricted TCN)**: дозволяє порту не поширювати сповіщення та зміни топології, отримані на цьому порту, на інші порти. Це можна використовувати для портів, підключених до мереж, які часто змінюються. Вибраний прапорець означає, що порт не буде поширювати повідомлення про зміну топології та інформаційні повідомлення, а порожній прапорець означає, що порт поширюватиме ці повідомлення;

- **Захист BPDU (BPDU Guard)**: увімкніть порт для роботи в режимі захисту BPDU. Ця функція змушує порт самостійно вимикатись, якщо на цей порт надходить повідомлення BPDU, як це могло статися, якщо міст, що не є STP, став частиною петлі в мережі кістякового дерева. Це налаштування не впливає на порти, що працюють як Граничні порти (Edge ports). Вибраний прапорець означає, що порт самостійно вимкнеться, якщо отримано пакет BPDU, а порожній прапорець означає, що порт самостійно не вимкнеться у такому випадку;
- **Точка-точка (Point-to-point)**: вказує, чи порт підключений до комутованої повнодуплексної локальної мережі (локальна мережа типу "точка-точка") або локальної мережі зі спільним середовищем. Дозволеними значеннями є "Автоматично", "Примусово дійсно" та "Примусово хибно" (Auto, Forced True та Forced False). "Автоматично" означає, що комутатор автоматично визначає, чи дозволено повнодуплексну роботу чи ні, "Примусово дійсно" означає, що порт завжди працюватиме як з'єднання типу "точка-точка", а "Примусово хибно" означає, що порт завжди буде розглядатися як спільне середовище. З'єднання типу "точка-точка" мають швидший перехід до стану пересилання, ніж з’єднання локальної мережі зі спільним середовищем.

Конфігурація звичайного порту CIST

- **Порт (Port)**: показує звичайні порти, які потрібно налаштувати в цьому рядку;
- **STP увімкнено (STP Enabled)**: увімкніть функцію STP на порту. Вибраний прапорець означає, що STP увімкнено, а порожній прапорець – вимкнено;
- **Вартість тракту (Path Cost)**: вказує значення вартості тракту, яке буде повідомлено портом на інші мости. Нижча вартість тракту означає вищу швидкість порту, і їх вибирають для пересилання трафіку за рахунок вищої вартості тракту. Дозволені значення: Автоматична та Конкретна (Auto та Specific). Якщо вибрано Автоматична, вартість тракту буде розраховуватись на основі можливостей швидкості порту, як рекомендовано стандартом 802.1D. Якщо вибрано Конкретна, використана вартість тракту буде вартістю тракту, визначеною користувачем у полі, дозволеному в стовпці Вартість тракту. Дозволеними значеннями вартості тракту є цілі числа від 1 до 200000000;
- **Пріоритет (Priority)**: вказує пріоритет порту. Якщо між мостами є два тракти з однаковою вартістю тракту, поле пріоритету буде використано для вибору, який порт повинен пересилати трафік. Менші значення означають вищий пріоритет для порту. Дозволеними значеннями є цілі числа від 0 до 240;
- **Адміністрування Граничного порту (Admin Edge)**: вказує прапорець стану для роботи у якості Граничного порту при ініціалізації порту. Допустимі значення – Не-граничний та Граничний порти. Не-граничний означає, що прапорець роботи у якості граничного порту буде ініціалізований зі значенням, що дорівнює 0, а Граничний означає, що прапорець роботи у якості граничного порту буде ініціалізований зі значенням, що дорівнює 1;
- **Автоматичне визначення Граничного порту (Auto Edge)**: увімкніть автоматичне визначення граничного порту на порту. Цей прапорець дозволяє комутатору автоматично визначати, чи є порт кістякового дерева граничним (Edge) або магістральним (Trunk). Вибраний прапорець означає увімкнене Автоматичне визначення Граничного порту, а порожній прапорець – вимкнено;

- **Обмежений (Restricted)**: вмикає функції захисту кореня. Якщо бажано контролювати порти, щоб не поширювати зміни топології або не бути кореневими портами, щоб гарантувати, що порти не знаходяться в головній мережі логічної топології, слід увімкнути функції захисту кореня. Можливі значення:
  - **Обмежена роль (Restricted Role)**: увімкнути функцію захисту Кореня. Цей прапорець дозволяє порту гарантувати, що порт не буде кореневим портом, навіть якщо це найкращий тракт до кореня. Вибраний прапорець означає, що порт не буде працювати в якості кореневого порту, а порожній прапорець означає, що порт може бути обраний як кореневий порт;
  - **Обмежений TCN (Restricted TCN)**: дозволяє порту не поширювати сповіщення та зміни топології, отримані на цьому порту, на інші порти. Це можна використовувати для портів, підключених до мереж, які часто змінюються. Вибраний прапорець означає, що порт не буде поширювати повідомлення про зміну топології та сповіщення, а порожній прапорець означає, що порт поширюватиме ці повідомлення;
- **Захист BPDU (BPDU Guard)**: увімкніть порт для роботи в режимі захисту BPDU. Ця функція змушує порт самостійно вимикатись, якщо на цей порт надходить повідомлення BPDU, як це могло статися, якщо міст, що не є STP, став частиною петлі в мережі кістякового дерева. Це налаштування не впливає на порти, що працюють як Граничні порти (Edge ports). Вибраний прапорець означає, що порт самостійно вимкнеться, якщо отримано пакет BPDU, а порожній прапорець означає, що порт самостійно не вимкнеться у такому випадку;
- **Точка-точка (Point-to-point)**: вказує, чи порт підключений до комутованої повнодуплексної локальної мережі (локальна мережа типу "точка-точка") або локальної мережі зі спільним середовищем. Дозволеними значеннями є "Автоматично", "Примусово дійсно" та "Примусово хибно" (Auto, Forced True та Forced False). "Автоматично" означає, що комутатор автоматично визначає, чи дозволено повнодуплексну роботу чи ні, "Примусово дійсно" означає, що порт завжди працюватиме як з'єднання типу "точка-точка", а "Примусово хибно" означає, що порт завжди буде розглядатися як спільне середовище. З'єднання типу "точка-точка" мають швидший перехід до стану пересилання, ніж з’єднання локальної мережі зі спільним середовищем.

8.6 Конфігурація портів MSTI

Меню "Налаштувань портів MSTI" (MSTI Ports Settings) дозволяє налаштовувати параметри CIST для кожного екземпляра MSTI. Даний порт може працювати як порт CIST для багатьох екземплярів MSTI, якщо цей порт належить більше ніж одного регіону. Таким чином, він може працювати в стані пересилання в даному екземплярі MSTI та в стані блокування для іншого MSTI. Меню MSTI дозволяє користувачеві налаштувати кожен екземпляр MSTI комутатора.

За замовчуванням у цьому меню з’явиться поле Вибір MSTI (Select MSTI). Поле MSTI містить список усіх регіонів MSTI, дозволених для створення в Reason S20. Виберіть потрібний екземпляр MSTI, а потім натисніть кнопку "Отримати" (Get). Якщо натиснути кнопку "Отримати", з’явиться таблиця конфігурації агрегованих портів MSTI та таблиця конфігурації звичайних портів MSTI.

Якщо бажано застосовувати одну конфігурацію для всіх екземплярів, тоді слід використовувати рядок "*", тобто конфігурація, виконана в рядку "*", буде відповідати всім екземплярам. Можливі наступні конфігурації.

Конфігурація агрегованих портів MSTI

- **Порт (Port)**: показує агреговані порти, які потрібно налаштувати в цьому рядку;
- **Вартість тракту (Path Cost)**: вказує значення вартості тракту, яке буде повідомлено портом на інші мости у тому самому екземплярі MSTI. Нижча вартість тракту означає вищу швидкість порту, і їх вибирають для пересилання трафіку за рахунок вищої вартості тракту. Дозволені значення: Автоматична та

Конкретна (Auto та Specific). Якщо вибрано Автоматична, вартість тракту буде розраховуватись на основі можливостей швидкості порту, як рекомендовано стандартом 802.1D. Якщо вибрано Конкретна, використана вартість тракту буде вартістю тракту, визначеною користувачем у полі, дозволеному в стовпці Вартість тракту. Дозволеними значеннями вартості тракту є цілі числа від 1 до 200000000;

- **Пріоритет (Priority)**: вказує пріоритет порту. Якщо між мостами є два тракти з однаковою вартістю тракту, поле пріоритету буде використано для вибору, який порт повинен пересилати трафік. Менші значення означають вищий пріоритет для порту. Дозволеними значеннями є цілі числа від 0 до 240;

Конфігурація звичайних портів MSTI

Параметри конфігурації для звичайних портів такі ж, як і для агрегованих портів.

9 Багатоадресна IP-передача (IPMC)

IP-зв’язок, як і Ethernet-зв'язок, дозволяє пристроям у мережі надсилати пакети на один хост або на всі хости, відповідно шляхом одноадресної або широкомовної передачі. Існує кілька варіантів застосування, які мають логічну архітектуру одного відправника до групи отримувачів, наприклад, схеми PMU. Для реалізації такого роду варіантів виконання використовується багатоадресна IP-передача (IP Multicast (IPMC)).

Слід бути уважним при використанні протоколів різних рівнів з механізмом багатоадресної передачі. Що стосується базового зв'язку в енергосистемах, існують можливості багатоадресної передачі рівня 2 та рівня 3.

Пристрої синхронізованих векторних вимірювань (PMU) використовують протокол UDP для передачі даних по всій мережі. Таким чином, у цьому контексті багатоадресні повідомлення – це повідомлення, надіслані на IP-адресу всередині діапазону IP-адрес, визначених як багатоадресні адреси.

GOOSE, Вибіркові величини та PTP повідомлення відображаються безпосередньо у кадрі Ethernet, а механізм багатоадресної передачі забезпечується призначенням MAC-адреси. Це означає, що ці повідомлення не можуть бути безпосередньо маршрутизовані (наприклад, вони не можуть бути передані в своїй оригінальній формі через глобальні мережі), і вони надсилаються на MAC-адресу, яка є не MAC-адресою кінцевого вузла, а є MAC-адресою багатоадресної передачі.

Як і слід було очікувати, одноадресна передача відбувається від одного відправника до конкретного отримувача. При широкомовній передачі повідомлення надсилається всім отримувачам у підмережі.
Використовуючи багатоадресні фільтри, обладнання, яке не очікує цих повідомлень, не отримає їх, на відміну від широкомовної передачі, де широкомовні повідомлення пересилаються на всі вузли в кожній локальній мережі. Без багатоадресної фільтрації багатоадресні повідомлення надсилаються так само, як широкомовні повідомлення.

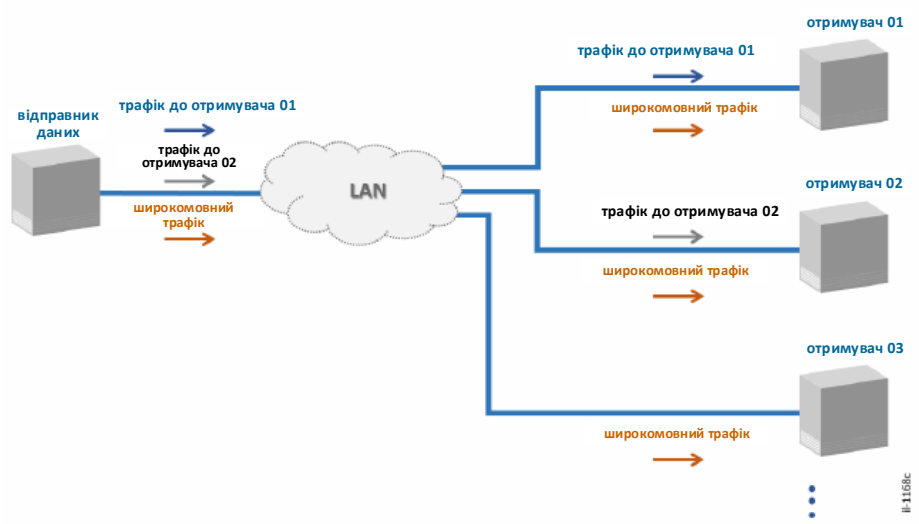


Рис. 40: Одноадресний та широкомовний зв’язок

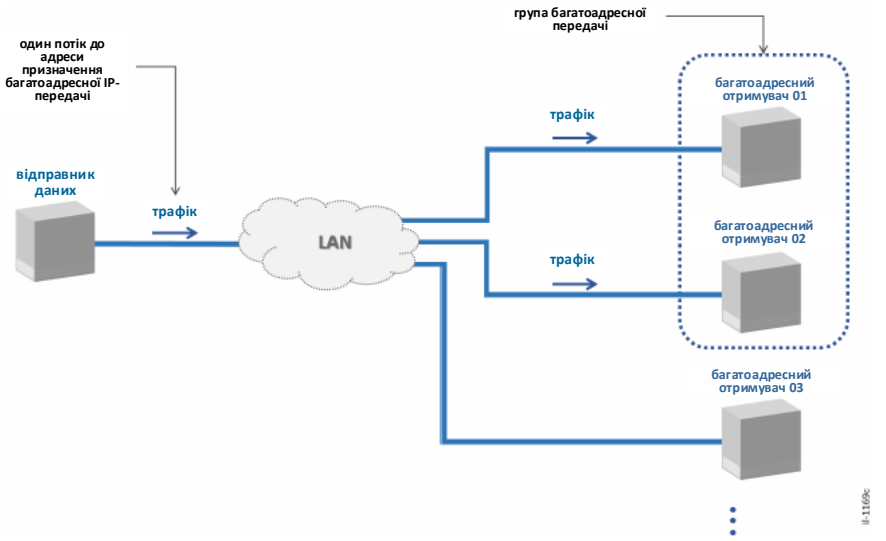


Рис. 41: Багатоадресний зв’язок

Меню профілю IPMC дозволяє налаштувати профіль, який буде використовуватися в потоках багатоадресної IP-передачі, що будуть використовуватися під час відстеження IGMP або MLD в якості правил фільтрації, що застосовуються при отриманні багатоадресного IP трафіку.
Меню профілю IPMC знаходиться в меню Налаштування > Профіль IPMC (Settings > IPMC Profile).

Меню IPMC дозволяє здійснювати конфігурацію основних налаштувань для функціонування багатоадресної IP передачі. Відстеження IGMP пов'язане із середовищами IPv4, а Відстеження MLD – із IPv6.
Меню IPMC знаходиться в меню Налаштування > IPMC (Settings > IPMC).

9.1 Профіль IPMC

Таблиця профілів IPMC

Меню "Таблиці профілів" (Profile Table) дозволяє користувачеві виконувати базову конфігурацію за визначенням профілю IPMC. Ці профілі будуть використовуватися в протоколах IGMP та MLD для визначення групи, якою слід користуватися в групі багатоадресної передачі. Дозволені конфігурації є наступними.

- **Режим глобального профілю (Global Profile Mode)**: вказує, чи слід увімкнути профілі в таблиці чи ні. Функції фільтрації виконуватимуться лише за умови активації профілів. Пристрій Reason S20 дозволяє створити до 64 профілів. Можливі значення цього поля: Увімкнено (Enabled) або Вимкнено (Disabled). Увімкнено означає, що дозволено реалізувати профіль фільтрації, а вимкнено означає, що профіль фільтрації виконуватися не буде.

Налаштування таблиці профілів IPMC

Вказує, які профілі створені. За замовчуванням на комутаторі не налаштовано жодного профілю. Якщо потрібен новий профіль, натисніть кнопку Додати новий профіль IPMC (Add New IPMC Profile). При натисканні з’являться наступні поля для налаштування:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити профіль у рядку;
- **Ім'я профілю (Profile Name)**: вказує ім'я, що буде використовуватися профілем, яке повинно бути унікальним у мережі. Дозволені значення – це буквено-цифрові символи, а максимальна довжина імені – 16 символів;
- **Опис профілю (Profile Description)**: вказує додатковий опис налаштованого профілю. Дозволені значення - це буквено-цифрові символи, а максимальна довжина імені - 64 символи;
- **Правило (Rule)**: дозволяє, натиснувши на кнопку  , вводити дані в налаштуваннях правил профілю IPMC,. При натисканні з’являться наступні поля для налаштування:
  - **Налаштування правил профілю IPMC (IPMC Profile Rule Settings)**: Вказує, які правила створюються в профілі. За замовчуванням для створених профілів не налаштовано жодне правило. Якщо потрібно нове правило, натисніть кнопку Додати останнє правило (Add Last Rule). При натисканні з’являться наступні поля для налаштування:
  - **Ім'я та індекс профілю (Profile Name & Index)**: відображає ім'я профілю, налаштованого в полі "Ім'я профілю" в меню "Налаштування таблиці профілів IPMC" (IPMC Profile Table), та номер індексу, що ідентифікує кожне правило. Кожне додане правило має індекс поступового зменшення, починаючи з індексу 1 і закінчуючи індексом 64. Вищі числа індексів (тобто раніше створені правила) мають вищий пріоритет при пошуку, а найвищий пріоритет виконується для першого створеного правила, яке має індекс номер 1;
  - **Назва запису (Entry Name)**: вказує, який запис використовуватиметься за цим правилом профілю. Записи створюються в меню "Введення адреси" (Address Entry) і дозволяють створювати імена та діапазони адрес багатоадресної IP-передачі, які будуть використовуватися в правилах профілю. Дозволені значення – це створені записи. Якщо запис не потрібен, символ "-" означає відсутність запису, використовуваного цим правилом;
  - **Діапазон адрес (Address Range)**: вказує діапазон адрес багатоадресної IP-передачі, дозволений для використання вибраним записом. Записи створюються в меню "Введення адреси" і дозволяють створювати імена та діапазони адрес багатоадресної IP-передачі, які будуть використовуватися в правилах профілю. Якщо жоден запис не вибрано, символ "~" означає, що жоден запис не вибрано;

- **Дія (Action)**: вказує групову навчальну дію, дозволену для виконання цим правилом. Після отримання повідомлень про приєднання або звітування стану від даної групи комутатор порівняє, чи діапазон IP-адрес сумісний з дозволеним діапазоном цього правила. Якщо отримане повідомлення багатоадресної IP-передачі збігається з дозволеним діапазоном адрес багатоадресної IP-передачі, у цьому полі буде вказано, яку дію буде виконано. Можливі значення: "Заборонити" та "Дозволити" (Deny та Permit). За замовчуванням вибрано параметр "Заборонити". Дія "Заборонити" означає, що повідомлення від групи з дозволеним діапазоном адрес слід відкинути, а дія "Дозволити" означає, що повідомлення від групи з дозволеним діапазоном адрес слід вивчити;
- **Журнал (Log)**: вказує перевагу запису в журнал після отримання повідомлень про приєднання або звітування стану від даної групи з дозволеним діапазоном IP-адрес цього правила. Можливі значення: "Вимкнути" та "Увімкнути" (Disable and Enable). За замовчуванням вибрано параметр "Вимкнути". "Вимкнути" запис у журнал означає, що інформація від групи з дозволеним діапазоном адрес не реєструватиметься, а "Увімкнути" запис у журнал означає, що інформація від групи з дозволеним діапазоном адрес буде реєструватися.

Після створення правила в останньому стовпці таблиці "Налаштувань правил профілю IPMC" відображатимуться чотири піктограми. Їх використання полягає в наступному:

- - Кнопка "Вставити нове правило" (Insert New Rule): дозволяє додавати нове правило в індекс вищого рівня, натисканням на цю кнопку. Створене правило буде вставлене в індексний номер рядка, в якому була натиснута кнопка. З її допомогою можна додавати правила вищих пріоритетів після створення інших;
- - Кнопка "Видалити правило" (Delete Rule): дозволяє видалити правило в рядку;
- - Перемістити правило на вищі рівні (Move Rule to higher levels): дозволяє керувати правилами, створеними шляхом переміщення заданого індексу правила на вищі рівні індексу правил;
- - Перемістити правило на нижчі рівні (Move Rule to lower levels): дозволяє керувати правилами, створеними шляхом переміщення заданого індексу правила на нижчі рівні індексу правил.

Введення адреси

Меню "Таблиці профілів" дозволяє користувачеві створювати записи, які будуть використовуватися в профілях, створених у меню "Таблиці профілів". Ці записи використовуються у профілях, що використовуються в протоколах IGMP та MLD, щоб визначити, яку групу слід використовувати в групі багатоадресної передачі. За замовчуванням жоден запис не налаштований на комутаторі. Якщо потрібен новий запис, натисніть кнопку "Додати нову адресу" (Діапазон) (Add New Address (Range)). При натисканні з’являться наступні поля для налаштування:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити запис у рядку;
- **Ім'я запису (Entry Name)**: вказує ім'я, що буде використовуватися записом, яке повинне бути унікальним у мережі. Дозволені значення – це буквено-цифрові символи, а максимальна довжина імені - 16 символів;
- **Початкова адреса (Start Address)**: вказує першу адресу діапазону адрес, дозволених у цьому записі. Дозволеними значеннями є адреси багатоадресної передачі IPv4 або IPv6. Адреси IPv4 потрібно вводити в десятковому форматі із крапками, а адреси IPv6 – у шістнадцятковому форматі з двокрапкою (":"), що розділяє кожне поле;

- **Кінцева адреса (End Address)**: вказує останню адресу діапазону адрес, дозволених у цьому записі. Дозволеними значеннями є адреси багатоадресної передачі IPv4 або IPv6. Адреси IPv4 потрібно вводити у десятковому форматі із крапками, а адреси IPv6 – у шістнадцятковому форматі з двокрапкою (":"), що розділяє кожне поле.

9.2 Відстеження мережевого трафіку IGMP

Протокол керування групами Інтернету (IGMP) був розроблений наприкінці 1980-х (перша версія RFC 1112), щоб задовольнити вимогу щодо використання багатоадресної передачі через IP-мережі (зокрема, мережі IPv4). Друга версія протоколу була визначена в RFC 2236, а остання версія – IGMPv3, визначена в RFC 3376.
У контексті Інтернету поширеними варіантами застосування, які потребують багатоадресної передачі, є потокове передавання відео та аудіо. Що стосується зв'язку в енергосистемах, протокол IGMP може бути використаний, коли існує багатоадресний зв’язок між Пристроєм синхронізованих векторних вимірювань (PMU) та Концентратором синхрофазорних даних (PDC).
Механізм відстеження трафіку IGMP показаний на рисунку нижче.

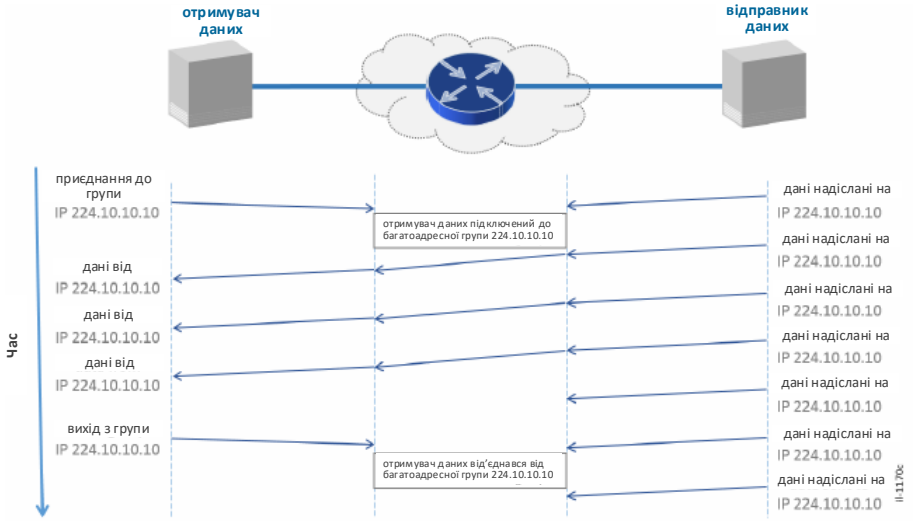


Рис. 42: Механізм протоколу IGMP

Коли отримувач хоче приєднатися до групи багатоадресної IP-передачі, він надсилає в мережу повідомлення "приєднатися до групи" (join group), де маршрутизатори позначають вхідну IP-адресу та інтерфейс для групи. Після того, як отримувач стає членом потрібної групи багатоадресної передачі, він починає отримувати дані. Слід зазначити, що відправник надсилатиме дані на визначену IP-адресу, яка буде не адресою отримувачів, а "віртуальною IP-адресою", яка відповідає IP-адресі багатоадресної передачі. Щоб припинити отримання даних, отримувач надсилає повідомлення "вийти з групи" (leave group) маршрутизаторам мережі.
Визначається діапазон IP-адрес, який використовується тільки для багатоадресної передачі. Коли маршрутизатори в мережі отримують кадр, адресований цим IP-адресам, вони маршрутизують кадри на основі груп багатоадресної передачі. IP-адреси багатоадресної передачі можуть бути:

- 224.0.0.1 – Адреса "Увесь хост";
- 224.0.0.2 – Адреса "Всі багатоадресні маршрутизатори"

У протоколі IGMP є дві адреси, які використовуються протоколом і не можуть бути використані як адреси багатоадресної передачі:

- Від 224.0.0.0 до 239.255.255.255 (адреса класу D);
- Адреси 224.0.0.0 та 224.0.0.255 зарезервовані для мережевих протоколів;

- Адреси 224.0.0.0 та 238.255.255.255 є приватними адресами і не можуть бути маршрутизовані;

Зарезервовані адреси не можна використовувати як IP-адреси багатоадресної передачі. На додаток до адрес, показаних вище, існують загальні служби, такі як багатоадресна передача PTP та багатоадресна передача NTP, які мають конкретні адреси. Переконайтеся, що вони не використовуються під час налаштування групи багатоадресної IP-передачі в мережі.

Функція відстеження мережевого трафіку IGMP виконується комутаторами, зчитуючи поле IP-заголовка вхідних пакетів. Якщо комутатор не може обробляти відстеження IGMP, багатоадресний IP-зв'язок переадресовується як широкомовна передача. Перевіряючи дані IP-заголовка на порту, який підключений до IGMP-сервера, комутатор може перевірити, чи пакети отримані від груп багатоадресної IP-передачі. Якщо це так, комутатор може прийняти розумне рішення про пересилання, доставляючи дані лише до інтерфейсів, підключених до групи багатоадресної передачі, та заощаджуючи пропускну здатність в інших інтерфейсах Ethernet.
Коли наявні багато комутаторів, наприклад, як у локальній мережі, відстеження трафіку IGMP ефективно заощадить пропускну здатність, оскільки дані пересилатимуть тільки тракти, пов’язані з групою багатоадресної передачі. Тракти між комутаторами, які не є членами групи багатоадресної передачі, не отримуватимуть її пакети.
На рисунку нижче показано, як відбувається багатоадресна IP-передача через комутатори, маршрутизатори та загальні комутатори, що підтримують відстеження трафіку IGMP. Оранжеві лінії означають трафік по тракту, а сині – відсутність трафіку на тракті. Вважається, що все обладнання є членом однієї VLAN.

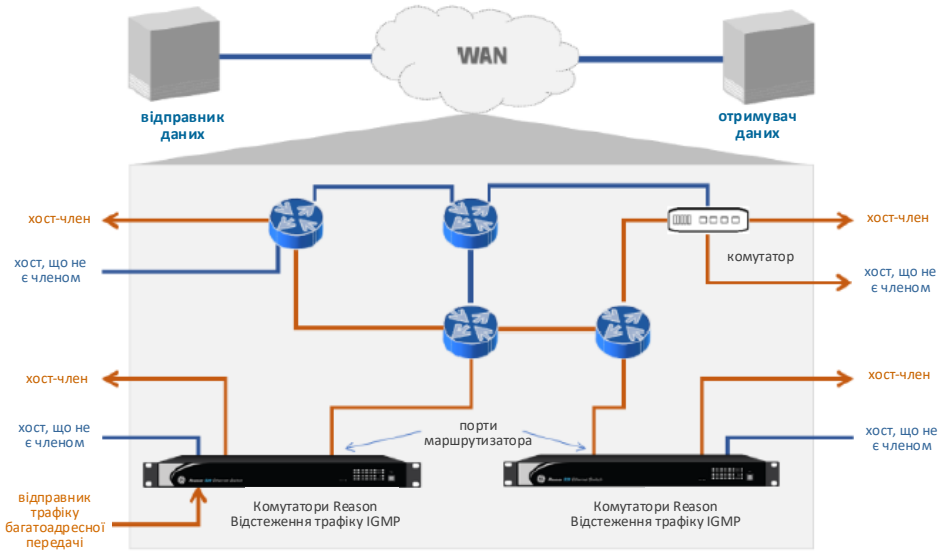


Рис. 43: Відстеження трафіку IGMP у певній локальній мережі

Функція відстеження трафіку IGMP пов’язана з VLAN у пристрої Reason S20. Якщо в мережі не використовується VLAN, відстеження трафіку IGMP у VLAN повинно бути налаштоване на роботу з ідентифікатором VLAN (VID) "1".

Якщо використовується багатоадресний протокол IGMP, переконайтеся, що все обладнання в Локальній або Глобальній мережі має підтримку протоколу IGMP і переконайтесь, що воно підтримує ту саму версію IGMP. Пристрій Reason S20 підтримує протоколи IGMPv1, IGMPv2 та IGMPv3.

Базова конфігурація

Конфігурація відстеження IGMP

- **Відстеження трафіку увімкнено (Snooping Enabled)**: увімкніть функцію відстеження трафіку IPMC на комутаторі. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Увімкнено незареєстроване лавинне розповсюдження IPMCv4 (Unregistered IPMCv4 Flooding Enabled)**: увімкніть незареєстроване лавинне розповсюдження трафіку IPMCv4 на комутаторі. Ця функція вступає в дію, тільки якщо увімкнено функцію відстеження трафіку IGMP. Незареєстроване лавинне розповсюдження трафіку – це невідомий багатоадресний трафік, і якщо його увімкнути, ця функція пересилатиме такі пакети як пакети загального призначення. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Діапазон SSM IGMP (IGMP SSM Range)**: вказує діапазон багатоадресної передачі з налаштуванням конкретного джерела (SSM). Функція SSM використовується, коли прослуховувач багатоадресної передачі повинен отримувати пакети тільки від заданого джерела, а не з усіх джерел багатоадресної передачі в даній локальній мережі, покращуючи захист та зменшуючи вимоги в мережі. Адреса SSM дозволить хостам та маршрутизаторам, що підтримують SSM, запускати служби SSM. Адреса повинна вводитися у десятковому форматі з крапками, а довжина маски представляється у вигляді бітів довжини маски;
- **Проксі виходу увімкнено (Leave Proxy Enabled)**: увімкніть проксі виходу IGMP, щоб уникнути пересилання непотрібних повідомлень про вихід на порт на стороні маршрутизатора. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Проксі увімкнено (Proxy Enabled)**: увімкніть проксі IGMP, щоб уникнути пересилання непотрібних повідомлень про приєднання та вихід на порт на стороні маршрутизатора. У цьому режимі комутатор буде працювати для сторони маршрутизатора як хост, обмінюючись повідомленнями про вихід і приєднання хоста. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено.

Конфігурація портів

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **Порт маршрутизатора (Router Port)**: увімкніть порт маршрутизатора для відстеження трафіку IGMP. Порт маршрутизатора – це порт на комутаторі, який підключений до джерела повідомлень багатоадресної передачі (багатоадресні пристрої рівня 3 або генератор запитів IGMP), тобто до порту локальної мережі на стороні джерела. Встановлений прапорець означає, що вибраним портом є порт маршрутизатора;
- **Швидкий вихід (Fast Leave)**: увімкніть процес швидкого виходу з відстеженням трафіку багатоадресної передачі на порту. Якщо увімкнено, комутатор припинить надсилати дані багатоадресної передачі заданому клієнту, як тільки від клієнта надійде повідомлення про вихід. В іншому випадку комутатор буде чекати відповіді від клієнта на повідомлення про Запит членства джерела багатоадресної передачі. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Дроселювання (Throttling)**: вказує максимальну кількість груп багатоадресної передачі, дозволених на порту. Можливі значення: "Необмежено" (Unlimited) і діапазон від 0 до 10. "Необмежено" означає, що для групи, яка належить до цього порту, немає обмежень, а числа показують максимально допустимі числа багатоадресних груп.

Якщо бажано застосувати одну конфігурацію до всіх портів, тоді слід використовувати рядок "*", тобто конфігурація, задана в рядку "*", відповідатиме всім портам. Після зміни однієї з описаних раніше конфігурацій з’являються кнопки, які дозволяють користувачеві зберігати або скидати конфігурації.

- Зберегти (Save): зберегти конфігурацію в "Робочій конфігурації" (Running Config);
- Скинути (Reset): скасувати зміни, внесені локально до Робочої конфігурації.

Конфігурація VLAN

Це меню дозволяє налаштувати відстеження трафіку IGMP на основі VLAN. За замовчуванням на комутаторі не налаштовано жодної VLAN. Якщо потрібен новий запис IGMP для конкретної VLAN, натисніть кнопку Додати нову IGMP VLAN (Add New IGMP VLAN). При натисканні з'являться наступні поля для налаштування:

- **Видалити (Delete)**: натисніть кнопку, щоб видалити запис VLAN у рядку;
- **Ідентифікатор VLAN (VLAN ID)**: вкажіть VLAN, яка очікується для прийому в кадрах багатоадресної передачі з адреси, вказаної в цьому записі. Дозволені значення – це дозволені значення VLAN (від 1 до 4095);
- **Відстеження трафіку увімкнено (Snooping Enabled)**: увімкніть функцію відстеження трафіку IPMC для цього запису. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Вибори генератора запитів (Querier Election)**: дозвольте VLAN у цьому записі брати участь у виборах генератора запитів. Якщо увімкнено, цей запис VLAN може перемогти у виборах генератора запитів і бути обраним як тракт до джерела багатоадресної передачі, що буде використовуватися клієнтами багатоадресної передачі. Вибраний прапорець означає, що функцію увімкнено, а порожній прапорець – вимкнено;
- **Адреса генератора запитів (Querier Address)**: вказує адресу IPv4 як адресу джерела, що використовується під час виборів генератора запитів. Вибори генератора запитів визначать, який маршрутизатор або комутатор відстеження трафіку IGMP перенаправлятиме трафік, якщо вони поділяють один і той же сегмент на основі його IP-адреси: пристрій із найнижчою IP-адресою виграє вибори генератора запитів, а потім перенаправлятиме трафік. Якщо не встановлено, використовувана IPv4-адреса буде IP-адресою інтерфейсу керування комутатором. Дозволені значення знаходяться в діапазоні адрес IP версії 4 (IPv4), і значення повинні бути налаштовані в десятковому форматі із крапками;
- **Сумісність (Compatibility)**: вказує, з якою версією IGMP цей запис повинен бути сумісним. Дозволеними значеннями є IGMP-автоматичний, Примусовий IGMPv1, Примусовий IGMPv2 і Примусовий IGMPv3. За замовчуванням вибрано IGMP-автоматичний, що означає, що комутатор самостійно визначатиме протокол, який працює у VLAN. Значення примусових IGMP дозволяють користувачеві конкретно налаштувати, яку версію запису слід використовувати;
- **PRI**: вказує пріоритет (біти PCP в Ethernet-кадрі) кадрів керування IGMP у мережі, щоб визначити пріоритет цих повідомлень на комутаторі, перенаправляючи їх до заданої черги. У мережі комутатор буде надсилати значення PCP на інші пристрої, вбудовані в кадр. Допустимими значеннями є значення діапазону PCP, від 0 до 7;
- **RV**: вказує значення змінної стійкості ("робастності") для використання в мережі цим записом. Це поле дозволяє налаштувати очікувану втрату даних у заданій мережі. У мережах, в яких втрачається багато пакетів, це число повинне бути збільшене. Значення RV не повинно бути рівним 0 або 1. За замовчуванням це значення встановлюється на 2. Дозволеними значеннями є цілі числа від 2 до 255;
- **QI (сек)**: вказує інтервал запитів, який буде використовуватися між загальними запитами цього запису. Такі загальні повідомлення-запити обмінюються між інтерфейсами IGMP, щоб усі вони мали знання про групу багатоадресної передачі. Дозволеними значеннями є цілі числа від 1 до 31.744 секунд. За замовчуванням інтервал запиту встановлений на 125 секунд;
- **QRI (0,1 сек)**: вказує інтервал відповіді на запит, тобто максимальний час, за який клієнти можуть відповісти на загальне повідомлення-запит. Допустимі значення - це цифри від 1 до 31.744 десятих секунд. За замовчуванням інтервал запиту встановлений на 100 (що означає 10 секунд);

- **LLQI (0,1 сек)**: вказує інтервал запиту останнього слухача цього запису. Таймер LLQI вказує максимальний час, дозволений клієнтом для відповіді на запит. Коли строк дії цього таймера закінчиться, генератор запитів та відстежувачі в мережі припинять надсилати багатоадресні дані цьому клієнту. За замовчуванням інтервал запиту встановлений на 100 (що означає 10 секунд);
- **URI (сек)**: вказує інтервал Незатребуваних звітів (Unsolicited Report) цього запису. Цей таймер вказує час між повтореннями первинного звіту хоста про членство в групі. Дозволеними значеннями є цілі числа від 1 до 31.744 секунд. За замовчуванням інтервал запиту встановлений на 1 секунду.

Після зміни однієї з описаних раніше конфігурацій з'являються кнопки, які дозволяють користувачеві зберігати або скидати конфігурації.

- Зберегти (Save): зберегти конфігурацію в "Робочій конфігурації" (Running Config);
- Скинути (Reset): скасувати зміни, внесені локально до Робочої конфігурації.

Профіль фільтрації портів

Це меню дозволяє налаштувати умови фільтрації, які застосовуватимуться до портів на основі профілю IPMC. Використовувані профілі IPMC – це профілі, додані в меню "Профіль IPMC" (IPMC Profile).

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **Профіль фільтрування (Filtering Profile)**: вказує, який профіль можна вибрати для використання цим портом. Дозволені значення – це імена профілів, налаштовані в таблиці профілів у меню "Профіль IPMC". Поле "-" означає, що до цього порту не застосовано жодного профілю фільтрації.

9.3 Відстеження трафіку MLD

Виявлення слухачів багатоадресної передачі (MLD) є частиною протоколу ICMPv6. Його було визначено в RFC 2710 (версія 1), а потім оновлено до версії 2 згідно з RFC 3810. Його використання схоже на IGMP, але замість багатоадресної передачі через мережі IPv4, MLD працює через мережі IPv6.

Механізм протоколу схожий на IGMP. Щоб бути частиною групи, яка отримує багатоадресні дані від відправника, отримувач трафіку MLD повинен надіслати повідомлення "приєднатися до групи", яке повинно бути зрозуміле хостам та маршрутизаторам мережі, що підтримують MLD. Якщо він хоче припинити отримання даних, тоді потрібно надіслати повідомлення "вийти з групи".

Відстеження трафіку MLD можна зрозуміти, з точки зору програмного застосування, як відстеження трафіку IGMP для мереж IPv6.

При використанні цієї функції як функції багатоадресної передачі, усе обладнання в мережі (маршрутизатори, комутатори) повинно мати можливість читати заголовки IP-пакетів та перевіряти групу багатоадресної передачі. У випадку комутаторів рівня 2 переваги багатоадресної передачі можна отримати лише в тому випадку, якщо комутатор може обробляти функцію відстеження трафіку MLD. Якщо ні, багатоадресні повідомлення будуть розглядатися як широкомовні повідомлення. Таким чином, усі члени локальної мережі (або VLAN) отримуватимуть дані, а не лише члени багатоадресної передачі. Визначається діапазон для IP-адрес, який використовується лише для багатоадресної розсилки. Маршрутизатори в мережі, отримуючи кадр, адресований цим IP-адресам, будуть маршрутизувати кадри на основі груп багатоадресної передачі. IP-адресами багатоадресної передачі можуть бути:

- Блок адрес FF00::/8 зарезервований для багатоадресної передачі;

Як і в протоколі IGMP, є адреси, які визначені, і не можуть використовуватися як адреси багатоадресної передачі:

- FF01::1 – адреса "Усі вузли в локальному інтерфейсі", що використовується хостами;

- FF02::2 – адреса "Все в локальному каналі", що використовується хостами;
- FF02::5 – адреса "Усі вузли на локальному сайті", що використовується маршрутизаторами.

Зарезервовані адреси не можна використовувати як IP-адреси багатоадресної передачі. На додаток до адрес, показаних вище, існують загальні служби, такі як багатоадресна передача PTP та багатоадресна передача NTP, які мають конкретні адреси. Переконайтеся, що вони не використовуються під час налаштування групи багатоадресної IP-передачі в мережі.

Базова конфігурація

Конфігурація відстеження трафіку IGMP може використовуватися як зразок для налаштування відстеження трафіку MLD, але з використанням синтаксисів IPv6.

10 Таблиця MAC-адрес

10.1 Основні принципи таблиці MAC-адрес

Комутатори Ethernet працюють в контексті прозорого моста з комутацією пакетів, що є основною концепцією комутації пакетів Ethernet. Отже, є деякі теми, які мають відповідати комутаторам Ethernet, серед них:

- Кожна станція (хост), приєднана до прозорого моста, має глобально унікальну адресу (MAC-адресу);
- Міст має інтерфейс, підключений до всіх локальних мереж, яким належить міст;
- Міст має інформацію, щоб досягати всіх станцій, до яких він підключений;
- Міст працює в невибірковому режимі, в якому він приймає всі кадри на всіх інтерфейсах, незалежно від адреси призначення;

Існує кілька додаткових функцій, які повинен виконувати комутатор, наприклад:

- Фільтрація пакетів;
  - Якщо MAC-адреса джерела даного пакета приєднана до інтерфейсу, де його було отримано, пакет буде відкинутий комутатором.
- Багатоадресна переадресація
  - Адресований кадр багатоадресної передачі повинен пересилатися на всі інтерфейси, крім інтерфейсу вхідного кадру.

