Лабораторна робота № 15
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПІДСИСТЕМИ ЖУРНАЛЮВАННЯ ПОДІЙ SYSLOG У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи підсистеми журналювання подій Syslog на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи підсистеми журналювання подій Syslog у мережі, побудованій на базі обладнання Cisco; дослідити процес роботи підсистеми журналювання подій Syslog та процеси передачі повідомлень протоколу Syslog у побудованій мережі.

Теоретичні відомості

Загальні відомості про організацію журналювання подій

Журналювання подій (Logging, Event Logging) – це процес запису інформації про певні події, що відбуваються з об'єктами (процесами) у системі. Поряд з терміном ,,журналювання подій" застосовуються терміни ,,протоколювання подій" та ,,реєстрація подій". Реєстрація інформації здійснюється у системному журналі. Особливістю системного журналу є те, що його записи створюються один по одному у хронологічному порядку. Подальший аналіз даних системного журналу дає змогу визначити, коли і за яких умов виникла та чи інша подія, тобто виконувати аудит подій. Підсистема журналювання подій є складовою підсистеми аудиту (моніторингу) подій, яка, у свою чергу, є невід'ємною складовою системи безпеки.

У різних ОС підсистеми журналювання подій базуються на різних принципах та підходах стосовно розміщення та ведення системних журналів, а також стосовно інформування адміністратора про події. Системний журнал може вестися як локально, так і централізовано. У першому випадку для кожного вузла ведеться окремий системний журнал. У другому випадку загальний системний журнал розміщується на виділеному сервері мережі (або кількох виділених серверах) і всі клієнти мережі надсилають серверові інформа-

цію про власні події з використанням спеціального комунікаційного протоколу.

Системний журнал може зберігатися або у структурованому текстовому файлі (Log-file), або у базі даних. У першому випадку простіше організувати збереження й аналіз даних, оскільки можна застосовувати прості стандартні засоби роботи з файлами. У другому випадку необхідно налагодити функціонування спеціалізованої системи керування базою даних журналювання та мати більш складні засоби обробки й аналізу даних цієї бази.

У деяких випадках результати журналювання зберігаються лише в оперативній пам'яті пристрою, а їх збереження у файлі чи базі даних потребує додаткових налаштувань системи. У багатьох системах підсистема журналювання подій паралельно із записом інформації про подію дає змогу вивести цю ж інформацію на екран комп'ютера мережного адміністратора або навіть надіслати її електронною поштою чи SMS-повідомленням.

Сучасні системи журналювання подій, як правило, є централізованими мережними системами, у яких для збереження інформації застосовуються бази даних (зокрема і розподілені). Централізований підхід до організації журналювання подій надає адміністраторові такі переваги:

– швидкий пошук записів про події, оскільки вся інформація міститься в одному системному журналі;

– полегшене поточне керування пристроями та користувачами мережі, оскільки на основі останніх даних системного журналу можна виконувати моніторинг поточного стану всіх пристроїв та користувачів мережі;

– полегшений аналіз даних системного журналу, оскільки великий централізований масив інформації дає змогу більш точно моніторити та прогнозувати поведінку як окремих пристроїв та користувачів мережі, так і їх поведінку в сукупності;

– зменшення ризику втрати даних, оскільки на більшості сучасних серверів застосовуються засоби резервного збереження даних;

– збільшення рівня захищеності мережі, оскільки оперативне виявлення аномальних подій, що пов’язані із втручанням зловмисника у роботу складових мережі, дає змогу заблокувати дії зловмисника та запобігти втратам інформації.

Загальні відомості про протокол журналювання подій Syslog

Програмний механізм Syslog (System Log, системний журнал) був розроблений і реалізований у 1980 р. відомим фахівцем Еріком Оллманом як частина проекту пересилки електронної пошти Sendmail, який, у свою чергу, був складовою проекту TCP/IP Berkeley Software Distribution (BSD), що проводився Каліфорнійським університетом. Цей механізм виявився настільки вдалим, зручним та стабільним в експлуатації рішенням, що його адаптували для застосування й іншими програмними додатками. З часом Syslog став стандартом de facto для ведення журналів у Unix та GNU Linux системах. Простота та можливість легкого масштабування забезпечили як можливість перенесення Syslog на інші ОС, так і застосування його у багатьох комунікаційних пристроях. Сьогодні під терміном Syslog фахівці розуміють як програмне забезпечення (додатки, бібліотеки), яке вирішує питання відправки й отримання системних повідомлень, так і стандарт передачі та реєстрації повідомлень у комп'ютерних мережах, що функціонують на основі протоколу IP. Надалі ці поняття будуть розглядатися як єдине ціле під назвою протокол Syslog.

Досить довго для Syslog не розроблялися формальні специфікації. Більшість розробників ПЗ та ОС мали свої власні реалізації, які мали проблеми сумісності або взагалі не були сумісними між собою. Перші кроки з уніфікації та стандартизації Syslog виконані IETF на початку 2001 року. Як результат у серпні 2001 року було опубліковано базовий стандарт RFC-3164 „The BSD Syslog Protocol", у якому було описано поточний стан протоколу, визначені його роль та значення в інформаційно-комунікаційних системах, формалізовано структуру повідомлення, розглянуті базові моделі розгортання та сформульовані можливі проблеми безпеки. У листопаді 2001 року було опубліковано стандарт RFC-3195 „Reliable Delivery for Syslog", у якому пропонувалися рішення, які давали можливість підвищити рівень надійності протоколу.

Сьогодні основним стандартом протоколу Syslog є опублікований у березні 2009 року стандарт RFC-5424 „The Syslog Protocol". У цей же період була опублікована ціла група стандар-

тів, що запропонували значне вдосконалення протоколу Syslog. Це стандарти RFC-5425 „Transport Layer Security (TLS) Transport Mapping for Syslog", RFC-5426 „Transmission of Syslog Messages over UDP", RFC-5427 „Textual Conventions for Syslog Management". Пізніше, у жовтні 2009 року, була опублікована ще одна група стантартів, у яких описані можливості взаємодії з протоколом SNMP. До цієї групи належать стандарти RFC-5674 „Alarms in Syslog", RFC-5675 „Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages", RFC-5676 „Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications". У 2010 році були опубліковані стандарти, пов'язані з підвищенням рівня захисту протоколу Syslog: RFC-5848 „Signed Syslog Messages" та RFC-6012 „Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog". У 2012 році було опубліковано стандарт RFC-6587 „Transmission of Syslog Messages over TCP". Нині розробляються нові стандарти протоколу, пов'язані із забезпеченням журналювання під час застосування хмарних обчислень та технології NAT.

У ході розробки протоколу Syslog було застосовано багаторівневий підхід – виділено три функціональних рівні, на кожен із яких покладаються певні завдання щодо забезпечення функціонування протоколу:

– рівень вмісту (Syslog Content Layer).

– рівень додатка (Syslog Application Layer).

– рівень транспортування (Syslog Transport Layer).

На рівні вмісту вирішуються питання управління інформацією, яка міститься у повідомленнях протоколу Syslog. На рівні додатка вирішуються питання формування (генерації), інтерпретації, маршрутизації та збереження повідомлень протоколу Syslog. Рівень транспортування відповідає за розміщення повідомлень у середовище передачі даних та отримання повідомлень із середовища.

Програмні модулі Syslog, які розміщуються на зазначених рівнях, можуть виконувати такі ролі:

– джерело (Syslog Originator).

– колектор (Syslog Collector).

– ретранслятор (Syslog Relay).

– транспортний відправник (Syslog Transport Sender).

– транспортний отримувач (Syslog Transport Receiver).

На Syslog Originator покладаються функції генерації інформації, яка буде розміщена у повідомленні протоколу. Фактично Syslog Originator – це Syslog-клієнт. На Syslog Collector покладаються функції збору інформації із Syslog-повідомлень із метою подальшого аналізу. Фактично Syslog Collector – це Syslog-сервер. На Syslog Relay покладаються функції пересилки та приймання повідомлень до/від джерел та інших ретрансляторів та відправку їх до колекторів або інших ретрансляторів. Транспортний відправник передає Syslog-повідомлення певному транспортному протоколу – виконує інкапсуляцію Syslog-повідомлення у повідомлення відповідного транспортного протоколу. Транспортний отримувач отримує Syslog-повідомлення від певного транспортного протоколу – виконує деінкапсуляцію Syslog-повідомлення з повідомлення відповідного транспортного протоколу.

Належність модулів до відповідних рівнів протоколу Syslog наведено на рис. 4.1.