Якщо одна з цих концепцій буде порушена, мережа не працюватиме належним чином.

Reason S20, за замовчуванням, налаштований працювати як прозорий міст, тобто як загальний комутатор.

Приклад Ethernet-кадру наведено на Рисунку 35 нижче.

Рис. 44: Ethernet-кадр

Як можна побачити, адреси призначення та джерела прив'язуються безпосередньо до Ethernet-кадру. Таким чином, комутатор повинен мати можливість принаймні обробляти ці поля для виконання своєї основної функції, будучи прозорим мостом у мережевому середовищі з комутацією пакетів.

Якщо хосту потрібно надіслати дані іншому хосту в комутованій локальній мережі, він перенаправить трафік зі своєї власної мережевої карти (карти мережевого інтерфейсу (NIC)) на інтерфейс, який підключений на комутаторі. Потім комутатор відобразить вхідну MAC-адресу в таблиці, відобразивши її в інтерфейсі. Продовжуючи цей процес, комутатор відобразить усі хости, щоб досягти всіх підключених до нього станцій. Слід зауважити, що для цієї операції передбачається відсутність дублювання при адресації хостів, тобто для кожного хоста існують різні MAC-адреси. На рисунку 36 наведено приклад таблиці MAC-адрес у даній локальній мережі.

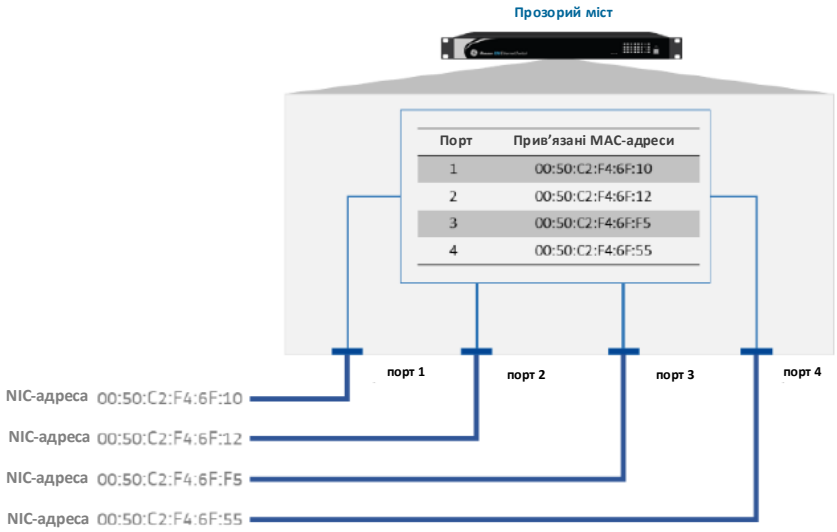


Рис. 45: Таблиця адрес на вказаному комутаторі

Оскільки комутатор знає, де знаходяться хости, вхідні дані на відображений хост будуть перенаправлятись через інтерфейс, до якого прикріплений пункт призначення, і дані не будуть надсилатися на інші інтерфейси, як показано нижче. Якщо вхідні дані надходять на хост, який не відображений як пункт призначення, комутатор може здійснити лавинне розповсюдження на порти, підключені до іншого комутаційного обладнання, або скинути пакети.

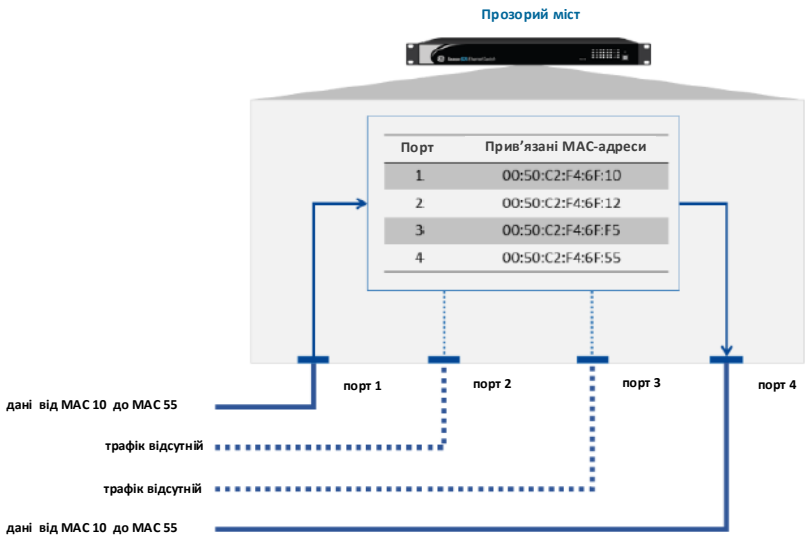


Рис. 46: Переадресація трафіку в Ethernet-комутаторі

Оскільки мережі не є статичними, і хости можуть бути підключені та відключені у будь-який час, комутатор повинен перевірити свою власну таблицю MAC-адрес, щоб оновити її.

Цей процес називається тривалістю існування MAC-адрес у таблиці, і він реалізований у комутаторі, який перевіряє MAC-адреси на вхідних та вихідних пакетах даних. Якщо відображена MAC-адреса перестає отримувати або надсилати дані, комутатор відкине адресу у таблиці MAC-адрес. Таким чином, час обробки для перевірки таблиці адрес зменшується, а продуктивність комутатора збільшується.
З міркувань безпеки можна обмежити доступ до локальної мережі комутатора, вручну вставляючи MAC-адреси дозволених хостів у заданий інтерфейс. У цьому випадку порт буде працювати в захищеному режимі, а обладнання буде перенаправляти трафік лише з встановлених MAC-адрес і буде видаляти дані з MAC-адрес, які не встановлені. Таким чином, можна обмежити доступ до локальної мережі лише MAC-адресами. На наступному рисунку показано, як функціонує керування MAC-доступом у комутаторі.

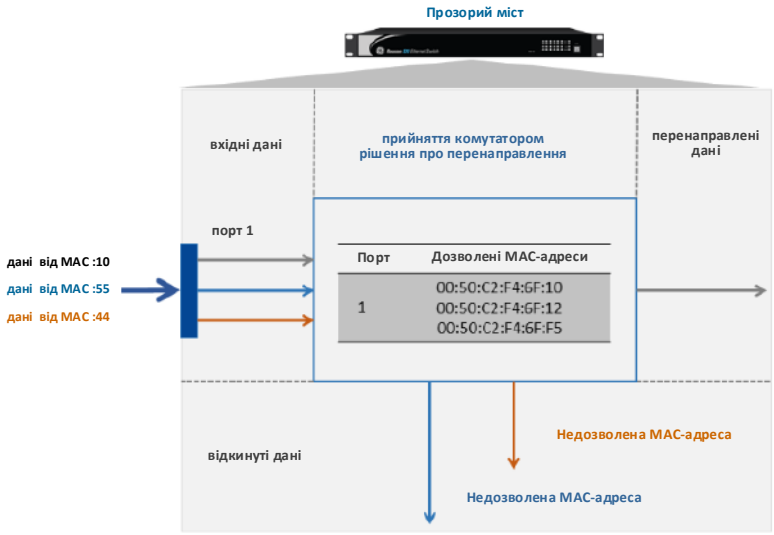


Рис. 47: Обмеження доступу до локальної мережі з конфігурацією MAC-адрес

10.2 Конфігурація таблиці MAC-адрес

Меню "Таблиці MAC-адрес" призначене для налаштування записів MAC-адрес пристрою Reason S20, що може мати до 8192 записів загалом, враховуючи динамічні та статичні записи. Це дозволяє налаштувати тривалість існування вивчених MAC-адрес, режим роботи та введення дозволених MAC-адрес через локальний інтерфейс комутатора.
Меню таблиці MAC-адрес знаходиться в меню Налаштування > Таблиця MAC-адрес (Settings > MAC Table).

Конфігурація тривалості існування

Ця функція дозволяє комутатору автоматично відкидати вивчену MAC-адресу після закінчення тривалості існування цього запису. Можливі наступні конфігурації.

- **Вимкнути автоматичну тривалість існування (Disable Automatic Aging):** вимкнути функцію автоматичної тривалості існування. Вибраний прапорець означає, що конфігурацію тривалості існування вимкнено, а порожній прапорець – увімкнено;
- **Тривалість існування (Aging time):** вказує час, коли закінчується строк дії записів. Дозволені значення – це цілі значення від 10 до 1000000 секунд;

Вивчення Таблиці MAC-адрес

Меню вивчення таблиці MAC-адрес (MAC Table Learning) дозволяє налаштувати поведінку комутатора у процесі вивчення MAC-адрес, тобто, чи комутатор буде використовувати фільтри, налаштовані для обмеження доступу до LAN або ні.

Кожен порт може мати свою функцію вивчення MAC-адрес, обрану окремо. Можливі наступні конфігурації.

- **Авто (Auto)**: виберіть, щоб дозволити процесу вивчення розпочинатися одразу після отримання кадру. Якщо MAC-адреса невідома, порт дізнається джерело або пункт призначення MAC-адреси та вставить її в запис таблиці адрес;
- **Вимкнути (Disable)**: виберіть, щоб вимкнути процес вивчення. Якщо MAC-адреса невідома, порт не дізнається джерело або пункт призначення MAC-адреси, щоб вставити її в запис таблиці адрес;
- **Захищений (Secure)**: виберіть, щоб дозволити розпочати процес вивчення, тільки якщо отриманий кадр надходить від MAC-адреси, налаштованої у конфігурації таблиці статичних MAC-адрес. Якщо MAC-адреса не налаштована, порт скине кадр.

Якщо порти налаштовані як Захищений (безпечний) режим, переконайтеся, що включено канал керування, який використовується для налаштування та контролю комутатора. Якщо ні, конфігурація комутатора буде доступна тільки через послідовний інтерфейс при підключенні USB (локальний інтерфейс).

Конфігурація таблиці статичних MAC-адрес

Таблиця статичних MAC-адрес може містити до 64 записів. Зверніть увагу, якщо порти налаштовані як Захищений режим (Secure mode), переконайтеся, що включено Канал керування, який використовується для налаштування та контролю комутатора. Якщо ні, конфігурація комутатора буде доступна тільки через послідовний інтерфейс при підключенні USB (локальний інтерфейс).

- **Видалити (Delete)**: натисніть кнопку, щоб видалити MAC-адресу в рядку;
- **Ідентифікатор VLAN (VLAN ID)**: вкажіть VLAN, яка передбачається для прийому у кадрах з цієї MAC-адреси. Дозволені значення – це дозволені значення VLAN (від 1 до 4095);
- **MAC-адреса (MAC Address)**: вкажіть номер MAC-адреси дозволеного запису. Значення повинні вводитися в шістнадцятковому форматі, і кожен октет повинен бути відокремлений символом "-";
- **Порти-члени (Port Members)**: вкажіть, які порти дозволяють введення кадрів з цієї MAC-адреси. Вибраний прапорець означає, що порту дозволено приймати кадри з цієї MAC-адреси, а порожній прапорець означає, що порту не дозволено.

11 Віртуальна локальна мережа (VLAN)

11.1 Топологія застарілих мереж LAN

У мережах з комутацією пакетів під локальною мережею (LAN) можна розуміти фізичний зв’язок між хостами (обладнанням, яке використовує локальну мережу для зв’язку між собою) та комутаційним обладнанням (комутаторами), яке буде мати справу з обміном даними від хостів.
Якщо компанія, що має багато відділів (багато типів трафіку даних), хоче розділити свою локальну мережу з метою керування та підтримання ефективності роботи локальної мережі, вона буде використовувати різну інфраструктуру LAN для кожного відділу. Весь трафік між ними повинен бути маршрутизований. Ця ситуація не була б проблемою, якби хости були статичними, що не є звичайною для них поведінкою. З’являються нові користувачі, які приєднуються до локальної мережі, мобільні користувачі, нові зміни в організаційній інфраструктурі, тощо.

Як приклад, уявіть організацію, показану нижче. Відділи A і B розташовані в різних приміщеннях, і локальна мережа кожного відділу фізично відокремлена одна від одної.

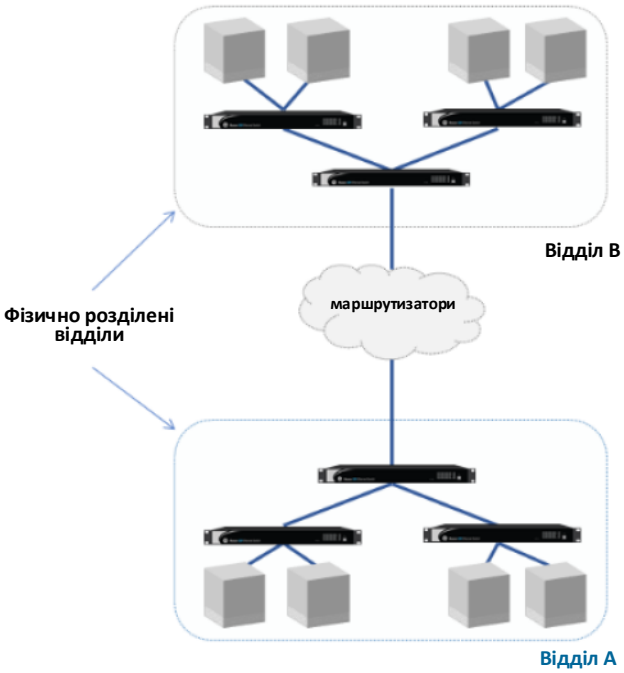


Рис. 48: Різні локальні мережі з різних відділів

А тепер уявіть, що потрібно збільшити кількість хостів у Відділі A, але у приміщенні відділу немає вільного місця, тому новий хост повинен розміщуватися у приміщенні Відділу B. При використанні застарілого (існуючого) обладнанням, яке не підтримує VLAN, таке розширення локальної мережі Відділу A буде здійснено, як показано нижче.

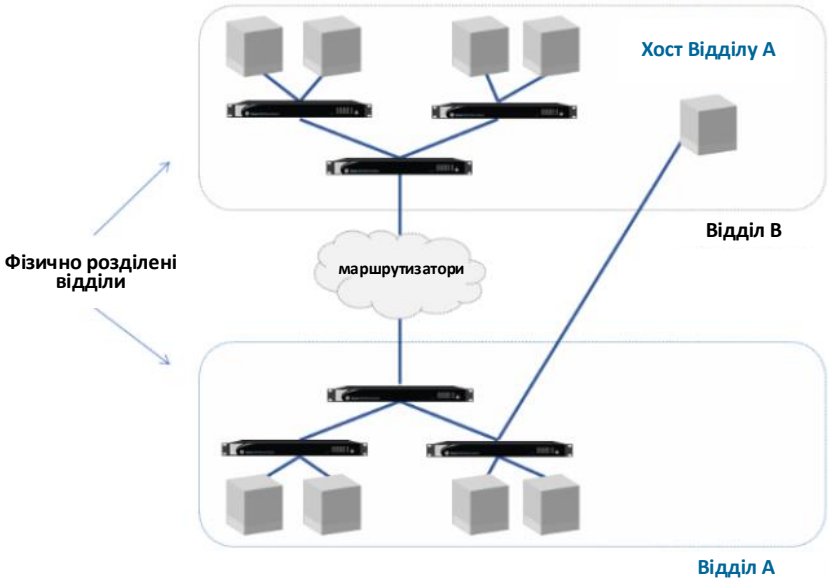


Рис. 49: Додавання нових хостів до застарілого обладнання, яке не підтримує VLAN

Це демонструє, що зміни та розширення в мережі, що не підтримує VLAN, можуть створити проблеми, оскільки буде потрібно змінити всі фізичні установки в мережі. У цьому контексті було створено механізм VLAN.
У сучасному зв'язку в енергосистемах використання тільки застарілого обладнання для передачі даних пристроїв IED через обладнання, що не підтримує VLAN, може створити проблеми у багатьох точках. Однією з них може бути те, що розділення (сегрегація) трафіку повідомлень GOOSE, Вибіркових величин та PTP здійснюватиметься за допомогою іншої фізичної установки LAN. Цей варіант, швидше за все, буде неприйнятним через вартість встановлення та труднощі з обслуговуванням.

11.2 Основні принципи віртуальних LAN

Технологія віртуальної локальної мережі (VLAN) дозволяє розділити мережу з використанням логічної та фізичної мереж. За допомогою інформації VLAN можна створювати логічні мережі на основі її використання замість фізичної установки, таким чином, забезпечуючи набагато більшу гнучкість у мережі.
У наведеному прикладі, якщо для розділення трафіку від різних відділів використовується технологія VLAN, фізична топологія може бути такою, як продемонстровано нижче. На рисунку видно, що кількість проблем із встановленням зменшиться, оскільки хости можуть бути підключені до будь-якого комутатора, що підтримує VLAN, у локальній мережі.

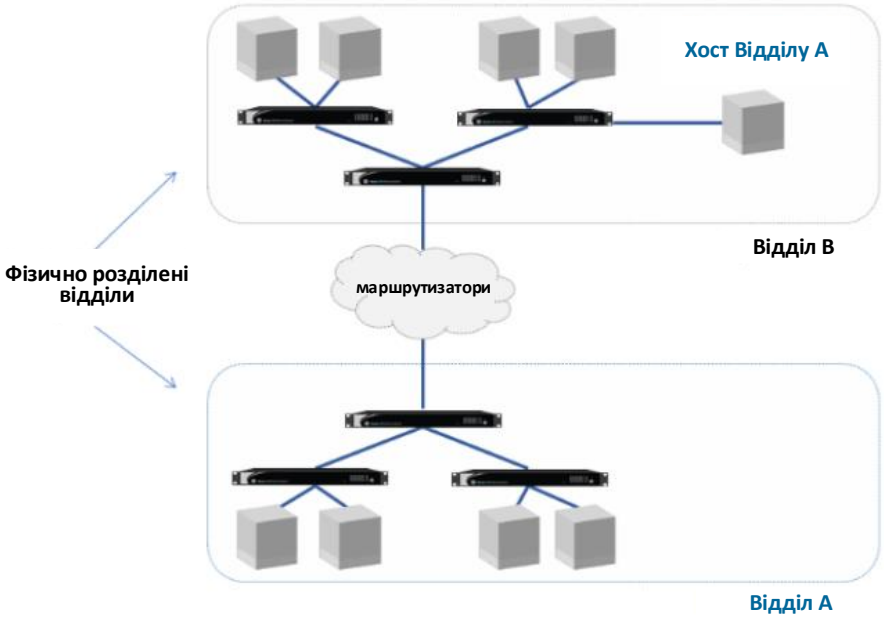


Рис. 50: Додавання нових хостів з підтримкою VLAN

Окрім фізичної установки, механізм VLAN змусить хости бачити одне одного, ніби вони перебувають в одній фізичній локальній мережі, як показано на наступному рисунку. Таким чином, більше немає залежності від підключень обладнання. За допомогою VLAN можна логічно групувати хости або повідомлення зі спільними інтересами.

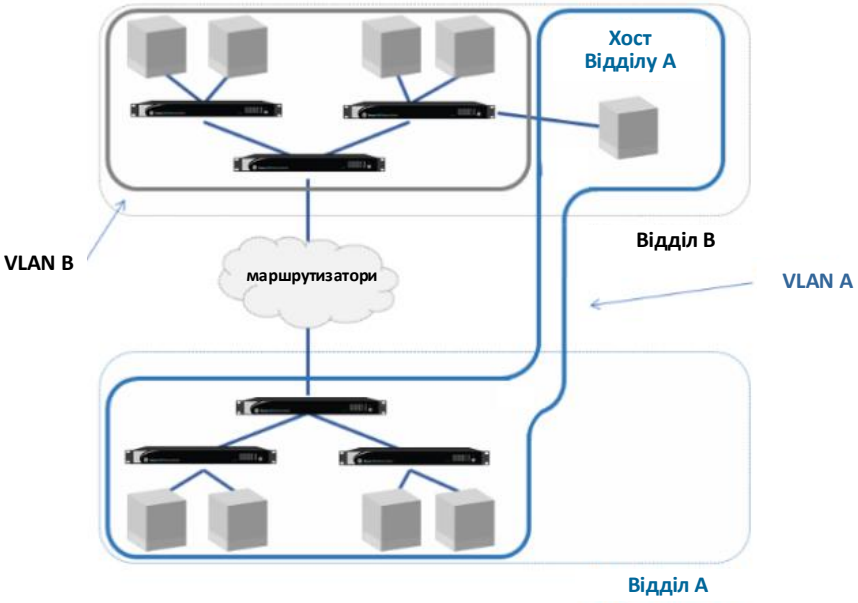


Рис. 51: Сегрегація VLAN у різних відділах

Розділення трафіку з використанням віртуальної локальної мережі (VLAN) стандартизовано документом IEEE 802.1Q. Стандартом було додано 4-байти до Ethernet-кадру, де міститься інформація про логічну локальну мережу, якій належить хост (або повідомлення). На рисунку нижче показано Ethernet-кадр та його позицію тегу 802.1Q.

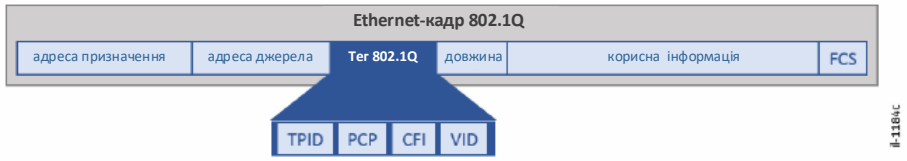


Рис. 52: Ethernet-кадр 802.1Q

Інформація за тегом 802.1Q розділена на 4 поля:

- TPID (Ідентифікатор протоколу тегування): 16-бітна довжина, це поле представляє протокол VLAN і буде дорівнювати 0x8100;
- PCP (Кодова точка пріоритету): 3-бітна довжина, це поле представляє пріоритет пакета в мережі;
- CFI (Одиниця стандартного ("канонічного") формату): 1-бітна довжина, це поле завжди встановлюється на 0 у зв'язку Ethernet;
- VID (ідентифікатор VLAN): 12-бітна довжина, це поле конкретно показує ідентифікатор номера VLAN, якому належить кадр. Його також називають тегом VLAN.

Використання тегів VLAN може мати в своїй основі багато концепцій. Насправді існує багато типів тегів VLAN, які використовуються в різних середовищах, та пов'язані з певними стандартами. Як приклад можна навести C-tag, S-tag та I-tag. Опис, наведений у цьому керівництві, стосується тегу клієнта (C-tag), найпоширенішого використання мережі VLAN у зв'язку в енергосистемі. Оскільки основне застосування Reason S20 полягає в тому, щоб бути трактом для забезпечення взаємозв'язку між обладнанням IED у системах зв'язку для енергосистем, інформації, що міститься в цьому керівництві, має бути достатньо для використання обладнання. Якщо застосування комутатора потребує використання певної VLAN для магістральних каналів, де використовується S-тег, службовий тег VLAN (S-tag) також підтримується пристроєм Reason S20.

Номер VID – це номер, який чітко визначає, до якої VLAN належить вхідний пакет. Теоретично існує 2^{12} (4096) можливостей чисел, оскільки це 12-бітове поле. Крім того, є два зарезервовані номери VID:

- VID = 0xFFF зарезервований і не повинен використовуватися;
- VID = 0x000 означає кадр, позначений тегом пріоритету. Цей кадр не пов'язаний з жодною ідентифікацією VLAN, але конкретно показує пріоритет пакета.

Використовуючи механізм VLAN, майте на увазі, що 0xFFF VLAN не використовується.

За замовчуванням кадри, позначені тегом-пріоритету (VID = 0x000), будуть відображені з власним ідентифікатором VLAN (VID = 0x001), а інформація про пріоритет буде видалена на вихідному кадрі.

11.3 LAN у системах передачі даних для сучасних енергосистем

Технологія віртуальної локальної мережі (VLAN) дозволяє розділити трафік з використанням логічної та фізичної мереж. У системах зв'язку для енергосистем, де очікуються повідомлення МЕК-61850 з різним пріоритетом та використанням, для кожного пристрою IED буде лише один фізичний тракт, і пакети повинні бути розділені логічно.

Розділення трафіку є особливо важливим для зв'язку сучасних енергосистем, оскільки очікується, що в мережі буде потік трафіку багатоадресної передачі. Повідомлення GOOSE, Вибіркових величин та Протоколу точного часу – це повідомлення багатоадресної передачі, і всі вони можуть бути відображені безпосередньо в Ethernet-кадрі, іншими словами, вони є протоколом зв'язку рівня 2. Оскільки механізм трафіку цих повідомлень багатоадресний, за замовчуванням комутатор передаватиме їх по всіх своїх інтерфейсах, крім вхідних повідомлень. При використанні розділення трафіку VLAN повідомлення багатоадресної передачі пересилаються лише у ту VLAN, якій належить повідомлення багатоадресної передачі. Таким чином, трафік GOOSE, Вибіркових величин та PTP буде протікати окремо один від одного. Наостанок, оскільки трафік відокремлений, обладнання IED, яке очікує отримувати лише повідомлення GOOSE, не буде стикатися з явищем переривання свого мережевого інтерфейсу даними вибіркових величин.

Приклад очікуваної сегрегації трафіку VLAN показаний нижче. Слід зауважити, що кільцева фізична топологія використовується тільки для прикладу, оскільки це загальна топологія фізичної мережі у зв'язку енергосистеми. Перш ніж звернутися до рисунка, є кілька припущень:

- Об’єднуючий пристрій (Merging Unit) – забезпечує повідомлення GOOSE та вибіркових величин, і це ведений годинник протоколу синхронізації PTP;
- Головний годинник PTP (PTP grandmaster) синхронізує обладнання, яке підтримує PTP, і не отримує даних GOOSE або вибіркових величин;
- Пристрій IED не синхронізуються через протокол PTP. Обидва вони очікують отримати повідомлення GOOSE від Об'єднуючого пристрою, і лише один з них очікує отримати Вибіркові величини;
- На задіяному обладнанні налаштовано 3 VLAN: одна для трафіку PTP, інша для трафіку Вибіркових величин та ще одна для трафіку повідомлень GOOSE.

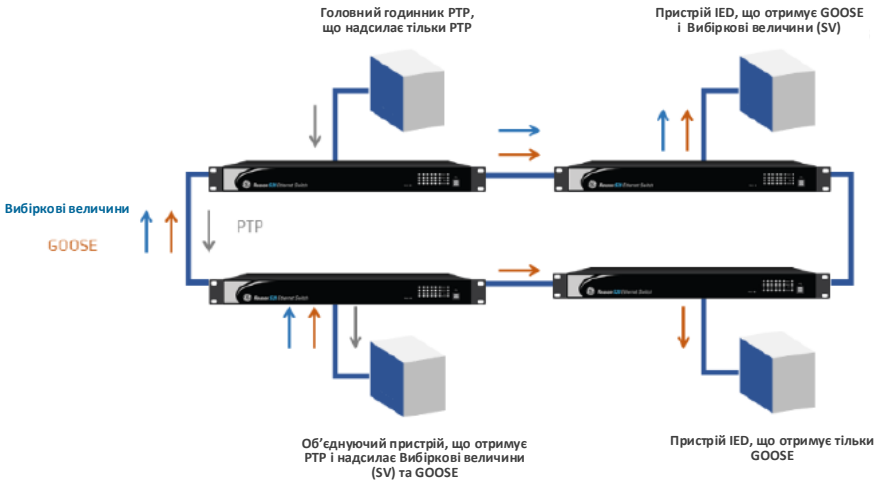


Рис. 53: Типова топологія в середовищі зв'язку енергосистеми

Логічна мережа, яку створюють комутатори при використанні розділення трафіку VLAN, показана нижче.

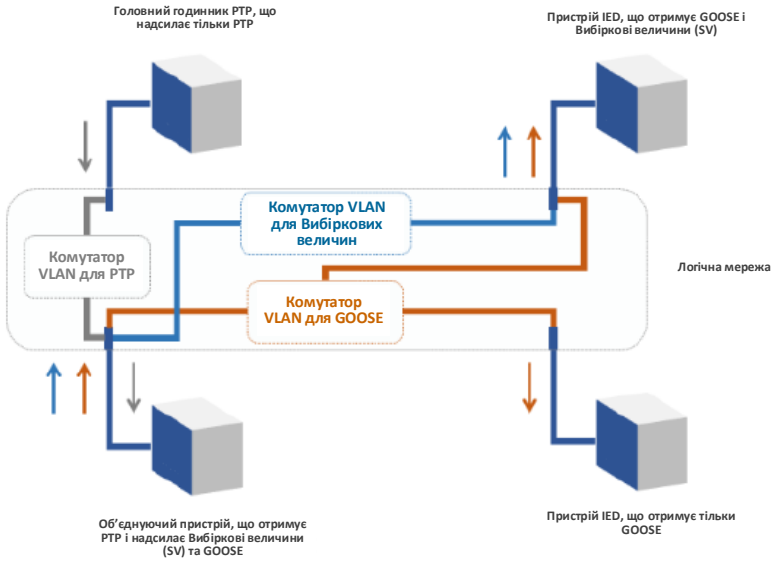


Рис. 54: Логічна топологія типового середовища зв'язку енергосистеми

Документи МЕК 61850 рекомендують використовувати різні методи резервування на шині зв'язку станції та процесу. Для спрощення ці вимоги щодо резервування не показані та не обговорюються у цьому пункті.

11.4 Принципи роботи комутатора згідно з IEEE 802.1Q

У попередніх пунктах можна було зрозуміти, що таке VLAN і, що очікується від використання пакетів з інформацією про VLAN. Цей пункт продемонструє основи роботи комутатора при обробці кадрів 802.1Q, що стосується Reason S20. На наступному рисунку показано потік трафіку даних всередині комутатора.

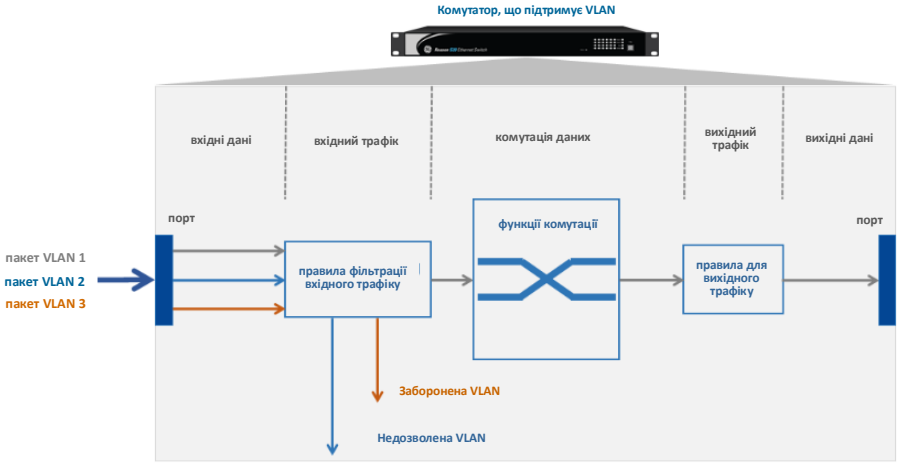


Рис. 55: Потік трафіку всередині комутатора 802.1Q

Як бачимо, немає керування вхідними даними, комутатор буде отримувати всі дані, які надсилає хост. Рішення про пересилання, таким чином, базується на застосованих правилах фільтрації вхідного трафіку. Правила для вхідного трафіку визначатимуть:

- Які кадри VLAN є прийнятними;
- Чи дозволені нетеговані кадри VLAN;

Якщо вхідний кадр надходить із недозволеної VLAN, він буде відкинутий. Крім того, якщо пакет – це кадр, позначений тегом пріоритету, або нетегований кадр, правила фільтрації вхідного трафіку будуть призначати кадр до VLAN, членом якої є порт.

Комутатори 802.1Q завжди працюють у режимі VLAN. Коли вхідні кадри не мають інформації про VLAN або програмні застосунки не потребують використання VLAN, комутатор інкапсулює кадр у кадрі 802.1Q, а правила обробки вихідного трафіку визначать, чи буде кадр надсилатися з інформацією VLAN чи без неї.

Коли дозволено переадресовувати кадр, функції комутації перевіряють, членом якої VLAN є кадр, і він буде перенаправлений на основі портів, які є членами цієї VLAN. Тоді таблиця MAC-адрес буде переадресовувати трафік, оскільки хости відображаються при використанні одноадресного зв'язку. При широкомовних та багатоадресних передачах комутатор буде здійснювати лавинне розповсюдження тільки до портів VLAN, які є членами VLAN вхідного кадру широкомовної передачі/ багатоадресної передачі.

Наприкінці процесу правила фільтрації вихідного трафіку визначать, чи буде комутатор підтримувати або відкидати інформацію про VLAN.

Якщо потрібно підтримувати 802.1Q, всі кадри залишать комутатор тегованим, включаючи ті, які надійшли без інформації тегів, які залишатимуть комутатор з ідентифікатором VLAN порту (PVID) вхідного порту. Кадри 802.1Q залишать комутатор такими, якими вони надійшли.

Якщо потрібно відкинути всю інформацію 802.1Q на кадрі, тоді всі кадри залишать комутатор нетегованими, включаючи ті, що надійшли з інформацією про теги.

Окрім вихідної фільтрації кадру 802.1Q, Reason S20 має третій варіант фільтрації вихідного трафіку: відкидати інформацію тільки з кадрів PVID. Якщо вони використовуються, нетеговані кадри, які були позначені на PVID, залишать комутатор без тегів, а теговані кадри залишать комутатор тегованими. Таким чином, теговані та нетеговані кадри можуть залишати комутатор такими, якими вони надходять.

11.5 Функціонування Reason S20

Reason S20 – це обладнання, яке підтримує VLAN, і його функціонал дозволяє використовувати розділення трафіку у якості прозорого мосту, використовуючи тегування 802.1Q. При використанні функції VLAN існують деякі терміни та визначення, які слід розуміти для налаштування правильної конфігурації.
Reason S20 працює тільки в режимі з підтримкою VLAN, і весь трафік обробляється згідно з принципами VLAN. Теговані дані VLAN будуть перенаправлені на VLAN, якій вони належать, а нетегований трафік буде перенаправлений на VLAN, встановлену на порту VLAN. На виході, за замовчуванням, нетеговані вхідні кадри будуть пересилатися без тегу VLAN, такими, якими вони надійшли на комутатор.

Режим роботи порту

Режим роботи можна визначити як порт доступу, магістральний порт або гібридний порт.
Порт доступу (Access port) використовується, коли підключено застаріле (існуюче) обладнання. Застаріле обладнання може бути обладнанням, яке не підтримує VLAN та технологію тегування VLAN для клієнтів, таким як обладнання IED. Ці порти будуть позначати нетегований вхідний трафік номером порту VLAN і переадресовувати трафік у цю VLAN. Коли вхідні кадри мають інформацію про VLAN, кадр буде спрямований до вказаної VLAN. На виході тег, який внутрішньо використовує комутатор для перенаправлення нетегованих кадрів, буде видалений.

Порти доступу завжди визначаються як С-порти, що дозволяють теговані та нетеговані вхідні кадри. На виході всі кадри є нетегованими. Доступ до трафіку дозволений лише порту VLAN. Заборонена VLAN на портах та вихідне тегування можуть бути налаштовані користувачем.

Магістральні порти (Trunk ports) приймають теговані кадри VLAN з багатьох VLAN. Ці порти дозволяють вхід кадрів, тегованих VLAN, і зберігатимуть свої теги на виході. В іншому випадку користувач повинен налаштувати, яку VLAN магістральний порт приймає чи ні. Ці порти можуть бути членами декількох VLAN, обмежених максимально дозволеною кількістю VLAN (4095 VLAN). Вхідні дані із недозволеної VLAN будуть відкинуті під час процесу входу в комутатор. За замовчуванням магістральні порти дозволяють передавати весь діапазон VLAN (1 - 4 095). Магістральні порти – це, як правило, порти, підключені до комутаторів або пристроїв IED, які надсилають дані до декількох VLAN, наприклад, до об'єднуючих пристроїв (одна VLAN для даних GOOSE, а інша – для даних Вибіркових величин).

Магістральні порти завжди визначаються як С-порти і дозволяють теговані та нетеговані вхідні кадри. Дозволена та заборонена VLAN на портах та вихідне тегування можуть бути налаштовані користувачем. При використанні обладнання, що забезпечує великий трафік VLAN, наприклад, IED, що отримує Вибіркові величини та повідомлення GOOSE на одному мережевому інтерфейсі, тип порту точки підключення IED до комутатора слід вважати магістральним портом.

Гібридні порти (Hybrid ports) дозволяють користувачеві налаштовувати всі параметри на даному порту, такі як вхідне фільтрування, порт VLAN (у разі нетегованого кадру), дозволені і заборонені VLAN. Гібридні порти можуть дозволити, якщо бажано, вхід пакетів із даної VLAN, яка не є членом або не є забороненою VLAN.

Гібридні порти дозволяють користувачам налаштувати всі можливі процеси обробки, які комутатор буде виконувати у VLAN, такі як порт VLAN, тип порту, фільтрування вхідного трафіку, прийняття вхідного трафіку, прийняття вихідного трафіку та налаштування дозволених та заборонених VLAN.

Концепція типу порту

На додаток до режиму роботи існує концепція типу порту, яку слід розуміти. Для типів портів можна встановити тип "Не підтримується", "С-порт", "S-порт" та "Користувацький-S-порт" (Unaware, C-Port, S-Port та S-Custom-Port).
Unaware-порт ("Не підтримується") використовується для підключення застарілого обладнання. Ці порти не враховують інформацію вхідних кадрів про VLAN, і всі вхідні кадри класифікуються за номером порту VLAN. При виході кадру тег порту VLAN видаляється.
Порт користувацького тегу (C- Port) – це порт, який має справу з кадрами, позначеними тегом C. Це загальні теговані кадри, такі як вхідні повідомлення GOOSE. Таким чином, при використанні обладнання, яке надсилає теговані кадри, саме цей тип порту потрібно використовувати. Вхідні кадри з інформацією про VLAN будуть спрямовані до VLAN, а кадри з тегами пріоритету або без тегів спрямовуються на VLAN порту.
Порт службового тегу (S-Port) – це порт, який передбачає роботу з кадрами з подвійним тегом. Кадри з подвійним тегом – це кадри, які мають кадр із тегом C всередині іншого тегу VLAN, який є тегом служби VLAN. Кадри з тегом S використовуються комутаційним обладнанням у мережі для створення VLAN для транспортування тегованих кадрів. Ці кадри використовуються тільки комутаційним обладнанням. Таким чином, якщо потрібен S-тег, переконайтеся, що S-порт підключений до іншого комутаційного обладнання, наприклад, до іншого комутатора.
Порт користувацького службового тегу (S-Custom-Port) використовується в середовищах, де традиційний S-тег не відповідає вимогам мережі. Поведінка цього порту дуже схожа на S-порт, за винятком того, що очікуване поле Ethertype у кадрах Ethernet користувацького S-порту визначається на комутаторі, тобто, поле Ethertype у кадрі слід налаштовувати вручну на комутаторі. Ці порти можуть використовуватися у схемах, де використовується нетрадиційне комутаційне обладнання, щоб забезпечити їх певну сумісність.
Існує кілька концепцій щодо обробки нетегованих кадрів, фільтрування на вході та на виході комутатора та діапазон VLAN, членом якої може бути порт, як пояснюється нижче.
Параметр VLAN порту – це VLAN, яку комутатор використовуватиме, якщо вхідний трафік не позначений тегами. Всі кадри, що знаходяться "всередині" комутатора, є тегованими кадрами, а нетеговані вхідні кадри будуть внутрішньо теговані у VLAN, визначеній у VLAN порту.
Фільтрування та прийняття вхідного трафіку можуть бути налаштовані користувачем, коли вибраний порт це дозволяє. Якщо використовується фільтрування на вході порту, порт може вибрати, чи він прийматиме теговані або нетеговані кадри. Якщо фільтрування не використовується, комутатор буде виконувати свою функцію в невибірковому режимі, тобто, будуть отримані всі вхідні дані.
Фільтрування та прийняття вихідного трафіку можуть бути налаштовані користувачем, коли вибраний порт це дозволяє. При використанні комутатор може бути налаштований на зняття тегів з усіх вихідних кадрів, призначення тегів всім вихідним кадрам та на зняття тегів (вирізання інформації про VLAN з кадру) PVID-кадрів. Якщо використовується "знімати теги з усіх кадрів" (untag all), то кадри завжди виходитимуть з комутатора без інформації про VLAN, включаючи ті кадри, що надійшли з інформацією про VLAN. Якщо використовується "тегування усіх кадрів" (tag all), то кадри завжди виходитимуть з комутатора з інформацією про VLAN, включаючи ті кадри, що надійшли без інформації про VLAN. У цьому випадку нетеговані вхідні кадри будуть інкапсульовані у кадр 802.1Q з ідентифікацією PVID. Нарешті, якщо використовується "знімати теги PVID" (untag PVID), інформація про VLAN буде відкинута тільки для кадрів з ідентифікатором PVID, а всі інші ідентифікатори VLAN будуть збережені.

Потрібна увага при змішаному використанні мережевого обладнання VLAN та обладнання, яке не підтримує VLAN, на одному порту. Якщо варіант застосування потребує цього, використовуйте ідентифікатори VLAN в обладнанні, що підтримує VLAN, які відрізняються від номера PVID, який буде використовуватися лише для обладнання, яке не підтримує VLAN, а потім виберіть "зняти тег" PVID при тегуванні вихідного трафіку. Якщо один і той самий ідентифікатор використовується як на обладнанні, що підтримує VLAN, так і на обладнанні, що не підтримує VLAN, в усіх кадрах з PVID (що надсилаються на хости, що підтримують VLAN, та хости, що не підтримують VLAN) інформація про 802.1Q буде відкидатися.