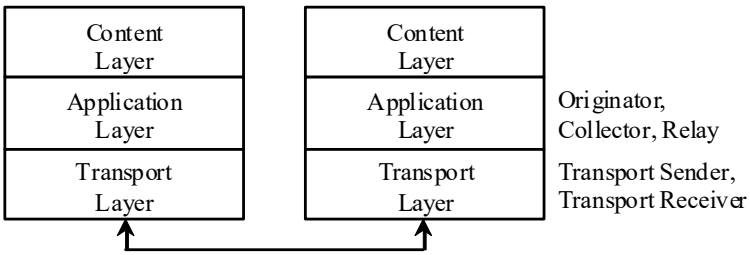

Рис. 4.1. Рівні та модулі протоколу Syslog

Для забезпечення функціонування засобів протоколу Syslog застосовуються такі принципи:

– протокол Syslog є симплексним протоколом, тобто не забезпечує підтвердження доставки повідомлень (можливе забезпечення підтвердження доставки за рахунок засобів відповідного транспортного протоколу);

– джерела та ретранслятори можуть бути налагоджені у такий спосіб, щоб надсилати одне і те ж Syslog-повідомлення кількома колекторам або ретрансляторам;

– джерело, ретранслятор та колектор можуть знаходитися у межах одного вузла (однієї системи).

Можливі схеми взаємодії програмних модулів протоколу Syslog наведені на рис. 4.2.

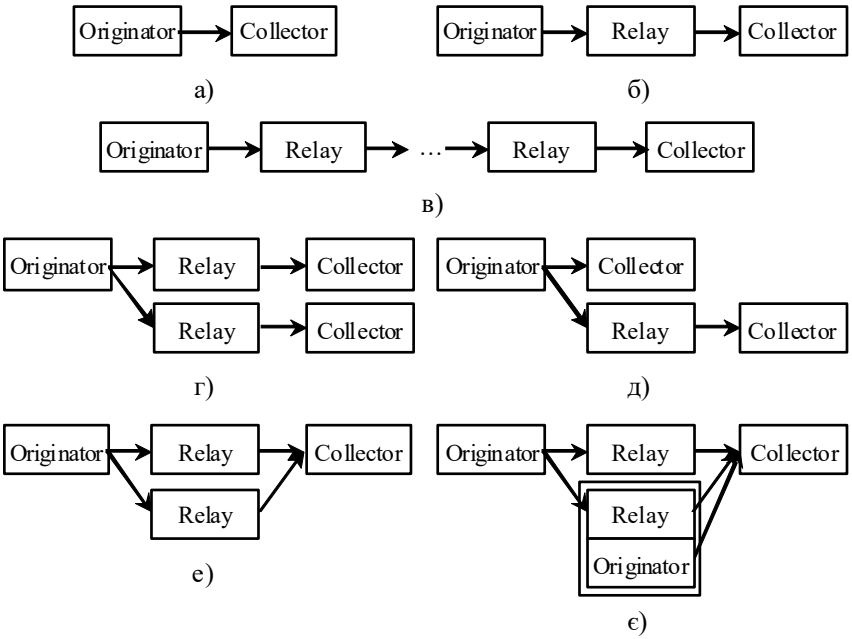

Рис. 4.2. Можливі схеми взаємодії програмних модулів протоколу Syslog

Стосовно моделі OSI та стеку TCP/IP протокол Syslog є протоколом прикладного рівня. Для транспортування повідомлень протоколу Syslog початково передбачалося застосування протоколу UDP (порт сервера 514). Пізніше були запропоновані рішення із застосуванням протоколу TCP (порт сервера 601). Для безпечної передачі Syslog-повідомлень застосовується механізм TLS (застосовується як протокол UDP (порт сервера 6514), так і протокол TCP (порт сервера 6514)).

Джерелами Syslog-повідомлень є служби (підсистеми, процеси, додатки) ОС вузла. Оскільки спочатку механізм Syslog розроблявся для Unix-подібних ОС, то багато концепцій цієї ОС були перенесені до протоколу Syslog. Це стосується і категорій системних об'єктів (Facilities), що формують повідомлення. Перелік та описи категорій системних об'єктів протоколу Syslog (Syslog Message Facilities) наведені у табл. 4.1.