Дозволені та заборонені VLAN – це поняття, що використовуються для визначення того, членом якої VLAN (або якого діапазону ідентифікаторів VLAN) буде порт. Магістральні та гібридні порти можуть бути членами якомога більшої кількості VLAN. Таким чином, такі порти можуть отримувати дані з усіх дозволених налаштованих VLAN. Окрім того, оскільки бажано чітко визначити, до якої VLAN не повинен належати порт, існує концепція забороненої VLAN. У цій концепції порту дозволено бути членом будь-якої VLAN, крім заборонених. Ця остання концепція особливо корисна, якщо наявні занадто багато VLAN, членом яких повинен бути порт, і кілька, членом яких він не повинен бути. Таким чином, можна налаштувати всі прийняті VLAN та короткий список неприйнятих. Наприклад, при застосуванні в енергосистемах така концепція може бути використана для того, щоб гарантувати, що дані Вибіркових величин (Sampled Values) не залишають шину процесу, таким чином підвищуючи захист пропускної здатності станційної шини.

11.6 Конфігурація VLAN

Меню VLAN дозволяє налаштовувати конфігурацію сегментів віртуальної локальної мережі для розділення широкомовних доменів. Інформація про VLAN відображається безпосередньо в Ethernet-кадрі і стандартизована згідно зі стандартом IEEE 802.1Q. VLAN – це основний спосіб розділити трафік станційної шини та шини процесу в Reason S20. Вибіркові величини, GOOSE, PTP, MMS та інші повідомлення можуть бути розділені одне від одного за допомогою VLAN, збільшуючи продуктивність їх використання в енергосистемах.
Меню VLAN знаходиться в меню Налаштування> VLAN (Settings > VLANs).

Глобальна конфігурація VLAN

Меню Глобальної конфігурації VLAN містить основні конфігурації, що використовуються функцією VLAN. Такими конфігураціями є VLAN з дозволеним доступом та Ethertype, які можна використовувати для користувацьких S-портів.

- **VLAN з дозволеним доступом (Allowed Access VLAN)**: вказує ідентифікатори VLAN, дозволені, коли режимом порту є "Доступ" (Access). За замовчуванням на портах, налаштованих як порти "Доступу", дозволений тільки VLAN ID 1. Якщо потрібно, до нього можна додати ідентифікатори VLAN. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095). Можна вставити конкретні ідентифікатори VLAN, розділені комами (наприклад, 1,2,10,40), діапазон ідентифікаторів VLAN з використанням символу "-" (наприклад, 10-40), а також комбінацію конкретних ідентифікаторів VLAN та ідентифікаторів діапазону VLAN (наприклад, 1,2,10-40);
- **Ethertype для користувацьких S-портів (Ethertype for Custom S-ports)**: вказує дозволений для входу Ethertype (на додаток до 0x8100 Ethertype, визначеного 802.1Q), якщо порт налаштований як Користувацький-S-порт. Коли кадр має налаштований Ethertype в цьому полі, він буде класифікований за ідентифікатором VLAN ID, вбудованим у кадр, або, якщо ідентифікатор VLAN ID не вбудований, він буде класифікований за ідентифікатором VLAN порту. Значення слід вставляти у шістнадцятковому форматі.

Конфігурація VLAN порту

Меню конфігурації VLAN порту (Port VLAN Configuration) містить дозволені конфігурації портів, що використовуються функцією VLAN. Це меню дозволяє здійснювати конфігурацію усіх налаштувань VLAN на певному порту. Режим роботи порту, дозволені ідентифікатори VLAN, правила фільтрації VLAN – це приклади конфігурації, яку дозволяє налаштувати це меню.
Якщо бажано застосувати одну конфігурацію до всіх портів, тоді слід використовувати рядок "*", тобто конфігурація, виконана в рядку "*", відповідатиме всім портам. Можливі наступні конфігурації.

- **Порт (Port)**: показує порт, який потрібно налаштувати в цьому рядку;
- **Режим (Mode)**: вказує режим роботи порту. Це поле визначатиме основну поведінку порту. Допустимі наступні значення:
  - **Доступ (Access)**: означає, що порт буде працювати як Порт доступу. Зазвичай це використовується кінцевими станціями, тобто обладнанням, яке не підтримує VLAN. Основними характеристиками цих портів є:
    - **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри перенаправляються на ідентифікатор VLAN порту VLAN, а теговані кадри перенаправляються на VLAN, вбудовану в кадр;
    - **Процес фільтрування на вході (Filtering ingress process)**: приймаються як теговані, так і нетеговані кадри, але кадри, які не належать до поля VLAN з дозволеним доступом або належать до поля заборонених VLAN, відкидаються;
    - **Процес виходу (Egress process)**: на всіх кадрах видаляється ідентифікатор VLAN, тобто порти доступу дозволяють вихід тільки нетегованих кадрів.
  - **Магістраль (Trunk)**: вказує, що порт буде працювати як Магістральний порт. Зазвичай це використовується підключенням мостів або обладнанням IED, яке приймає кадри від декількох VLAN на одному порту. Наприклад, Об'єднуючий пристрій, що надсилає Вибіркові величини та повідомлення GOOSE через один і той же інтерфейс Ethernet, повинен бути підключений до Магістрального порту, оскільки він буде отримувати обидва повідомлення VLAN. Основними характеристиками цих портів є:
    - **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри перенаправляються на ідентифікатор VLAN порту VLAN, а теговані кадри перенаправляються на VLAN, вбудовану в кадр;
    - **Процес фільтрування на вході (Filtering ingress process)**: фільтрування вхідного процесу буде залежати від конфігурації поля Тегування на виході. Магістральний порт може приймати як теговані, так і нетеговані кадри, якщо для Тегування на виході встановлено значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту". У цьому випадку кадри, які не належать до поля Дозволених VLAN або належать до поля Заборонених VLAN, відкидаються. Магістральний порт може приймати лише теговані кадри, якщо для Тегування на виході встановлено "Тегування всіх кадрів у процесі виходу". У цьому випадку кадри, які не належать до поля Дозволених VLAN або належать до поля Заборонених VLAN, відкидаються;
    - **Процес виходу (Egress process)**: поведінка виходу буде залежати від конфігурації поля Тегування на виході (Egress Tagging). Магістральний порт можна встановити на значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (тобто нетеговані кадри залишають комутатор без тегів, а теговані кадри залишають комутатор з тегами) або на "Тегування всіх кадрів".

- **Гібридний (Hybrid)**: означає, що порт буде працювати як Гібридний порт. Це найбільш гнучкий режим порту, оскільки гібридні порти дозволяють налаштувати кожен процес у функції VLAN. Основними характеристиками цих портів є наступні:
  - **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри перенаправляються на ідентифікатор VLAN порту VLAN, а теговані кадри перенаправляються на VLAN, вбудовану в кадр;
  - **Процес фільтрування на вході (Filtering ingress process)**: можна визначити чи будуть прийматися тільки теговані, тільки нетеговані або як теговані, так і нетеговані кадри. Крім того, кадри, які не належать до поля VLAN з дозволеним доступом або належать до поля Заборонених VLAN, відкидаються. Фільтрування прийняття на вході не залежить від процесу Тегування на виході;
  - **Процес виходу (Egress process)**: поведінка на виході буде залежати від конфігурації поля Тегування на виході (Egress Tagging). Для гібридного порту можна встановити параметр "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (тобто нетеговані кадри залишають комутатор без тегів, а теговані кадри залишають комутатор з тегами) або "Тегування всіх кадрів". Фільтрування Тегування на виході не впливає на фільтр Прийняття на вході.

- **VLAN порту (Port VLAN)**: Визначте номер VLAN (від 1 до 4095) для кожного порту Ethernet.
- **Тип порту (Port Type)**: Визначте форму типу для кожного порту наступним чином:
  - **Не підтримується (Unaware)**: вказує, що порт буде працювати як не підтримуваний у процесі входу. Ці порти класифікують усі кадри за ідентифікатором VLAN порту, незалежно від наявності ідентифікатора VLAN або його відсутності;
  - **C-порт (C-Port)**: вказує, що порт буде працювати як C-порт у процесі входу. Ці порти класифікують нетеговані кадри за ідентифікатором VLAN порту та перенаправляють теговані кадри до VLAN, вбудованої у кадр. У процесі виходу C-порти пересилають теговані кадри (якщо вони налаштовані для цього) з ідентифікатором VLAN C-тегу;
  - **S-порт (S-Port)**: вказує, що порт буде працювати як S-порт у процесі входу. Ці порти класифікують нетеговані кадри за ідентифікатором VLAN порту. Теговані кадри з Ethertype 0x8100 або 0x88A8 будуть перенаправлені на VLAN, вбудовану у кадр. У процесі виходу S-порти пересилають теговані кадри (якщо вони налаштовані для цього) з ідентифікатором VLAN S-тегу;
  - **Користувацький-S-порт (S-Custom-Port)**: вказує, що порт буде працювати як Користувацький-S-порт в процесі входу. Ці порти класифікують нетеговані кадри за ідентифікатором VLAN порту. Теговані кадри з Ethertype 0x8100 або зі значенням, налаштованим на Ethertype для користувацьких S-портів, будуть перенаправлені на VLAN, вбудовану у кадр. У процесі виходу S-порти пересилають теговані кадри (якщо вони налаштовані для цього) з ідентифікатором VLAN S- тегу;
- **Вхідне фільтрування (Ingress Filtering)**: Увімкніть функцію фільтрування кадрів на вході. Якщо увімкнено, кадри, класифіковані до VLAN, членом якої не є порт, відкидаються. Таким чином, будуть прийматися тільки ідентифікатори дозволених VLAN та ідентифікатори, які не належать до кадрів заборонених VLAN. Вибраний прапорець означає, що фільтрування на вході увімкнено, а порожній прапорець – вимкнено;

- **Приймання на вході (Ingress Acceptance)**: вказує правила приймання на вході, які застосовуватимуться, якщо увімкнене фільтрування приймання. Дозволеними значеннями є "теговані та не теговані", "тільки теговані" та "тільки нетеговані" кадри, а можливими конфігураціями є наступні:
  - **Теговані та нетеговані (Tagged and Untagged)**: означає, що порт буде приймати як теговані, так і нетеговані кадри (з дотриманням правил дозволених VLAN та заборонених VLAN);
  - **Тільки теговані (Tagged Only)**: означає, що порт буде приймати тільки теговані кадри (з дотриманням правил дозволених VLAN та заборонених VLAN). Нетеговані кадри будуть відкинуті;
  - **Тільки нетеговані (Untagged Only)**: означає, що порт прийматиме тільки нетеговані кадри, які будуть переадресовані на ідентифікатор VLAN порту VLAN. Теговані кадри будуть відкинуті;
- **Тегування на виході (Egress Tagging)**: вказує правила тегування на виході, що застосовуються в процесі виходу кадрів на порту. Дозволеними значеннями є "Знімати теги на порту VLAN", "Тегування усіх кадрів", "Знімати теги усіх кадрів", а можливими конфігураціями є наступні:
  - **Знімати теги на порту VLAN (Untag Port VLAN)**: означає, що всі ідентифікатори VLAN залишатимуться такими, якими вони надійшли на комутатор, крім ідентифікаторів VLAN, що дорівнюють номеру VLAN порту. Якщо ідентифікатор VLAN (VID) кадру у вихідній черзі, дорівнює VLAN порту, комутатор видалить VID, і кадр буде пересилатися як нетегований кадр. На інші номери VID це не впливає, і вони перенаправляються разом із тегом ідентифікатора VLAN;
  - **Тегування усіх кадрів (Tag All)**: означає, що всі кадри у вихідній черзі будуть перенаправлятися як теговані кадри, включаючи кадри, які надійшли на комутатор як нетеговані кадри;
  - **Знімати теги з усіх кадрів (Untag All)**: означає, що всі кадри у вихідній черзі будуть перенаправлятися як нетеговані кадри, включаючи кадри, які надійшли на комутатор як теговані;
- **Дозволені VLAN (Allowed VLANs)**: вкажіть VLAN, членом яких може стати порт. На портах доступу це поле вимкнене, і ці порти можуть бути лише членами ідентифікатора VLAN з дозволеним доступом. Магістральні та гібридні порти можуть бути членами багатьох VLAN, і це поле вказує всі VLAN, членами яких можуть бути порти у цих режимах. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095). Можна вставити конкретні ідентифікатори VLAN, розділені комами (наприклад, 1,2,10,40), діапазон ідентифікаторів VLAN з використанням символу "-" (наприклад, 10-40), а також комбінацію конкретних ідентифікаторів VLAN та ідентифікаторів діапазону VLAN (наприклад, 1,2,10-40). За замовчуванням магістральні та гібридні порти є членами всього діапазону VLAN (1 - 4095);
- **Заборонені VLAN (Forbidden VLANs)**: вказує на VLAN, членом яких не може стати порт. Порти доступу, магістральні та гібридні порти можна налаштувати на відмову від трафіку багатьох ідентифікаторів VLAN, і це поле вказує всі VLAN, членами яких не можуть бути ці порти. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095). Можна вставити конкретні ідентифікатори VLAN, розділені комами (наприклад, 1,2,10,40), діапазон ідентифікаторів VLAN з використанням символу "-" (наприклад, 10-40), а також комбінацію конкретних ідентифікаторів VLAN та ідентифікаторів діапазону VLAN (наприклад, 1,2,10-40). За замовчуванням на усіх портах це поле порожнє, що означає відсутність обмежень VLAN.

12 Якість обслуговування (QoS)

Функція якості обслуговування використовується для гарантування пріоритету трафіку, коли мережа LAN (або VLAN) перевантажена. Існує кілька способів відокремлення пріоритетного трафіку від трафіку загального призначення, пристрій Reason S20 підтримує функцію QoS на бітах CoS та DSCP для зв'язку 2 і 3 рівня відповідно.
Таким чином, у цьому пункті увагу буде зосереджено на використанні бітів CoS (Класу обслуговування (Class-of-Service)), в Ethernet-кадрах 802.1Q, що є одним із типів QoS. Як показано у пункті VLAN, кадри 802.1Q містять 3-бітове поле для визначення пріоритету позначеного пакета VLAN. Як пояснюється в цьому пункті, пристрої Reason S20 також підтримують Точку коду диференційованих послуг (DSCP) в IP-трафіку.

12.1 Основні принципи QoS

Слід вважати, що пропускна здатність мережі занадто велика, як показано нижче, всі вхідні дані обробляються та пересилаються. Пакети даних можна розуміти як Ethernet-кадри, що обробляються комутатором. Крім того, цю філософію можна екстраполювати на інші протоколи багаторівневого представлення.

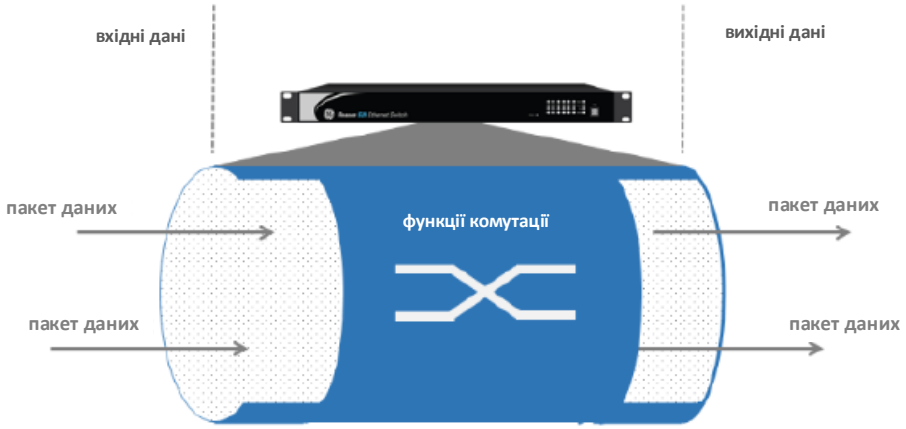


Рис. 56: Трафік при великій пропускній здатності

Якщо при отриманні вхідних даних спостерігаються спорадичні незначні часові піки, комутатор зберігає пакети, які не можуть бути доставлені у внутрішньому буфері, а потім, коли піковий трафік закінчується, дані перенаправляються, а пам'ять буфера стає порожньою.
Крім того, якщо трафік вхідних даних збільшується на час, який перевищує час, що підтримується буферами, що знаходяться в комутаторі, дані будуть втрачені.
У системі зв'язку енергосистеми широко застосовуються протоколи зв'язку без встановлення з'єднання, тобто протоколи, які не гарантують доставку відправлених даних. Протокол часу NTP, як приклад, використовує транспортний протокол UDP. Протоколи GOOSE та Вибіркових величин (Sampled Values) відображаються безпосередньо у кадрі Ethernet і використовують багатоадресний транспортний механізм, таким чином, будучи протоколами без встановлення з'єднання. Протокол PTP може бути відображений безпосередньо в Ethernet, як GOOSE і Вибіркові величини, або в UDP, як протоколи NTP. У цій ситуації, щоб гарантувати, що дані з вищим пріоритетом не будуть втрачені, слід забезпечити певну якість мережевих служб.

Якщо трафік не можна скинути, він повинен використовувати певний механізм Якості обслуговування (QoS), щоб гарантувати, що дані не будуть втрачені. Цей механізм захищатиме частину своєї смуги пропускання, яку використовуватимуть лише ці повідомлення. Загальний трафік зберігатиметься в черзі для перенаправлення, а трафік вищого пріоритету матиме іншу чергу для зберігання перед тим, як перенаправлятися. Під час пересилання даних комутатор спочатку доставить дані, що мають вищий пріоритет, і переадресує залишок трафіку після порожньої черги даних із високим пріоритетом. Якщо дані з нижчим пріоритетом досягнуть своєї пропускної здатності, дані будуть втрачені, але на дані з вищим пріоритетом це не вплине, оскільки вони мають гарантію пропускної здатності. На Рисунку нижче показаний приклад такої ситуації.

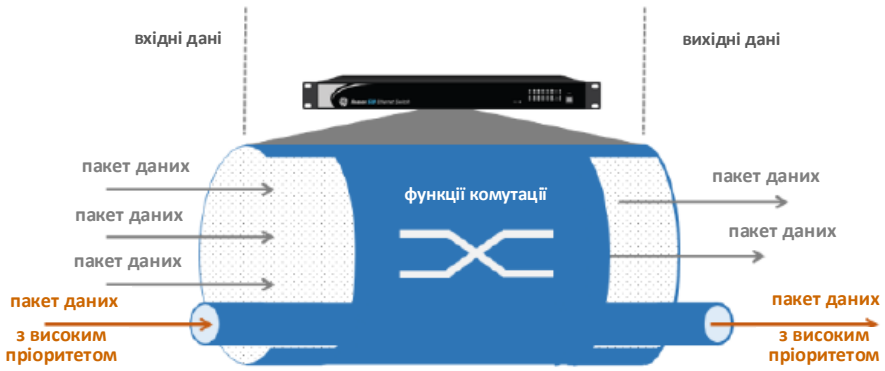


Рис. 57: Мережа з пріоритизацією трафіку

На рівні каналу передачі даних можуть використовуватися Біти пріоритету в кадрі 802.1Q. На мережевому рівні також може використовуватися інформація DSCP у заголовку IP-протоколу, тощо.

Біти класу обслуговування (CoS) QoS

Перша розробка стандарту, що включає пріоритизацію трафіку, розпочалася зі стандартом IEEE 802.1p, який на сьогодні входить до стандарту IEEE 802.1Q. В останньому, наявне 3-бітове поле, біти класу обслуговування (CoS), що використовуються для встановлення пріоритету, який мережа повинна використовувати для цього кадру. На наступному рисунку показано біти 802.1Q і CoS, які називаються Кодовою точкою пріоритету (PCP).

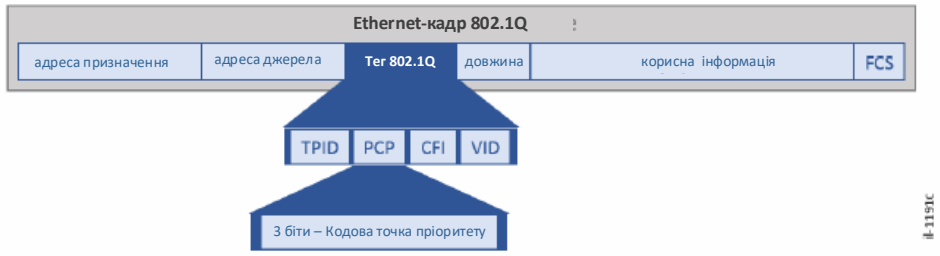


Рис. 58: Біти CoS всередині і кадр 802.1Q

Існує загальна згода, що термін QoS стосується засобів, за допомогою яких обладнання гарантує якість при визначеному виді трафіку в певній мережі. Таким чином, Якість обслуговування може бути реалізована різними рівнями та різними способами. Крім того, термін CoS, який є одним із механізмів QoS, використовує інформацію про пріоритет всередині кадру Ethernet 802.1Q. У цьому керівництві термін QoS використовується як засіб, за допомогою якого у мережі забезпечується якість певного сервісу, а CoS використовується як спосіб реалізації QoS у певній локальній мережі шляхом перевірки кадрів 802.1Q.

Оскільки це 3-бітове поле, існує можливість використовувати вісім значень пріоритету, від 0 до 7. Стандарт 802.1Q показує, як ці біти слід використовувати для забезпечення пріоритетності трафіку, як показано на рисунку нижче.

Важливим моментом є те, що значення 1 є найнижчим пріоритетом. Застаріле обладнання, яке не підтримує кадри 802.1Q, розуміється як число пріоритету 0. Пріоритет 0, за стандартом, відображається як негарантована якість доставки (режим максимальних зусиль - Best Effort), вище числа 1. Це забезпечує, що трафік застарілого обладнання не завжди буде трактуватися як фоновий трафік при комбінуванні з обладнанням, що підтримує 802.1Q. Крім того, навіть незважаючи на те, що пріоритет 7 є найвищим, не рекомендується використовувати цей пріоритет у трафіку, який не належить до контролю або керування мережею.

Таблиця 6: Пріоритет трафіку CoS

Пріоритет	Скорочення	Тип трафіку
1 (Найнижчий пріоритет)	BE	Фон
0 (За замовчуванням	EE	Негарантована якість
2	CA	Відмінна якість
3	VI	Критичні застосунки
4	VO	"Відео", <100 мс затримка та джиттер
5	IC	"Звук", <100 мс затримка та джиттер
6	BE	Міжмережеве керування
7 (Найвищий пріоритет)	EE	Керування мережею

Крім того, Технічний звіт МЕК 61850-90-4 рекомендує відображати біти CoS, як показано нижче. Додатково, документ визначає використання пріоритету "Високий" для даних Вибіркових величин (Sampled Values) та пріоритету "Середній" або "Високий" для повідомлень про синхронізацію. Згідно з технічним звітом, MMS-повідомлення, які використовуються для зв'язку IED в енергосистемі та інших трафіках через мережі TCP/IP, повинні використовувати пріоритет "Низький" або "Середній".

Таблиця 7: Класифікація CoS згідно з рекомендаціями МЕК 61850-90-4

Пріоритет	QoS	Типове застосування
7	Критичний	Керування мережею (за допомогою VLAN)
6	Високий	GOOSE-повідомлення, що використовуються для вимкнення та залежного вимкнення
5	Середній	Повідомлення GOOSE, що використовуються для блокування об’єднуючих пристроїв
4	Середній	Повідомлення GOOSE, що використовуються для інших цілей
3	Середній	Автоматизація підстанції (з використанням VLAN)
2	Звичайний	Інженерно-технічні роботи (з використанням VLAN)
1	Звичайний	Якість обліку електроживлення
0	Звичайний	Системи безпеки, лічильники, IP камери.

Опис черги, наведений нижче, відомий як черга з суворим пріоритетом. За замовчуванням Reason S20 працює в режимі Черги із суворим пріоритетом. Якщо даній локальній мережі потрібно динамічно визначити пріоритет трафіку, який є передачею вищих класів, але не зупиняється при передачі трафіку нижчих класів, тоді можуть бути використані функції формування портів або WRED.

Важливим моментом використання бітів CoS є те, що пріоритетність трафіку буде пов’язана з VID (VLAN ID) кадру. Таким чином, цей механізм QoS надає пріоритет трафіку з однієї VLAN над іншою. Оскільки існує пріоритизація трафіку, пов'язана з VLAN, цей механізм передбачає, що дані в заданій VLAN повинні мати пріоритет.

Обладнання IED, у системах зв'язку енергосистеми, повинне надсилати пакети, що містять VLAN та інформацію про пріоритет. Таким чином, коли пристрої IED надсилають пакети, класифіковані за визначеним CoS, комутатор за замовчуванням поставить пакет у чергу, визначену CoS. Якщо всі IED правильно налаштовані для надсилання повідомлень GOOSE, Вибіркових величин та PTP, комутатор класифікує пакети за замовчуванням, не потребуючи конфігурацій QoS.

Якщо основне мережеве обладнання має певну філософію щодо пріоритизації трафіку значень CoS, яка відрізняється від граничного обладнання, можна заново відобразити кадри до заданого CoS на комутаторі. Існує кілька застосувань, в яких наявна потреба змінити вхідний кадр CoS, щоб адаптувати його до мережі. Таким чином, вхідний кадр із заданого CoS буде зберігатися в іншій черзі CoS і буде пересилатися з новими значеннями CoS.

Якщо варіант застосування вимагає, щоб комутаційне обладнання могло перевіряти тип трафіку, щоб визначити його пріоритет, можна відобразити повідомлення з визначеним значенням CoS, і тоді буде забезпечуватися ефективна пріоритизація трафіку, що визначається типом трафіку, а не VLAN. Можна визначити пріоритет трафіку на основі транспортного протоколу Ethertype, UDP або TCP, тощо.

Точка коду диференційованих послуг (DSCP)

Використання конкретного поля в IP-заголовках було стандартизовано в документі RFC 2474. Він визначає використання 6-бітового поля, бітів Точки коду диференційованих послуг (DSCP), які використовуються для встановлення пріоритету, який мережа повинна використовувати для вхідних IP-кадрів. Слід зауважити, що тоді як біти CoS відображаються на рівні каналу передачі даних, DSCP використовується на мережевому рівні, отже, в середовищі IP-зв'язку. Таке середовище включає протоколи NTP та PTP (якщо вони зіставлені з транспортом UDP), але їм заборонено передавати дані GOOSE або Вибіркових величин. На рисунку нижче показано IP-заголовок та біти DSCP

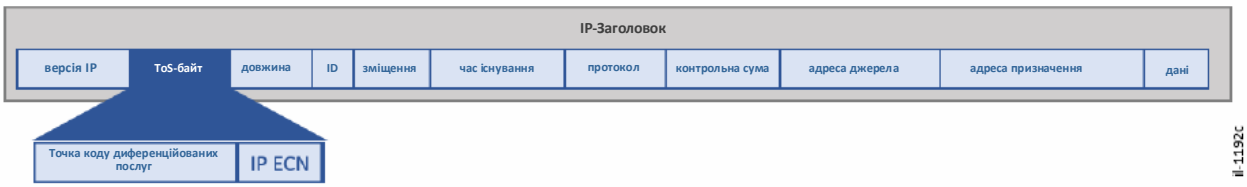


Рис. 59: Пояснення кадру IP-заголовка та Точки коду диференційованих послуг

Байт типу обслуговування (ToS) має дві підгрупи, одна – біти Точки коду диференційованих послуг (DSCP) із 6-бітовим полем, що дозволяє IP-заголовку переносити пріоритетну інформацію про вхідні дані. Крім того, залишаються два біти, Явне повідомлення про перевантаження (ECN), визначене в документі RFC 3168.

ECN дозволяє IP-пакетам нести інформацію, якщо пакет зазнав перевантаження при передачі даних. Таким чином, оскільки пакет має позначення, що він постраждав від перевантаження на шляху між відправником і отримувачем, відправник може скоригувати свою пропускну здатність відповідно до мережі, щоб уникнути втрати даних. Цей механізм робить QoS більш надійним, оскільки в пакеті з'являтиметься повідомлення про перевантаження, і тоді хости зможуть самостійно налаштуватися, щоб запобігти втраті даних. В іншому випадку єдиним способом перевірити, чи перевантажена мережа, буде втрата пакетів.

Якщо основне мережеве обладнання має певну філософію щодо значень DSCP, яка відрізняється від граничного обладнання, можна заново відобразити кадри до заданої DSCP на комутаторі. Існує декілька варіантів застосування, в яких є потреба змінити вхідний кадр DSCP, щоб адаптувати його до мережі. Таким чином, вхідний кадр із заданої DSCP буде позначений як нове значення DSCP і буде перенаправлений з цим новим значенням DSCP.

Можливості QoS у GE Reason S20

Пристрій GE Reason S20 дозволяє користувачеві застосовувати QoS у мережевих застосунках на протоколах рівня 2. Для застосунків рівня 3 також підтримується QoS на основі DSCP. Доступні два типи якості обслуговування (QoS):

- Значення CoS QoS;
  - Пряме значення CoS на кадрах 802,1Q;
  - Відображення протоколів до CoS;
  - Відображення DSCP до CoS.
- DSCP значення QoS.

Як показано у попередніх пунктах, кадри з тегами VLAN завжди містять інформацію про пріоритизацію пакетів. Таким чином, якість обслуговування гарантується з вищим пріоритетом ідентифікації VLAN перед нижчими значеннями, оскільки кожне значення CoS має певну чергу при прийнятті рішення про перенаправлення.

Якщо обладнання IED правильно надсилає інформацію про пріоритет на кадрах, які надсилаються по всій мережі, то Reason S20 буде виконувати свої функції QoS без необхідності конфігурації, оскільки конфігурація за замовчуванням забезпечує правильну чергу CoS. Це також означає, що для IP-зв'язку відправляється значення бітів DSCP, яке інформує мережеве IP-обладнання про його пріоритет над мережею. Таким чином, якщо немає застарілого обладнання без можливостей CoS, конфігурація може не знадобитися. Крім того, суворого пріоритету, як правило, достатньо для забезпечення послуг QoS. Таким чином, використання зважених черг або виявлених перевантажень WRED слід чітко розуміти перед використанням, оскільки ці механізми підвищують складність мережі.

Конфігурація QoS застосовується, коли підключено застаріле обладнання, оскільки воно не дозволяє самостійне визначення пріоритетів. Крім того, суворий пріоритет можна змінити на зважені черги, або можна отримати раннє виявлення перевантажень через IP-протоколи із функцією WRED, коли моделювання мережі показує, що продуктивність мережі можна збільшити без збільшення пропускної здатності мережі.

За замовчуванням порти класифікуються до черги пакетів, несумісних з 802.1Q, за числом 0 пріоритету CoS (негарантована послуга - "Best Effort") і використовують інформацію CoS з вхідних кадрів 802.1Q для постановки у чергу в заданій черзі значень CoS. Крім того, можна увімкнути класифікацію за тегами, щоб змінити, яка черга буде використовуватися вхідними даними з інформацією CoS. Кожен порт має незалежну класифікацію, що дозволяє користувачеві самостійно перемаркувати значення CoS на кожному порту. При обробці пакетів на виході можна перемаркувати значення CoS у пакетах із заданої черги, таким чином, дозволяючи ще раз відобразити вхідні дані з іншим значенням CoS, як показано на рисунку нижче.

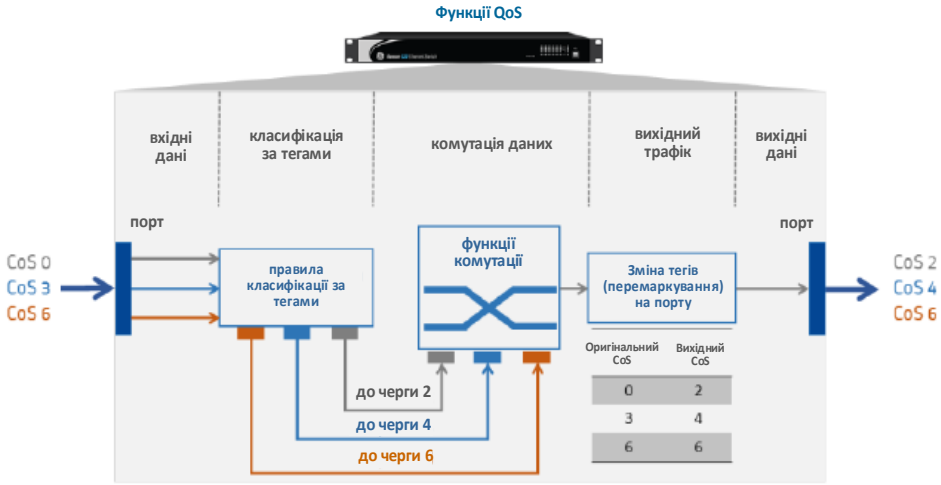


Рис. 60: Черги CoS та функції перемаркування

Крім того, можливо налаштувати вхідний трафік порту, щоб гарантувати клас обслуговування, обмежуючи пропускну смугу на даному порту, тим самим заощаджуючи обробку на портах, до яких підключені такі хости як IED або мережі низького пріоритету. Ця функція називається "Обмеження трафіку черги" (Queue Policing). Крім того, керування потоками може використовуватися для надсилання призупинених кадрів замість того, щоб їх відкидати. Ця функція в Reason S20 називається "Обмеження трафіку порту" (Port Policing).

За замовчуванням черги Reason S20 плануються та перенаправляються у режимі суворого пріоритету, тобто лише якщо черги вищого пріоритету CoS порожні, дана черга CoS почне переадресовувати трафік. Це гарантує, що черги з вищим пріоритетом завжди перенаправлятимуть трафік перед чергами з нижчим пріоритетом. Крім того, можна змінити заплановані черги на виході та поведінку портів на пересилання трафіку на основі середнього трафіку, щоб гарантувати, що середній трафік у даній черзі чи на порту буде надійним. Ці функції дозволяються лише для черг CoS з числом пріоритету від 0 до 5 і поділяються на функції Планувальника портів та Формування портів (Port Scheduler та Port Shaping). Черги пріоритетів CoS 6 та CoS 7 функціонують тільки в режимі суворого пріоритету.

Функції планувальника портів дозволяють користувачеві встановити значення ваги, щоб визначити пріоритет деяких з них на основі розрахунків середнього значення. Таким чином, з миттєвої точки зору спостерігатиметься певна передача трафіку з чергами нижчого пріоритету, але середній трафік черг CoS з вищим пріоритетом буде вищим і базуватиметься на його вазі при передачі. Для обмеження пропускної смуги на даному порту, виходячи з ваги та конфігурацій планувальника портів, передбачена функція Формування портів. При використанні режиму суворого пріоритету ці функції виконуватимуться шляхом обмеження трафіку портів та черг.

Якщо IP-пакети, що передаються в комутатор, несуть інформацію про пріоритет у бітах DSCP, комутатор може обробляти IP-пакети з більш високим пріоритетом, щоб забезпечити меншу затримку при їх передачі порівняно з пакетами з нижчим пріоритетом. За замовчуванням цю функцію вимкнено.

Якщо увімкнено, QoS на основі DSCP буде виконувати свої функції, подібно до того, як це роблять біти CoS, також є можливість увімкнути DSCP незалежно на кожному порту комутатора, класифікувати кожен пріоритет у певній черзі для прийняття рішень щодо пересилання, а потім перетворити (транслювати) вхідне значення DSCP в інше перед виходом пакета, як показано нижче.

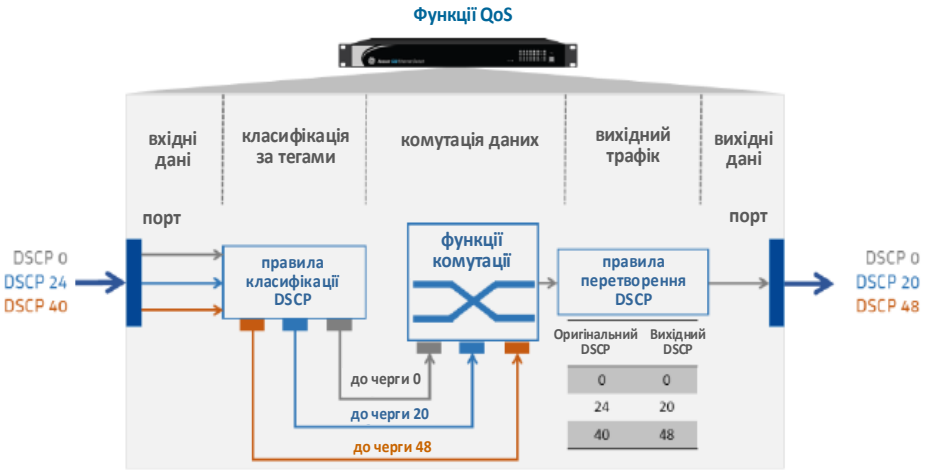


Рис. 61: Черги DSCP та функції трансляції

Як пояснювалося у попередніх пунктах, може виникнути потреба встановити взаємозв'язок між значеннями DSCP і CoS, поєднати механізми пріоритетів IP та 802.1Q та підвищити їх продуктивність у мережі. У Reason S20 ця функція називається класифікацією DSCP, і передбачена можливість прямого відображення значень DSCP до кожного можливого значення CoS. За замовчуванням усі пріоритети DSCP класифікуються як CoS 0 (негарантована послуга або так званий режим максимальних зусиль - Best Effort).

Якщо в даній локальній мережі немає прямого відображеного пріоритету VLAN або механізму IP DSCP, комутатор може шукати трафік або залучені адреси, щоб відобразити їх як певну чергу QoS (значення CoS та значення DSCP), створюючи реальну функцію пріоритетного трафіку. Якщо з якихось причин пристрої IED або хости в даній мережі не дозволяють налаштовувати певні повідомлення на VLAN, цей механізм можна використовувати для забезпечення пріоритизації типів повідомлень над іншими. Пристрій Reason S20 може виконувати відображення протоколу в CoS за кількома фільтрами, де є свобода вибору портів, призначених для фільтрування. Для планування трафіку в певних чергах, Reason S20 використовує наступні методи:

- MAC-адреса призначення;
- MAC-адреса джерела;
- Параметри VLAN:
  - Нетеговані кадри для черги CoS;
  - Конкретні теговані кадри для черги CoS;
  - Діапазон тегованих кадрів для черги CoS;
- Значення CoS та DEI;
- Тип кадру:
  - Специфічний Ethertype для черги CoS;
  - Конкретні параметри LLC для черги CoS;
  - Значення PID SNAP для черги CoS;
  - IP-пакети (як IPv4, так і IPv6).
    - Конкретне значення або діапазон IP-адрес джерела та призначення для черги CoS;
    - Конкретне значення або діапазон TCP-портів джерела та призначення для черги CoS;
    - Конкретне значення або діапазон UDP-портів джерела та призначення для черги CoS;
    - Конкретне значення або діапазон значень DSCP для черги CoS.

Таким чином, якщо Вибіркові значення (Sampled Values) та повідомлення GOOSE знаходяться в одній і тій же VLAN, можна встановити пріоритет одного з них над іншим, використовуючи його Ethertype, MAC-адресу призначення, тощо.

Крім того, для протоколу NTP можна визначити його пріоритет, використовуючи його UDP-порт для перенаправлення цього трафіку до певної черги CoS. Існує декілька способів надання послуг з пріоритизації трафіку, якщо біти CoS вхідних даних не можна використовувати безпосередньо. Reason S20 допускає до 256 правил у списку керування QoS, які виконують цю функцію.

Однією з основних функцій QoS є запобігання надмірному потоку повідомлень на даному порту, що може виникати при одноадресних, широкомовних або багатоадресних транспортних механізмах. Ці функції називаються Обмежувачами мережевих штормів (Storm policers), і їх може виконувати Reason S20. Кожен порт можна налаштувати незалежно для обмеження пропускної полоси при передачі одноадресних, багатоадресних та широкомовних повідомлень.

Нарешті, якщо суворий пріоритет не забезпечує продуктивності, необхідної для даної локальної мережі, тоді функція Виваженого довільного раннього виявлення (WRED) може бути використана як метод відкидання кадрів на основі попередніх припущень. Для вибору того, який кадр можна скинути в цьому механізмі, використовуються біти DEI у кадрі 802.1Q. Таким чином, пакети з DEI 0 ніколи не вибираються для відкидання, а пакети з DEI 1 є пакетами, що відповідають критеріям відкидання. Дозволяється вибрати до 3 черг для виявлення перевантажень, від 0 до 5 пріоритетів черг CoS. Черги з пріоритетами CoS 6 та CoS 7 не можна використовувати. Вибір черг, які будуть використовуватися для виявлення перевантажень, здійснюється за класифікацією вхідних портів, де кожен порт класифікується за рівнем пріоритету відкидання (DPL), від 0 до 3. DPL, що дорівнює 0, означає, що ці пакети не можна втратити, а рівень DPL 1, 2 або 3 означає, що пакети можуть бути відкинуті. Увімкнення черги дозволить комутатору виконувати функцію WRED у цій черзі. Передбачено чотири поля, які необхідно налаштувати, щоб функція WRED виконувалася правильно: Мінімальний поріг, Максимальна ймовірність відкидання 1, 2 і 3.

Поле "Мінімального порогу" (Minimum Threshold) представляє середній рівень заповнення черги, в якій комутатор почне довільно відкидати кадри. Кадри з DEI = 1 у черзі будуть пакетами, що відповідають критеріям відкидання. Таким чином, до того, як у мережі виникне перевантаження, комутатор відкине кадри, щоб запобігти перевантаженню, після того, як екстраполюється середнє навантаження даної черги. Поля "Максимальна ймовірність відкидання" (Maximum Drop Probability) визначають максимальну ймовірність відкидання даного трафіку в черзі, який потрібно скинути. Таким чином, якщо середній рівень заповнення даної черги наближається до 100%, ймовірність відкидання наближається до визначеної ймовірності відкидання. Вибір рівнів DPL здійснюється за класифікацією портів, де кожен порт має певний DPL (рівень пріоритету відкидання), який можна використовувати. DPL, що дорівнює 0, означає, що жоден пакет не повинен використовуватися у виборах, а рівень 1, 2 або 3 вибере, яку чергу буде використовувати порт з пороговими значеннями, налаштованими на максимальних рівнях ймовірності відкидання (DP).

12.2 Класифікація портів

Меню "Класифікації портів" (Port Classification) дозволяє налаштувати базову класифікацію входу QoS на даному порту. Якщо бажано застосувати одну конфігурацію до всіх портів, тоді слід використовувати рядок "*", тобто конфігурація, виконана в рядку "*", відповідатиме всім портам.

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **CoS**: вказує CoS, який буде використовуватися в процесі входу. Ці порти класифікують нетеговані кадри до класу CoS, налаштованого в цьому полі, і перенаправляють теговані та пріоритетні теговані кадри до черги CoS, вбудованої в біти PCP у кадрі 802.1Q. За замовчуванням усі нетеговані кадри класифікуються до черги CoS 0, що означає найнижчий пріоритет класу обслуговування для цих пакетів.

Крім того, за замовчуванням використовується відображення "один до одного" бітів CoS та PCP. Дозволеними значеннями є значення діапазону бітів PCP (від 0 до 7);

- **DPL**: вказує рівень пріоритету відкидання, який буде використовуватися в процесі входу. Ці порти класифікують нетеговані кадри до класу DPL, налаштованого в цьому полі, і будуть перенаправляти теговані та пріоритетні теговані кадри до DPL, вбудованого у кадр. Рівень 0 DPL означає, що пакет не можна відкинути, а рівень 1, 2 і 3 означає, що пакет можна відкинути довільним чином на основі порогу WRED. За замовчуванням усі нетеговані кадри класифікуються за DPL 1. Допустимі значення – від 0 до 3;
- **PCP**: вказує PCP, який буде використовуватися в процесі входу. Ці порти класифікують нетеговані кадри до класу PCP, налаштованого в цьому полі, і будуть перенаправляти теговані та пріоритетні теговані кадри до черги PCP, вбудованої в біти PCP у кадрі 802.1Q. За замовчуванням усі нетеговані кадри класифікуються до черги PCP 0, що означає клас обслуговування з негарантованою якістю доставки (так званий режим максимальних зусиль - Best Effort) для цих пакетів. Дозволеними значеннями є значення діапазону бітів PCP (від 0 до 7);
- **Індикатор допустимості видалення (DEI)**: вказує прапорець індикатора допустимості видалення, який буде використовуватися в процесі входу. Ці порти класифікують нетеговані кадри до класу DEI, налаштованого в цьому полі, і будуть перенаправляти теговані та пріоритетні теговані кадри в DEI, вбудований у кадр. Рівень DEI 0 означає, що пакет не можна відкинути, а рівень 1 означає, що пакети дозволено відкидати. За замовчуванням усі нетеговані кадри класифікуються за DPL 0. Допустимі значення – 0 і 1;
- **Клас тегу (Tag Class)**: вказує режим класифікації, який буде використовуватися портом. Поле Клас тегу – це гіперпосилання, яке дозволяє отримати доступ до Класифікації тегів вхідного порту QoS, де дозволяється самостійно налаштовувати чергу PCP до QoS на кожному порту. Ця конфігурація застосовується лише до тегованих кадрів або кадрів із пріоритетним тегуванням, тобто кадрів з інформацією PCP. Можливі значення: Вимкнено та Увімкнено. Вимкнено означає, що PCP, що використовується у тегованих кадрах та пріоритетних тегованих кадрах, буде значенням, вбудованим у кадр, а увімкнено означає, що черга QoS, обрана кожним значенням PCP, буде такою, як налаштована на цьому порту. Можливі конфігурації після натискання гіперпосилання Класу тегу є наступними:
- **Класифікація тегів (Tag Classification)**: вказує, чи слід увімкнути класифікацію тегів для тегованих кадрів чи ні. Можливі значення: Увімкнено та Вимкнено. Вибір параметра "Увімкнути" (Enable) дозволяє порту відображати вхідні значення PCP для налаштованої черги QoS, а вибір "Вимкнути" (Disable) дозволяє порту відображати вхідні значення PCP для відповідної черги QoS;
  - **PCP**: показує значення PCP, які можна налаштувати;
  - **DEI**: показує значення DEI, які можна налаштувати;
  - **Клас QoS (QoS class)**: вказує, на яку чергу QoS слід перенаправляти кадри зі значеннями PCP та DEI у рядку. Це дозволяє перенаправляти вхідні кадри з одного рівня PCP до іншої черги;
  - **Рівень DP (DP level)**: вказує, до яких рівнів DP слід перенаправляти кадри зі значеннями PCP та DEI у рядку. Це дозволяє налаштувати вхідні кадри з заданих значень PCP та DEI до визначеного параметра DPL;
- **На основі DSCP (DSCP Based)**: вмикає функцію QoS на основі DSCP на порту. Якщо дозволені біти DSCP, цей прапорець дозволяє комутатору використовувати цю інформацію в IP-пакеті для виконання функцій QoS. Вибраний прапорець означає, що QoS на основі DSCP увімкнено, а порожній прапорець – вимкнено.

12.3 Обмеження трафіку портів

Меню "Обмеження трафіку портів" (Port Policing) дозволяє налаштувати обмеження трафіку для портів.

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **Увімкнено (Enabled)**: увімкніть функцію обмеження трафіку портів на порту. Вибраний прапорець означає що функцію увімкнено, а порожній прапорець – вимкнено;
- **Швидкість (Rate)**: вказує максимально дозволений трафік на цьому порту. Швидкість трафіку на порту, що перевищує це поле, не дозволяється, якщо функцію увімкнено, тоді трафік, близький до ліміту, почне втрачати пакети на основі налаштованої QoS. Дозволені значення – це цілі числа, а ліміти залежать від використовуваної одиниці. Діапазон від 100 до 1.000.000 допускається, коли використовуються одиниці вимірювання кбіт/с (kbps) або кадрів на секунду (fps). Діапазон від 1 до 32.000 дозволяється, коли використовуються одиниці Мбіт/с (Mbps) або тис. кадрів на секунду (kfps);
- **Одиниця виміру (Unit)**: вказує, яку одиницю слід використовувати зі значенням швидкості для обмеження трафіку. Допустимими значеннями є кбіт/с, Мбіт/с, к/с та тис. к/с (kbps, Mbps, fps і kfps);

12.4 Обмеження трафіку черги

Меню "Обмеження трафіку черги" (Queue Policing) дозволяє налаштувати обмеження трафіку для кожної черги на порту.

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **Увімкнення обмеження трафіку черги (Queue enable)**: увімкнення функції обмеження трафіку черги на порту. Вибраний прапорець означає що функцію увімкнено, а порожній прапорець – вимкнено. Reason S20 має таблицю з кількістю рядків, що дорівнює кількості портів, і кількість стовпців, що дорівнює кількості черг QoS. Таким чином, кожна черга на кожному порту може бути незалежно налаштована для забезпечення контролю трафіку черги. Якщо даний порт у даній черзі увімкнено, стовпець "Черга" (Queue) відображає можливу конфігурацію цієї черги. Можлива наступна конфігурація:
  - **Швидкість (Rate)**: вказує максимально дозволений трафік на цьому порту. Швидкість трафіку на порту, що перевищує це поле, не дозволяється, якщо функцію увімкнено, тоді трафік, близький до ліміту, почне втрачати пакети на основі налаштованої QoS. Дозволені значення – це цілі числа, а ліміти залежать від використовуваної одиниці. Діапазон від 100 до 1.000.000 допускається, коли використовуються одиниці вимірювання кбіт/с (kbps) або кадрів на секунду (fps). Діапазон від 1 до 32.000 дозволяється, коли використовуються одиниці Мбіт/с (Mbps) або тис. кадрів на секунду (kfps);
  - **Одиниця виміру (Unit)**: вказує, яку одиницю слід використовувати зі значенням швидкості для обмеження трафіку. Допустимими значеннями є кбіт/с, Мбіт/с, к/с та тис. к/с (kbps, Mbps, fps і kfps);

12.5 Планувальник портів

Меню "Планувальника портів" (Port Scheduler) дозволяє налаштувати тип пріоритету на кожному порту. За замовчуванням Reason S20 працює із суворим пріоритетом. За необхідності можна зважити до 6 черг (крім 6 та 7 черг CoS), таким чином, процес відкидання пакетів повинен зважувати черги, а не чекати порожніх черг вищого рівня пріоритету. Крім того, процес зважування зберігатиме надлишок даних у внутрішньому буфері, який буде відправлений пізніше, отже, ця функція потребуватиме пам'яті, доступної для зберігання кадрів. Можливі наступні конфігурації.

- **Порт (Port)**: вкажіть порти, які потрібно налаштувати в цьому рядку. Поле порту – це гіперпосилання, яке дозволяє отримати доступ до налаштувань Планувальника вихідних портів QoS та налаштувань Формувача. Меню планувальника портів дозволяє налаштувати порт для роботи в режимі Планувальника із суворим пріоритетом або в режимі зважених 6 черг. Можливі налаштування після натискання гіперпосилання на номер порту є наступними:
  - **Режим планувальника (Scheduler Mode)**: вказує, який режим планувальника портів працює. Кожен порт може бути вільно налаштований для роботи в суворому або зваженому режимі. Дозволеними значеннями є суворий пріоритет та 6 зважених черг. Суворий пріоритет означає, що черга з нижчим пріоритетом почне пересилати кадри тільки після того, як черга з вищим пріоритетом буде порожньою. 6 зважених черг означають, що черги CoS від 0 до 5 будуть зважені, а кадри будуть довільно відкинуті на основі конфігурації ваги;
  - **Формувач черги (Queue Shaper)**: вказує швидкість черги, яка буде використана функцією формування. Кожна черга має свою власну конфігурацію формувача. Якщо в даній черзі на порту виникає перевантаження, формувачі черги виконуватимуть функції комутації, щоб гарантувати, що середній трафік у цій черзі не перевищує налаштовану швидкість формувача черги. Можливі наступні конфігурації:
    - **Увімкнути (Enable)**: увімкнути функцію формувача черги в черзі Cos. Вибраний прапорець означає, що функцію увімкнено для цієї черги, а порожній прапорець – вимкнено;
    - **Швидкість (Rate)**: вказує максимальний середній рівень дозволеного трафіку в черзі. Спорадичний піковий трафік буде зберігатися у внутрішньому буфері для пересилання, коли піковий трафік буде нижче значення швидкості формувача черги. Дозволені значення – це цілі числа, а ліміти залежать від використовуваної одиниці. Діапазон від 100 до 1.000.000 допускається, коли використовуються одиниці вимірювання кбіт/с (kbps) або к/с (fps). Діапазон від 1 до 32.000 дозволяється, коли використовуються одиниці Мбіт/с (Mbps) або тис. к/с (kfps);
    - **Одиниця виміру (Unit)**: вказує, яку одиницю слід використовувати зі значенням швидкості для обмеження трафіку. Допустимими значеннями є кбіт/с, Мбіт/с, к/с та тис. к/с (kbps, Mbps, fps і kfps);
    - **Надлишок (Excess)**: дозволяє цій черзі використовувати (за необхідності) надлишок пропускної здатності порівняно зі значенням швидкості формувача черги. Вибраний прапорець означає, що для цієї черги увімкнено функцію, а порожній прапорець – вимкнено.
  - **Планувальник черг (Queue Scheduler)**: вказує вагу черги в алгоритмі динамічної ваги. Ця конфігурація дозволена, тільки якщо для режиму планувальника встановлено 6 зважених черг. Дозволена конфігурація є наступною:
    - **Вага (Weight)**: вказує вагу, яку черга матиме у процесі формування. Це число буде використовуватися внутрішнім алгоритмом для визначення, скільки середньої смуги пропускання може використовувати ця черга;
    - **Відсоток (Percent)**: показує відсоткове значення, яке черга заповнить у дозволеній пропускній смузі для черг у зваженому режимі.
  - **Формувач портів (Port Shaper)**: вказує швидкість порту, яка буде використана функцією формування. Кожен порт має свою власну конфігурацію формувача, і кожна черга на певному порту також має свою власну конфігурацію. Якщо на даному порту виникає перевантаження, формувачі портів виконуватимуть функції комутації, щоб гарантувати, що середній трафік на цьому порту не перевищує налаштовану швидкість формувача портів. Можливі наступні конфігурації:

- **Увімкнути (Enable)**: увімкнути функцію формувача трафіку портів на порту. Вибраний прапорець означає, що функцію увімкнено для цієї черги, а порожній прапорець – вимкнено;
- **Швидкість (Rate)**: вказує максимальний середній рівень дозволеного трафіку в черзі. Спорадичний піковий трафік буде зберігатися у внутрішньому буфері для пересилання, коли піковий трафік буде нижче значення швидкості формувача черги. Дозволені значення – це цілі числа, а ліміти залежать від використовуваної одиниці. Діапазон від 100 до 1.000.000 допускається, коли використовуються одиниці вимірювання кбіт/с (kbps) або к/с (fps). Діапазон від 1 до 32.000 дозволяється, коли використовуються одиниці Мбіт/с (Mbps) або тис. к/с (kfps);
- **Одиниця виміру (Unit)**: вказує, яку одиницю слід використовувати зі значенням швидкості для обмеження трафіку. Допустимими значеннями є кбіт/с, Мбіт/с, к/с та тис. к/с (kbps, Mbps, fps і kfps);

- **Режим (Mode)**: показує режим роботи пріоритетної черги, налаштований у меню планувальника вихідних портів QoS та меню Формувачів;
- **Вага**: показує значення у відсотках від ваги черг на цьому порту. Якщо порт працює у режимі суворого пріоритету (Strict Priority), тоді символ "-" відображатиметься як значення ваги, що означає, що жоден процес зважування не використовується. Якщо робота порту є зваженою, тоді відображаються значення з дозволених черг, від CoS 0 до 5.

12.6 Формування трафіку портів

Меню "Формування портів" (Port Shaping) та "Планувальника портів" (Port Scheduler) працюють разом, щоб дозволити налаштувати конфігурацію типу пріоритету на кожному порту та кожній черзі. У той час як Планувальник портів відображає режим кожного порту та вагу черг, Формування портів відображає значення кожного формувача портів, розділені на черги. Тобто значення швидкості, налаштовані у планувальнику портів, відображаються в цьому меню. За замовчуванням Reason S20 працює із суворим пріоритетом. За необхідності можна зважити до 6 черг (крім 6 та 7 черг CoS), таким чином, процес відкидання пакетів повинен зважувати черги, а не чекати, поки черги вищого рівня пріоритету будуть порожніми. Крім того, процес зважування зберігатиме надлишок даних у внутрішньому буфері, який буде відправлений пізніше, отже, ця функція потребуватиме пам'яті, доступної для зберігання кадрів. Параметри конфігурації подібні до Планувальника портів, крім:

- **Формувачі (Shapers)**: показує черги з пріоритетами та загальні значення формувачів портів, налаштованих в меню Планувальника вихідних портів QoS та меню Формувачів. Якщо порт працює у режимі суворого пріоритету, тоді слово "вимкнути" (disable) відображатиметься як значення формувача, що означає, що жоден процес формування не використовується. Якщо робота порту є зваженою, тоді відображувані значення – це значення швидкості, налаштовані для кожної черги та порту в меню Планувальника вихідних портів QoS і меню Формувачів.

12.7 Повторне маркування портів

Меню "Повторного маркування портів" (Port Tag Remarking) дозволяє налаштувати логіку обробки кадрів на виході. Таким чином, це меню дозволяє повторно відображати всі кадри, які мають інформацію про пріоритет у процесі входу. Порти можна налаштувати таким чином, щоб не змінювати значення PCP при виході кадру, використовувати тільки одну визначену PCP для всіх кадрів або зіставляти кожну чергу QoS з певним значенням PCP.

Можливі наступні конфігурації.

- **Порт (Port)**: вкажіть порти, які потрібно налаштувати в цьому рядку. Поле порту – це гіперпосилання, яке дозволяє отримати доступ до налаштувань Повторного маркування ("перемаркування") вихідних портів QoS. Меню Повторного маркування портів дозволяє налаштувати логіку роботи порту, пов'язану з кадрами, що виходять з порту. Після натискання гіперпосилання на номер порту для вибраного порту відобразиться меню Повторного маркування вихідних портів QoS (QoS Egress Port Tag Remarking). Режим повторного маркування вказує логіку роботи портів. Дозволеними значеннями є "Класифіковані", "За замовчуванням" і "Відображені" (Classified, Default та Mapped). Можливі наступні конфігурації:
  - **Класифіковані (Classified)**: вказує логіку роботи портів як класифіковане повторне маркування тегів QoS. У цьому режимі вихідні нетеговані кадри пересилаються зі значенням QoS за замовчуванням для порту (PCP = 0). Теговані та пріоритетні теговані кадри пересилаються з бітами PCP, що дорівнюють бітам PCP, вбудованим у вхідний кадр 802.1Q;
  - **За замовчуванням (Default)**: вказує логіку роботи портів як повторне маркування тегів QoS за замовчуванням. У цьому режимі вихідні нетеговані, теговані та пріоритетні теговані кадри перенаправляються із налаштованим значенням QoS за замовчуванням. Коли вибрано цей режим, відображаються поля PCP за замовчуванням та DEI за замовчуванням, що дозволяє користувачеві налаштувати значення PCP та DEI для використання у всіх перенаправлених кадрах. Можливі наступні конфігурації:
    - **PCP за замовчуванням (Default PCP)**: вказує, яке значення PCP має бути прикріплене до всіх вихідних кадрів. Допустимі значення – це значення діапазону бітів PCP, від 0 до 7;
    - **DEI за замовчуванням (Default DEI)**: вказує, яке значення DEI має бути прикріплене до всіх вихідних кадрів. Допустимі значення – це значення діапазону бітів DEI, 0 або 1.
  - **Відображені (Mapped)**: вказує логіку роботи портів як відображене повторне маркування тегів QoS. У цьому режимі вихідні нетеговані, теговані та пріоритетні теговані кадри перенаправляються із налаштованим значенням QoS. Кожне вбудоване значення PCP та значення DEI можуть бути зіставлені з певним PCP для незалежного процесу виходу. Коли вибрано цей режим, доступна таблиця відображення (Клас QoS, рівень DP) до (PCP, DEI), що дозволяє користувачеві налаштувати значення PCP та DEI для використання у всіх перенаправлених кадрах на кожну чергу. Можливі наступні конфігурації:
    - **Клас QoS (QoS class)**: показує чергу QoS, яку потрібно налаштувати в цьому рядку;
    - **Рівень DP (DP level)**: показує рівень DP, який потрібно налаштувати в цьому рядку;
    - **PCP**: вказує, яке значення PCP потрібно приєднати до кадрів із класом QoS (біти PCP) і рівнем DP, показаним у стовпцях класу QoS та рівня DP. Тобто, заданий кадр PCP із заданим рівнем DP повинен бути повторно маркований у процесі виходу до значення PCP, налаштованого в цьому полі. Допустимі значення – це значення діапазону бітів PCP, від 0 до 7;
    - **DEI за замовчуванням (Default DEI)**: вказує, яке значення DEI має бути приєднане до кадрів із класом QoS (біти PCP) та рівнем DP, показаним у стовпцях класу QoS та рівня DP. Тобто, заданий кадр PCP із заданим рівнем DP повинен бути повторно маркований у процесі виходу до значення DEI, налаштованого в цьому полі. Дозволеними значеннями є значення діапазону бітів DEI, 0 або 1.

12.8 DSCP портів

Меню "DSCP портів" (Port DSCP) дозволяє ввімкнути функцію DSCP QoS та базову конфігурацію. У цьому меню можна увімкнути, чи DSCP буде використовуватися як механізм якості обслуговування, та визначити основну логіку його роботи. Можливі наступні конфігурації.

- **Порт (Port)**: показує порт, який потрібно налаштувати в цьому рядку;
- **Трансляція (Translate)**: вказує, чи повинен цей порт використовувати трансляцію на вході. Цей прапорець використовується разом із полем "Класифікація" (Classify) для визначення вхідних правил функції DSCP. Вибраний прапорець означає, що трансляцію на вході увімкнено, а порожній прапорець – вимкнено;
- **Класифікація (Classify)**: вказує, як слід виконувати класифікацію DSCP на вході. Можлива наступна конфігурація:
  - **Вимкнено (Disable)**: вказує, що DSCP на вході не використовується. Це означає, що DSCP-аналіз функції QoS на порту вимкнено;
  - **DSCP = 0**: вказує, що слід класифікувати лише кадри з бітами DSCP, що дорівнюють 0. Класифікація класів DSCP до QoS буде такою, як налаштована у полі Класифікації DSCP;
  - **Вибрані (Selected)**: вказує, що класифікувати слід тільки кадри з маркованими бітами DSCP. Якщо вибрано, меню Трансляції DSCP слід використовувати для вибору того, які рівні DSCP слід класифікувати;
  - **Усі (All)**: означає, що всі кадри з бітами DSCP будуть класифіковані. Якщо вибрано, усі кадри будуть класифіковані до черги DSCP.
- **Вихід (Egress)**: вказує, як слід виконувати процес переписування DSCP на виході. Можлива наступна конфігурація:
  - **Вимкнути (Disable)**: означає, що перезапис DSCP на виході не використовується. Це означає, що біти DSCP даного вхідного кадру будуть відкинуті в процесі виходу;
  - **Увімкнути (Enable)**: вказує на те, що використовується перезапис DSCP на виході, але немає повторного відображення бітів DSCP. Це означає, що біти DSCP даного вхідного кадру будуть зберігатися в процесі виходу;
  - **Повторне відображення (Remap)**: вказує на те, що перезапис DSCP на виході використовується, і біти DSCP будуть повторно відображені зі значеннями, налаштованими у меню Трансляції DSCP. Це означає, що біти DSCP даного вхідного кадру будуть змінені відповідно до налаштованого користувачем процесу виходу.

12.9 Якість обслуговування на основі DSCP

Меню "QoS на основі DSCP" (DSCP-Based QoS) дозволяє увімкнути DSCP QoS на основі відображення класів DSCP в QoS. У цьому меню можна зіставити кожне значення DSCP із заданою чергою класу QoS та рівнями DPL. Можливі наступні конфігурації.

- **DSCP**: показує рівень DSCP, який слід налаштувати в цьому рядку;

- **Довіра (Trust)**: вказує, чи значення DSCP є надійним, а, отже, його можна повторно відобразити до класу QoS та налаштованого DPL. Тільки надійні (довірені) рівні DSCP повторно відображаються, як налаштовано у стовпцях класу QoS та DPL. Ненадійні кадри DSCP розглядаються комутатором як кадри, що не належать до IP. Вибраний прапорець означає надійний рівень DSCP, а порожній прапорець означає ненадійний;
- **Клас QoS (QoS Class)**: вказує, до якої черги класу QoS слід повторно відобразити кадр рівня DSCP. Кожне значення DSCP можна незалежно налаштувати на запитувану чергу Класу QoS. Допустимі значення – це значення діапазону бітів PCP, від 0 до 7;
- **DPL**: вказує, до якого правила рівня DPL слід повторно відобразити кадр рівня DSCP. Кожне значення DSCP можна незалежно налаштувати до запитуваного рівня DPL. Дозволені значення – це значення дозволеного діапазону DPL від 0 до 3.

12.10 Трансляція DSCP

Меню "Трансляції DSCP" (DSCP Translation) дозволяє вибрати, які рівні DSCP можна повторно відображати на інший рівень, а також налаштувати параметри трансляції. Якщо трансляція DSCP порту увімкнена (вибираючи "Вибрану класифікацію на вході" (Selected Ingress Classify) в меню DSCP портів), значення, які потрібно повторно відображати в процесі входу та виходу, будуть налаштовані в цьому меню. Можливі наступні конфігурації.

- **DSCP**: показує рівень DSCP, який слід налаштувати в цьому рядку;
- **Трансляція (Translate)**: вказує, до якого значення DSCP потрібно транслювати (перетворити) DSCP у рядку. У даному рядку буде вказаний рівень DSCP, який потрібно налаштувати. Вхідні кадри з цим рівнем DSCP будуть повторно відображені в процесі входу до рівня DSCP, вибраного в полі "Трансляція". Дозволені значення – це діапазон значень DSCP, від 0 до 63;
- **Класифікація (Classify)**: вказує, чи повинен цей порт використовувати вибрану трансляцію на вході. Цей прапорець увімкне параметр "Вибрані" (Selected) у "Класифікації" в меню "DSCP портів". Таким чином, якщо для порту встановлено значення "Вибрані", у цьому полі буде вказано, які рівні DSCP будуть класифіковані на порту. Вибраний прапорець означає, що рівень DSCP буде класифікований як налаштований, а порожній прапорець означає, що порт не класифікує цей рівень DSCP;
- **Повторне відображення (Remap)**: вказує, до якого значення DSCP потрібно транслювати (перетворити) DSCP у рядку. У даному рядку буде вказаний рівень DSCP, який потрібно налаштувати. Кадри, внутрішньо оброблені цим рівнем DSCP, будуть повторно відображені в процесі виходу до рівня DSCP, вибраного в полі "Повторне відображення". Дозволені значення – це діапазон значень DSCP, від 0 до 63.

12.11 Класифікація DSCP

Меню "Класифікації DSCP" (DSCP Classification) дозволяє вибрати, які рівні DSCP слід застосовувати до заданого значення CoS (PCP) на Ethernet- кадрі. Хоча класифікація вхідного трафіку QoS на основі DSCP дозволяє відобразити, до якої черги QoS слід відобразити значення DSCP, тобто дозволяє зіставити DSCP з CoS, класифікація DSCP дозволяє вибрати класифікацію CoS-до-DSCP. Таким чином, можливо включити QoS на основі бітів PCP у філософію DSCP QoS. Можливі наступні конфігурації.

- **Клас QoS (QoS Class)**: показує клас QoS, який слід налаштувати в цьому рядку;
- **DSCP**: вказує, до якого рівня DSCP слід відобразити клас QoS у рядку. Це поле ефективно налаштовуватиме конфігурацію CoS-до-DSCP, оскільки можливості CoS показані в стовпці Клас QoS. Дозволеними значеннями є діапазон значень DSCP, від 0 до 63.

12.12 Список керування QoS

Меню "Списку керування QoS" (QoS Control List) дозволяє налаштувати функцію QCL. QCL – це спосіб визначити якість обслуговування для даного трафіку на основі багатьох налаштувань, таких як MAC-адреси призначення або джерела, тип кадру, тощо. Щоб визначити трафік, що підлягає класифікації, потрібно створити запис керування QoS (QCE), який визначатиме всі параметри та дії, які потрібно реалізувати.
За замовчуванням QCE не налаштовано. Щоб додати запис керування, натисніть на кнопку. Після натискання цієї кнопки відкривається меню конфігурації QCE. У цьому меню відображатимуться всі можливі конфігурації, які будуть застосовані в QCE для використання в QCL. У меню конфігурації QCE після натискання кнопки, показаної нижче, можливі наступні конфігурації.

- **Порти-члени (Port Members)**: вказує, який порт буде членом цього запису QCE. Якщо вибрано, порт застосовуватиме правила, налаштовані за ключовими параметрами та параметрами дії. Вибраний прапорець означає, що порт є членом QCE, а порожній прапорець означає, що порт не є членом запису;
- **Ключові параметри (Key Parameters)**: вказує всі параметри, що застосовуються. Якщо кадри відповідають усім налаштованим ключовим параметрам, тоді кадр буде оброблятися так, як налаштовано в Параметрах дії (Action Parameters). Можливі наступні конфігурації:
  - **DMAC**: вказує тип MAC-адреси призначення. Можливі значення – "Будь-яка" (Any), що означає всі типи MAC-адрес, одноадресні, багатоадресні та широкомовні MAC-адреси;
  - **SMAC**: вказує значення OUI MAC-адреси джерела, що застосовується як фільтр. Можливі значення – "Будь-яка" (Any), що означає всі MAC-адреси та "Конкретна" (Specific) MAC-адреса. Якщо вибрано"Конкретна", як параметр буде використано поле OUI MAC-адреси. Дозволені значення – це шістнадцяткові значення, і кожен байт повинен бути відокремлений символом "-";
  - **Тег (Tag)**: вказує, чи буде кадр, який застосовуватиметься в цьому QCE, тегованим або нетегованим. Можливі значення – "Будь-який" (Any), що означає відсутність фільтра на основі ідентифікаційного номера VLAN, та значення "Тегований" (Tagged) або "Нетегований" (Untagged);
  - **VID**: вказує ідентифікатор VLAN, який буде використовуватися як фільтр, якщо значення "Будь-який" або "Тегований" було вибрано як параметри в полі "Тег". Можливими значеннями є "Будь-який", що означає всі ідентифікаційні номери VLAN, "Конкретні" та "Діапазон" (Specific та Range). Якщо вибрано "Конкретні", поле "Значення" (Value) має бути заповнене бажаним номером VID, а дозволеними значеннями є значення діапазону VLAN (від 1 до 4095). Якщо вибрано "Діапазон", поля "Від" і "До" повинні бути заповнені бажаними номерами діапазону VID, а допустимими значеннями є значення діапазону VLAN (від 1 до 4095);
  - **PCP**: вказує значення PCP, що застосовуються як фільтр за ключовими параметрами. Допустимими значеннями є значення діапазону PCP, від 0 до 7;
  - **DEI**: вказує значення DEI, яке застосовується як фільтр для ключових параметрів. Дозволеними значеннями є значення діапазону DEI, 0 або 1;

- **Тип кадру (Frame Type)**: вказує тип кадру, який буде використовуватися як фільтр за ключовими параметрами. Дозволеними значеннями є "Будь-який", EtherType, LLC, SNAP, IPv4 та IPv6. Можлива наступна конфігурація:
  - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
  - **EtherType**: вказує, який тип ethertype буде дозволений у цьому QCE. Якщо вибрано, відображатимуться параметри Ethertype. Можлива наступна конфігурація:
  - **Ethertype**: вказує, який фільтр слід застосовувати на основі поля ethertype у кадрі. Можлива наступна конфігурація:
  - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
  - **Конкретний (Specific)**: на цьому QCE буде використовуватися лише налаштований ethertype, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи його значення ethertype. Значення потрібно вставляти у шістнадцятковому форматі.
  - **LLC**: вказує, які значення LLC дозволятимуться в цьому QCE. Якщо вибрано, відображатимуться параметри LLC. Можлива наступна конфігурація:
    - **Адреса DSAP (DSAP Address)**: вказує, який фільтр слід застосовувати на основі поля Точки доступу до послуги призначення (DSAP) у кадрі. Можлива наступна конфігурація:
      - **Будь-яка (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
      - **Конкретна (Specific)**: у цьому QCE буде використовуватися тільки налаштована DSAP, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи його значення DSAP. Значення потрібно вставляти у шістнадцятковому форматі.
    - **Адреса SSAP (SSAP Address)**: вказує, який фільтр слід застосовувати на основі поля Точки доступу до послуги джерела (SSAP) у кадрі. Можлива наступна конфігурація:
      - **Будь-яка (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
      - **Конкретна (Specific)**: у цьому QCE буде використовуватися тільки налаштована SSAP, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи його значення SSAP. Значення слід вставляти у шістнадцятковому форматі.
    - **Керування (Control)**: вказує, який фільтр слід застосовувати на основі поля Керування в байтах LLC у кадрі. Можлива наступна конфігурація:
      - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;

- **Конкретний (Specific)**: на цьому QCE будуть використовуватися тільки налаштовані значення керування, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи його значення "Керування". Значення слід вставляти у шістнадцятковому форматі.

- **SNAP**: вказує, який Протокол доступу до підмережі (SNAP) буде дозволений у цьому QCE. Якщо вибрано, відображатимуться параметри SNAP. Можлива наступна конфігурація:
  - **PID**: вказує, який фільтр слід застосовувати на основі поля PID (поле ідентифікатора протоколу в полі SNAP) у кадрі. Можлива наступна конфігурація:
    - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
    - **Конкретний (Specific)**: у цьому QCE будуть використовуватися тільки налаштовані ідентифікатори протоколу (PID), тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи його значення PID. Значення слід вставляти у шістнадцятковому форматі.
- **IPv4**: вказує, які значення IPv4 будуть дозволені в цьому QCE. Якщо вибрано, відображатимуться параметри IPv4. Можлива наступна конфігурація:
  - **Протокол (Protocol)**: вказує, який фільтр слід застосовувати на основі поля номера протоколу IPv4 у кадрі. Можлива наступна конфігурація:
    - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
    - **UDP**: вказує, що в цьому QCE буде використовуватися тільки UDP, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи, якщо це протокол UDP. Якщо вибрано, відображатимуться параметри UDP. Можлива наступна конфігурація:
      - **Sport/Dport**: Sport вказує, які UDP-порти джерела будуть використовуватися на цьому QCE. З іншого боку, Dport вказує, які UDP-порти призначення будуть використовуватися. Можлива наступна конфігурація:
        - **Будь-який (Any)**: вказує, що всі вхідні кадри будуть використовуватися на цьому QCE;

- **Конкретний (Specific)**: вказує, що на цьому записі QCE буде використовуватися тільки визначений UDP-порт. Значення потрібно вставляти в десятковому форматі;
- **Діапазон (Range)**: вказує на те, що на цьому QCE буде використовуватися тільки діапазон визначених UDP-портів. Значення потрібно вставляти в десятковому форматі.

- **TCP**: вказує, що на цьому QCE буде використовуватися тільки TCP, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи, якщо це протокол TCP. Якщо вибрати цей параметр, параметри TCP відображатимуться подібно до UDP, як описано вище.
- **Інше (Other)**: вказує, який номер IP-протоколу буде використовуватися на цьому QCE, тобто цей запис буде відображати кадри на основі багатьох параметрів, включаючи, якщо вказаний IP-протокол. Значення потрібно вставляти в десятковому форматі.

- **SIP**: вказує, який фільтр слід використовувати на основі адреси джерела IPv4 у кадрі. Можлива наступна конфігурація:
  - **Будь-яка (Any)**: вказує на те, що всі кадри з IP-адреси джерела будуть використовуватися в цьому QCE;
  - **Конкретна (Specific)**: вказує, що у цьому QCE буде використовуватися тільки визначена IP-адреса. Значення дозволеної IP-адреси та маски – десяткове значення з крапками;
- **IP-фрагмент (IP Fragment)**: вказує, чи дозволені фрагментовані кадри IPv4 у цьому записі QCE. Дозволеними значеннями є "Так" (Yes) або "Ні" (No), де "Так" означає, що приймаються фрагментовані кадри для цього запису, а "Ні" означає, що фрагментовані кадри не приймаються у цьому кадрі;
- **DSCP**: вказує, які значення DSCP дозволяються в цьому записі QCE. Можливі значення – "Будь-яке", "Конкретне" та "Діапазон". Можлива наступна конфігурація:
  - **Будь-яке (Any)**: вказує, що всі вхідні кадри будуть використовуватися в цьому QCE;
  - **Конкретне (Specific)**: вказує, що в цьому QCE будуть використовуватись тільки визначені рівні DSCP. Допустимими значеннями є значення діапазону DSCP (від 0 до 63);

- **Діапазон (Range)**: вказує, що в цьому записі QCE буде використовуватися тільки діапазон визначених рівнів DSCP. Допустимими значеннями є значення діапазону DSCP (від 0 до 63).

- **Параметри дії (Action Parameters)**: вказує всі параметри дії, що застосовуються, коли кадр відповідає ключовим параметрам. Якщо кадри відповідають усім налаштованим ключовим параметрам, тоді кадр буде оброблятися так, як налаштовано в Параметрах дії. Можливі наступні конфігурації:
  - **CoS**: вказує, до якої черги CoS повинен бути перенаправлений вхідний кадр із ключовими параметрами. Дозволеними значеннями є значення діапазону CoS, від 0 до 7;
  - **DPL**: вказує, до якого рівня DPL повинен бути перенаправлений вхідний кадр із ключовими параметрами. Дозволеними значеннями є значення діапазону DPL, від 0 до 3;
  - **DSCP**: вказує, до якого рівня DSCP повинен бути перенаправлений вхідний кадр із ключовими параметрами. Дозволеними значеннями є значення діапазону DSCP, від 0 до 63;

12.13 Обмеження широкомовного шторму

Меню "Обмеження широкомовного шторму" (Storm Policing) дозволяє налаштувати функцію запобігання шторму. Запобігання шторму – це спосіб забезпечити якість обслуговування для даної локальної мережі.

- **Порт (Port)**: показує порти, які потрібно налаштувати в цьому рядку;
- **Кадри одноадресної передачі (Unicast Frames)**: вказує конфігурацію, яка застосовується, коли кадри надходять із хостів одноадресної передачі. Можлива наступна конфігурація:
  - **Увімкнено (Enabled)**: увімкнути функцію обмеження трафіку кадрів одноадресної передачі на порту. Вибраний прапорець означає що функцію увімкнено, а порожній прапорець – вимкнено;
  - **Швидкість (Rate)**: вказує швидкість, яка застосовується до функції Обмеження широкомовного шторму на цьому порту. Швидкість трафіку на порту, що перевищує це поле, не дозволяється, якщо функцію увімкнено. Дозволені значення – це цілі числа, а ліміти залежать від використовуваної одиниці. Діапазон від 100 до 1.000.000 допускається, коли використовуються одиниці вимірювання кбіт/с (kbps) або к/с (fps). Діапазон від 1 до 32.000 дозволяється, коли використовуються одиниці Мбіт/с (Mbps) або тис. к/с (kfps);
  - **Одиниця виміру (Unit)**: вказує, яку одиницю слід використовувати зі значенням швидкості для обмеження трафіку. Допустимими значеннями є кбіт/с, Мбіт/с, к/с та тис. к/с (kbps, Mbps, fps і kfps);
- **Кадри широкомовної передачі (Broadcast Frames)**: вказує конфігурацію, яка застосовується, коли кадри надходять із хостів широкомовної передачі та до них. Можлива конфігурація така ж, як і для одноадресних кадрів.
- **Невідомі кадри (Unknown Frames)**: вказує конфігурацію, яка застосовується, коли кадри надходять від і до невідомих хостів, тобто відбувається лавинне розповсюдження кадрів по всій мережі. Можлива конфігурація така ж, як і для одноадресних кадрів.

12.14 WRED

Меню WRED (Виважене довільне раннє виявлення) дозволяє налаштовувати конфігурацію для запобігання шторму на основі функції алгоритму раннього виявлення. Ця функція застосовується лише тоді, коли реалізована виважена QoS, і це поле дозволяє налаштувати поріг черг із виваженим пріоритетом. Запобігання шторму – це спосіб забезпечити якість обслуговування для даної локальної мережі. Можливі наступні конфігурації.

- **Черга (Queue)**: показує черги, які потрібно налаштувати в цьому рядку;
- **Увімкнено (Enabled)**: увімкнути функцію WRED у черзі. Вибраний прапорець означає що функцію увімкнено, а порожній прапорець – вимкнено;
- **Мінімальний поріг (Min. Threshold)**: вказує мінімальний середній трафік, при якому комутатор починає відкидати пакети черг від 0 до 5 на основі ваги, налаштованої в меню Планувальника вихідних портів QoS і меню Формувачів. Значення поза цією межею означають відсутність ймовірності відкидання пакетів. Значення вказані у відсотках, а допустимі значення – від 0 до 100. 0 означає відсутність трафіку, а 100 означає всю пропускну здатність трафіку на даному порту;
- **Максимальний DP1 (Max. DP1)**: вказує ймовірність відкидання кадрів DPL 1, коли трафік у черзі становить 100%. Це поле дозволяє встановити ймовірність втрати пакетів, позначених Рівнем пріоритету відкидання (DPL) 1. Значення вказані у відсотках, а дозволені значення - від 0 до 100. 0 означає відсутність трафіку, а 100 означає всю пропускну здатність трафіку у даній черзі;
- **Макс. DP2**: вказує ймовірність відкидання кадрів DPL 2, коли трафік у черзі становить 100%. Це поле дозволяє встановити ймовірність втрати пакетів, позначених Рівнем пріоритету відкидання (DPL) 2. Значення вказані у відсотках, а дозволені значення - від 0 до 100. 0 означає відсутність трафіку, а 100 означає всю пропускну здатність трафіку у даній черзі;
- **Макс. DP3**: вказує ймовірність відкидання кадрів DPL 3, коли трафік у черзі становить 100%. Це поле дозволяє встановити ймовірність втрати пакетів, позначених Рівнем пріоритету відкидання (DPL) 3. Значення вказані у відсотках, а дозволені значення - від 0 до 100. 0 означає відсутність трафіку, а 100 означає всю пропускну здатність трафіку у даній черзі;

На рисунку нижче показано криві ймовірності відкидання у порівнянні із середнім рівнем заповнення рівнів DPL.