Таблиця 4.1

Категорії системних об'єктів, що формують повідомлення протоколу Syslog

Код об'єкта	Назва категорії об'єкта	Позначення	Опис
0	Kernel Messages	kern	Ядро операційної системи
1	User-Level Messages	user	Програмне забезпечення користувача
2	Mail System	mail	Поштова служба (підсистема)
3	System Daemons	daemon	Системні служби (демони)
4	Security/ Authorization Messages	auth	Служби системи безпеки (авторизації)
5	Messages Generated Internally By Syslogd	syslog	Власні повідомлення служби Syslog
6	Line Printer Subsystem	lpr	Підсистема друку
7	Network News Subsystem	news	Підсистема груп новин
8	UUCP Subsystem	uucp	Підсистема копіювання файлів Unix-to-Unix
9	Clock Daemon	cron	Служба часу
10	Security/ Authorization Messages	authpriv	Служби системи безпеки (авторизації) – привілейований режим
11	FTP Daemon	ftp	Служба копіювання файлів
12	NTP Subsystem	ntp	Підсистема мережного часу
13	Log Audit	log audit	Служба журналу аудиту
14	Log Alert	log alert	Служба журналу аварій
15	Clock Daemon (Note 2)	cron	Служба часу
16	Local0	local0	Локально визначена служба 0
17	Local1	local1	Локально визначена служба 1
18	Local2	local2	Локально визначена служба 2
19	Local3	local3	Локально визначена служба 3
20	Local4	local4	Локально визначена служба 4
21	Local5	local5	Локально визначена служба 5
22	Local6	local6	Локально визначена служба 6
23	Local7	local7	Локально визначена служба 7

Повідомлення протоколу Syslog мають 8 рівнів важливості (Syslog Message Severities). Встановлення рівня важливості повідомлення здійснюється на основі типу і важливості умов виникнення помилки чи події у системі. Чим нижче значення рівня важливості,

тим важливішим є повідомлення. Перелік та описи рівнів важливості повідомлень протоколу Syslog наведені у табл. 4.2.

Таблиця 4.2

Рівні важливості повідомлень протоколу Syslog

Рівень важливості	Назва	Позначення	Опис
0	Emergency	EMERG*	Повідомлення про непрацездатність системи
1	Alert	ALERT	Повідомлення про потребу термінового втручання
2	Critical	CRIT	Повідомлення про критичний стан системи
3	Error	ERR**	Повідомлення про виникнення помилки у системі
4	Warning	WARNING***	Повідомлення про умови, які потребують уваги
5	Notice	NOTICE	Повідомлення про нормальні, але важливі події
6	Informational	INFO	Інформаційне повідомлення
7	Debug	DEBUG	Повідомлення відлагодження

Примітка: * – стара назва PANIC; ** – стара назва ERROR; *** – стара назва WARN.

Стандартом не накладаються обмеження на довжину повідомлення протоколу Syslog. Вони визначаються тим транспортним протоколом, який застосовується. Але для всіх транспортних протоколів передбачається дотримання такої умови – максимум довжини повідомлення не повинен бути меншим 480 байтів. Будь-який отримувач повідомлення повинен приймати повідомлення до 480 байтів включно. Для всіх реалізацій протоколу рекомендується забезпечити отримувачеві можливість приймання повідомлень довжиною до 2048 байтів включно. Отримувачі можуть приймати повідомлення і з більшою, ніж 2048 байтів, довжиною. Якщо адресат отримує повідомлення з більшою, ніж він підтримує, довжиною, то надлишкова частина повідомлення відкидається й обробка повідомлення виконується за встановленими для адресата правилами. Розробники обладнання і програмного забезпечення можуть встановлювати свої обмеження довжини Syslog-повідомлення, зокрема, фірма Cisco встановлює максимальну довжину 1024 байти.

Узагальнена структура повідомлення протоколу Syslog наведена на рис. 4.3.

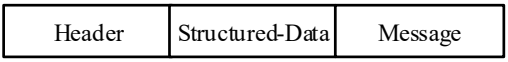

Рис. 4.3. Узагальнена структура повідомлення протоколу Syslog

До складу заголовка Header входять поля, які містять загальну інформацію про відправника повідомлення: PRI, Version, Timestamp, Hostname, App-Name, ProcID, MsgID. Поле PRI містить службові символи та підполе PRIVAL, яке містить коди об'єктів і рівні важливості повідомлення. Поле Version містить номер версії протоколу, нині використовується версія 1. Поле Timestamp містить часові параметри події. Решта полів відповідно ідентифікують вузол-відправник повідомлення (тестова назва чи IP-адреса), додаток-відправник повідомлення, ідентифікатор процесу, ідентифікатор повідомлення. До складу поля Structured-Data входять поля SD-Element, SD-Param, SD-ID, Param-Name, Param-Value, SD-Name. Дані поля використовуються для представлення інформації у більш точному і зручному для опрацювання форматі. Поле Message містить текст повідомлення про подію у довільному записі. Правила формування полів Syslog-повідомлення детально описані у RFC-5424.