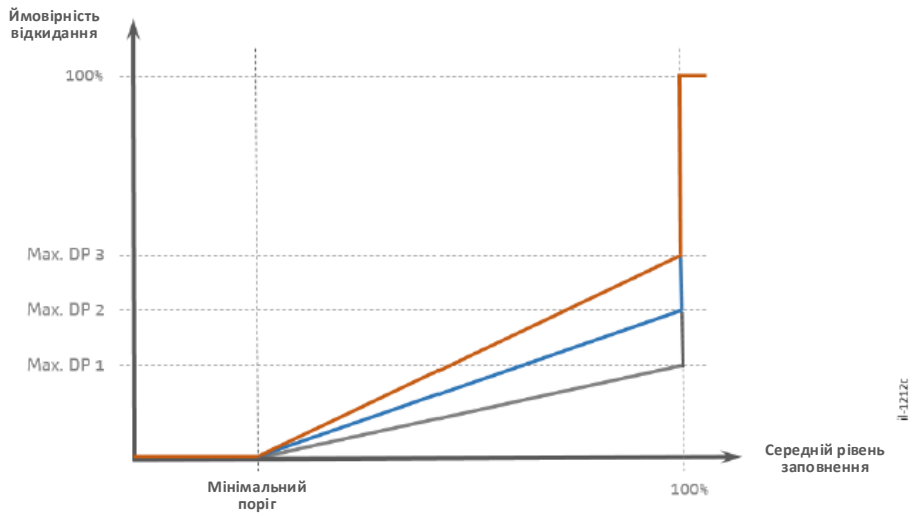


Рис. 62: Використання рівнів пріоритету відкидання (DPL)

13 Дзеркальне відображення портів

13.1 Основні принципи дзеркального відображення портів

Дзеркальне відображення ("дзеркалювання") портів – це функція, яка використовується як стратегія моніторингу в мережах з комутацією пакетів. Якщо увімкнено, дзеркалювання портів створює копію вхідних та вихідних даних із певного порту. Дзеркальний порт можна підключити до аналізатора мережі, що було б доцільним для аналізу та налагодження даних або діагностики помилок мережі.

Рис. 63: Дзеркалювання портів, виконане комутатором

Reason S20 має функції дзеркального відображення портів, які в основному можуть бути виконані двома способами:

- Дзеркалювання портів на одному комутаторі;
- Дзеркалювання портів на різних комутаторах.

Дзеркалювання портів на одному комутаторі, що говорить само за себе, виконується лише одним комутатором, який повинен бути налаштований на дзеркальний тип. Дзеркальний порт і порт, що використовуються для виведення дзеркальних даних, знаходяться на одному обладнанні.

У режимі роботи дзеркального типу Reason S20 може дзеркально відображати трафік усіх портів, тільки вхідні дані (Rx) або тільки вихідні дані (Tx) з кожного порту. Крім того, можна вибрати більше одного порту для дзеркалювання тільки з одним портом для виведення дзеркального трафіку.

Рис. 64: Дзеркалювання портів на одному комутаторі

Дзеркалювання портів на різних комутаторах потрібно, коли порт одного комутатора повинен бути дзеркально відображений до іншого комутатора. Поширеним варіантом застосування такого режиму є віддалений моніторинг трафіку, тобто, коли потрібно перевірити трафік в іншому приміщенні, де не встановлено аналізатор мережевого трафіку. При використанні дзеркалювання на різних комутаторах, всі комутатори у даній локальній мережі повинні бути налаштовані на дзеркалювання. Використовуючи пристрій Reason S20, потрібно налаштувати комутатори за типами: "джерело", "проміжний" та "адресат", залежно від положення комутатора у потоці трафіку. На рисунку нижче показаний приклад такого застосування, де проілюстровано комутатори за типами "Джерела", "Проміжного" та "Адресата".

Рис. 65: Дзеркалювання портів на кількох комутаторах

У режимі роботи типу "Джерела" комутатор буде налаштований як збирач даних потоку даних моніторингу. Порт, який потрібно контролювати, буде увімкнено для дзеркалювання, а один фіксований мідний порт RJ45 повинен бути вибраний як порт-відбивач. Порт-відбивач неактивний і не здійснює обміну даними, і це повинен бути фіксований мідний порт RJ45. Як оптичні, так і електричні SFP не працюватимуть як порти-відбивачі. Нарешті, або проміжні порти, або порти-адресати можуть бути налаштовані на "Джерело" для зв'язку з іншим комутатором або надсилання дзеркальних даних до адресата трафіку, відповідно.
У режимі роботи типу "Проміжного" комутатор буде працювати як вузол у мережі потоку даних моніторингу. Потрібно вибрати порти, які знаходяться в потоці моніторингу. У наведеному вище прикладі проміжними портами повинні бути порти, підключені до комутатора "Джерела" та комутатора "Адресата".
У режимі роботи типу "Адресата", комутатор буде працювати як кінцевий вузол мережі потоку даних моніторингу. Потрібно вибрати порти, які знаходяться в потоці моніторингу, і порт, до якого підключений Аналізатор мережевого трафіку. Можна вибрати більше одного порту в якості адресата, щоб дозволити підключення кількох аналізаторів мережевого трафіку. На наступному рисунку показано, як повинні бути налаштовані порти при дзеркалюванні портів на різних комутаторах.

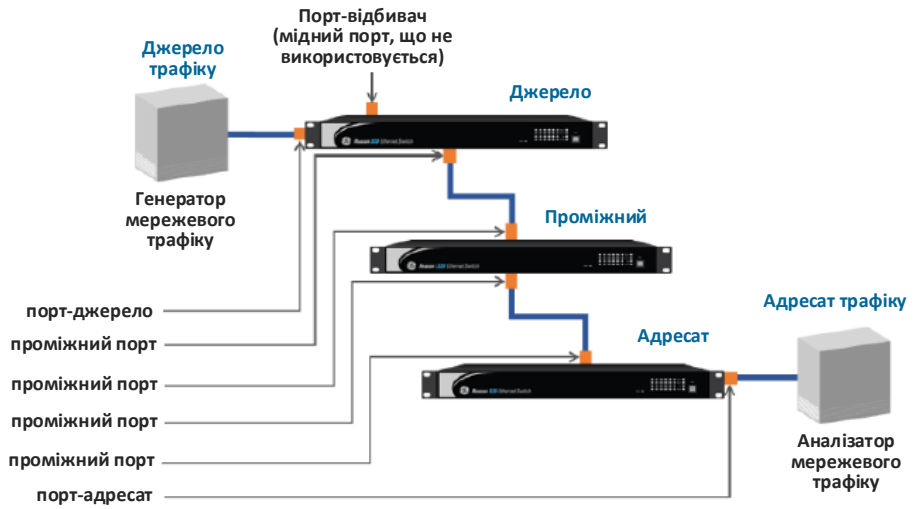


Рис. 66: Мережа потоку даних моніторингу

Меню Дзеркалювання знаходиться в Налаштування> Дзеркалювання (Settings > Mirroring)

13.2 Класифікація дзеркального відображення портів

Загальна конфігурація

Загальні налаштування відображають основну конфігурацію функції дзеркального відображення (дзеркалювання). Можливі наступні конфігурації.

- **Режим (Mode)**: вмикає функцію дзеркалювання. "Увімкнути" (Enable) дозволить роботу функції, а "Вимкнути" (Disable) припинить роботу функції дзеркалювання;
- **Тип (Type)**: вказує тип роботи комутатора. Допустимі значення є наступними:
  - **Дзеркало (Mirror)**: вказує на те, що комутатор буде працювати в дзеркальному режимі, тобто на цьому комутаторі знаходиться порт джерела та адресата (призначення);
  - **Джерело (RMirror) (Source (RMirror))**: вказує, що комутатор буде працювати у режимі джерела, тобто порт-адресат знаходиться на іншому комутаторі. На цьому комутаторі знаходяться порт джерела та проміжний порт;
  - **Проміжний (RMirror) (Intermediate (RMirror))**: вказує, що комутатор буде працювати у режимі проміжного порту, тобто порт джерела та порт-адресат знаходяться на іншому комутаторі. На цьому комутаторі знаходяться тільки проміжні порти;
  - **Адресат (RMirror) (Destination (RMirror))**: вказує на те, що комутатор буде працювати у режимі адресата, тобто порти джерела знаходяться на іншому комутаторі. На цьому комутаторі знаходяться проміжні порти та порти -адресати;
- **Ідентифікатор VLAN (VLAN ID)**: вказує, до якої VLAN функція дзеркалювання повинна відображати трафік. Це поле визначає, який трафік VLAN для дзеркалювання повинен бути перенаправлений, і використовується комутаторами при виконанні віддаленого дзеркалювання. Це поле не дозволене, якщо Тип дзеркалювання – "Дзеркало", тобто тільки функція віддаленого дзеркалювання перенаправлятиме трафік до конкретної VLAN. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095);
- **Порт-відбивач (Reflector Port)**: вказує основний порт Джерела функції віддаленого дзеркалювання. Порт-відбивач – це порт, на комутаторі типу Джерела (RMirror), який буде отримувати трафік від усіх дзеркальних портів і пересилати його на Проміжний (RMirror) комутатор або Комутатор-адресат (RMirror) віддаленого дзеркалювання. Портами-відбивачами можуть бути тільки електричні порти (RJ45 та UTP-кабель), і тільки ці порти відображаються у списку. Тільки один порт може бути портом-відбивачем на даному комутаторі.

На портах-відбивачах повинні бути вимкнені вивчення таблиць MAC-адрес та Протоколи кістякового дерева. Тільки фіксовані мідні Ethernet-порти RJ45l можна налаштувати як порти-відбивачі.

Конфігурація VLAN джерела

Конфігурація VLAN джерела відображає конфігурацію VLAN джерела, яка буде використана для функції дзеркалювання. Це поле дозволяє дзеркальне відображення на основі VLAN, вставляючи ідентифікатори дозволених VLAN у це поле. Можливі наступні конфігурації.

- **VLAN джерела (Source VLANs)**: вказує на те, функція дзеркалювання якої VLAN повинна здійснювати дзеркальне відображення трафіку. Це поле дозволяє налаштувати дзеркалювання на основі VLAN, на додаток до дзеркалювання портів. Існує можливість незалежно контролювати конкретні VLAN та порти з різних VLAN. Дозволеними значеннями є значення діапазону VLAN (від 1 до 4095);

Конфігурація порту

Конфігурація порту відображає конфігурацію, дозволену для кожного порту для виконання функції дзеркального відображення. Це поле дозволяє визначити порти джерела, проміжні порти та порти-адресати та визначити, чи відображатиметься весь трафік, тільки TX або тільки RX-трафік. Можливі наступні конфігурації.

- **Порт (Port)**: вказує порти, які потрібно налаштувати в цьому рядку;
- **Джерело (Source)**: вказує, чи порт є портом джерела, і який тип трафіку дзеркально відображається. Це поле дозволене тільки в тому випадку, якщо комутатор працює у режимі "Дзеркала" або "Джерела" (RMirror). Можливі наступні значення:
  - **Вимкнено (Disabled)**: вказує на те, що порт дзеркально не відображається, тобто порт працює в нормальному режимі і дзеркалювання трафіку з цього порту не виконується;
  - **Обидва (Both)**: вказує на те, що порт дзеркально відображається, а весь трафік (отримані та передані кадри) дзеркально відображається;
  - **Тільки Rx (Rx Only)**: вказує на те, що порт дзеркально відображається і трафік Rx (отримані кадри) дзеркально відображається;
  - **Тільки Tx (Tx Only)**: вказує на те, що порт дзеркально відображається, і трафік Tx (передані кадри) дзеркально відображається;
- **Проміжний (Intermediate)**: дозволяє порту працювати як проміжний порт. Проміжні порти – це порти, що з'єднують комутатори, які виконують віддалене дзеркалювання. Вибраний прапорець означає, що порт буде працювати як проміжний порт, тобто джерелом трафіку цього порту буде порт-відбивач (Reflector port) або інший проміжний порт. Порожній прапорець означає, що порт не буде працювати як проміжний порт, тобто порт буде працювати у нормальному режимі без дзеркалювання (якщо порт-адресат також вимкнено) або порт буде працювати як порт-адресат;

На проміжних портах повинне бути вимкнене вивчення таблиць MAC-адрес.

- **Адресат (Destination)**: дозволяє порту працювати як порт-адресат. Порти-адресати – це порти, які підключають комутатор-адресат (RMIrror), що здійснює віддалене дзеркалювання до кінцевої станції, тобто аналізатора трафіку. Вибраний прапорець означає, що порт буде працювати як порт-адресат, тобто джерелом трафіку цього порту буде порт-відбивач або інший проміжний порт. Порожній прапорець означає, що порт не буде працювати як порт-адресат, тобто порт працюватиме у нормальному режимі без дзеркалювання (якщо проміжний порт також вимкнено) або порт буде працювати як проміжний порт;

На портах-адресатах повинне бути вимкнене вивчення таблиць MAC-адрес.

14 Протокол точного часу (PTP) - IEEE 1588v2

Протокол IEEE1588v2 можна увімкнути шляхом ліцензування S20. Протокол точного часу (PTP) визначається стандартом IEEE 1588, який описує протокол синхронізації точного часу для мережевих систем вимірювання та керування. На пристроях S20 протокол IEEE 1588v2 також може використовуватися для синхронізації внутрішнього системного часу.
Зверніть увагу, що версія IEEE1588v2 не має зворотної сумісності з версією 1.

14.1 Функціонал протоколу точного часу (PTP)

Протокол точного часу (PTP) використовує Ethernet- кадри для передачі повідомлень синхронізації для забезпечення синхронізації часу декількох IED, підключених до мережі. Сам протокол дозволяє використовувати повідомлення рівня 2 (транспортний механізм багатоадресної передачі) або рівня 3 (транспортний механізм UDP), з яких один обраний залишиться відповідно до вимог застосування.

Хоча протокол PTP дозволяє використовувати як Ethernet (багатоадресна передача), так і IP (транспортний механізм UDP), у Технічному звіті МЕК 61850-90-4 зазначено, що тільки зв'язок рівня 2 має необхідну точність для варіантів застосування в енергосистемах, таких як синхронізація обладнання IED. Виходячи з цього, рекомендується використовувати зв'язок Рівня 2 для енергосистем.

Повідомлення передаються за методом ведучий-ведений (master-slave). На відміну від протоколу NTP, коли ведений пристрій надсилає запит ведучому на отримання даних про час, у мережі PTP ведучий пристрій використовує багатоадресну передачу для передачі своїх повідомлень синхронізації по всій мережі, а ведені пристрої приймають повідомлення циклічно, тоді як ведучий продовжує надсилати їх до мережі.

У мережі PTP існує кілька елементів. Основними елементами середовища, що підтримує PTP, є наступні:

- **Головний годинник (Grand Master Clock) (GMC):** Цей годинник є годинником верхнього рівня у мережі, зазвичай годинником на основі GPS;
- **Ведучий годинник (Master Clock) (MC):** Ведучий годинник на заданих дочірніх піддоменах, який може бути годинником GMC або граничним годинником;
- **Звичайний годинник (Ordinary Clock) (OC):** Годинник у мережі PTP, який може бути або ведучим, або веденим годинником.
- **Прозорий годинник (Transparent Clock) (TC):** Годинник, який пересилає повідомлення синхронізації із значенням затримки процесу переадресації, включеним у повідомлення;
- **Граничний годинник (Boundary Clock) (BC):** Годинник, який має ведений порт, синхронізований ведучим годинником, і ведучий порт, який синхронізує час на піддоменах;

Робота PTP у мережі показана нижче.

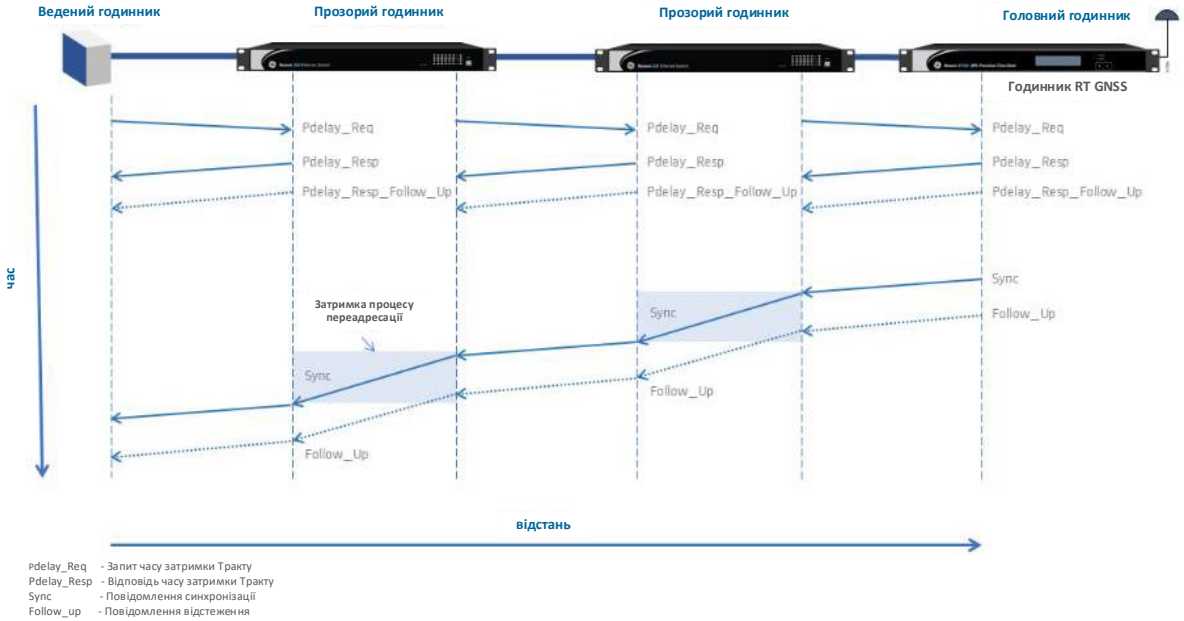


Рис. 67: Механізм протоколу PTP

У циклічному режимі Головний годинник (GMC) надсилає повідомлення синхронізації по всій мережі за допомогою механізму багатоадресної передачі. Типовий цикл – 1 секунда, тобто кожну секунду мережа отримуватиме повідомлення синхронізації від GMC.

Кожен тракт обмінюватиметься інформацією для обчислення часу затримки тракту. Таким чином, на кожному прозорому годиннику (TC) буде час, який буде враховано перед відправкою повідомлення веденому пристрою, таким чином мінімізуючи похибку від GMC до веденого годинника. Врешті-решт, всі затримки тракту та затримки процесу переадресації на TC будуть скориговані, і тоді ведений годинник отримає позначку часу, яку відправив годинник GMC.

У двоетапному режимі TC збереже позначку часу отриманого кадру синхронізації та перешле її без корекції. Після отримання повідомлення синхронізації, TC обчислить суму з корекцією вхідного повідомлення синхронізації, власною затримкою переадресації та заздалегідь розрахованою затримкою тракту, а потім надішле Повідомлення про відстеження з корекцією, яку повинні зробити інші годинники в мережі.

Якщо в мережі більше одного ведучого пристрою, обладнання, що підтримує ведучого, проведе вибори, щоб визначити, який годинник має найкращу точність у мережі, на основі повідомлення- сповіщення. Таким чином, мережа PTP, що має більше одного ведучого, матиме механізм захисту від відмови безпосередньо в протоколі, щоб забезпечити надійність синхронізації мережі.

Механізм визначення затримки між рівноправними вузлами (peer-to-peer - P2P) обчислює затримку тракту та затримку процесу переадресації кожного компонента в мережі. PTP також дозволяє використовувати механізм визначення затримки між кінцевими вузлами (наскрізна передача) (end-to-end -E2E), який є подібним до механізму, що використовується в протоколах NTP. У цьому механізмі всі затримки між ведучим та веденим пристроями будуть розглядатися як одне значення, значення "затримки тракту".

Reason S20 може працювати в режимах P2P або E2E. Що стосується варіантів застосування в енергосистемах, у Технічному звіті МЕК 61850-90-4 зазначено, що механізм E2E не має бажаної точності. Таким чином, рекомендується використовувати механізм визначення затримки P2P.

14.2 PTP у GE Reason S20

Якщо увімкнено, існує чотири режими роботи під час використання Reason S20 у мережах PTP:

- Прозорий годинник (TC);
- Граничний годинник (BC);
- Тільки Ведучий;
- Тільки Ведений.

За замовчуванням PTP вимкнено в Reason S20.

Під час роботи в мережі PTP IEEE1588v2 можна послідовно визначити, які порти будуть увімкнені та якою є затримка асиметрії для кожного з них.

Меню PTP знаходиться в меню Налаштування > PTP (Settings > PTP).

Загальні налаштування

- **Режим (Mode)**: для визначення режиму роботи PTP Ethernet-комутатора.
  - **Прозорий годинник (Transparent Clock)**: згідно з IEEE1588v2, прозорий годинник має кілька портів PTP і вимірює час, який повідомлення про подію PTP витрачає на проходження транзитного тракту мережі, і надає цю інформацію звичайним годинникам (веденим пристроям), які отримують це повідомлення про подію PTP, щоб вони могли компенсувати кожну затримку тракту;
  - **Граничний годинник (Boundary Clock)**: згідно з IEEE1588v2, граничний годинник має декілька портів PTP (один працює як ведений, а інші як ведучі) у номері домену і підтримує часовий масштаб, що використовується в домені. З веденим портом PTP, синхронізованим за головним годинником PTP (grandmaster), він служить ведучим годинником для ведених пристроїв IED, використовуючи решту портів;
  - **Тільки ведучий (Master only)**: згідно з IEEE1588v2, це джерело часу, яке синхронізує усі інші годинники на цьому тракті. S20 використовує свій внутрішній час для синхронізації звичайних (ведених) годинників. На відміну від Граничного годинника, параметр "Тільки Ведучий" не має веденого порту для синхронізації комутатора з іншим головним годинником.
  - **Тільки ведений (Slave only)**: визначений як звичайний годинник згідно з IEEE1588v2, цей режим використовується тільки для синхронізації внутрішнього годинника S20 на основі головного (Grandmaster) годинника PTP. Зауважте, цього також можна досягти в інших трьох режимах, увімкнувши опцію налаштування системного часу.
- **Профіль (Profile)**:
  - **Визначено користувачем (Custom)**: усі параметри PTP можна вільно налаштовувати;
  - **Енергосистема – МЕК/IECC 61850-9-3/2016 (Power Utility – IEC/IECC 61850-9-3/2016)**: Параметри PTP попередньо визначені відповідно до профілю енергосистеми PTP – МЕК61850-9-3.
  - **Профіль потужності – IEEE C37.238/2017 (Power Profile – IEEE C37.238/2017)**: Параметри PTP попередньо визначені відповідно до профілю потужності PTP – IEEE C37.238: 2017.
- **Номер домену (Domain Number)**: номер домену є ідентифікатором мережі PTP, тому Reason S20 взаємодіятиме тільки з повідомленнями PTP з цього домену. Діапазон від 0 до 255.
- **Мережевий протокол (Network Protocol)**: транспортний протокол, що використовується механізмом протоколу PTP.

  - **Ethernet**: PTP з використанням Ethernet (рівень 2), багатоадресна передача;
  - **Багатоадресний IPv4 (IPv4 Multicast)**: PTP з використанням IPv4/UDP (рівень 3), багатоадресна передача;
  - **Змішаний IPv4 (IPv4 Mixed)**: PTP із використанням комбінації IPv4/UDP (рівень 3), багатоадресна та одноадресна передачі;
  - **Одноадресний IPv4 (IPv4 Unicast)**: PTP з використанням IPv4/UDP (рівень 3), одноадресна передача. Одноадресна передача IPv4 можлива тільки при роботі в режимі "Тільки ведучий" або "Тільки ведений".
    При роботі в режимі одноадресної передачі IPv4, Reason S20 може мати до 5 налаштованих ведучих IP-адрес. Потім ведений пристрій запитує повідомлення-сповіщення від усіх налаштованих ведучих пристроїв. Ведений пристрій використовує алгоритм BMC, щоб вибрати один з пристроїв як ведучий годинник, а потім ведений запитує повідомлення синхронізації від вибраного ведучого годинника.
- **VLAN**: увімкнення/вимкнення тегування VLAN для кадрів PTP.
  - **Ідентифікатор VLAN (VLAN ID)**: ідентифікатор VLAN, що використовується для тегування кадрів PTP.
  - **Пріоритет VLAN (VLAN Priority)**: Значення кодової точки пріоритету (PCP), що використовується для кадрів VLAN PTP.
- **Режим роботи (Operation Mode)**: режим роботи PTP, Reason S20 підтримує тільки двоступеневий режим. У двоступеневому режимі інформація про синхронізацію надсилається одним пакетом даних, а інформація про позначку часу надсилається іншим пакетом даних відразу після цього.
- **Механізм визначення затримки (Delay Mechanism)**: механізм, що використовується для компенсації затримок у мережі.
  - **Наскрізний механізм визначення затримок між кінцевими вузлами (End-to-End)**: вимірювання затримки в мережі між ведучим та веденим годинником;
  - **Механізм визначення затримок між рівноправними вузлами (Peer-to-Peer)**: вимірювання затримки виконується в режимі "hop by hop" (послідовно), виконуючись усіма пристроями, що підтримують PTP, включаючи комутатори, коли вони працюють як прозорий або граничний годинники.
- **Пріоритети №1 та №2 (Priority #1 and #2)**: Коли налаштовано як ведучий пристрій, необхідно визначити пріоритети критеріїв розриву з'єднання (так званого "відкидання зайвого" - tie breaking) для алгоритму визначення найкращого ведучого годинника (BMC). Значення пріоритету можуть варіюватися від 0 до 255, чим нижче присвоєне значення, тим вищим є пріоритет. Пріоритет №1 використовується спеціально для проектування одного годинника пріоритету, а не інших – це перша умова розриву з’єднання. Пріоритет №2 – це останній критерій розриву з'єднання PTP, що йде після класу, точності та відхилення годинника. Після пріоритету №2 MAC-адреса використовується як останній ресурс для розриву з'єднання.
- **Інтервал синхронізації (Sync Interval)**: для вибору частоти надсилання повідомлень синхронізації. Діапазон між 16 повідомленнями на секунду та одним повідомленням кожні 32 секунди.
- **Інтервал запиту затримки (Delay Request Interval)**: вибрати частоту надсилання повідомлень-запитів часу затримки. Діапазон між 16 повідомленнями на секунду та одним повідомленням кожні 32 секунди.
- **Інтервал сповіщення (Announce Interval)**: вибрати частоту надсилання повідомлень сповіщення при роботі в режимі ведучого або граничного годинника. Діапазон між 16 повідомленнями на секунду та одним повідомленням кожні 32 секунди.

- **Час очікування сповіщення (Announce Timeout)**: час очікування отримання повідомлення-сповіщення. Якщо повідомлення сповіщення не отримано протягом цього інтервалу часу, Reason S20 припускає, що поточний ведучий годинник недоступний, і виконує алгоритм BMC для вибору іншого ведучого годинника. Діапазон – від 2 до 255 секунд.

Налаштування системного часу

- **Налаштувати системний час (Adjust System Time)**: вибирає, чи буде PTP коригувати внутрішній системний час чи ні. Це налаштування буде вимкнено, навіть якщо воно раніше було увімкнене, щоразу, коли вмикається режим NTP-клієнта.

Конфігурація порту

Щоб вибрати, які порти будуть увімкнені та працюватимуть у екземплярі PTP відповідно до загальних налаштувань. Також можна налаштувати асиметрію затримки на кабелі з кожного порту комутатора. Конфігурація налаштовується в наносекундах за такою формулою:

асиметрія затримки = затримка прийому RX - затримка передачі TX.

15 Протокол інформації маршрутизації (RIP)

15.1 Основні принципи RIP

RIP – це протокол дистанційно-векторної маршрутизації, який широко використовується в IP-мережах, переважно малого та середнього розміру. Іншими словами, маршрутизатор, на якому запущений RIP, надсилає інформацію про свою доступність усім сусіднім маршрутизаторам, яка потім зберігається в таблиці маршрутизації кожного маршрутизатора. Періодично, всі маршрутизатори обмінюються інформацією про свою таблицю маршрутизаторів між собою, так що кожен маршрутизатор знає найменшу відстань (кількість хопів (переходів)) до пункту призначення (адресата). Кількість хопів підтримує до 15 хопів, і оскільки 16-й хоп вважається недосяжним.

Існує дві версії RIP:

- **RIPv1**: Визначений стандартом RFC 1058, RIPv1 є протоколом маршрутизації з використанням класів, що означає, що всі пристрої в одному домені маршрутизації повинні використовувати одну і ту ж маску підмережі. Крім того, RIPv1 не підтримує автентифікацію, і він використовує широкомовну передачу для оновлення таблиці маршрутизації.
- **RIPv2**: Визначений у стандарті RFC 2453, RIPv2 є безкласовим протоколом маршрутизації, що дозволяє використовувати маски підмережі змінної довжини, оскільки маски підмережі включаються в оновлення маршрутизації. RIPv2 підтримує автентифікацію (відкритий текст, MD5) і використовує багатоадресну передачу для оновлення таблиці маршрутизації. Усі маршрутизатори, на яких запущений RIPv2, повинні мати однакові налаштування Дати/Часу, щоб автентифікація ланцюга ключів RIPv2 працювала належним чином; це можна зробити за допомогою протоколу мережевого часу (NTP).

15.2 Конфігурація RIP

RIP доступний, тільки якщо на пристрої S20 увімкнено ліцензування Рівня 3.

Конфігурація знаходиться в меню Налаштування > RIP (Settings > RIP).

Загальна конфігурація

- **Режим (Mode)**: визначає, увімкнена або вимкнена функція RIP;
- **Версія (Version)**: вибирає версію протоколу, RIP версії 1 або 2;

- **Таймер оновлення (Update timer)**: Інтервал у секундах між оголошеннями таблиці маршрутизації. Значення за замовчуванням – 30 секунд, допустимий діапазон – від 5 до 65.535 секунд.
- **Таймер часу очікування (Timeout timer)**: Інтервал у секундах для оголошення недійсним маршрутизатора, який більше не надсилає оновлення. Значення за замовчуванням – 180 секунд, допустимий діапазон – від 5 до 65.535 секунд.
- **Таймер "збирача сміття" (Garbage timer)**: Інтервал у секундах, щоб видалити маршрутизатор без оновлень із таблиці маршрутизації. Значення за замовчуванням – 240 секунд, допустимий діапазон – від 5 до 65.535 секунд.

Віртуальні локальні мережі (VLAN)

RIP можна активувати окремо для кожної VLAN. Усі порти на заданій VLAN передаватимуть протокол RIP і оброблятимуть інформацію про маршрутизацію від інших маршрутизаторів з увімкненим RIP. Якщо пакет RIP надсилається до порту, для якого VLAN вимкнено, пакет RIP ігнорується.
Зверніть увагу, що у цій конфігурації відображаються лише VLAN із налаштованою IP-адресою (Налаштування> Система> IP) (Settings > System > IP).

- **VLAN**: номер VLAN, від 1 до 4095;
- **Увімкнути (Enable)**: виберіть, щоб увімкнути RIP на відповідній VLAN;
- **Режим автентифікації (Authentication mode)**: доступний тільки на RIPv2. Вибирає метод автентифікації для передачі протоколу RIP у VLAN. Допустимі значення: немає, текст або MD5 (none, text або MD5).
- **Ланцюг ключів (Keychain)**: доступний лише на RIPv2. Ланцюг ключів може містити один або кілька паролів, що валідують протокол RIP. Кожна VLAN матиме пов’язаний з нею ланцюг.

Сусідні пристрої

Сусідні пристрої є довіреними шлюзами для отримання протоколу RIP. Якщо жоден сусідній пристрій не налаштований, усі отримані пакети будуть прийняті. Якщо вказаний один або декілька сусідніх пристроїв, приймаються пакети RIP від налаштованих сусідніх пристроїв, а пакети з інших джерел ігноруються.

- **Додати сусідній пристрій (Add Neighbor)**: введіть IP-адресу сусіднього маршрутизатора та натисніть кнопку зберегти. Натисніть "видалити" та "зберегти" (delete та save), щоб видалити налаштований сусідній пристрій.

Ланцюги ключів

Як зазначалося раніше, ланцюги ключів використовуються для зберігання одного або декількох ключів для валідації обміну інформацією RIP у мережі. Ланцюги пов'язані з VLAN. Одночасно буде дійсним один ключ, який буде включений до всіх надісланих відповідей RIP та перевірятиметься на всіх отриманих відповідях RIP. Паролі підтримуються тільки у RIP версії 2, а у версії 1 ігноруються.

- **Додати ланцюг ключів (Add Keychain)**: введіть ім'я ланцюга, від 1 до 32 символів, і натисніть "Додати ланцюг ключів", щоб ввести наступні параметри.
- **Видалити (Delete)**: натисніть, щоб видалити створений ланцюг ключів.
- **Ідентифікатор (ID)**: ідентифікатор ключа. Він повинен бути унікальним, але ігнорується для відкритого (незашифрованого) пароля. Допустимі значення знаходяться в діапазоні від 0 до 255.
- **Рядок (String)**: Рядок ключа. Рядок може містити від 1 до 16 великих та малих буквено-цифрових символів, а перший символ не може бути числом.
- **Час початку/закінчення (Start/End time)**: необов’язково введіть період (час початку/ закінчення), протягом якого ключ буде дійсним. Якщо встановлено лише час пуску, термін дії ключа ніколи не закінчиться.
  Формат часу – "години : хвилини: рік / місяць / день" ("hh:mm yyyy/mm/dd").

У випадку кількох ключів, якщо відбувається накладення (перекриття) періодів, ключ з найпізнішим часом закінчення або нижчим ідентифікатором буде мати пріоритет на вихідних пакетах. Якщо термін дії всіх ключів закінчився, буде використовуватися той, термін дії якого закінчився останнім або з нижчим ідентифікатором. Якщо жоден ключ ще не дійсний, жоден не надсилається. Вхідні пакети приймаються, якщо вони містять дійсний ключ, ключ, який буде дійсним протягом наступних 24 годин, або який був дійсним протягом попередніх 24 годин.

15.3 Інтерфейс командного рядка (CLI)

Загальна конфігурація

Команда	Опис	Одиниця	За замовчуванням	Параметр маршрутизації
`router rip`	Увімкнути RIP.			
`rip version <1|2>`	Вибрати версію протоколу.		2	`ripv2`
`rip timer update <5-65535>`	Встановити інтервал між оголошеннями таблиці маршрутизації.	с	30	
`rip timer timeout <5-65535>`	Встановити інтервал без оновлень, необхідний, щоб анулювати маршрут.	с	180	
`rip timer garbage <5-65535>`	Встановити інтервал без оновлень, необхідний, щоб видалити маршрут із таблиці маршрутизації.	с	240	
`rip neighbor <ip>`	Додати сусідній маршрутизатор для обміну інформацією про маршрутизацію. Максимум 64 сусідні пристрої.			`trust_gatewa`

Конфігурація ланцюга ключів

Команда	Опис	Параметр маршрутизації
`rip keychain <word32> key <uint8> key-string <kword80> [ start <hhmm> <date> [ { end <hhmm> <date> } | { duration <uint> } ] ]`	Додати ключ до ланцюга ключів	`passwd`
`keychain <word32>`	Ім'я ланцюга ключів. Максимально до 4 ланцюгів ключів.	
`key <0-255> Set key`	Встановити ідентифікатор ключа. Максимум 8 ключів для кожного ланцюга ключів.	

Команда	Опис	Параметр маршрутизації
key-string <kword16>	Встановити рядок ключа. Рядок може містити від 1 до 16 великих та малих буквено-цифрових символів, але перший символ не може бути числом.	
start <hhmm> <date> [end <hhmm> <date> | duration <uint>]	Вказати період, з якого можна використовувати ключ. Найбільш рання прийнятна дата – 1 січня 1993 року.	

Конфігурація інтерфейсу

Команда	Опис	Параметр маршрутизації
interface vlan <vlan_list>		
rip	Увімкнути RIP на інтерфейсі.	
no rip rip authentication mode {text | md5}	Вимкнути RIP на інтерфейсі. Встановити метод автентифікації для RIPv2.	no_rip passwd, md5_passwd
rip authentication keychain {key}	Пов’язати ланцюг ключів для автентифікації RIP на інтерфейсі.	passwd, md5_passwd

Команди стану

Команда	Опис
show router rip keychain	Відображати ланцюги ключів.
show router rip neighbour	Відображати сусідні пристрої.

16 Протокол вибору доступного найкоротшого маршруту (OSPF)

16.1 Основні принципи OSPF

OSPF – це протокол маршрутизації для IP-мереж, який зазвичай застосовується у мережах від середнього до великого розмірів. У ньому використовується протокол маршрутизації на основі стану каналу в рамках протоколу внутрішнього шлюзу (IGP) для розповсюдження інформації про IP-маршрутизацію по єдиній автономній системі (AS) в IP-мережі. Версія OSPF 2 використовується для IPv4, як визначено у стандарті RFC 2328.

Використовуючи алгоритм маршрутизації по першому найкоротшому шляху, OSPF будує та обчислює найкоротший шлях до всіх відомих адресатів. Оновлення стану каналу з кожного маршрутизатора OSPF надсилаються в мережу, і кожен маршрутизатор зберігає копію стану каналу інших маршрутизаторів. Завдяки використанню цієї інформації, розраховується найкоротший шлях до всіх адресатів.

Для великих мереж можна створити області OSPF у вигляді меж, щоб уникнути лавинного розповсюдження даних мережевого обміну про стани каналів. Коли використовуються, комутатори всередині області називаються внутрішніми маршрутизаторами, і вони мають однакову базу даних стану каналів; комутатори на межі називаються граничними маршрутизаторами області (ABR), і вони працюють як магістральні, описуючи стан каналів кожної області.
У порівнянні з RIP, OSPF має ряд наступних переваг: відсутність обмежень щодо кількість хопів, концепція областей для великих мереж та швидша конвергенція.

16.2 Конфігурація OSPF

OSPF доступний, тільки якщо на пристрої S20 увімкнено ліцензування Рівня 3. Конфігурація знаходиться в Налаштування> OSPF (Settings > OSPF).

Загальна конфігурація

- **Режим (Mode)**: визначає, увімкнено чи вимкнено функціонування OSPF;
- **Ідентифікатор маршрутизатора (Router ID)**: визначає ідентифікатор маршрутизатора від цього пристрою в мережі OSPF;
- **Затримка SPF (SPF delay)**: інтервал у секундах між отриманням оновлення бази даних стану каналу та початком обчислення Першого найкоротшого шляху (SFP). Значення за замовчуванням – 1 секунда, допустимий діапазон – від 1 до 10 секунд;
- **Час утримання SPF (SPF holdtime)**: Інтервал у секундах між послідовними обчисленнями SPF. Значення за замовчуванням – 5 секунд, допустимий діапазон – від 1 до 5 секунд.

Області

Області (Areas)– це логічні колекції мереж OSPF, маршрутизаторів (або комутаторів L3) та інтерфейсів з однаковою ідентифікацією області. Вони обмежують сферу поширення інформації про маршрути. Якщо використовується кілька областей, для коректної роботи протоколу потрібно додати магістральну область (0.0.0.0). Крім того, області дозволяють захистити від несанкціонованого доступу до ідентифікованої області за допомогою ключа автентифікації. У цій конфігурації відображаються тільки області з налаштованим режимом автентифікації.

- **Видалити (Delete)**: Виберіть, щоб видалити попередньо створену область;
- **Ідентифікатор (ID)**: ідентифікація області у форматі [0-255]. [0-255]. [0-255]. [0-255];
- **Режим автентифікації (Authentication Mode)**: виберіть метод автентифікації для кожної області. Виберіть текст, щоб використовувати відкритий (нешифрований) текст як автентифікацію, або md5, щоб використовувати хеш MD5.

Інтерфейси

Налаштуйте інтерфейси (пов’язані з VLAN), доступні для маршрутизації OSPF. Зверніть увагу, що у цій конфігурації відображаються тільки VLAN із налаштованою IP-адресою (Налаштування> Система> IP) (Settings > System > IP).

- **VLAN**: відображає ідентифікатори VLAN, доступні для використання OSPF;
- **Увімкнути (Enable)**: встановіть прапорець, щоб увімкнути OSPF на даній VLAN;
- **Ідентифікатор області (Area ID)**: введіть ідентифікатор області OSPF, в якій повинен бути маршрутизований інтерфейс;
- **Вартість (Cost)**: Вартість інтерфейсу для маршрутизації даних. Значення за замовчуванням - 10, допустимий діапазон - від 1 до 65.535. Чим більша вартість, тим менша ймовірність використання інтерфейсу у тракті маршрутизатора;

- **Пріоритет (Priority)**: Пріоритет маршрутизатора. Якщо встановлено значення 0, маршрутизатор не відповідає критеріям призначеного маршрутизатора або резервного призначеного маршрутизатора. Чим вище пріоритет, тим більша ймовірність того, що інтерфейс буде призначений у тракті маршрутизатора.
- **Інтервал (-и) повторної передачі (Retransmit Interval(s))**: Інтервал у секундах між передачами оголошень про стан каналу. Значення за замовчуванням - 5 секунд, допустимий діапазон - від 5 до 3.600 секунд.
- **Затримка (-и) передачі (Transmit delay (s))**: Інтервал у секундах для очікування перед надсиланням пакета оновлення стану каналу. Значення за замовчуванням - 1 секунда, допустимий діапазон - від 1 до 3.600 секунд.
- **Інтервал (и) Hello (Hello interval (s))**: Інтервал у секундах між пакетами Hello, що надсилаються між інтерфейсами з увімкненим OSPF. Значення має бути однаковим для всіх вузлів мережі. Значення за замовчуванням - 10 секунд, допустимий діапазон - від 1 до 65.535 секунд.
- **Інтервал (и) простою (Dead interval (s))**: Таймер бездіяльності сусіднього пристрою. Коли сусідній пристрій був неактивним протягом періоду, що дорівнює або перевищує інтервал простою, стан інтерфейсу встановлюється як вимкнений. Сусідні пристрої, які були неактивними більше доби (24 годин), повністю видаляють. Значення за замовчуванням – 40 секунд, допустимий діапазон - від 2 до 2.147.483.647 секунд.