Засоби організації журналювання подій на базі протоколу Syslog

У більшості сучасних ОС наявні засоби, які забезпечують функціонування механізмів протоколу Syslog. Якщо вести мову про ОС Unix/Linux, то у більшості клієнтських та серверних версій цих ОС згадані модулі є невід'ємними їх частинами та активуються за замовчуванням при початковому встановленні системи. Якщо вести мову про ОС Windows та деякі інші ОС, то в них наявні власні засоби журналювання і для здійснення журналювання подій із використанням протоколу Syslog потрібне виконання певних додаткових дій щодо встановлення та активації засобів забезпечення його функціонування. У багатьох ОС, що застосовуються для керування роботою комутаторів, маршрутизаторів, міжмережних екранів та інших комунікаційних пристроїв такі засоби теж наявні й активовані за замовчуванням.

В ОС Unix наявна стандартна реалізація протоколу Syslog у вигляді пакета **syslogd** та однойменного демона. Даний демон здійснює приймання повідомлень із порту 514 UDP та від локальних джерел (сокет /dev/log). **Syslogd** дає змогу записувати повідом-

лення у локальний системний журнал, виводити повідомлення на консоль та термінал, пересилати повідомлення на інший сервер.

В ОС Linux реалізація протоколу Syslog виконання у вигляді пакета **sysklogd**, до складу якого входить пакет **syslogd** та пакет **klogd**, який читає повідомлення ядра, визначає їх рівень, перетворює адреси команд в імена програм і передає повідомлення **syslogd**. Нині замість пакета **sysklogd** широко впроваджуються нові пакети **syslog-ng** та **rsyslogd**, що мають покращений функціонал. Ці пакети підтримуються такими ОС Linux, як: Red Hat, Debian, Ubuntu, OpenSUSE, Gentoo, а також ОС FreeBSD, ОС Solaris, ОС AIX.

Для ОС Windows розробники пропонують великий набір як платних фірмових, так і безкоштовних відкритих програмних продуктів, які реалізовують функції Syslog-серверів та Syslog-агентів, а також забезпечують можливості опрацювання отриманих даних. Деякі з них є досить простими і забезпечують мінімум функціоналу. Наприклад, відкритий продукт SysRose Syslog Desktop реалізує лише отримання Syslog-повідомлень, виведення їх вмісту на екран та збереження у файл. Деякі реалізації є досить складними і забезпечують максимум можливостей для збереження й опрацювання отриманої інформації, зокрема використання для збереження повідомлень бази даних, пересилку повідомлення про певну подію електронною поштою чи з використанням СМС-повідомлення тощо. Серед них слід згадати розробки фірми Datagram Consulting – Datagram Syslog Server та фірми SolarWinds – Kiwi Syslog. Розробки SolarWinds широко застосовуються фахівцями для підготовки до сертифікації Cisco різних рівнів.

Перелік та характеристики найпоширеніших продуктів Syslog для ОС Windows наведені у табл. 4.3

Таблиця 4.3

Перелік та характеристики найпоширеніших продуктів Syslog для ОС Windows

Назва	Сайт виробника	Сервер	Агент	Додаткові засоби перегляду
SysRose Syslog Desktop	sysrose.com	+	–	–
Datagram Syslog Server	syslogserver.com	+	+	+
Kiwi Syslog Server	kiwisyslog.com	+	–	+

Intersect Alliance Syslog	intersectalliance.com	–	+	–
Syslog-ng	balabit.com	+	+	–
WinSyslog	winsyslog.com	+	–	+
Visual Syslog Server	maxbelkov.github.io/	+	–	–

Організація журналювання подій на пристроях Cisco

На комунікаційних пристроях Cisco розробниками Cisco IOS передбачено застосування різних варіантів організації журналювання подій. Зокрема, це такі варіанти:

1. Консольне журналювання (Console Logging).
2. Локальне журналювання (Buffered Logging).
3. Термінальне журналювання (Terminal Logging).
4. Журналювання на базі протоколу Syslog.
5. Журналювання на базі протоколу SNMP (SNMP Traps).
6. Журналювання на базі моделі AAA (AAA Accounting).