Залежно від вибраного в цій області Режиму автентифікації потрібно ввести або ключ автентифікації у вигляді відкритого тексту, або ключ дайджесту повідомлення алгоритму хешування MD5.

- **Ключ автентифікації (Authentication key)**: встановіть до 8 символів для автентифікації у вигляді відкритого (незашифрованого) тексту.
- **Ключ дайджесту повідомлення (Message digest key)**: ключ повідомлення, що використовується для автентифікації за допомогою алгоритму хешування MD5, довжиною до 16 символів.
- **Ідентифікатор ключа (Key ID)**: Ідентифікатор ключа автентифікації, що використовується для автентифікації MD5, тому його слід використовувати тільки тоді, коли також налаштовано ключ дайджесту повідомлення. Значення за замовчуванням – 0, допустимий діапазон – від 0 до 255.

16.3 Інтерфейс командного рядка (CLI)

Загальна конфігурація

Команда	Опис	Одиниця	За замовчуванням	Параметр ospfd
`router ospf`	Увімкнути OSPF			
`ospf router-id <ipv4_addr>`	Встановіть ідентифікатор маршрутизатора. Якщо не вказано, буде використана найнижча IP-адреса маршрутизатора.			`router-id`
`ospf timer spf-delay <1-10>`	Встановіть затримку між отриманням зміни до розрахунку SPF.	с	1	`spf-delay`
`ospf timer spf-holdtime <1-5>`	Встановіть затримку між першим та другим розрахунком SPF.	с	5	`spf-holdtime`

Конфігурація інтерфейсу

Команда	Опис	За замовчуванням	Параметр ospfd
`interface vlan <vlan_list>`			

`ospf`
 	
`no ospf`
	Увімкнути OSPF на інтерфейсі.
	
	Вимкнути OSPF на інтерфейсі.		

`ospf area <ipv4_addr>`	Встановити область, на якій працює інтерфейс.		`area`
`ospf cost <1-65535>`	Встановити вартість надсилання пакета через інтерфейс.	10	`metric`
`ospf retransmit-interval <5-3600>`	Встановити кількість секунд між передачами оголошень про стан каналу.	5	`retransmit-interval`

`ospf transmit-delay <1-3600>`
 	
`ospf priority <0-255>`
	Встановити кількість секунд очікування перед надсиланням пакета оновлення стану каналу.
	
	Встановити пріоритет маршрутизатора. Якщо встановлено значення 0, маршрутизатор не відповідає критеріям призначеного маршрутизатора або резервного призначеного маршрутизатора.
		1
		
		1
			`transmit-delay`
			
			`router-priority`

`ospf hello-interval <1-65535>`	Встановити кількість секунд між пакетами-hello, надісланими через інтерфейс OSPF. Значення має бути однаковим для всіх вузлів мережі.	10	`hello-interval`
`ospf dead-interval <2-2147483647>`	Встановити час простою (dead time) маршрутизатора (таймер бездіяльності сусідніх пристроїв). Коли сусідній пристрій був неактивним протягом часу простою маршрутизатора, його стан встановлюється як ВИМКНЕНО (DOWN). Сусідні пристрої, які були неактивними більше 24 годин, повністю видаляються.	40	`router-dead-time`
`ospf authentication-key <string8>`	Встановити ключ автентифікації у вигляді відкритого (незашифрованого) тексту автентифікації.		`auth-key`
`ospf message digest-key <0-255> md5 <string16>`	Встановити ключ автентифікації та його ідентифікатор для автентифікації з використанням хешування MD5.		`auth-md`

Конфігурація області

Команда	Опис	Параметр ospfd
`ospf area <ipv4_addr> authentication [ message-digest ]`	Дозволити захист від несанкціонованого доступу до визначеної області за допомогою ключа автентифікації.	`auth-type`

17 Протокол резервування віртуальних маршрутизаторів (VRRP)

17.1 Основні принципи VRRP

Використання статично налаштованого маршрутизатора за замовчуванням є загальноприйнятим у багатьох мережах, коли IP-адреси з терміналів є фіксованими та добре відомими, оскільки це мінімізує час опрацювання маршрутизації. Проте статична маршрутизація створює єдину точку відмови, і якщо маршрутизатор за замовчуванням стає недоступним, пристрої, які використовують його як свій маршрутизатор першої транзитної ділянки (перший хоп), ізолюються від мережі.
Як визначено стандартом RFC 2338, VRRP призначений для усунення єдиної точки відмови, властивої статичному маршрутизованому середовищу за замовчуванням. Протокол досягає цього шляхом створення декількох віртуальних маршрутизаторів, з яких один є ведучим, а решта – резервними маршрутизаторами. Якщо ведучий маршрутизатор виходить з ладу, один із резервних маршрутизаторів стає новим ведучим маршрутизатором, що забезпечує віртуальну платформу маршрутизації за замовчуванням і дозволяє маршрутизувати трафік по локальній мережі, не покладаючись на один маршрутизатор за замовчуванням.
Перевага, отримана від використання VRRP, полягає у більшій доступності без необхідності налаштування динамічної маршрутизації або протоколів виявлення маршрутизатора на кожному кінцевому хості.

17.2 Конфігурація VRRP

VRRP доступний, тільки якщо на пристрої S20 увімкнено ліцензування Рівня 3. Крім того, тільки VLAN із налаштованою IP-адресою можуть брати участь у групі VRRP, і кожна VLAN може мати тільки одну та ексклюзивну віртуальну IP-адресу. Таким чином, розподіл навантаження VRRP недоступний у S20. Значення пріоритету визначатиме, який маршрутизатор є ведучим, а які маршрутизатори резервними у мережі VRRP.
Конфігурація знаходиться в меню Налаштування> VRRP (Settings > VRRP).

Загальна конфігурація

- **Режим (Mode)**: керує увімкненням або вимкненням функції VRRP;

Інтерфейси

Налаштуйте інтерфейси (пов'язані з VLAN), доступні для маршрутизації VRRP. Зверніть увагу, що у цій конфігурації відображаються лише VLAN із налаштованою IP-адресою (Налаштування> Система> IP) (Settings > System > IP).

- **VLAN**: відображає ідентифікатори VLAN, доступні для використання VRRP;
- **Увімкнути (Enable)**: встановіть прапорець, щоб увімкнути VRRP на даній VLAN;
- **Ідентифікатор віртуального маршрутизатора (Virtual Router ID)**: ідентифікатор групи VRRP, повинен бути ексклюзивним для кожної VLAN. Допустимі значення знаходяться в діапазоні від 0 до 255;
- **Віртуальна IP-адреса (Virtual IP Address)**: віртуальна IP-адреса для вказаної групи VRRP. Ця адреса повинна знаходитися в тій самій підмережі, що і адреса IPv4 інтерфейсу;
- **Довжина маски (Mask Length)**: мережева маска у форматі CIDR. Допустимі значення знаходяться в діапазоні від 1 до 32, за замовчуванням – 24;
- **Пріоритет (Priority)**: рівень пріоритету маршрутизатора в групі VRRP. Кожен маршрутизатор у групі віртуальних маршрутизаторів має певний пріоритет, це число від 1 до 255. Маршрутизатор з найвищим пріоритетом (або найбільшим числом) обирається Ведучим (Master), тоді як усі інші маршрутизатори вважаються резервними (Backup). Значення за замовчуванням – 100;

- **Режим пріоритетного заміщення (Preemption Mode)**: коли увімкнено режим пріоритетного заміщення, ведучий маршрутизатор стає резервним, якщо інший маршрутизатор надійде з вищим пріоритетом;
- **Пароль автентифікації (Authentication Password)**: пароль для текстової автентифікації. Можна вказати до 8 символів;
- **Інтервал (и) оголошення (Advertisement Interval (s))**: Інтервал у секундах між надсиланням пакетів оголошень. Ведучий пристрій VRRP надсилає оголошення VRRP на інші маршрутизатори VRRP з тієї ж групи. Допустимі значення знаходяться в діапазоні від 1 до 255, за замовчуванням 1.

17.3 Інтерфейс командного рядка (CLI)

Загальна конфігурація

Команда	Опис
router vrrp	Увімкнути VRRP
no router vrrp	Вимкнути VRRP

Конфігурація інтерфейсу

Команда	Опис	За замовчуванням	Параметр ospfd
`interface vlan <vlan_list>`	Перелічіть усі доступні інтерфейси VLAN.		
`vrrp`	Увімкнути VRRP на інтерфейсі.		
`no vrrp`	Вимкнути VRRP на інтерфейсі.		
`vrrp <0-255>`	Встановити ідентифікатор групи (ідентифікатор віртуального маршрутизатора).		`serverid`
`vrrp address <ipv4_addr> <1-32>`	Встановити віртуальну IP-адресу та довжину маски для вказаної групи VRRP. Ця адреса повинна бути в тій самій підмережі, що і адреса IPv4 інтерфейсу. Маска мережі повинна бути у форматі CIDR та за замовчуванням значення дорівнює 24.		`addr`
`vrrp priority <1-255>`	Встановити рівень пріоритету маршрутизатора в групі VRRP (ідентифікатор маршрутизатора).	100	`priority`
`vrrp authentication <string8>`	Встановити пароль для автентифікації у вигляді відкритого (незашифрованого) тексту. Текстовий пароль має до восьми буквено-цифрових символів.		`password`

vrrp preempt	Увімкнути пріоритетне заміщення VRRP.	Увімкнено	preempt_mode
vrrp advertisement-interval <1-255>	Встановлює інтервал часу в секундах між надсиланням кадрів оголошення.	1	

18 Сигналізація переходу у безпечний режим

Пристрій Reason S20 містить перелік функцій сигналізації переходу у безпечний режим, які можуть бути записані як подія системного журналу та/або локально керувати спрацюванням світлодіода "Безпечного режиму" (Failsafe) на передній панелі та контакту реле на задній панелі. Функціональні можливості сигналізації переходу у безпечний режим за замовчуванням вимкнені, а меню налаштувань знаходиться в Розширені налаштування> Сигналізація переходу у безпечний режим (Advanced Settings > Failsafe Alarm).
Сигнали переходу у безпечний режим починають працювати через 60 секунд після завантаження обладнання.

Приклади роботи світлодіодів / сигналізації

Як приклад того, як працюють аварійні сигнали безпечного режиму, розглянемо сигнал про відмову живлення. Світлодіод/сигналізація негайно активується, коли виникає відмова, і залежно від конфігурації може залишатися активним або повертатися до неактивного стану, як тільки джерело живлення повертається до нормальної роботи, як показано на прикладах нижче.

Приклад 1: У випадку, якщо параметр збереження вимкнено, і якщо стан відмови триває довше мінімального активного часу, світлодіод/сигналізація залишатиметься активним до тих пір, поки триває відмова.

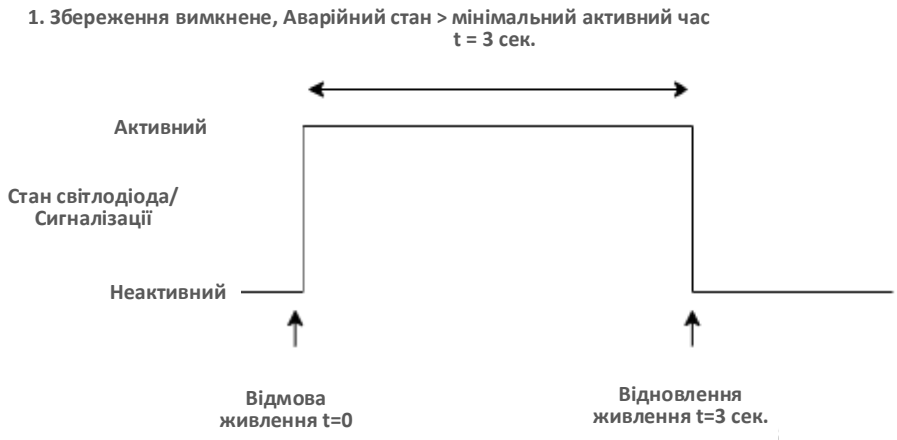


Рис. 68: Приклад 1 роботи світлодіода/сигналізації

Приклад 2: Якщо параметр збереження вимкнено, і відмова триває менше, ніж мінімальний активний час, світлодіод/сигналізація залишатиметься активним, протягом часу, налаштованого як мінімальний активний час.

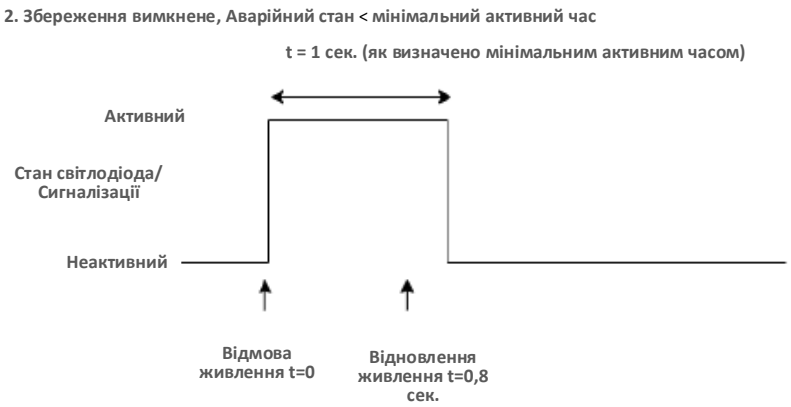


Рис. 69: Приклад 2 роботи світлодіода/сигналізації

Приклад 3: Якщо увімкнено параметр збереження, світлодіод/сигналізація залишатиметься активним до тих пір, поки користувач не натисне кнопку "очистити спрацювання" (знаходиться у Монітор> Сигналізація переходу у безпечний режим (Monitor > Failsafe Alarm)), незалежно від того, чи джерело живлення повертається до нормальної роботи або конфігурації мінімального активного часу .

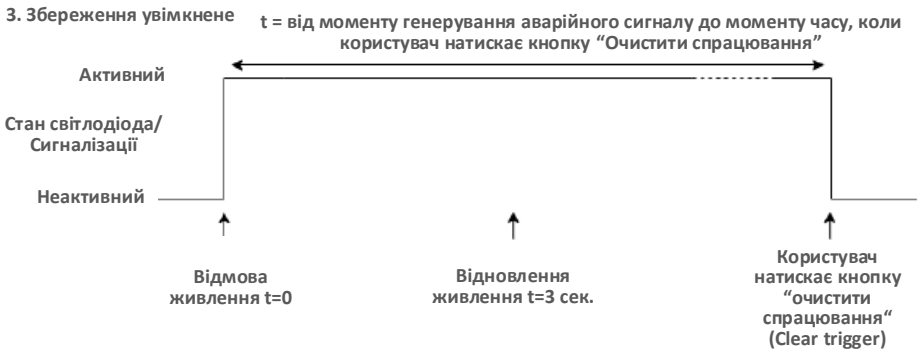


Рис. 70: Приклад 3 роботи світлодіода/сигналізації

Параметри конфігурації

- **Мінімальний активний час (сек) світлодіода та реле (Led & Relay minimum active time (sec))**: Мінімальний час у секундах, протягом якого світлодіод та реле залишаться активними після активації сигналізації.
- **Назва аварійного сигналу (Alarm Name)**: Список подій, які можуть бути записані в системному журналі та/або призводити до спрацювання світлодіода/сигналізації переходу у безпечний режим, щоб локально сигналізувати про подію:
  - **Невідповідна швидкість або dpx (Inconsistent Speed or dpx)**: сигналізує, якщо будь-який робочий порт налаштований на невідповідну швидкість або dpx (напівдуплекс/ повний дуплекс);
  - **Недійсна конфігурація (Invalid configuration)**: сигналізує при завантаженні недійсної конфігурації (у меню Технічне обслуговування > Конфігурація> Завантаження (Maintenance > Configuration > Upload));
  - **Зміна каналу: увімкнений або вимкнений (Link change: up or down)**: сигналізує, якщо будь-який стан каналу порту змінюється з увімкненого на вимкнений або з вимкненого на увімкнений. Це корисно для виявлення втрати будь-якого підключення до порту або підключення до комутатора будь-якого непередбаченого пристрою;
  - **Помилка авторизації MAC-адреси (MAC address authorization failed)**: Цей сигнал спрацьовує, коли таблиця MAC-адрес заповнена, тобто вона вивчила всі можливі записи, не тільки статично, а й динамічно;

- **Порушена безпека порту (Port security violated)**: якщо на порту активовано функцію Контролю обмеження (Limit Control) і межа перевищує налаштоване значення, цей сигнал спрацьовує. Щоб налаштувати контроль обмеження порту, перейдіть у меню Розширені налаштування> Безпека> Мережа> Контроль обмеження (Advanced Settings > Security > Network > Limit Control);
- **Відмова джерела живлення (Power Supply Failure)**: сигналізує про несправність основного або резервного джерела живлення. Якщо Reason S20 має лише одне джерело живлення, цей параметр потрібно вимкнути, інакше безпечний режим сигналізуватиме про відмову живлення, оскільки резервного джерела живлення немає;
- **Отриманий циклічний BPDU (Received looped-back BPDU)**: сигналізує, якщо в архітектурі мережі виявлена петля, як описано у пункті щодо захисту від петель;
- **Температура процесора поза межами діапазону (CPU temperature out of range)**: Цей сигнал спрацьовує, коли температура процесора виходить за межі встановлених значень. Значення встановлюються в градусах Цельсія.
- **Навантаження процесора поза межами діапазону (CPU load out of range)**: Цей сигнал спрацьовує, коли навантаження процесора перевищує встановлене значення. Значення встановлюється у відсотках.
- **Використання оперативної пам'яті вище обмеження (RAM use above the limit)**: Цей сигнал спрацьовує, коли використання оперативної пам'яті перевищує встановлене значення. Значення встановлюється у відсотках.
- **Вилучення модуля X (Module X removal)**: сигналізує, якщо вказаний модуль X був вилучений або не вдалося зв’язатися з головною платою. Модуль 1 складається з портів від 1 до 4, модуль 2 з портів від 5 до 8 і так далі; Примітка: X представляє допустиму кількість модулів, до 5 для моделі S2020 та до 6 для моделі S2024.
- **Вилучення порту X (Port X removal)**: сигналізує про те, що було вилучено трансивер SFP із зазначеного порту X (цей параметр не застосовується до фіксованих портів Ethernet RJ45).
- **Підключення до порту X (Port X link up)**: сигналізує, якщо стан зв'язку Ethernet для даного порту змінюється з вимкненого на увімкнений.
- **Вимкнення порту X (Port X link down)**: сигналізує, якщо стан зв'язку Ethernet для даного порту змінюється з увімкненого на вимкнений.
  Примітка: X – це кількість дійсних портів на комутаторі, до 20 для моделі S2020 та до 24 для моделі S2024.

- **Увімкнено (Enabled)**: встановіть прапорець, щоб увімкнути відповідну функцію;
- **Системний журнал (Syslog)**: встановіть прапорець, щоб записати подію у системному журналі;
- **Рівень (Level)**: щоб вибрати рівень системного журналу, який слід записати. Це може бути: помилка (серйозність 3), попередження (серйозність 4), повідомлення (серйозність 5) або інформація (серйозність 6);
- **Світлодіод/реле (Led/Relay)**: встановіть прапорець, щоб увімкнути локальну сигналізацію за допомогою світлодіода "Безпечного режиму" на передній панелі та реле з сухими контактами на задній панелі;
- **Збереження (Persist)**: Сигнали, позначені як "Збереження", утримуватимуть стан світлодіода/реле активованим доти, доки користувач не здійснить вручну дію при натисканні кнопки "Очистити спрацювання" (Clear Triggered) (знаходиться в Монітор> Сигналізація переходу у безпечний режим (Monitor > Failsafe Alarm)) Вимкнено за замовчуванням.
- **Нижній поріг (Lower Threshold)**: якщо застосовується, нижній поріг визначає найнижчу величину, нижче якої спрацьовує конкретний аварійний сигнал. Допустимі значення: залежить від аварійного сигналу.

- **Верхній поріг (Upper Threshold)**: якщо застосовується, верхній поріг визначає найвищу величину, вище якої спрацьовує конкретний аварійний сигнал. Допустимі значення: залежить від аварійного сигналу.

19 Приклади застосування

19.1 Налаштування VLAN в мережі цифрової підстанції

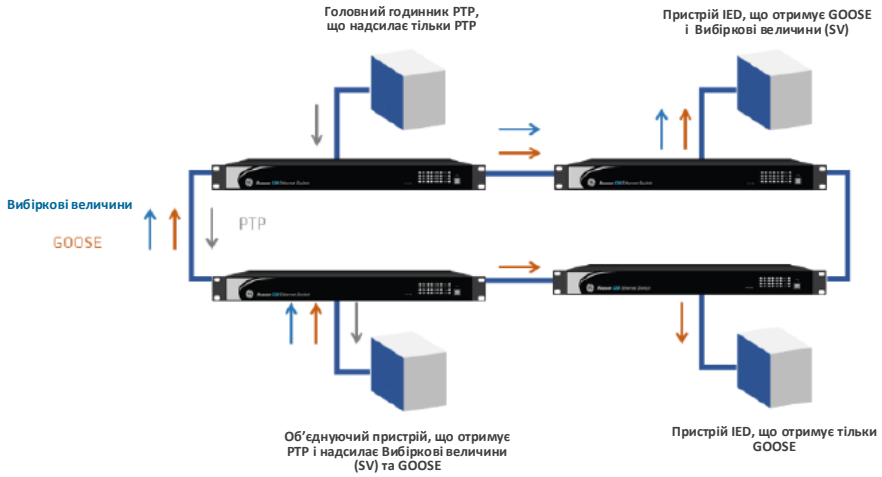


Рис. 71: Топологія, яку потрібно налаштувати у середовищі VLAN

Як практичний приклад, вважається необхідним налаштування VLAN, щоб віртуально розділити різні протоколи, як показано на наведеному вище рисунку, де в мережі присутні Вибіркові величини (Sampled values), повідомлення GOOSE та PTP. Розглянемо наступні припущення:

1. Об'єднуючий пристрій надсилає GOOSE та Вибіркові величини з інформацією про теги VLAN та отримує повідомлення PTP з інформацією про VLAN;
2. Головний годинник PTP (Grandmaster Clock) надсилає інформацію про VLAN у своїх пакетах PTP;
3. Пристрій IED, що отримує GOOSE і Вибіркові величини, може отримувати обидва повідомлення з тегом VLAN;
4. IED, який отримує тільки повідомлення GOOSE, не підтримує VLAN, тому повідомлення GOOSE повинні надходити на це обладнання без інформації про VLAN;
5. Усі використовувані інтерфейси керування обладнанням знаходяться на тому самому порту, що використовується для інших повідомлень, а керування інформаційним обміном (TCP/IP) здійснюється за допомогою нетегованих кадрів;
6. IED, що отримує тільки GOOSE та обладнання Головного годинника PTP, можуть зазнати збою, якщо трафік Вибіркових величин подається на його Ethernet-порт. Інше обладнання має пропускну здатність для обробки трафіку Вибіркових величин, якщо воно є членом VLAN Вибіркових величин;
7. Номер VID GOOSE – 10;
8. Номер VID Вибіркових величин - 20;
9. Номер VID PTP – 30;

Керуюча VLAN, яка буде внутрішньо використовуватися комутатором, буде номером VID. З інформацією, наведеною нижче, можна перейти до меню Налаштування> VLAN (Settings > VLANs), щоб розпочати процес налаштування конфігурації. Конфігурація VLAN повинна бути наступною:

Конфігурація VLAN для Об’єднуючого пристрою

Цей порт буде отримувати нетеговані та теговані кадри та надсилати теговані кадри з багатьох VID, оскільки Об’єднуючі пристрої здійснюватимуть багатоадресну передачу GOOSE та Вибіркових величин та отримуватимуть повідомлення PTP. Крім того, програмне забезпечення для керування буде обмінюватися даними з обладнанням на цьому порту. Таким чином, порти конфігурації Об’єднуючого пристрою повинні мати наступні характеристики:

- **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри будуть перенаправлені до VID VLAN порту, а теговані кадри перенаправляються до VLAN, яка вбудована у кадр;
- **Процес фільтрування на вході (Filtering ingress process)**: цей порт повинен приймати як нетеговані, так і теговані кадри;
- **Процес виходу (Egress process)**: для процесу виходу слід встановити значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (Untag only frames with Port VLAN identifier).

Таким чином, для цього порту може бути рекомендована наступна конфігурація VLAN:

- Режим порту, вибраний як Магістральний порт (Trunk port);
- VLAN порту вибрано як 1;
- Для магістральних портів тип порту не можна змінювати з C-порту (C-Port);
- Для магістральних портів фільтрування на вході не можна змінювати з увімкненого;
- Для магістральних портів прийняття на вході не можна змінювати з тегованих та нетегованих;
- Тегування на виході вибрано як "Знімати теги VLAN порту" (Untag Port VLAN);
- Вибрані дозволені VLAN: 1, 10, 20, 30;
- Заборонені VLAN не налаштовані.

Конфігурація VLAN для інших комутаторів

Цей порт буде отримувати нетеговані та теговані кадри та надсилати теговані та нетеговані кадри з багатьох VID, оскільки весь трафік від комутаторів повинен проходити через ці порти. Таким чином, конфігурація цих портів повинна мати наступні характеристики:

- **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process):** нетеговані кадри будуть перенаправлені до VID VLAN порту, а теговані кадри перенаправляються до VLAN, яка вбудована в кадр;
- **Процес фільтрування на вході (Filtering ingress process):** цей порт повинен приймати як нетеговані, так і теговані кадри;
- **Процес виходу (Egress process):** для процесу виходу слід встановити значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (Untag only frames with Port VLAN identifier).

Таким чином, для цього порту може бути рекомендована наступна конфігурація VLAN:

- Режим порту, вибраний як Магістральний порт (Trunk port);
- VLAN порту вибрано як 1;
- Для магістральних портів тип порту не можна змінювати з C-порту (C-Port);
- Для магістральних портів фільтрування на вході не можна змінювати з увімкненого;
- Для магістральних портів прийняття на вході не можна змінювати з тегованих та нетегованих;
- Тегування на виході вибрано як "Знімати теги VLAN порту" (Untag Port VLAN);
- Вибрані дозволені VLAN: 1, 10, 20, 30;
- Заборонені VLAN не налаштовані.

Конфігурація VLAN для головного годинника PTP

Цей порт буде отримувати нетеговані кадри та надсилати нетеговані та теговані кадри з VID PTP, оскільки головний годинник (Grandmaster Clock) буде передавати повідомлення PTP за допомогою багатоадресної передачі. Крім того, програмне забезпечення для керування буде обмінюватися даними з обладнанням на цьому порту. Таким чином, порти конфігурації Головного годинника PTP повинні мати наступні характеристики:

- **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри будуть перенаправлені до VID VLAN порту, а теговані кадри перенаправляються до VLAN, яка вбудована у кадр;
- **Процес фільтрування на вході (Filtering ingress process)**: цей порт повинен приймати нетеговані кадри;
- **Процес виходу (Egress process)**: для процесу виходу слід встановити значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (Untag only frames with Port VLAN identifier).

Таким чином, для цього порту може бути рекомендована наступна конфігурація VLAN:

- Режим порту, вибраний як Магістральний порт (Trunk port);
- VLAN порту вибрано як 1;
- Для магістральних портів тип порту не можна змінювати з C-порту (C-Port);
- Для магістральних портів фільтрування на вході не можна змінювати з увімкненого;
- Для магістральних портів прийняття на вході не можна змінювати з тегованих та нетегованих;
- Тегування на виході вибрано як "Знімати теги VLAN порту" (Untag Port VLAN);
- Вибрані дозволені VLAN: 1, 30;
- Вибрані заборонені VLAN: 10, 20.

Конфігурація VLAN для пристроїв IED, які отримують GOOSE та Вибіркові величини (SV)

Цей порт отримуватиме нетеговані та теговані кадри та надсилатиме нетеговані кадри, що використовуються тільки для зв'язку з програмним забезпеченням для керування. Таким чином, порти конфігурації IED, що отримує GOOSE та Вибіркові величини, повинні мати наступні характеристики:

- **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри будуть перенаправлені до VID VLAN порту, а теговані кадри не очікуються. Таким чином, теговані кадри можуть бути перенаправлені до VLAN, що вбудована у кадр.
- **Процес фільтрування на вході (Filtering ingress process)**: цей порт повинен приймати як нетеговані, так і теговані кадри;
- **Процес виходу (Egress process)**: для процесу виходу слід встановити значення "Знімати теги тільки з кадрів з ідентифікатором VLAN порту" (Untag only frames with Port VLAN identifier).

Таким чином, для цього порту може бути рекомендована наступна конфігурація VLAN:

- Режим порту, вибраний як Магістральний порт (Trunk port);
- VLAN порту вибрано як 1;
- Для магістральних портів тип порту не можна змінювати з C-порту (C-Port);
- Для магістральних портів фільтрування на вході не можна змінювати з увімкненого;
- Для магістральних портів прийняття на вході не можна змінювати з тегованих та нетегованих;
- Тегування на виході вибрано як "Знімати теги VLAN порту" (Untag Port VLAN);
- Вибрані дозволені VLAN: 1, 10, 20;
- Заборонені VLAN не налаштовані.

Конфігурація VLAN для пристроїв IED, які отримують тільки GOOSE

Цей порт отримуватиме нетеговані та теговані кадри та надсилатиме нетеговані кадри, що використовуються тільки для зв'язку з програмним забезпеченням для керування. Таким чином, порти конфігурації IED, що отримує тільки GOOSE, повинні мати наступні характеристики:

- **Процес входу ідентифікатора VLAN (VLAN Identifier Ingress process)**: нетеговані кадри будуть перенаправлені до VID VLAN порту, а теговані не очікуються. Таким чином, теговані кадри можуть бути перенаправлені до VLAN, що вбудована у кадр.
- **Процес фільтрування на вході (Filtering ingress process)**: цей порт повинен приймати як нетеговані, так і теговані кадри, але на цьому порту є критична точка для повідомлень Вибіркових величин. Таким чином, бажано встановити VLAN Вибіркових величин як заборонену;
- **Процес виходу (Egress process)**: для процесу виходу слід встановити значення "Знімати теги з усіх кадрів" (Untag all frames), оскільки це обладнання не розуміє інформацію VLAN.

Таким чином, для цього порту може бути рекомендована наступна конфігурація VLAN:

- Режим порту, вибраний як Гібридний порт (Hybrid port);
- VLAN порту вибрано як 1;
- Тип порту вибрано як C-порт (C-Port);
- Фільтрування на вході вимкнено;
- Прийняття на вході вибрано як Теговані та Нетеговані;
- Тегування на виході вибрано як "Знімати теги з усіх кадрів" (Untag all);
- Вибрані дозволені VLAN: 1, 10;
- Вибрані заборонені VLAN: 20.

Цих налаштувань конфігурації VLAN має бути достатньо, щоб гарантувати, що їх отримає тільки обладнання, яке очікує отримати певний трафік. Крім того, розділення (сегрегація) трафіку підвищить надійність мережі, оскільки перевантаження однієї VLAN не вплине на інші.

19.2 Налаштування RSTP у кільцевій топології мережі

Розглядаючи той самий випадок, що і у попередньому прикладі, у цьому пункті на практиці продемонстровано, як налаштувати RSTP у кільцевій топології мережі.

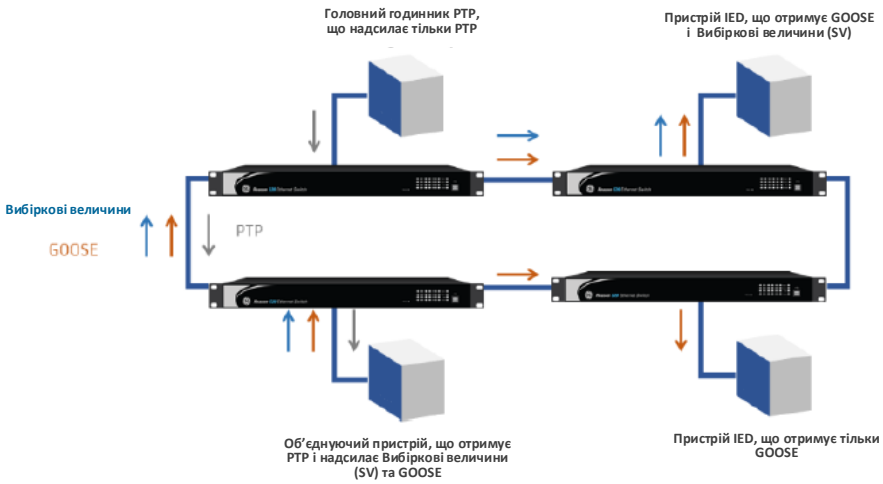


Рис. 72: Топологія, яку потрібно налаштувати в середовищі RSTP

У цій топології всі комутатори вважаються комутаторами, що підтримують RSTP, тобто всі комутатори можуть брати участь у виборах Кореневого комутатора (Root) і використовувати його значення для логічної архітектури.
Reason S20 підтримує наступні протоколи кістякового дерева: STP, RSTP та MSTP. За замовчуванням протокол MSTP встановлено як протокол для вирішення проблеми петель у мережі. Для цих варіантів застосування немає жодної основної конфігурації, яку потрібно виконати, крім зміни версії протоколу на RSTP, оскільки конфігурація за замовчуванням готова надсилати та отримувати пакети BPDU, а потім використовувати їх для вирішення проблеми петель у мережі. Параметри за замовчуванням наступні:

- Налаштування мосту:
  - Протокол, що використовується – MSTP;
  - Пріоритет мосту – 32768;
  - Затримка пересилання – 15;
  - Максимальний строк зберігання - 20 років;
  - Максимальна кількість хопів – 20.
- Налаштування портів:
  - Використання STP на всіх портах увімкнено;
  - Вартість тракту на всіх портах є автоматичною;
  - Пріоритет усіх портів – 128;
  - Усі порти налаштовані як автоматично-граничні (Auto-edge);
  - Усі порти налаштовані щодо з'єднання "точка-точка" як "Автоматичні" (Auto);

Для архітектури, наведеної вище, всі комутатори підтримують STP, тому функція безпеки BPDU не потрібна.
З інформацією, наведеною вище, можна перейти до меню Налаштування > Кістякове дерево > Налаштування мосту (Settings > Spanning Tree > Bridge Settings), щоб розпочати процес налаштування конфігурації.
У цій ситуації єдиною конфігурацією, яку потрібно виконати, є зміна версії протоколу на RSTP. Сам протокол вибере кореневий міст, призначений, кореневий, альтернативний та резервний порти, і може вирішувати проблеми, пов'язані з петлями в мережі в середовищі RSTP.
Якщо є один конкретний міст, який бажано зробити кореневим, виберіть найнижче число пріоритету мосту для цього мосту, після чого буде виконано конфігурацію. Повторіть ці дії на всіх комутаторах у топології, і після того, як усі вони будуть налаштовані, налаштування базового використання RSTP буде завершено.

19.3 Прозорий годинник PTP

Розглядаючи той самий випадок, що і у попередньому прикладі, у цьому пункті на практиці продемонстровано, як налаштувати Reason S20 як Прозорий годинник PTP у кільцевій топології мережі.

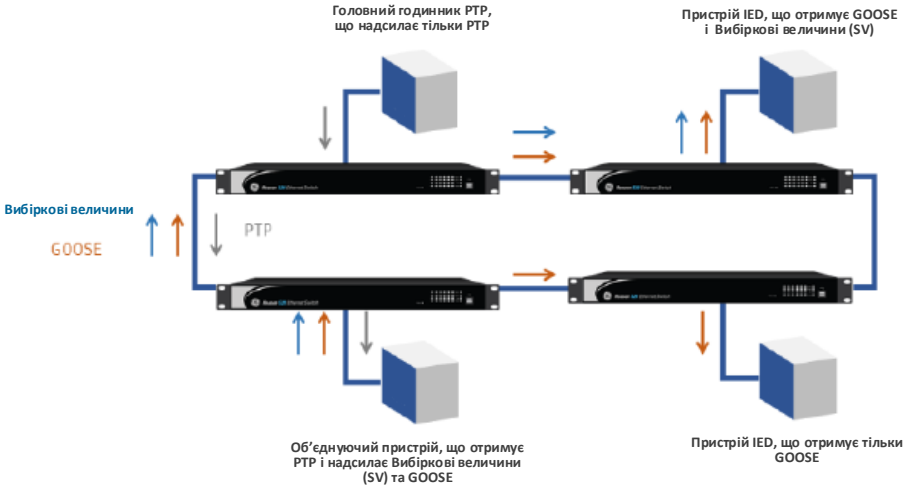


Рис. 73: Топологія, яку потрібно налаштувати в середовищі PTP

Конфігурація PTP у мережі VLAN

Першим кроком буде перевірити інформацію PTP, яку надає Головний годинник PTP (PTP Grandmaster Clock). У цьому випадку припустимо, що головний годинник налаштований наступним чином:

- Домен 0;
- Передається через Ethernet з VID 30 і PCP 4;
- Режим роботи двоступеневий;
- Механізм затримки – це механізм вимірювання затримок між рівноправними вузлами (Peer-to-peer).

У цій ситуації переконайтеся, що VLAN 30 створено, а порти, які повинні бути членами VLAN PTP, правильно налаштовані в меню Налаштування> VLAN (Settings > VLANs). За потреби перший приклад цього пункту може бути використаний, щоб допомогти вам налаштувати VLAN у Reason S20.

Повертаючись до конфігурації PTP, необхідно створити екземпляр, який буде використовуватися як прозорий годинник P2P.

- **Режим (Mode)**: прозорий годинник;
- **Профіль (Profile)**: користувацький;
- **Номер домену (Domain Number)**: 0;
- **Мережевий протокол (Network Protocol)**: Ethernet;
- **VLAN**: увімкнено;
- **Ідентифікатор VLAN (VLAN ID)**: 30;
- **Пріоритет VLAN (VLAN Priority)**: 4;
- **Механізм затримки (Delay Mechanism)**: Механізм вимірювання затримок між рівноправними вузлами (Peer-to-peer);
- **Інтервал затримки запиту та інтервал/час очікування оголошення (Delay Request Interval та Announce Interval/Timeout)** можуть бути налаштовані як специфікація мережі PTP. Рекомендовані значення за замовчуванням.

Загальна конфігурація PTP, яка залишилася, не залежить від режиму прозорого годинника. Після виконання загальних налаштувань PTP, встановіть прапорці у Конфігурації портів PTP (PTP Port Configuration), що визначити, які порти будуть членами екземпляра PTP. У наведеному прикладі портами, які повинні знаходитись в одному екземплярі параметрів, є:

- Порт, на якому підключений головний годинник PTP (PTP Grandmaster Clock);
- Порт, на якому наявні з'єднання між комутаторами;
- Порт, на якому підключені ведені годинники PTP. У цьому прикладі порт, до якого підключений Об'єднуючий пристрій.

Повторіть ці кроки на всіх комутаторах, які працюють як Прозорі годинники (Transparent Clock). У цьому прикладі всі комутатори повинні бути налаштовані, як показано, а порти, що з'єднують між собою комутатори та годинники PTP, повинні бути відмічені прапорцями як члени екземпляра мережі.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 6: Контроль за допомогою веб-інтерфейсу

У цьому розділі міститься огляд щодо контролю функцій, що належать до меню Налаштування (Settings), коли доступ до обладнання здійснюється за допомогою веб-інтерфейсу.

1 Керування системою

Меню системи містить онлайн-інформацію про меню системи, завантаження процесора, стану IP, журналу та детального системного журналу.
Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Інформація

Інформація про систему представляє основну інформацію про комутатор.

- Система:
  - Контакт системи;
  - Ім'я контакту системи;
  - Розташування системи.
- Ключ:
  - Номер ключа, що означає номер активації ключа;
  - PTP дозволений. Якщо "1", функція PTP увімкнена, а якщо "0", функція PTP вимкнена.
- Апаратне забезпечення:
  - Номер MAC-адреси комутатора;
  - Серійний номер комутатора;
- Час:
  - Системна дата у форматі "YYYY-MM-DDTHH:MM:SS-Часовий пояс";
  - Час роботи системи, що означає час після останнього увімкнення;
- Програмне забезпечення
  - Версія програмного забезпечення, яка є поточною прошивкою, запущеною на комутаторі;
  - Дата програмного забезпечення;
  - Підтвердження, де посилання "Відомості" (Details) відображає всі відкриті вихідні коди, що використовуються комутатором.

Завантаження процесора

Параметр Завантаження процесора (CPU Load) дозволяє користувачеві графічно переглядати використання процесора комутатора у режимі онлайн. Графік має шкали 25%, 50% і 75% відсотків для інформування користувача про завантаження процесора, і графік оновлюється з веб-сторінкою. Таким чином, для онлайн-моніторингу слід встановити прапорець "Автоматичного оновлення" (Auto Refresh) у верхній частині веб-сторінки. Час збільшується зліва направо.

Зелена лінія вказує на середнє завантаження процесора за 100 мс, блакитна – середнє завантаження процесора за 1 секунду, а пурпурова – середнє завантаження центрального процесора за 10 секунд.

Стан IP

Ця сторінка відображає стан рівня протоколу IP. Стан визначається IP-інтерфейсами, IP-маршрутами та станом кешу сусідніх пристроїв (кеш ARP).