У разі застосування консольного журналювання всі повідомлення про події в системі виводяться через консольне підключення у вікно термінального додатка адміністратора. Локальне журналювання передбачає, що у системі виділена певна область оперативної пам'яті – внутрішній буфер, у якому зберігається більшість останніх повідомлень про події. Оскільки розмір буфера обмежений (кілька кілобайтів), то старіші повідомлення з буфера видаляються, їх місце займають новіші. Локальне журналювання на пристроях Cisco активоване за замовчуванням. Термінальне журналювання аналогічне консольному, за винятком того, що у даному випадку підключення до пристрою здійснюється через мережу за допомогою відповідного протоколу віддаленого доступу. Журналювання на базі протоколу Syslog передбачає, що вбудований Syslog-клієнт Cisco IOS надсилає повідомлення про події на один або кілька зовнішніх Syslog серверів із використанням протоколу Syslog. Журналювання на базі протоколу SNMP передбачає, що SNMP-клієнт Cisco IOS надсилає повідомлення SNMP Traps на відповідний SNMP-сервер. Журналювання на базі моделі AAA передбачає, що пристрій Cisco надсилає відповідні повідомлення на пристрій NAS (Network Access Server).

Перші три варіанти журналювання мають один суттєвий недолік – при вимкненні або перезавантаженні пристрою записи

про події зникають. Цього недоліку не мають решта варіантів, оскільки у них збереження записів про події здійснюється засобами відповідних серверів на жорстких дисках або інших постійних носіях. Також останні три варіанти журналювання не мають обмежень на об'єм збережених повідомлень про події.

Параметри журналювання подій за замовчуванням для пристроїв Cisco наведені у табл. 4.4.

Таблиця 4.4

Параметри журналювання подій для пристроїв Cisco за замовчуванням

Параметр	Значення за замовчуванням
Консольне журналювання	Активоване
Рівень важливості консольного журналювання	DEBUG
Файл журналювання	Не зазначено
Розмір буфера журналювання	4096 байтів
Розмір таблиці історії повідомлень	1 повідомлення
Часові мітки	Відключені
Синхронне журналювання	Відключене
Сервер журналювання	Відключений
IP-адреса сервера журналювання	Не встановлена
Журналювання змін конфігурації	Відключене
Категорія системного об'єкта сервера	Local7
Рівень важливості сервера	INFO

Рекомендації стосовно налагодження журналювання подій на базі протоколу Syslog

Застосування журналювання подій на базі протоколу Syslog має певні особливості, які можуть впливати на функціонування мережі в цілому. По-перше, генерується досить великий об'єм трафіка, що може впливати на роботу як Syslog-клієнта, так і Syslog-сервера. По-друге, для деяких критичних систем важливим є забезпечення детального журналювання подій. По-третє, у протоколі Syslog відсутні засоби забезпечення інформаційної безпеки. Тому при налагодженні та експлуатації підсистеми журналювання подій на базі протоколу Syslog слід дотримуватися таких базових рекомендацій:

1. Здійснювати збереження Syslog-повідомлень централізовано (на одному або кількох серверах).

2. Забезпечити сервер(и) достатнім об'ємом ресурсів для збереження й опрацювання даних.

3. Обмежити, за можливості, кількість Syslog-повідомлень, що передаються пристроєм.

4. Активувати більш детальне журналювання подій на вибраних критичних системах чи системах, на які впливають користувачі.

5. Використовувати коди об'єктів для кращої організації збереження та обробки даних на Syslog-серверах.

6. Не застосовувати консольного журналювання на пристроях.

7. Призначити IP-адресу відправника Syslog-повідомлень пристрою (типово IP-адресу Loopback-інтерфейсу або IP-адресу інтерфейсу керування).

8. Активувати застосування часових міток (за потреби у деталізованому вигляді).

9. Забезпечити збереження інформації журналювання у базі даних, система керування якою має належні механізми пошуку та обробки даних.

10. Застосовувати, за потреби, захищені з'єднання/канали зв'язку для передачі даних від Syslog-клієнтів до Syslog-серверів.

11. Забезпечити, за потреби, криптографічний захист даних (баз даних, файлів журналювання), що збережені на Syslog-серверах.

12. Синхронізувати системний час Syslog-сервера та Syslog-клієнтів з еталонним джерелом часу за допомогою протоколу NTP.

Порядок налагодження функціонування підсистеми журналювання подій Syslog на пристроях Cisco

Налагодження функціонування підсистеми журналювання подій Syslog на пристроях Cisco при умові застосування зовнішнього Syslog-сервера згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Налагодити параметри системного часу та дати (локально чи за допомогою сервера мережного часу), часового поясу, переходу на літній/зимовий час тощо (рекомендовано).

2. Налагодити детальні параметри часових міток (рекомендовано).

3. Активувати нумерацію Syslog-повідомлень (рекомендовано).

4. Активувати функціонування протоколу Syslog на пристрої (обов'язково).

5. Зазначити IP-адресу основного сервера журналювання (обов'язково).

6. Зазначити IP-адресу (IP-адреси) допоміжного (допоміжних) сервера (серверів) журналювання (необов'язково).