- IP-інтерфейси: показує IP-адреси інтерфейсів керування.
  - Інтерфейс VLAN. Якщо внутрішній інтерфейс, відображається текст "OS: Io";
  - Тип інтерфейсу, тобто тип та версія протоколу;
  - Адреса інтерфейсу;
  - Стан інтерфейсу.
- IP-маршрути: показує IP-маршрути
  - Тип: тип протоколу маршрутизації;
  - Мережа: IP-мережа призначення або адреса хосту цього маршруту;
  - Шлюз: адреса шлюзу маршруту;
  - Стан: прапорці стану маршруту.
- Кеш сусідніх пристроїв: використовуваний кеш ARP.
  - IP-адреса сусідніх пристроїв;
  - Адреса каналу сусідніх пристроїв, тобто сусідніх VLAN та MAC-адрес.

Системний журнал

Параметр моніторингу системного журналу дозволяє користувачеві переглядати повідомлення журналу обладнання за допомогою веб-інтерфейсу. Ці повідомлення – це не всі повідомлення, що внутрішньо використовуються обладнанням, проте ці повідомлення журналу дозволяється надсилати на сервер системних журналів.
Можна вибрати рівень для відображення повідомлень журналу. Допустимі рівні – це повідомлення про помилки, попередження, сповіщення та інформаційні повідомлення (Error, Warning, Notice та Informational messages). Якщо бажано відображати всі повідомлення, виберіть опцію Усі (All). Повідомлення журналу накопичуються з плином часу, отже, повідомлення з нижчими числами ідентифікаторів є старішими повідомленнями журналу. Ідентифікатор журналу – це посилання, яке при натисканні відображає безпосередньо меню Детального журналу вибраного ідентифікатора.
Щоб видалити журнальні повідомлення з пам'яті, кнопка "Очистити" (Clear) дозволяє користувачеві видалити збережені повідомлення журналу. Ліва та права кнопки перемикають відображувані сторінки. За замовчуванням на сторінці відображається 20 повідомлень журналу.
Наявна наступна інформація:

- Ідентифікатор повідомлення журналу;
- Рівень повідомлення журналу, відповідно до його інформації;
- Позначка часу повідомлення журналу на основі внутрішнього годинника комутатора;
- Опис повідомлення.

Детальний журнал

Параметр моніторингу Детального журналу дозволяє користувачеві переглядати детальну інформацію для даного ідентифікатора (ID) повідомлення журналу. Доступ до цього меню можна отримати, натиснувши номер ID повідомлення журналу у меню "Журнал" (Log).
У верхній частині веб-сторінки можна ввести ID повідомлення журналу, яке потрібне. Коли є дійсний ідентифікатор, відображається наступна інформація для кожного журналу:

- Рівень повідомлення журналу;

- Позначка часу повідомлення журналу на основі внутрішнього годинника комутатора;
- Опис повідомлення, тобто повідомлення, яке містить цей запис.

2 Порти

Це меню забезпечує онлайн-моніторинг щодо стану, перегляду трафіку, статистики QoS, стану QCL та детальної статистики по кожному порту.
Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Стан

Параметр "Стан" (State) дозволяє користувачеві переглядати основну інформацію про кожний порт. Кожний можливий тип порту представлений на рисунку, тобто на рисунках показано, чи тип порту – роз'єм ST, роз'єм LC або роз'єм RJ45, як показано нижче:


Відображення роз'єму RJ45 у веб-інтерфейсі;


Відображення роз'єму LC SFP у веб-інтерфейсі;


Відображення роз’єму RJ45 SFP у веб-інтерфейсі;

Крім цього відображається стан порту:

Порт вимкнений;

Порт увімкнений і підключений, тобто з підключеним каналом та зв’язком;

Порт увімкнено і не підключено, тобто без підключення або зв'язку;

Перегляд трафіку

Параметр перегляду трафіку (Traffic Overview) дозволяє користувачеві переглядати основну інформацію про трафік даних. На екрані відображається таблиця, що містить наступну інформацію:

- Номер порту;
  - Цей номер – це посилання, яке переадресовує на меню детальної статистики, пояснене в меню "Детальна статистика" (Detailed Statistics).
- Пакети: Отриманий та переданий трафік, у кількості пакетів;
- Байти: Отриманий та переданий трафік, у байтах;
- Помилка: Отримані пакети, що містять помилки, і неповні передані пакети;
- Відкинуті: Отримані пакети, які були відкинуті внаслідок перевантаження на вході та передані пакети, які були відкинуті внаслідок перевантаження на виході.
- Відфільтровані: отримані кадри, відфільтровані у процесі пересилання.

Статистика QoS

Параметр "Статистика QoS" (QoS Statistics) представляє основну інформацію про QoS, що виконується на кожному порту, як описано нижче:

- Ідентифікатор порту;
- Черги (черги від Q0 до Q7): отримані (RX) та передані (TX) кадри в черзі;

Стан QCL

Параметр "Стан QCL" (QCL Status) дозволяє користувачеві переглядати інформацію про Список керування QoS (QCL), налаштований на комутаторі. Відображається таблиця, що містить наступну інформацію:

- Користувач;
- Ідентифікатор QCE;
- Порти-члени QCL;
- Тип кадру, налаштований в QCL;
- Дія, виконана цим QCL, коли вхідні кадри відповідають фільтру QCL. У стовпцях дії відображається інформація про значення CoS, DPL та DSCP;
- Конфліктна інформація, тобто якщо в QCE був конфлікт на представленому QCL.

Детальна статистика

Параметр "Детальна статистика" (Detailed Statistics) дозволяє користувачеві переглядати детальну інформацію про трафік для даного порту. Доступ до цього меню можна отримати, натиснувши на номер порту в меню "Перегляд трафіку" (Traffic Overview).

У верхній частині веб-сторінки можна вибрати, який порт потрібен. Інформація наведена нижче:

- Загальна кількість отриманих кадрів на цьому порту, включаючи помилкові кадри. Ця інформація розподіляється на всі пакети, усі октети, усі одноадресні передачі, усі багатоадресні передачі, всі широкомовні передачі та всі отримані кадри-паузи;
- Загальна кількість переданих кадрів на цьому порту, включаючи помилкові кадри. Ця інформація розподіляється на всі пакети, усі октети, усі одноадресні передачі, усі багатоадресні передачі, всі широкомовні передачі та всі отримані кадри паузи;
- Лічильник розміру загальної кількості отриманих кадрів, який представляє всі кадри, поділені за розміром. Показані значення складають 64-байтові кадри до 1527 і вище кадрів;
- Лічильник розміру загальної кількості переданих кадрів, який представляє всі кадри, поділені за розміром. Показані значення складають 64-байтові кадри до 1527 і вище кадрів;
- Лічильники загальної кількості отриманих черг, у пакетах.
- Лічильники загальної кількості переданих черг, у пакетах.
- Лічильники загальної кількості отриманих помилок у пакетах, розділені на: Відкинуті, CRC/Узгодження, Неповного розміру, Надлишкового розміру, Фрагменти, Незмістовні та Відфільтровані (Drop, CRC / Alignment, Undersize, Oversize, Fragments, Jabber і Filtered).
- Лічильники загальної кількості переданих помилок у пакетах, розділені на: Відкинуті, CRC/Узгодження, Менші номінального, Більші номінального, Фрагменти, Незмістовні та Відфільтровані.

3 Безпека

Цей пункт описує основні можливості онлайн-моніторингу безпеки на пристрої Reason S20, такі як Статистика керування доступом, Мережа, AAA (автентифікація, авторизація та керування обліковими записами) та RMON.

Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Статистика керування доступом

Параметр "Статистика управління доступом" (Access Management Statistics) дозволяє користувачеві переглядати основну інформацію про трафік даних (отримані, дозволені та відкинуті пакети), розділений за інтерфейсними протоколами (HTTP, HTTPS, TELNET та SSH). Крім того, це меню також надає інформацію про трафік SNMP (отримані, дозволені та відкинуті пакети SNMP).

Мережа

Параметр "Мережа" (Network) представляє інформацію про мережу, до якої підключений комутатор.

- Безпека порту (Port Security): забезпечує інформацію про стан безпеки порту. Безпека портів – це модуль, який не має певної прямої конфігурації; оскільки це набір конфігурації, виконаний на комутаторі. Інформація, показана в цьому меню, включає стан порту (користувачів, стан та MAC-адреси) та детальну інформацію про порти (MAC-адреса на даному порту, ідентифікатор VLAN, час з моменту введення даної MAC-адреси у таблицю MAC-адрес, тощо);
- NAS: якщо сервер NAS доступний і використовується, меню NAS надає таку інформацію як стан адміністратора та порту та детальний опис порту.
- Стан ACL (ACL Status): при використанні Списку керування доступом (ACL) у цьому меню представлена інформація про користувача ACL, ідентифікатор запису керування доступом (ACE), тип кадру, дію, обмежувач швидкості, центральний процесор, лічильник та конфлікт на певному ACL;
- ARP-перевірка (ARP inspection): забезпечує інформацію про таблицю динамічної ARP-перевірки. Показані значення – номер порту, ідентифікатор VLAN, MAC-адреса та IP-адреса даного номера порту, що бере участь у функції перевірки ARP;
- Безпека IP джерела (IP Source Guard): забезпечує інформацію про таблицю безпеки IP джерела, таку як номер порту, ідентифікатор VLAN, IP-адресу та MAC-адресу даного номера порту, що бере участь у функції IP Source Guard.

AAA

Параметр AAA (автентифікація, авторизація та керування обліковими записами) дозволяє користувачеві переглядати інформацію про RADIUS-сервер для віддаленої автентифікації користувачів. Інформація представлена наступним чином:

- Перегляд Radius (Radius Overview): показує основну інформацію про функцію RADIUS на комутаторі, таку як ідентифікатор номера RADIUS-сервера, IP-адресу сервера, UDP-порт автентифікації, стан автентифікації для даного сервера (Вимкнено, Не готово, Готово або Не відповідає (Disabled, Not Ready, Ready or Dead) (кількість секунд, що залишились)), UDP-порт керування обліковими даними та стан функції керування обліковими даними (Вимкнено, Не готово, Готово або Не відповідає (кількість секунд, що залишились));
- Деталі Radius (Radius Details): відображає деталі RADIUS AAA для кожного сервера. Відображається статистика автентифікації та керування отриманими та переданими обліковими даними, IP-адреса, стан (Вимкнено, Не готово, Готово або Не відповідає, включаючи кількість секунд, що залишилися) та час на передачу та підтвердження прийому обраним сервером.

Комутатор

Параметр "Комутатор" (Switch) дозволяє користувачеві переглядати інформацію про RMON-сервер при використанні RMON. Інформація наведена нижче:

- Статистика (Statistics): показує статистичну інформацію про функцію моніторингу RMON, таку як індекс записів статистики, джерело даних (ідентифікатор порту, який слід контролювати), відкидання пакетів, загальна кількість даних в октетах, загальна кількість даних у пакетах, дані адрес широкомовної передачі, дані адрес багатоадресної передачі, пакети помилок CRC, виявлені пакети неповного розміру, виявлені пакети надлишкового розміру, виявлені фрагментовані пакети,

кадри розміром більше 64 байт, отримані з недійсним CRC, найкраща оцінка кількості виявлених колізій (конфліктів), загальна кількість отриманих пакетів довжиною 64 байти, загальна кількість отриманих кадрів розміром від 65 до 127 байтів, загальна кількість кадрів, отриманих розміром від 128 до 255 байтів, загальна кількість кадрів, отриманих розміром від 256 до 511 байтів, загальна кількість кадрів, отриманих розміром від 512 до 1023 байтів, і загальна кількість кадрів, отриманих розміром від 1024 до 1588 байтів;

- Історія (History): показує перегляд історії записів RMON, таких як індекс записів історії, індекс записів даних, початок записів даних, відкинуті пакети, загальна кількість даних в октетах, загальна кількість даних у пакетах, дані адрес широкомовної передачі, дані адрес багатоадресної передачі, пакети з помилками CRC, виявлені пакети неповного розміру, виявлені пакети надлишкового розміру, виявлені фрагментовані пакети та оцінка використання фізичного рівня мережі;
- Сигналізація (Alarm): показує перегляд записів сигналізації RMON, таких як номер індексу аварійного сигналу, інтервал для вибірки та порівняння порогових значень, змінні величини для вибірки, тип вибірки, статистичні величини за останній період вибірки, сигналізація при запуску, зростання порогового значення, зростання індексу подій, зниження порогового значення та зниження індексу подій;
- Подія (Event): показує перегляд таблиці подій RMON, наприклад, номер індексу події, індекс запису журналу, позначку часу даної події журналу та опис події журналу.

4 Протокол керування агрегуванням каналів (LACP)

У цьому пункті описано онлайн-інформацію про функціональні можливості агрегування, представляючи стан системи, стан портів та статистику портів (System Status, Port Status та Port Statistics), які знаходяться в меню LACP.
Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Стан системи

Параметр контролю стану системи LACP дозволяє користувачеві переглядати основну інформацію про поточне використання агрегування.

- Aggr ID є ідентифікатором агрегування показаного екземпляра;
- Ідентифікатор системи-партнера, що є MAC-адресою (ідентифікатором системи) партнера з агрегування;
- Ключ партнера, який є ключем, що використовується в цьому екземплярі агрегування;
- Пріоритет партнера;
- Востаннє змінено, це останній раз, коли кожен екземпляр змінювався;
- Локальні порти, представляє ідентифікатор комутатора та номер порту, розділені один від одного символом ":".

Стан портів

Параметр стану LACP дозволяє користувачеві переглядати інформацію про поточне використання LACP на кожному порту. У той час як Стан системи надає інформацію про екземпляри агрегування на даному обладнанні, Стан портів дозволяє перевіряти онлайн-стан використання агрегування. Інформація наведена нижче:

- Номер порту;
- Інформація LACP для цього порту:
  - Так, це означає, що LACP увімкнено та канал підключений;
  - Ні, це означає, що LACP вимкнено або канал відключений;

  - Резервний порт означає невикористаний порт при агрегуванні, але дозволений і, який може приєднатися до групи агрегування, якщо один із агрегованих портів покине групу.
- Ключ, призначений на порту;
- Ідентифікатор агрегування;
- Ідентифікатор системи-партнера, що є MAC-адресою (ідентифікатором системи) партнера агрегування;
- Порт партнера;
- Пріоритет партнера.

Статистика портів

Статистика портів LACP представляє інформацію про повідомлення LACP, якими обмінюються партнери. Це меню дозволяє перевірити, чи є повідомлення LACP, отримані, передані та відкинуті обладнанням. Інформація представлена наступним чином:

- Номер порту;
- Загальна кількість отриманих повідомлень LACP на кожен порт, представлена у кадрах;
- Загальна кількість переданих повідомлень LACP на кожен порт, представлена у кадрах;
- Загальна кількість відкинутих повідомлень LACP на кожен порт, представлена у кадрах. Відкинуті кадри відображаються розділеними на невідомі та заборонені відкинуті кадри.

5 Захист від утворення петель

У цьому пункті описані можливості моніторингу стосовно захисту від утворення петель за допомогою веб-інтерфейсу у Reason S20.
Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Захист від утворення петель

Параметр "Моніторингу стану захисту від утворення петель" (Loop Protection Status monitoring) дозволяє користувачеві переглядати основну інформацію про захист від утворення петель, що працює в Reason S20. Дозволена наступна інформація:

- Номер порту;
- Дією, налаштованою на виконання в інтерфейсі при виявленні петлі, може бути "Вимкнення", "Здійснення запису в системному журналі" та "Вимкнення + Здійснення запису в системному журналі" (Shutdown, Log та Shutdown + Log);
- Передача (Transmit), що вказує, чи увімкнено надсилання повідомлень по мережі, або ні;
- Петлі (Loops), що представляє загальну кількість петель, виявлених на порту з моменту ввімкнення функції;
- Стан (Status), що представляє стан виявлення петель на даному порту. Дозволеними значеннями є "Увімкнено" та "Вимкнено", де "Увімкнено" – активний канал, а "Вимкнено" – неактивний канал. Якщо канал вимкнено через виявлену петлю, позначка часу останньої виявленої петлі відображається в наступному стовпці;
- Час останньої петлі (Time of Last Loop), який представляє позначку часу останньої виявленої петлі. Позначка часу, показана у цьому стовпці, базується на внутрішньому годиннику системи.

6 Контроль параметрів кістякового дерева

У цьому пункті описуються можливості моніторингу стосовно функції кістякового дерева, такі як стан мосту, стан порту та статистика портів (Bridge Status, Port Status та Port Statistics).

Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Стан мосту

Параметр Стан мосту (Bridge Status) дозволяє користувачеві переглядати основну інформацію про налаштовані значення кістякового дерева на мосту та поточну інформацію про топологію.

- MSTI, що представляє екземпляр мосту. Якщо MSTP не використовується, відображається тільки CIST. Представлене ім'я MSTI – це також посилання, що спрямовує до меню Стану мосту STP. Якщо здійснюється доступ до посилання MSTI, дозволена наступна інформація:
  - Стан мосту STP (STP Bridge Status): ця таблиця містить детальну інформацію про поточний стан STP на мосту. Дозволена інформація в таблиці є наступною:
    - Екземпляр мосту;
    - Ідентифікатор мосту, тобто ідентифікаційний номер мосту, у форматі "Пріоритет.Міст-MAC-адреса" (Priority.Bridge-MAC-Address);
    - Ідентифікатор кореневого пристрою, тобто ідентифікаційний номер кореневого мосту, у форматі "Пріоритет.Міст-MAC-адреса";
    - Вартість маршруту до кореневого пристрою, який є вартістю тракту від поточного мосту до кореневого мосту;
    - Кореневий порт, який є поточним портом, що працює як кореневий порт;
    - Регіональний кореневий пристрій, тобто регіональний кореневий пристрій MSTP у екземплярі, який перевіряється;
    - Внутрішня вартість маршруту до кореневого пристрою;
    - Прапорець топології, тобто поточне значення прапорця змін у цьому екземплярі;
    - Кількість змін топології, тобто всі повідомлення про зміну топології, отримані в екземплярі;
    - Остання зміна топології, що представляє останній час, коли у вибраному екземплярі змінювалась топологія;
  - Таблиця портів CIST та стану агрегування, де відображається інформація про порти STP. Допустимі наступні значення:
    - Номер порту, вказаний у рядку. У цій таблиці показані тільки порти, на яких запущений обмін BPDU у мережі;
    - Ідентифікатор порту, тобто ідентифікаційний номер порту, у форматі "Порт- Пріоритет.Міст-Порт-Номер" (Port-Priority.Bridge-Port-Number);
    - Роль на порту, тобто стан порту кістякового дерева. Ролями можуть бути Кореневий порт, Призначений порт, Альтернативний порт та Резервний порт (RootPort, DesignatedPort, AlternatePort і BackupPort);
    - Стан порту, який може бути пересиланням або відкиданням;
    - Вартість тракту порту, тобто вартість тракту, що використовується цим портом при передачі пакетів BPDU у мережі;

  - Граничний (Edge), тобто чи порт є граничним портом або ні. Дозволеними значеннями є "Так" чи "Ні" (Yes або No). "Так" означає, що порт є граничним портом, а "Ні" означає, що порт – це магістральний порт (не граничний);
  - Точка-точка (Point-to-Point), тобто, якщо зв'язок порту – це точка-точка або середовище спільного каналу;
  - Час безперебійної роботи, який представляє час, протягом якого порт активний.
- Ідентифікатор мосту, тобто ідентифікаційний номер мосту, у форматі "Пріоритет.Міст-MAC-адреса" (Priority.Bridge-MAC-Address);
- Ідентифікатор кореневого пристрою, тобто ідентифікаційний номер кореневого мосту, у форматі "Пріоритет.Міст-MAC-адреса";
- Кореневий порт, який є поточним портом, що працює як кореневий порт;
- Вартість маршруту до кореневого пристрою;
- Прапорець топології, тобто поточне значення прапорця змін у цьому екземплярі;
- Остання зміна топології, що представляє останній час, коли у вибраному екземплярі змінювалась топологія;

Стан порту

Параметр моніторингу стану порту STP дозволяє користувачеві переглядати основну інформацію про всі порти на комутаторі, що стосуються кістякового дерева.

- Номер порту, показаний у рядку;
- Роль CIST на порту, тобто стан порту кістякового дерева. Ролями можуть бути Кореневий порт, Призначений порт, Альтернативний порт, Резервний порт та Вимкнено (RootPort, DesignatedPort, AlternatePort, BackupPort та Disabled);
- Стан CIST порту, який може бути пересиланням або відкиданням;
- Час безперебійної роботи, який представляє час, протягом якого порт активний.

Статистика портів

Параметр моніторингу статистики STP дозволяє користувачеві переглядати інформацію про обмін пакетами на портах, що обмінюються пакетами BPDU.

- Номер порту, вказаний у рядку. Показані тільки порти, дозволені для передачі або прийому пакетів BPDU;
- Передані пакети BPDU, у кількості повідомлень BPDU. Є чотири стовпці, де обмін пакетами BPDU розділений на повідомлення MSTP, RSTP, STP та загальні повідомлення TCN (Сповіщення про зміни топології), передані на даному порту;
- Отримані пакети BPDU, у кількості повідомлень BPDU. Є чотири стовпці, де обмін пакетами BPDU розділений на повідомлення MSTP, RSTP, STP та загальні повідомлення TCN (Сповіщення про зміни топології), отримані на даному порту;
- Відкинуті кадри BPDU, отримані на даному порту, розділені на "Невідомі" та "Заборонені" (Unknown та Illegal) отримані кадри BPDU.

7 IPMC

У цьому пункті описуються основні можливості моніторингу багатоадресної IP-передачі (IPMC), що використовуються в Reason S20, надаючи інформацію про Відстеження трафіку IGMP та MLD, такі як стан, інформація про групи та інформація про IP SFM.

Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Відстеження трафіку IGMP (багатоадресне середовище IPv4)

- Стан: відображає інформацію про стан таблиці IGMP.
  - Номер ідентифікатора VLAN (VID) запису;
  - Версія генератора запитів (IGMPv1, IGMPv2 або IGMPv3);
  - Версія хоста (IGMPv1, IGMPv2 або IGMPv3);
  - Стан генератора запитів. Дозволеними значеннями є стан активного та неактивного генератора запитів;
  - Передані запити, у кількості запитів;
  - Отримані запити, у кількості запитів;
  - Отримані звіти IGMPv1, у кількості звітів;
  - Отримані звіти IGMPv2, у кількості звітів;
  - Отримані листи IGMPv2, у кількості звітів;
  - Отримані звіти IGMPv3, у кількості звітів.
  - Порт маршрутизатора: відображає інформацію про порт маршрутизатора IGMP на комутаторі, тобто порти, які працюють як порти маршрутизатора.
    - Номер порту;
    - Стан порту, тобто чи порт є маршрутизатором або ні.
- Інформація про групи: містить інформацію про групи таблиці IGMP, дозволені на комутаторі.
  - Номер ідентифікатора VLAN (VID) групи у рядку;
  - Діапазон адрес групи у рядку;
  - Порти-члени, де відображається, які порти є членами групи.
- Інформація про IGMP SFM, тобто інформація про багатоадресну передачу, відфільтрована джерелом IGMP. Ця інформація стосується тільки протоколів IGMPv3 та MLDv2, які підтримують підписку на канали.
  - Номер ідентифікатора VLAN (VID) групи;
  - Діапазон адрес групи для групи;
  - Порти-члени, де відображається, які порти є членами групи;
  - Режим фільтрації SSM, який вказує режим фільтрації (номер VID, номер порту, діапазон адрес групи);
  - Адреса джерела, тобто IP-адреса джерела багатоадресної передачі;
  - Тип фільтрації SSM (режим джерела);
  - Апаратний фільтр/комутатор, який вказує, чи може площина даних, надіслана джерелом групи, опрацьовуватися мікросхемою чи ні.

Відстеження трафіку MLD (багатоадресне середовище IPv6)

- Стан: відображає інформацію про стан таблиці MLD. Дозволена наступна інформація:
  - Номер ідентифікатора VLAN (VID) запису;
  - Версія генератора запитів (MLDv1 або MLDv2);
  - Версія хоста (MLDv1 або MLDv2);
  - Стан генератора запитів. Дозволеними значеннями є стан активного та неактивного генератора запитів;

- Передані запити, у кількості запитів;
- Отримані запити, у кількості запитів;
- Отримані звіти MLDv1, у кількості звітів;
- Отримані листи MLDv1, у кількості звітів;
- Отримані звіти MLDv2, у кількості звітів;
- Порт маршрутизатора: відображає інформацію про порт маршрутизатора MLD на комутаторі, тобто порти, які працюють як порти маршрутизатора.
  - Номер порту;
  - Стан порту, тобто чи порт є портом маршрутизатора або ні.

- Інформація про групи: містить інформацію про групи таблиці MLD, дозволені на комутаторі.
  - Номер ідентифікатора VLAN (VID) групи в рядку;
  - Діапазон адрес групи у рядку;
  - Порти-члени, де відображається, які порти є членами групи.
- Інформація про MLD SFM, тобто інформація про багатоадресну передачу, відфільтрована за джерелом MLD. Ця інформація стосується тільки протоколів IGMPv3 та MLDv2, які підтримують підписку на канали.
  - Номер ідентифікатора VLAN (VID) групи;
  - Діапазон адрес групи для групи;
  - Порти-члени, де відображається, які порти є членами групи;
  - Режим фільтрації SSM, який вказує режим фільтрації (номер VID, номер порту, діапазон адрес групи);
  - Адреса джерела, тобто IP-адреса джерела багатоадресної передачі;
  - Тип фільтрації SSM (режим джерела);
  - Апаратний фільтр/комутатор, який вказує, чи може площина даних, надіслана джерелом групи, опрацьовуватися мікросхемою чи ні.

8 Таблиця MAC-адрес

У цьому пункті описано MAC-адресу, представлену у веб-інтерфейсі для цілей моніторингу.

Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Таблиця MAC-адрес

У таблиці MAC-адрес представлена поточна таблиця адрес, яка використовується комутатором. Рядки в таблиці вказують записи таблиці MAC-адрес, а стовпці упорядковують відображену інформацію. Ця таблиця використовується для прийняття рішення про пересилання мостом.

- Тип, який вказує тип процесу вивчення. Порти, налаштовані як "Автоматичні" (Auto), відображатимуться як порти типу Динамічного вивчення (Dynamic learning type), а порти, налаштовані як "Захищені" (Secure), відображатимуться як порти типу Статичного вивчення (Static learning type);
- Ідентифікатор VLAN (VID) MAC-адреси;
- MAC-адреса відображена та включена до таблиці MAC-адрес;

- Порти-члени, розділені на стовпці, по одному на порт. Якщо конкретна MAC-адреса може бути членом даного порту, символ буде позначений у цьому рядку MAC-адреси та стовпці Порту.

9 VLAN

У цьому пункті представлена таблиця та порти VLAN для цілей моніторингу, а також інформація про меню "Членство та порти VLAN" (VLANs Membership and Ports). Якщо потрібно оновити веб-екран автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Членство VLAN

Таблиця стану членства VLAN для комбінованих користувачів дозволяє контролювати поточні VLAN, налаштовані та запущені на комутаторі.

- Ідентифікатор VLAN;

  Порти-члени, розділені прапорцями для кожного порту.

  - Символ ☑, показаний у стовпці порту, означає, що порт є членом ідентифікатора VLAN, пов'язаного з рядком;
  - Символ ☐, показаний у стовпці порту, означає, що порт не є членом ідентифікатора VLAN, пов'язаного з рядком.

Порти VLAN

Таблиця стану портів VLAN для комбінованих користувачів дозволяє контролювати поточну інформацію про VLAN порту, налаштовану та запущену на комутаторі.

- Номер порту;
- Тип порту, тобто чи порт є портом типу "Не підтримується", "C-Порт", "S-Порт", "Користувацький-S-Порт" (Unaware, C-Port, S-Port, S-Custom-Port);
- Фільтрування на вході в порт. Увімкнений прапорець означає, що порт виконує фільтрування на порту, а вимкнений прапорець означає, що порт не виконує фільтрування на порту;
- Тип кадру. Якщо увімкнено фільтрування вхідного трафіку, стовпець типу кадру відображатиме, які типи кадрів дозволені на цьому порту. Можливі значення: Усі, Теговані або Нетеговані (All, Tagged або Untagged);
- Ідентифікатор VLAN порту;
- Тегування Tx порту, тобто налаштована логіка тегування при передачі. Можливі значення "Знімати теги з усіх кадрів", "Тегування усіх кадрів", "Знімати теги PVID" (Untag All, Tag All та Untag PVID);
- Нетегований ідентифікатор VLAN, який вказує на логіку роботи кадрів в процесі виходу;
- Стан конфліктів VLAN. Конфліктами можуть бути функціональні конфлікти або апаратне обмеження (конфлікт між користувацькими модулями).

10 PTP

У цьому пункті описані можливості моніторингу PTP за допомогою веб-інтерфейсу. Якщо потрібно оновити веб-екран Reason S20 автоматично, встановіть прапорець "Автоматичного оновлення" (Auto Refresh) вгорі, щоб виконати його. Якщо вибрано, веб-сторінка моніторингу буде оновлена автоматично через 3 секунди після останнього оновлення.

Конфігурація годинника PTP

Конфігурація годинника PTP демонструє екземпляр годинника PTP, налаштований на комутаторі. Оскільки можливий тільки один екземпляр PTP, стовпець "Inst" завжди відображатиме "0", і натискаючи його далі, відображатимуться деталі PTP. Решта інтерфейсів моніторингу:

- **Тип пристрою (Device Type)**: Продемонстровано, що режим PTP в Reason S20 працює;
- **Список портів (Port List)**: Якщо ✓ це означає, що зазначений порт є членом налаштованого екземпляра PTP. Якщо порожній, PTP вимкнено для цього порту.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 7: Обслуговування, виявлення та усунення несправностей

1 Діагностика мережі

1.1 Ping

Меню Ping ("пінг" – перевірка зв'язку) дозволяє використовувати повідомлення IPv4 Ping для діагностики мережі. Повідомлення Ping – це пакети ICMP, які використовуються для перевірки того, чи є хост доступним у середовищі IP-мережі. Крім того, повідомлення Ping можуть повертатися, якщо хост доступний, із зазначенням часу на передачу і підтвердження прийому.
Reason S20 дозволяє використовувати свій IP-інтерфейс керування в якості ініціатора повідомлення ping. Таким чином, можна перевірити доступність IP-хостів за допомогою комутатора, виконуючи основні функції діагностики в мережі.
Меню Ping знаходиться в меню Діагностика> Ping (Diagnostics > Ping).

IP-адреса

Це поле дозволяє налаштувати IP-адресу хоста, підключеного до мережі, щоб перевірити, доступний він для комутатора чи ні. IP-адресу потрібно вводити у десятковому форматі з крапками.

Довжина Ping

Налаштуйте довжину Ping, тобто розмір корисного навантаження пакета Ping. Дозволеними значеннями є цілі числа від 2 до 1452 байт. За замовчуванням розмір корисного навантаження Ping становить 56 байт.

Лічильник Ping

Визначте, скільки разів відповіді на ping-повідомлення повинні надсилатися на вказану адресу. Допустимі значення – це цілі числа від 1 до 60 разів. За замовчуванням Ping виконується 5 разів.

Інтервал Ping

Це поле дозволяє налаштувати інтервал Ping для кожного надісланого Ping-повідомлення. Дозволеними значеннями є цілі числа від 0 до 30 секунд. За замовчуванням інтервал Ping виконується раз на секунду (значення = 1).
Після зміни однієї з описаних раніше конфігурацій з’являється кнопка, яка дозволяє користувачеві запустити функцію, як показано нижче.

- Запуск (Start): розпочніть надсилання Ping-повідомлень через IP-інтерфейс комутатора.

1.2 Ping6

Меню Ping6 дозволяє використовувати повідомлення ping IPv6 для діагностики мережі. Повідомлення Ping – це пакети ICMP, які використовуються для перевірки того, чи є хост доступним у середовищі IP-мережі. Крім того, повідомлення Ping можуть повертатися, якщо хост доступний, із зазначенням часу на передачу і підтвердження прийому.
Reason S20 дозволяє використовувати свій IP-інтерфейс керування в якості ініціатора повідомлення ping. Таким чином, можна перевірити доступність IP-хостів за допомогою комутатора, виконуючи основні функції діагностики в мережі.
Меню Ping знаходиться в меню Діагностика> Ping6 (Diagnostics > Ping6).

IP-адреса

Це поле дозволяє налаштувати IP-адресу хоста, підключеного до мережі, щоб перевірити, доступний він для комутатора чи ні. IP-адресу потрібно вводити у шістнадцятковому форматі з символом (":"), що розділяє кожне поле.

Довжина Ping

Налаштуйте довжину Ping, тобто розмір корисного навантаження пакета Ping. Дозволеними значеннями є цілі числа від 2 до 1452 байт. За замовчуванням розмір корисного навантаження Ping становить 56 байт.

Лічильник Ping

Визначте, скільки разів відповіді на ping-повідомлення повинні надсилатися на вказану адресу. Допустимі значення – це цілі числа від 1 до 60 разів. За замовчуванням Ping виконується 5 разів.

Інтервал Ping

Це поле дозволяє налаштувати інтервал Ping для кожного надісланого Ping-повідомлення. Дозволеними значеннями є цілі числа від 0 до 30 секунд. За замовчуванням інтервал Ping виконується раз на секунду (значення = 1).

Інтерфейс виходу

Це поле дозволяє вказати, який ідентифікатор VLAN слід використовувати на інтерфейсі виходу, який буде використовуватися для надсилання пакетів Ping ICMP. Допустимі значення VLAN становлять від 1 до 4.095. За замовчуванням це поле порожнє, а це означає, що функція Ping6 сама визначить найкращий інтерфейс для використання.
Після зміни однієї з описаних раніше конфігурацій з’являється кнопка, яка дозволяє користувачеві запустити функцію, як показано нижче.

- Запуск (Start): розпочніть надсилання Ping-повідомлень через IP-інтерфейс комутатора.

1.3 VeriPHY

VeriPHY – це функція, яку виконує сам Reason S20 для перевірки цілісності електричних кабелів, підключених до комутатора, з метою діагностики.
Ця функція виконується безпосередньо на мікросхемах PHY (фізичного рівня), які здійснюють взаємодію між зв'язком рівня 2 і рівня 1. Мікросхеми PHY перевіряють якість більшості каналів на основі імпедансу, виміряного на кожній парі в кабелі CAT-5.

Перевірка кабелю VeriPHY може використовуватися лише на електричних кабелях, тобто кабелях CAT-5 або більш високої якості, підключених через роз'єм RJ45. Ця функція не підтримує оптичні канали зв'язку.

Під час роботи функція VeriPHY може порушити зв'язок на порту, який використовується цією функцією. Таким чином, якщо ви використовуєте функцію VeriPHY, переконайтеся, що протягом періоду роботи функції не буде серйозних проблем із втратою даних.

Порт

Виберіть порт, який потрібен для перевірки кабелю VeriPHY.

Після зміни однієї з описаних раніше конфігурацій з’являється кнопка, яка дозволяє користувачеві запустити функцію, як показано нижче.

- Запуск (Start): розпочніть перевірку VeriPHY.

Результат відображається в таблиці, де рядки представляють порти, а стовпці – кожну пару в кабелі CAT-5. Стовпці поділяються на пари (пари A, B, C і D) і довжину (довжина пари A, B, C і D).

За замовчуванням усі клітинки відображаються символом "-". Після завершення діагностики відображаються результати для перевірки будь-якої виявленої проблеми. Можливі наступні результати:

- Стовпець пари:
  - Добре (OK): означає, що кабель не має пошкоджень;
  - Обрив (Open): означає, що пара, представлена в цій клітинці, має обрив;
  - Закорочення (Short): означає, що пара, представлена в цій клітинці, закорочена;
  - Закорочена пара (Short Pair): може бути для пари A, B, C або D. Означає, що відбулося перехресне закорочення пари;
  - Перехрещення пари (Cross Pair): може бути для пари A, B, C або D. Означає, що має місце аварійне перехрещення пар.
- Стовпець довжини:
  - Довжина (у метрах) пари кабелю (точність 5 метрів).

2 Обслуговування

2.1 Перезапуск пристрою

Якщо потрібно перезапустити обладнання, за допомогою веб-інтерфейсу можна отримати доступ до меню "Перезапустити пристрій" (Restart Device), що знаходиться в розділі "Технічне обслуговування" (Maintenance). Робоча конфігурація обладнання буде втрачена після перезапуску пристрою. Після перезапуску процес завантаження завантажить конфігурацію запуску, замінюючи попередню робочу конфігурацію.

Повідомлення на веб-інтерфейсі попереджає, якщо користувач хоче перезапустити пристрій:

- Так (Yes): Після натискання цієї кнопки система виконає перезапуск, і фактична робоча конфігурація буде втрачена. У процесі завантаження конфігурація запуску (startup-config) замінить робочу конфігурацію (running-config);
- Ні (No): вийдіть з цього меню і не перезавантажуйте пристрій.

2.2 Заводські налаштування за замовчуванням

Якщо потрібно відновити заводські налаштування за замовчуванням, за допомогою веб-інтерфейсу можна отримати доступ до меню "Заводські налаштування за замовчуванням" (Factory Defaults), що знаходиться у розділі "Технічне обслуговування" (Maintenance). Крім того, користувач може повернути пристрій до заводських налаштувань за замовчуванням, створивши петлю між портами 1 і 2, як це пояснювалося раніше у пункті "Скидання до заводських налаштувань" (Factory Reset).
Відкриваючи меню "Заводські налаштування за замовчуванням", користувач може вибрати наступні параметри:

- Так (Yes): скидання пристрою. Після натискання цієї кнопки система виконає скидання, і всі конфігурації будуть втрачені. У процесі завантаження конфігурація запуску (startup-config) та робоча конфігурацію (running-config) будуть замінені заводською конфігурацією за замовчуванням (default config);
- Ні (No): вийдіть з цього меню і не скидайте налаштування пристрою.

2.3 Завантаження програмного забезпечення

Reason S20 виконує безпечне оновлення вбудованого ПЗ (прошивки), використовуючи контрольну суму для перевірки цілісності та цифровий підпис для забезпечення автентифікації. Протокол передачі файлів, який використовується для оновлення прошивки, є захищеним (SFTP).
S20 використовує два різні програмні файли: прикладний та базовий.

- Прикладне програмне забезпечення доступне для користувачів на веб-сайті GE як оновлення (patch) для нових функцій, покращення продуктивності та надійності, тощо.

Файли .dat використовувались до версії FW 06A02, в якій був введений цифровий підпис. З цієї причини FW 06A02 має як файли .dat, так і .sdt. Перший повинен використовуватися при завантаженні з попередньої версії FW на FW 06A02. У разі пошкодження FW06A02 слід використовувати файл .sdt. Починаючи з FW 07A00 і далі надається лише файл .sdt. У FW 07A04 прикладне програмне забезпечення залишається як файл з розширенням .sdt

- Базове програмне забезпечення, як випливає з назви, є базовим програмним забезпеченням, на якому встановлено прикладне програмне забезпечення. Крім того, воно також включає завантажувач. За потреби його можна отримати через контактний центр GE.

Базове програмне забезпечення було вперше представлено у FW 07A04 із використанням розширення файлу .sbs

Меню завантаження прикладного програмного забезпечення та базового програмного забезпечення знаходиться в розділі Технічне обслуговування > Завантаження програмного забезпечення (Maintenance > Software Upload).

- Виберіть Файл відповідно для прикладного або базового програмного забезпечення:
  - .dat або .sdt для прикладного програмного забезпечення, або;
  - .sbs-файл для базового програмного забезпечення
- Завантажити: після вибору дійсного файлу ця кнопка виконує функцію завантаження програмного забезпечення.

Під час оновлення прошивки, веб-доступ не працює. Під час оновлення прошивки світлодіод на передній панелі блимає зеленим/згасає з частотою 10 Гц. Не перезавантажуйте та не вимикайте пристрій у цей час, інакше комутатор може не працювати після цього.

Після завантаження образу програмного забезпечення на сторінці з'являється повідомлення про те, що розпочато оновлення прошивки/ базового програмного забезпечення. Приблизно через хвилину прошивка оновлюється, і комутатор перезавантажується.

Процес завантаження програмного забезпечення займає кілька хвилин (за винятком оновлення FW 06A02, яке триває до 15 хвилин). Поки завантажується програмне забезпечення, комутатор залишатиметься недоступним.

2.4 Ліцензія

S20 має дві функції, які можна увімкнути за допомогою ліцензування, протокол синхронізації часу IEEE 1588v2 та/або функціональні можливості рівня L3, включаючи RIP v1/2, OSPF та VRRP. Такі функції можна або увімкнути під час замовлення обладнання, або модернізувати пізніше, замовивши новий файл ліцензії. S20 оновить та активує функції, просто завантаживши на обладнання новий замовлений файл ліцензії.
Крім того, користувач може перевірити, які функції активовані на пристрої, і завантажити поточний файл ліцензії за бажанням.

2.5 Конфігурація

Reason S20 зберігає у внутрішній пам'яті три файли конфігурації, які користувач може вільно вибрати для активації. Одним з них є основний файл активної конфігурації - файл робочої конфігурації (running configuration file), який використовується комутатором, який втрачається при перезапуску обладнання. Інший – це файл конфігурації запуску (startup configuration file), тобто файл, який стане активним у процесі завантаження комутатора. Останній – це заводський файл конфігурації за замовчуванням. Файли конфігурації та їх описи наведені нижче.