7. Зазначити граничний рівень важливості повідомлень, що будуть журналюватися (рекомендовано).

8. Зазначити об'єкти, повідомлення яких будуть журналюватися (рекомендовано).

9. Обмежити швидкість генерації Syslog-повідомлень (необов'язково).

10. Відключити консольне журналювання (рекомендовано).

11. Активувати та налагодити параметри локального журналювання (рекомендовано).

12. Налагодити журналювання успішних спроб входу в систему за допомогою протоколів віддаленого доступу (рекомендовано).

13. Налагодити журналювання невдалих спроб входу в систему за допомогою протоколів віддаленого доступу (рекомендовано).

14. Зазначити вихідний інтерфейс – відправник Syslog-повідомлень (рекомендовано).

15. Активувати включення у Syslog-повідомлення додаткової інформації: назви пристрою, імені користувача тощо (необов'язково).

Команди налагодження функціонування журналювання подій на пристроях Cisco

Налагодження функціонування журналювання подій може здійснюватися на більшості комунікаційних пристроїв, вироблених фірмою Cisco. Сам процес налагодження є достатньо уніфікованим як для пристроїв із досить простим функціоналом, які працюють під управлінням ОС Cisco IOS, так і для спеціалізованих пристроїв, які працюють під управлінням інших ОС – Cisco NX-OS, Cisco IOS XR, Cisco IOS XE. Деякі відмітності можуть виникати через особливості синтаксису команд та версій ОС.

Налагодження системи журналювання подій на пристроях Cisco має певні особливості. Вони пов'язані з тим, який варіант (варіанти) журналювання буде застосовуватися. Загальні параметри функціонування системи журналювання подій налагоджуються у режимі гло-

бальної конфігурації. Специфічні параметри можуть налагоджуватися у режимі конфігурування лінії. У першу чергу, це стосується консольного журналювання та термінального журналювання. За замовчуванням на пристроях Cisco налагоджене локальне журналювання подій.

Слід пам'ятати, що важливим аспектом функціонування системи журналювання подій є коректне встановлення параметрів системних годинників пристроїв та параметрів часового поясу. Рекомендовано, щоб усі пристрої мережі синхронізували свої параметри часу від одного джерела.

Основною командою, від якої походить решта команд для налагодження засобів журналювання подій, у Cisco IOS є команда **logging**. До переліку похідних команд входять такі команди, як: **logging**, **logging alarm**, **logging buffered**, **logging buginf**, **logging cns-events**, **logging console**, **logging count**, **logging delimiter tcp**, **logging discriminator**, **logging esm**, **logging exception**, **logging facility**, **logging filter**, **logging history**, **logging host**, **logging message-counter**, **logging monitor**, **logging on**, **logging origin-id**, **logging persistent**, **logging queue-limit**, **logging rate-limit**, **logging reload**, **logging server-arp**, **logging source-interface**, **logging synchronous**, **logging trap**, **logging userinfo**.

Важливою командою, яка відіграє особливу роль при налагодженні часових параметрів для протоколу Syslog і яку необхідно використовувати для ефективного функціонування системи, є команда **service timestamps** та похідні від неї команди **service timestamps debug** та **service timestamps log**. Також варто застосовувати команду **service sequence-numbers**. Доцільним також є активація журналювання подій, що відбуваються при підключенні та аутентифікації користувача в системі. Для цього застосовуються параметри журналювання команд входу в систему **login on-failure log**, **login on-success log**. Призначення та синтаксис усіх вищезгаданих команд наведено нижче.

Для активації функціонування протоколу Syslog застосовується команда **logging on**. Встановлення імені або IP-адреси Syslog-сервера здійснюється за допомогою команди **logging** із відповідним параметром. Активація можливості відправки сигнальних повідом-

лень пристрою журналювання та встановлення меж рівнів важливості здійснюється за допомогою команди **logging alarm**. Для налагодження розміру буфера журналювання та зазначення подій, які потрібно фіксувати, застосовується команда **logging buffered**. Як параметр цієї команди може використовуватися або числове, або текстове позначення рівня важливості подій. Команда **logging buginf** дозволяє згенерувати повідомлення відлагодження для стандартного системного буфера журналювання. Для попередження ситуації перевантаження процесора пристрою при включеному режимі відлагодження рекомендується цю команду відключати.