- **Робоча конфігурація (Running Config)**: Цей файл містить фактичну конфігурацію комутатора. Якщо в будь-якому меню налаштувань натиснути кнопку збереження, зміни, внесені в конфігурацію, будуть збережені в цьому файлі. Якщо комутатор перезавантажується, ця конфігурація відкидається, і комутатор замінить цей файл робочої конфігурації після перезавантаження файлом конфігурації запуску;
- **Конфігурація запуску (Startup Config)**: Цей файл містить конфігурацію, яку комутатор буде запускати після увімкнення або перезапуску. Якщо були внесені зміни у Робочій конфігурації, і Робочу конфігурацію необхідно використовувати під час запуску конфігурації, користувач повинен зберегти її у налаштуванні "Зберегти Робочу конфігурацію" (Save Running Configuration) як конфігурацію запуску в меню Технічне обслуговування (Maintenance);
- **Конфігурація за замовчуванням (Default Config)**: Цей файл містить заводську конфігурацію комутатора за замовчуванням. За необхідності його можна завантажити за допомогою програмного забезпечення для заміни фактичної робочої конфігурації або файлу конфігурації запуску.

Збереження конфігурації запуску

Меню "Зберегти конфігурацію запуску" (Save startup-config) знаходиться у розділі Технічне обслуговування > Конфігурація > Зберегти конфігурацію запуску (Maintenance > Configuration > Save startup-config).

Користувачеві наполегливо рекомендується зберігати у файлі конфігурації запуску зміни, внесені на пристрої, час від часу, оскільки це гарантує, що вже налаштовані конфігурації не будуть втрачені після перезапуску пристрою або циклу вимкнення/увімкнення живлення.

Щоб зберегти робочу конфігурацію як конфігурацію запуску, натисніть кнопку "Зберегти конфігурацію" (Save Configuration). Після цього робоча конфігурація зберігається як конфігурація запуску.

Скачування

Меню "Скачування" знаходиться в розділі Технічне обслуговування> Конфігурація> Скачування (Maintenance > Configuration > Download).

У цьому меню можна скачати конфігурацію як файл, який буде використаний як резервний файл конфігурації для відновлення системи, наприклад. Можна скачати конфігураційні файли робочої конфігурації, конфігурації за замовчуванням та конфігурації запуску.

Щоб скачати конфігурацію, виберіть конфігурацію, яку потрібно скачати, і натисніть кнопку "Скачати конфігурацію". Крім того, увімкнено команду копіювання SFTP для скачування конфігурації за допомогою інтерфейсу командного рядка (CLI).

Завантажити

Меню "Завантаження" (Upload) знаходиться в розділі Технічне обслуговування> Конфігурація > Завантажити (Maintenance > Configuration > Upload).

У цьому меню можна завантажити попередньо скачаний файл конфігурації, який буде використаний як файл конфігурації для відновлення системи, якщо це потрібно. Можна завантажити конфігураційний файл як файл робочої конфігурації та файл конфігурації запуску. Крім того, можна створити новий файл конфігурації (тоді будуть наявні файли робочої конфігурації, конфігурації запуску та новий файл), якщо потрібно.

Якщо файл завантаження буде використовуватися як робоча конфігурація, можна вибрати заміну робочої конфігурації або об'єднання робочої конфігурації із завантаженою конфігурацією. У цьому останньому варіанті буде збережена робоча конфігурація, і будуть завантажені тільки розбіжності між робочою конфігурацією та завантажувальним файлом.

Щоб завантажити конфігурацію, виберіть конфігурацію, яку потрібно завантажити, а потім натисніть кнопку "Завантажити конфігурацію" (Upload Configuration). Після цього вибрана конфігурація буде завантажена. Крім того, увімкнено команду копіювання SFTP для завантаження конфігурації за допомогою CLI.

Активація

Меню "Активації" (Activate) знаходиться в розділі Технічне обслуговування > Конфігурація > Активація (Maintenance > Configuration > Activate).

У цьому меню можна активувати конфігурацію (або конфігурацію за замовчуванням, або конфігурацію запуску) як робочу конфігурацію.

Для цього виберіть, яку конфігурацію потрібно активувати, а потім натисніть кнопку "Активувати конфігурацію" (Activate Configuration). Після цього вибрана конфігурація буде активована як файл робочої конфігурації.

Видалення

Меню "Видалення" (Delete) знаходиться в розділі Технічне обслуговування> Конфігурація> Видалення (Maintenance > Configuration > Delete).

Це меню надає можливість видалення файлу конфігурації запуску.

Щоб видалити його, виберіть конфігурацію запуску і натисніть кнопку "Видалити файл конфігурації" (Delete Configuration File). Після цього файл конфігурації буде видалено з внутрішньої пам'яті комутатора.

3 Виявлення та усунення несправностей

У цьому пункті описані найбільш поширені проблеми, які можуть виникнути при використанні пристрою Reason S20. У наведених нижче випадках показані проблеми, які можуть виникнути, та міститься опис дій, які необхідно виконати для вирішення проблеми.

Світлодіоди живлення не горять

Якщо світлодіоди живлення вимкнені – це означає відсутність живлення. Перевірте, чи правильно підключені кабелі живлення до відповідних гвинтів, перевірте, чи правильно вставлений роз'єм живлення або увімкнено живлення в системі, перевіривши напругу на роз'ємах джерела живлення.

Я не знаю IP-адреси керування комутатором

Якщо IP-адресу інтерфейсу керування було втрачено, можна виконати певні дії для її відновлення. Основні дії описані нижче:

- **Підтримка конфігурації комутатора:** підключіть термінал до USB-інтерфейсу комутатора. Після встановлення зв'язку команда для відновлення IP-адреси є наступною:

  ```
  show ip interface brief
  ```

- **Втрата конфігурації комутатора:** На вимкненому комутаторі, підключіть порти 1 і 2, щоб створити петлю між ними. Потім увімкніть подачу живлення на комутатор. Ця процедура відновить конфігурацію до заводських налаштувань за замовчуванням, тоді IP-адресою обладнання буде 192.168.4.88, а довжина маски - 255.255.255.0.

Не вдається отримати доступ до веб-інтерфейсу

Якщо термінал, до якого планується отримати доступ, не може бути досягнутий навіть тоді, коли відома IP-адреса, потрібно виконати кілька кроків, щоб перевірити, чи може термінал підключитися до обладнання.

- **Перевірте, чи правильно працюють кабелі, що з'єднують термінал та комутатор.** Крім того, якщо можливо, перевірте, чи блимають світлодіоди, що відповідають порту, який використовується терміналом, показуючи, що зв’язок здійснюється на порту;
- **Переконайтеся, що термінал знаходиться в тій самій IP-підмережі, що й інтерфейс комутатора.** Перевірте це, перевіривши довжину маски інтерфейсу керування та IP-адресу комутатора і довжину маски та IP-адресу терміналу. Увімкнені біти, що стосуються довжини маски, порівняно з IP-адресою, повинні бути однаковими як для терміналу, так і для інтерфейсу керування, що означає обладнання знаходиться в одній і тій же IP-мережі;
- **Переконайтеся, що порт, до якого підключений термінал, знаходиться у VLAN інтерфейсу керування.** Якщо VLAN не налаштовано, переконайтеся, що VLAN налаштованого інтерфейсу керування є VLAN за замовчуванням (VID = 1);
- **Спробуйте виконати команду PING від терміналу до інтерфейсу керування комутатора.** Якщо комутатор відповідає на повідомлення PING, але веб-інтерфейс не може відкрити інтерфейс керування, переконайтеся, що використання проксі у веб-браузері правильно налаштовано, щоб дозволити інтерфейс керування комутатора.

Електричний зв'язок не працює належним чином

Якщо електричні канали зв'язку не працюють належним чином, необхідно перевірити два варіанти:

- **Канал працює, але пакети втрачаються довільним чином.** У цьому випадку можливою причиною проблеми є обрив неекранованої витої пари UTP-кабелю. Це можна перевірити за допомогою функції VeriPHY, яка покаже обірвану пару, або замінивши Ethernet-кабель. Його також можна перевірити, змінивши швидкість порту, наприклад, порти 100 Мбіт/с

використовують 2 пари, тоді як порт 1 Гбіт/с - 4 кабельних пари. Таким чином, зниження швидкості порту може надати інформацію про якість кабелю. Крім того, ця проблема повинна бути вирішена після заміни UTP-кабелю на UTP-кабель належної якості;

- **Канал не працює.** У цьому випадку можливою причиною проблеми є обрив кабелю, обрив роз'єму RJ45 або вимкнення порту. Якщо порт вимкнений, увімкніть його у веб-інтерфейсі. Щоб увімкнути порти, перейдіть в меню Порти (Ports), виберіть порт, який потрібно увімкнути, а потім виберіть правильну швидкість порту. У випадку обриву кабелю або роз'єму, ця проблема повинна бути вирішена після заміни UTP-кабелю на UTP-кабель належної якості.

Мені не потрібні VLAN. Чи потрібно змінювати налаштування за замовчуванням?

За замовчуванням усі порти є членами VLAN ID 1 у пристрої Reason S20. Інтерфейс керування налаштований як член VLAN ID 1, усі вхідні кадри класифікуються до VLAN ID 1, а всі вихідні кадри пересилаються без тега VLAN. Таким чином, все підключене обладнання буде членом однієї VLAN, а також буде отримувати і передавати інформацію, оскільки знаходиться в одній і тій же LAN. Таким чином, якщо в мережі не використовується VLAN, налаштування за замовчуванням змінювати не потрібно.

Я використовую VLAN, але, схоже, вони не працюють

При використанні VLAN існує кілька аспектів, які користувач повинен з'ясувати при налаштуванні комутаторів. Переконайтеся, що наступні вимоги були виконані, якщо VLAN не працює належним чином.

- **Тип порту повинен бути правильним.** Переконайтеся, що обладнання, підключене до порту, на якому налаштовується VLAN, є правильним. В іншому випадку вхідний фільтр повинен відкидати пакети або змінювати вхідні кадри ідентифікатора (ID) VLAN на ID VLAN вхідного порту, таким чином, даний кадр VID буде перенаправлений на VID VLAN порту;
- **Чи дотримуються правила фільтрування портів.** Якщо фільтрування на вході увімкнене, нетеговані або теговані кадри можуть бути відкинуті, в залежності від налаштованого фільтра. Переконайтеся, що для цього порту правильно налаштоване фільтрування вхідного трафіку;
- **Параметри тегування вихідного трафіку працюють відповідно до вимог хоста.** Фільтрування на виході може підтримувати теги VLAN, знімати теги VLAN або забороняти тільки кадри з тегом VID порту. Таким чином, переконайтеся, що тегування вихідного трафіку налаштоване відповідно до потреб хоста. Якщо хост підтримує VLAN, переконайтеся, що при фільтруванні вихідного трафіку надсилається тег VLAN, який хост очікує отримати. Якщо хост не підтримує VLAN, переконайтеся, що кадри пересилаються без тега VLAN;
- **Переконайтеся, що VLAN дозволена для порту, і переконайтеся, що VLAN не заборонена для цього порту.** Кадри з інформацією про VLAN можуть пересилатися тільки в тому випадку, якщо вони надходять на порт, якому дозволено приймати VLAN кадру. В іншому випадку пакет буде відкинутий. Крім того, кадри з ідентифікатором VLAN, забороненим для даного порту, також будуть відкинуті.

Дата або час неправильні

Внутрішній годинник Reason S20 оновлюються на основі NTP, PTP 1588 або вручну, у зазначеному порядку пріоритету. Якщо дата або час неправильні, виконайте наступні дії:

- Переконайтеся, що NTP-клієнт правильно налаштований. Це можна перевірити в меню Налаштування > Система > NTP (Settings > System > NTP);

- Переконайтеся, що NTP-сервер мережі доступний. Його можна протестувати за допомогою внутрішньої команди PING комутатора, де необхідно відправити команду PING налаштованому NTP-серверу;
- Переконайтеся, що часовий пояс (Timezone) налаштований правильно в меню Налаштування > Система > Час (Settings > System > Time). Якщо використовується перехід на літній час (Daylight Saving Time), перевірте, чи правильно він налаштований.
- Якщо ви хочете використовувати PTP як джерело часу, обов'язково вимкніть NTP-клієнт і перевірте, чи правильно налаштований PTP, в тому числі увімкнений параметр PTP > Налаштування системного часу (PTP > Adjust system time).

Прошивка повинна бути оновлена

Якщо необхідне оновлення вбудованого ПЗ (прошивки), насамперед необхідно направити запит до компанії GE для отримання файлу прошивки. Після отримання цього файлу скопіюйте файл на ПК, на якому виконується інтерфейс керування комутатором.

Меню оновлення прошивки знаходиться в меню Технічного обслуговування. Щоб оновити прошивку, перейдіть в меню Технічне обслуговування > Програмне забезпечення > Завантажити (Maintenance > Software > Upload), виберіть правильний файл прошивки (файл .dat) і натисніть кнопку "Завантажити" (Upload).

Як я можу гарантувати, що файл конфігурації не буде втрачено при перезавантаженні комутатора?

При зміні конфігурації насамперед необхідно забезпечити, щоб нові налаштування працювали правильно. Після зміни і збереження конфігурації переконайтеся, що збережена конфігурація (робоча конфігурація (running config)) працює правильно, протестувавши мережу Ethernet. Переконавшись, що поточна робоча конфігурація працює, збережіть її у конфігурації запуску, що знаходиться в меню Технічне обслуговування > Конфігурація > Зберегти конфігурацію запуску (Maintenance > Configuration > Save startup-config). Після того, як робоча конфігурація збережена в конфігурації запуску, гарантується, що конфігурація не буде втрачена в процесі перезавантаження.

Переконайтеся, що між портами 1 і 2 немає петлі при перезавантаженні комутатора, якщо відновлення заводських конфігурацій не потрібно.

4 Повернення обладнання

Всі частини та компоненти, включаючи пристрої Reason, мають бути відремонтовані виключно компанією GE. У випадку несправності обладнання замовник повинен зв'язатися з Контактним центром GE і в жодному разі не намагатися самостійно відремонтувати пристрій.

Щоб замовити ремонт обладнання, зателефонуйте GE для з'ясування можливого варіанту доставки та отримання коду замовлення технічної допомоги.

Обладнання повинно бути упаковане в оригінальну упаковку або підходящу упаковку, що забезпечує захист від механічних пошкоджень та вологи.

5 Інструкції щодо ремонту/обслуговування обладнання для сервісного персоналу

Інструкції, представлені у цьому пункті, повинні виконуватися тільки сервісним персоналом GE.

У разі необхідності проведення будь-якого ремонту обладнання слід дотримуватися наведеної нижче процедури, щоб забезпечити техніку безпеки під час виконання робіт.

1) Від'єднайте джерело живлення;
2) Від'єднайте всі інші з'єднання, залишивши від'єднання шини заземлення наприкінці;
3) Виконайте візуальний огляд, щоб переконатися, що обладнання ізольовано;
4) Розмістіть пристрій там, де є вільне місце для роботи, і обов'язково встановіть відповідні робочі та попереджувальні застереження в зоні розміщення, також забезпечте доступність всіх інструментів та допоміжних засобів, які будуть використовуватися;
5) Зачекайте кілька хвилин, щоб конденсатори могли розрядитися;
6) Розберіть пристрій, викрутивши гвинти з корпусу та потягнувши верхню панель корпусу; після цього виконуйте належний ремонт. Майте на увазі, що при розбиранні обладнання може бути відкрита чутлива електронна схема. Для запобігання пошкодженню обладнання необхідно вжити відповідних застережних заходів для захисту від електростатичного розряду (ESD).

Після завершення ремонту дотримуйтесь наведеної нижче процедури, щоб перевірити безпечний стан обладнання та відновити його роботу.

1) Повторно підключіть всі внутрішні кабелі, які були від'єднані для виконання ремонту;
2) Виконайте візуальний огляд пристрою, щоб переконатися, що всередині корпусу немає залишків від ремонту або відсутні будь-які інші невідповідності;
3) Встановіть на місце верхню панель корпусу та закріпіть її за допомогою відповідних гвинтів;
4) Приєднайте шину заземлення, а потім джерело живлення до обладнання;
5) Зачекайте, поки обладнання ініціалізується. Це може тривати близько однієї хвилини;
6) Дотримуйтесь процедур, описаних у Розділ 2: Інформація про техніку безпеки.

GE Reason S20

Промисловий керований Ethernet-комутатор

Розділ 8: Технічні характеристики

1 Загальні комутаційні характеристики

Таблиця 8: Загальні комутаційні характеристики

Параметр	Опис
Комутаційна здатність	68 Гбіт/с
Затримка комутації	3 мкс
Кількість VLAN	до 4095
Записи таблиці MAC-адрес	до 8192 (64 статичні)
Рівні класу обслуговування (CoS)	до 8

2 Передача даних за допомогою Ethernet-з'єднання

Таблиця 9: Характеристики Ethernet-з'єднання

Параметр	Опис
Кількість	24 Гігабітних портів (до 6 інтерфейсних модулів з 4 Ethernet-портами на кожен)
Типи	Кожен інтерфейсний модуль (4 Ethernet-порти) може бути або: Фіксований RJ45: 10/100 Мбіт/с або 10/100/1000Мбіт/с Слоти SFP: порожній, з оптоволоконними SFP-трансиверами (варіанти 100 Мбіт/с або 1000 Мбіт/с) або з електричними RJ45 SFP-трансиверами (10/100/1000 Мбіт/с)
Монтаж	Монтаж на задній панелі

3 Передача даних за допомогою USB-з'єднання

Таблиця 10: Характеристики USB-з'єднання

Параметр	Опис
Консольний порт	1 x USB Тип B 2.0 на передній панелі корпусу
Швидкість	11520 бітів на секунду
Біти даних	8
Стопові біти	1
Контроль парності	Немає
Керування потоком	Немає

4 Синхронізація часу

Таблиця 11: Характеристики синхронізації часу

Параметр	Опис
PTP IEEE 1588v2	Доступний на всіх портах, якщо увімкнено. Апаратне встановлення позначок часу. Робота в режимі прозорого, граничного або веденого годинника.
NTP-клієнт	Можливість налаштування до 5 зовнішніх NTP-серверів.
NTP-сервер	Може функціонувати як NTP-сервер на всіх портах. Час джерела залежить або від: Зовнішнього NTP-сервера або IEEE 1588v2 (PTP) або налагоджується вручну.
Годинник реального часу (RTC)	При вимкненні живлення годинник реального часу залишаються активним протягом 2 діб.

5 Підтримувані мережеві стандарти

Таблиця 12: Підтримувані мережеві стандарти

Стандарт	Опис
IEEE 802.3i	10BASE-T
IEEE 802.3u	100BASE-T(X)/100BASE-FX
IEEE 802.3ab	1000BASE-T(X)
IEEE 802.3z	1000BASE-SX/LX/ZX
IEEE 802.3x	Повнодуплексний режим, керування потоком

Стандарт	Опис
IEEE 802.1D	Мости керування доступом до середовища передачі даних (MAC-мости).
IEEE 802.1w	Високошвидкісний протокол кістякового дерева (RSTP).
IEEE 802.1s	Протокол множинних кістякових дерев (MSTP).
IEEE 802.1Q	VLAN (Віртуальні локальні комп'ютерні мережі).
IEEE 802.1p	Клас обслуговування.
IEEE 802.1X	Керування мережевим доступом на базі портів.
IEEE 802.3ad	Протокол керування агрегуванням каналів (LACP).
МЕК 61850	Мережі та системи зв'язку на електричних підстанціях (випробування проведені лабораторією KEMA).
IEEE 1588 v2 PTP	Стандарт IEEE протоколу синхронізації точного часу для мережевих вимірювальних систем і систем керування.

6 Мережеві стандарти RFC

Таблиця 13: Мережеві стандарти - Запити коментарів (RFC)

Стандарт	Опис
RFC 4363	База керуючої інформації (MIB) VLAN
RFC 2819	Віддалений мережевий моніторинг (RMON)
RFC 1213	MIB II
RFC 1215	MIB Traps (Пасток)
RFC 4188	MIB Мосту
RFC 4292	MIB Таблиці IP-передачі
RFC 4293	MIB Інтернет-протоколу (IP)
RFC 5519	MIB Виявлення членів груп багатоадресної передачі
RFC 4668	MIB Клієнта автентифікації RADIUS
RFC 4670	MIB Ведення облікових записів RADIUS
RFC 3635	Ethernet-подібна MIB
RFC 2863	MIB групи інтерфейсів з використанням SMI v2
RFC 3636	MIB 802.3 MAU (модулю доступу до середовища)
RFC 4133	MIB Об'єкта Версія 3
RFC 3411	Інфраструктура керування SNMP
RFC 3414	Модель забезпечення захисту на рівні користувачів для SNMPv3

Стандарт	Опис
RFC 3415	Модель керування доступом на основі представлення для SNMP
RFC 5171	Виявлення односпрямованого каналу (UDLD)
RFC 5905	Синхронізація NTP
RFC 5424	Повідомлення системного журналу (Syslog)
RFC 5426	Повідомлення системного журналу з використанням протоколу UDP
RFC 1157	Протокол SNMP
RFC 3418	MIB SNMP
RFC 3584	SNMP v1, v2c, v3
RFC 4604	Відстеження трафіку IGMPv3 & MLDv2
RFC 3260	Точка коду диференційованих послуг (DSCP)
RFC 6040	Явне повідомлення про перевантаження (ECN)
RFC 1058	Протокол інформації маршрутизації (RIP), версія 1
RFC 2453	Протокол інформації маршрутизації (RIP), версія 2
RFC 2328	Протокол вибору доступного найкоротшого маршруту (OSPF), версія 2
RFC 2338	Протокол резервування віртуального маршрутизатора (VRRP)

7 Ethernet-порти RJ45 (10/100/1000 Мбіт/с)

Таблиця 14: Характеристики Ethernet-портів RJ45

Параметр	Опис	Примітки
Тип	Два фіксованих варіанти (FE або GE) Один SFP варіант RJ45	Код замовлення SFP: SFP1GCU02K
Швидкість	10/100/1000 Мбіт/с (SFP або фіксований) 10/100 Мбіт/с (тільки фіксований)	Автоматичне узгодження
Дуплекс	FDX/HDX (Повно/Напівдуплексний)	Автоматичне узгодження
Тип кабелю	Категорія	Екранований/Неекранований
Стандарти монтажних з'єднань проводки	TIA/EIA T568A/B	Автоматичне визначення перехрещення пар, Автоматичне визначення полярності
Максимальна відстань	100 m	
Роз'єм	RJ45	
Ізоляція	1,5 кВ	RMS 1-хвилина

Щоб уникнути ризику ураження електричним струмом при використанні мідних кабелів довжина підключеного кабелю повинна бути менше 3 м і не повинна виходити за межі шафи, в якій використовується пристрій. Крім того, обладнання, підключене до обох кінців кабелю RJ45, має бути підключене безпосередньо до спільної точки заземлення в одній шафі, щоб уникнути небезпеки стрибкоподібної напруги (підвищення потенціалу землі).

8 Оптичні трансивери (100/1000 Мбіт/с)

Таблиця 15: Характеристики оптичних трансиверів

Модель	Швидкість	Макс. довжина кабелю (тип оптоволокна)	Довжина хвилі	Оптична потужність передавача (мін./ макс.)	Макс. чутливість / перевантаження приймача
SFP1GFO05K	1.25 Гбіт/с	0,5 км (MMF)	850 нм	-9 / -3 дБм	-17 / 0 дБм
SFP1GFO20K	1.25 Гбіт/с	20 км (SMF)	1310 нм	-9 / -3 дБм	-23 / -3 дБм
SFP1GFO40K	1.25 Гбіт/с	40 км (SMF)	1310 нм	-5 / 0 дБм	-23 / -3 дБм
SFP1GFO80K	1.25 Гбіт/с	80 км (SMF)	1550 нм	0 / +5 дБм	-23 / -3 дБм
SFP01GFO2K	155 Мбіт/с	2 км (MMF)	1310 нм	-20 / -14 дБм	-31 / -3 дБм
SFP01GFO20K	155 Мбіт/с	20 км (SMF)	1310 нм	-14 / -8 дБм	-32 / -3 дБм

НІКОЛИ не втручайтеся у оптичні волокна або оптичні вихідні з'єднання. Завжди використовуйте вимірювачі оптичної потужності, щоб визначити справний стан або рівень сигналу.

9 Джерело живлення

Таблиця 16: Характеристики джерела живлення

Джерело живлення високої напруги AC/DC	Діапазон вхідної напруги
Діапазон номінальної напруги	110-240 В змін. струму, 50/60 Гц 125-250 В пост. струму
Діапазон робочої напруги	88-264 В змін. струму, 50/60 Гц ± 3 Гц 88-300 В пост. струму
Максимальне споживання струму	0,5 А
Споживана потужність	60 ВА макс.

10 Реле безпечного режиму

Таблиця 17: Характеристики реле безпечного режиму

Параметр	Значення
Тип виходу	Сухі контакти типу "Form C": Нормально замкнений (NC) та Нормально розімкнений (NO)
Максимальна пропускна здатність по змінному струму	250 В змін. струму / 2 А
Максимальна пропускна здатність по постійному струму	2 А при 24 В пост. струму 700 мА при 48 В пост. струму 200 мА при 125 В пост. струму 100 мА при 250 В пост. струму (макс. напруга)

11 Умови навколишнього середовища під час експлуатації / зберігання

Таблиця 18: Умови навколишнього середовища під час експлуатації/зберігання

Тип	Рівень
Діапазон робочих температур	від -40°C до +55°C (постійно) від -40°C до +85°C (16 годин)
Система охолодження	Без вентилятора
Зберігання / транспортування	від -40°C до +85°C
Висота	≤ 2000 м
Вологість	5-95% відносної вологості, без конденсації
Ступінь захисту оболонки/корпусу	IP20 задня та бічні панелі IP30 передня панель
Ступінь забруднення	II

12 Фізичні характеристики

Таблиця 19: Фізичні характеристики

Параметр	Значення
Розміри	монтаж у 19-дюймовій стійці (43,6 мм ширина без кронштейну) 1U висота (43,7 мм) 310 мм глибина
Вага	приблизно 3,2 кг (без упаковки)
Конструкція	Сталь мінімізована Z100 0,95 мм

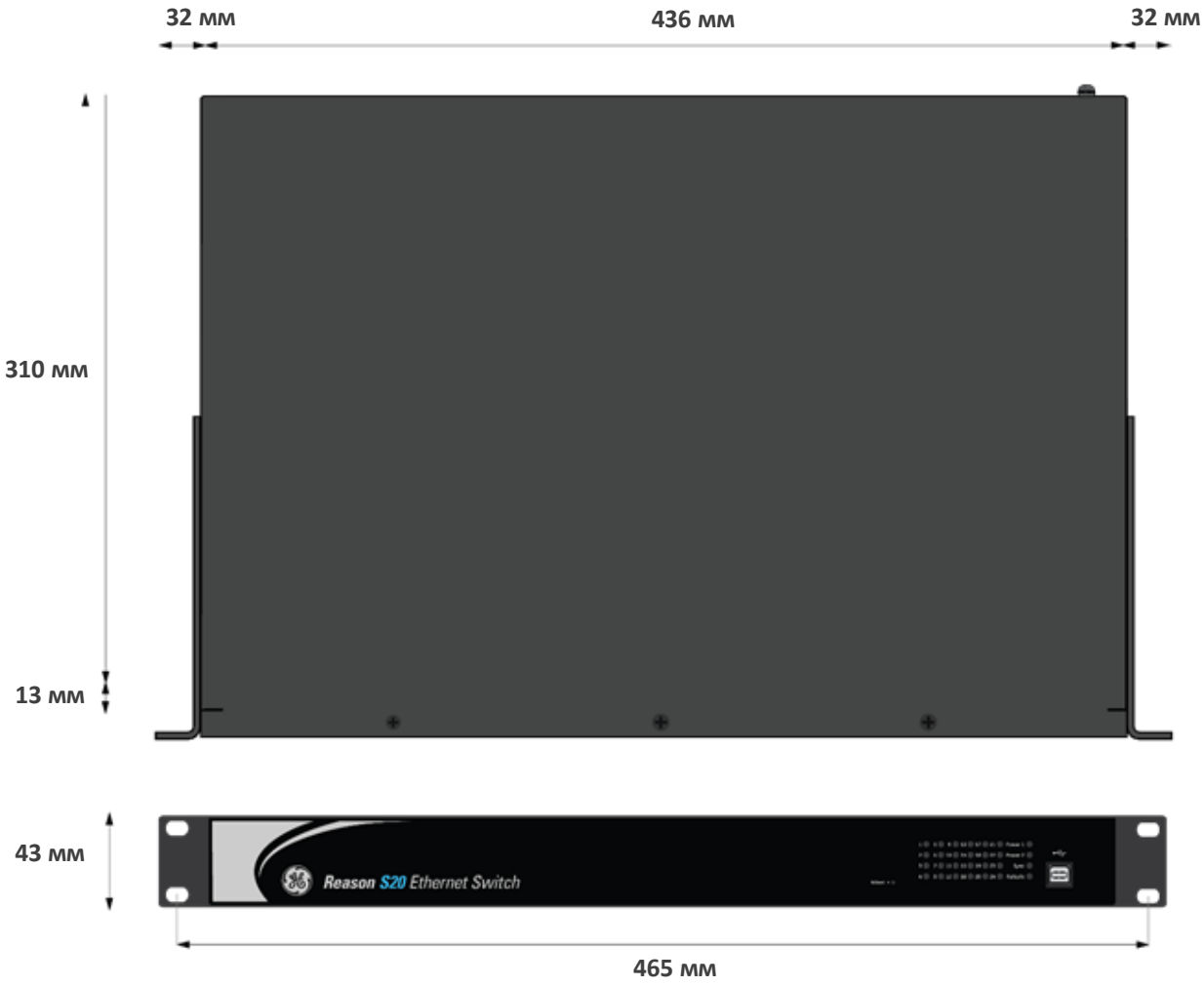


Рисунок 74: Розміри S20

13 Відповідність нормам безпеки

Таблиця 20: Випробування на відповідність вимогам щодо безпеки

UL 60950-1	Загальні вимоги безпеки	Номер нормативного документа E484801	
МЕК 60255-27	Імпульсна витримувана напруга	Джерело живлення	5 кВ
		Вихідні контакти реле	5 кВ
		Порти зв'язку - не застосовується через подвійну ізоляцію на PS та контактах реле	
МЕК 60255-27	Напруга, витримувана діелектриком	Джерело живлення	3,25 кВ змін. струму
		Вихідні контакти реле	3,25 кВ змін. струму
		Порти зв'язку - не застосовується через подвійну ізоляцію на PS та контактах реле	
МЕК 60255-27	Горючість	Корпус	Метал, негорючий

		Кришка	Метал, негорючий
		Клеми	V-0 (UL94)
		Плати PCB	V-0 (UL94)
		(Вхідні) трансформатори	V-0 (UL94)
		Вихідні реле	V-1
		Проводка	V-1
МЕК 60255-27	Умови одиничної відмови	без ризику пожежі	
МЕК 60255-27	Опір ізоляції	> 100 МОм при 500 В ПОСТ. СТРУМУ	

14 Випробування на вплив навколишнього середовища

Таблиця 21: Кліматичні випробування

МЕК 60068-2-1	Випробування на роботу та зберігання в умовах низьких температур	Температура	-40 °C
		Тривалість впливу	16 годин
		Тип випробувань	Ad
МЕК 60068-2-2	Випробування на роботу та зберігання в умовах впливу сухого тепла	Температура	+85 °C
		Тривалість впливу	16 годин
		Тип випробувань	Bd
МЕК 60068-2-14	Випробування на стійкість до зміни температур	Нижня температура	-40 °C
		Верхня температура	+55 °C
		Тривалість впливу	5 теплових циклів
		Період витримки/відновлення	9 годин
		Період усталеного режиму	3 годин
		Тип випробувань	Nb
МЕК 60068-2-30	Випробування при циклічних впливах температури та вологи	Нижня температура	+25 °C, ±3 °C
		Верхня температура	+55 °C, ±2 °C
		Відносна вологість при низькій температурі	97%, -2%, +3%
		Відносна вологість при високій температурі	93%, ±3%
		Тривалість впливу	6 циклів по 24 години (12+12 годин)
		Період відновлення	від 1 до 2 годин
МЕК 60068-2-78	Випробування на вплив вологого тепла у сталому режимі	Температура	+40 °C
		Відносна вологість	93%
		Тривалість	10 діб
		Тип випробувань	Cab

Таблиця 22: Випробування механічних властивостей

МЕК 60255-21-1	Реакція на вплив вібрації	клас 2	
		Діапазон частоти	від 10 до 150 Гц
		Перехідна частота	59 Гц
		Пікове зміщення до переходу	0,075 мм
		Пікове прискорення після переходу	1,0 gn
		Кількість циклів хитання на вісь	1
МЕК 60255-21-1	Вібраційна витривалість	клас 2	
		Діапазон частоти	від 10 до 150 Гц
		Пікове прискорення	2,0 gn
		Кількість циклів хитання на вісь	20
МЕК 60255-21-2	Реакція на ударне навантаження	клас 2	
		Пікове прискорення	10 gn
		Тривалість імпульсу	11 мс
		Кількість імпульсів у кожному напрямку	3
МЕК 60255-21-2	Витримувана ударна міцність	клас 1	
		Пікове прискорення	15 gn
		Тривалість імпульсу	11 мс
		Кількість імпульсів у кожному напрямку	3
МЕК 60255-21-3	Сейсмостійкість	клас 2	
		Діапазон частоти	від 1 до 35 Гц
		Перехідна частота	8 Гц
		Пікове зміщення до переходу X і Y	7,5 мм
		Пікове зміщення до переходу Z	3,5 мм
		Пікове прискорення після переходу X і Y	2,0 gn
		Пікове прискорення після переходу Z	1,0 gn
		Кількість циклів хитання на вісь	1

15 Випробування на електромагнітну сумісність (EMC)

Таблиця 23: Електромагнітна сумісність (EMC) – випробування на випромінювання

CISPR 11 (нижче 1 Гбіт/с)	Емісійне випромінювання	Клас A	
		Частота	від 30 до 230 МГц
		Рівень	50 дБ (мкВ/м) квазіпіковий при 3 м
		Частота	230 до 1000 МГц
		Рівень	57 дБ (мкВ/м) квазіпіковий при 3 м
CISPR 22 (вище 1 Гбіт/с)	Емісійне випромінювання	Клас A	
		Частота	1 до 3 Гбіт/с
		Рівень	56 дБ (мкВ/м) середній; 76 дБ (мкВ/м) піковий при 3 м
		Частота	3 до 6 ГГц
		Рівень	60 дБ (мкВ/м) середній; 80 дБ (мкВ/м) піковий при 3 м
CISPR 22	Кондуктивне та емісійне випромінювання	Клас A	
		Частота	0.15 до 0.50 МГц
		Рівень	79 дБ (мкВ) квазіпіковий; 66 дБ (мкВ) середній
		Частота	0.5 до 30 МГц
		Рівень	73 дБ (мкВ) квазіпіковий; 60 дБ (мкВ) середній

Таблиця 24: Електромагнітна сумісність (EMC) – Випробування на стійкість до завад

МЕК 61000-4-18	Випробування на стійкість до загасаючої коливальної хвилі	Випробувальний рівень 3	
		Частота	100 кГц та 1 МГц
		Джерело живлення (CM)	2,5 кВ
		Джерело живлення (DM)	1,0 кВ
		Вихідні контакти реле (CM)	2,5 кВ
		Вихідні контакти реле (DM)	1,0 кВ
		Порти зв'язку (CM)	2,5 кВ
IEEE C37.90.1	Випробування на стійкість до загасаючої коливальної хвилі 1 МГц	Зона A	
		Джерело живлення (CM)	2,5 кВ
		Джерело живлення (DM)	2,5 кВ
		Вихідні контакти реле (CM)	2,5 кВ
		Вихідні контакти реле (DM)	2,5 кВ
		Порти зв'язку (CM)	2,5 кВ

МЕК 61000-4-2	Випробування на стійкість до електростатичних розрядів	Випробувальний рівень 4	
		Контактний розряд на струмопровідній поверхні	8 кВ
		Контактний розряд на пластинах зв'язку	8 кВ
		Повітряні розряди	15 кВ
IEEE C37.90.3	Випробування на стійкість до електростатичних розрядів	Зона А	
		Контактний розряд на струмопровідній поверхні	8 кВ
		Контактний розряд на пластинах зв'язку	8 кВ
		Повітряні розряди	15 кВ
МЕК 61000-4-3	Випробування на стійкість до випромінюваного радіочастотного електромагнітного поля	Випробувальний рівень 3	
		Напруженість електромагнітного поля	10 В/м
		Діапазон частот	від 80 до 1000 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
		Напруженість електромагнітного поля	10 В/м
		Діапазон частот	від 1400 до 2700 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
		Напруженість електромагнітного поля	10 В/м
		Фіксовані частоти	80, 160, 380, 450, 900, 1850, 2150 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
IEEE C37.90.2	Випробування на радіочастотну сприйнятливість	Зона А	
		Напруженість електромагнітного поля	20 В/м
		Діапазон частот	від 80 до 1000 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
		Напруженість електромагнітного поля	10 В/м
		Діапазон частот	від 1000 до 3800 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
		Напруженість електромагнітного поля	8.5 В/м
		Фіксовані частоти	від 1000 до 6000 МГц
		Амплітудна модуляція (АМ)	1 кГц, 80%
МЕК 61000-4-4	Випробування на стійкість до швидких електричних перехідних процесів	Випробувальний рівень 4	
		Джерело живлення (СМ)	+/- 4 кВ при 5 кГц
		Вихідні контакти реле (СМ)	+/- 4 кВ при 5 кГц
		Порти зв'язку (СМ)	+/- 4 кВ при 5 кГц
		Функціональний канал заземлення (СМ)	+/- 4 кВ при 5 кГц

IEEE C37.90.1	Випробування на стійкість до швидких електричних перехідних процесів	Зона A	
		Джерело живлення (CM/DM)	+/- 4 кВ при 5 кГц
		Вихідні контакти реле (CM/DM)	+/- 4 кВ при 5 кГц
		Порти зв'язку (CM/DM)	+/- 4 кВ при 5 кГц
		Функціональний канал заземлення (CM/DM)	+/- 4 кВ при 5 кГц
МЕК 61000-4-5	Випробування на стійкість до кидків напруги	Джерело живлення, контакти реле, порти зв'язку: Випробувальний рівень 4 /Зона A	
		Джерело живлення (Між фазою і землею)	4,0 кВ
		Джерело живлення (Між фазами)	2,0 кВ
		Вихідні контакти реле (Між фазою і землею)	4,0 кВ
		Вихідні контакти реле (Між фазами)	2,0 кВ
		Порти зв'язку (Між фазою і землею)	4,0 кВ
МЕК 61000-4-6	Випробування на стійкість до кондуктивних завад, наведених радіочастотними електромагнітними полями	Випробувальний рівень 3 / Зона A	
		Джерело живлення, контакти реле, земля, порти зв'язку	
		Рівень	10 В
		Діапазон частот	від 150 кГц до 80 МГц
		Фіксовані частоти	27 та 68 МГц
		Амплітудна модуляція (AM)	1 кГц; 80%
МЕК 61000-4-8	Випробування на стійкість до завад в умовах магнітного поля промислової частоти	Випробувальний рівень 5 / Зона A	
		Частота	50 Гц / 60 Гц
		Постійне магнітне поле	180 сек.
		Рівень	100 А/м
		Короткочасне магнітне поле	3 сек.
		Рівень	1000 А/м
МЕК 61000-4-9	Випробування на стійкість до імпульсного магнітного поля	Випробувальний рівень 5	
		Кількість імпульсів у кожному напрямку	5
		Рівень	1000 А/м
МЕК 61000-4-10	Випробування на несприйнятливість до згасного коливального магнітного поля	Випробувальний рівень 5 / Зона A	
		Частота	100 кГц
		Рівень	100 А/м
		Частота	1 МГц
		Рівень	100 А/м
МЕК 61000-4-11	Випробування на несприйнятливість до провалів напруги змінного струму	Залишкова напруга	0%
		Тривалість (50/60 Гц)	1/1 циклів
		Залишкова напруга	40%
		Тривалість (50/60 Гц)	50/60 циклів
		Залишкова напруга	70%

		Тривалість (50/60 Гц)	25 / 30 циклів
		Залишкова напруга	80%
		Тривалість (50/60 Гц)	250 / 300 циклів
	Випробування на несприйнятливість до короткочасних переривань напруги змінного струму	Залишкова напруга	0%
		Тривалість (50/60 Гц)	250 / 300 циклів
МЕК 61000-4-29	Випробування на несприйнятливість до провалів напруги постійного струму	Залишкова напруга	0%
		Тривалість	50 мс
		Залишкова напруга	40%
		Тривалість	100 мс
		Залишкова напруга	70%
		Тривалість	100 мс
	Випробування на несприйнятливість до короткочасних переривань напруги постійного струму	Залишкова напруга	0%
		Тривалість	5 сек.
	Випробування на несприйнятливість до змін напруги постійного струму	Залишкова напруга	80, 85 та 120%
		Тривалість	10 сек.
МЕК 61000-4-17	Випробування на стійкість до пульсацій напруги електроживлення постійного струму	Випробувальний рівень 4	
		Рівень	15%
		Частота	100/120 Гц
		Форма хвилі	Синусоїдальна
МЕК 60255-26	Плавне керування зупином/пуском (для джерел живлення постійного струму)	Лінійне прискорення при зупині	60 сек.
		Вимкнений стан	5 хв.
		Лінійне прискорення при пуску	60 сек.
МЕК 61000-4-12	Випробування на несприйнятливість до дзвінкої хвилі (100 кГц)	Випробувальний рівень 3	
		Джерело живлення (CM)	2 кВ
		Джерело живлення (DM)	1 кВ
		Вихідні контакти реле (CM)	2 кВ
		Вихідні контакти реле (DM)	1 кВ