Для активації можливості журналювання розсилки повідомлень у форматі XML через CNS Event Bus (Cisco Networking Services Event Bus) застосовується команда **logging cns-events**. Активація можливості пересилки Syslog-повідомлень на всі доступні TTY-лінії та обмеження розсилки по цих лініях на основі рівнів важливості виконується за допомогою команди **logging console**. Для активації можливості підрахунку помилок журналювання використовується команда **logging count**. За замовчуванням підрахунок помилок відключено. Команда **logging delimiter tcp** застосовується для додавання символу нового рядка, який є роздільником між Syslog-повідомленнями в разі використання транспортного протоколу TCP.

Для створення дискримінатора Syslog-повідомлень передбачена команда **logging discriminator**. За її допомогою можна створити описи та задати правила фільтрації подій. Для дозволу змін конфігурації від фільтрів вбудованого менеджера Syslog ESM (Embedded Syslog Manager) застосовується команда **logging esm**. Обмеження розміру буфера виведення інформації про виняткові ситуації здійснюється командою **logging exception**. Для активації відправки повідомлень про помилки/події, що стосуються певного системного об'єкта, застосовується команда **logging facility**.

Зазначення розміщення модулів фільтрації, що застосовуються вбудованим менеджером Syslog ESM, здійснюється за допомогою команди **logging filter**.

Для обмеження запису Syslog повідомлень з певним рівнем важливості до таблиці історії подій пристрою застосовується команда

logging history. Обмеження кількості записів здійснюється командою **logging history size**.

Команда **logging host** застосовується для зазначення параметрів з'єднання з віддаленим вузлом, на якому будуть журналюватися події. За допомогою цієї команди можна зазначити як адресні параметри вузла, так і обрати та налагодити необхідний транспортний протокол.

Активація застосування лічильників повідомлень журналювання здійснюється командою **logging message-counter**. Для активації термінального журналювання та налагодження його параметрів застосовується команда **logging monitor**. Додавання ідентифікатора системи (імені, IP-адреси тощо) до Syslog-повідомлення активується командою **logging origin-id**. Збереження повідомлень журналювання подій на підключеному до пристрою зовнішньому носієві активується та налагоджується за допомогою команди **logging persistent**. Обмеження кількості повідомлень у черзі для подальшого опрацювання у системі здійснюється командою **logging queue-limit**. Обмеження швидкості журналювання (кількості повідомлень за секунду) здійснюється командою **logging rate-limit**. Для встановлення рівня перевантаження застосовується команда **logging reload**. Активація відправки ARP-запиту з метою отримання адреси Syslog-сервера під час процесу завантаження ОС пристрою здійснюється командою **logging server-arp**. Зазначення інтерфейсу виходу Syslog-повідомлень здійснюється командою **logging source-interface**. Застосування цієї команди є корисним, коли необхідно примусово зазначити інтерфейс, IP-адреса якого застосовується як адреса для Syslog-повідомлень. Синхронізація виведення Syslog-повідомлень для кількох отримувачів (консольне журналювання, термінальне журналювання тощо) здійснюється командою **logging synchronous**. Зазначення рівня важливості Syslog-повідомлень, які потрібно журналювати, здійснюється командою **logging trap**. Активація журналювання інформації про користувача системи здійснюється командою **logging userinfo**.

Команди **service timestamps debug** та **service timestamps log** застосовуються для деталізації структури часових міток, які виводяться на екран та додаються у Syslog-повідомлення. Деталізація струк-

тури часових міток надає адміністраторові більш точну інформацію про час виникнення тих чи інших подій.

Команда **service sequence-numbers** застосовується для активації нумерації Syslog-повідомлень, які генеруються пристроєм. Наявність порядкового номера у повідомленні полегшує роботу адміністратора з аналізу системного журналу і у разі підробки записів зловмисником полегшує виявлення цього факту.

Команди **login on-failure log** та **login on-success log** застосовуються для активації журналювання подій при підключенні та аутентифікації користувача у системі. Вказані команди активують журналювання подій про неуспішні та успішні спроби відповідно. Команда **security authentication failure** встановлює кількість дозволених невдалих спроб входу в систему (за хвилину), перевищення якої викличе генерацію повідомлення для журналювання подій.

Необхідно відмітити, що у багатьох протоколах та технологіях, що застосовуються на обладнанні Cisco, існують можливості виконання операцій журналювання подій. У деяких випадках, наприклад, для протоколу мережного часу NTP, необхідна активація журналювання подій адміністратором (із цією метою застосовується команда **ntp logging**), в інших, наприклад для функції безпеки Port Security, журналювання подій активується автоматично.

Синтаксис команди **logging** (режим глобального конфігурування):

logging { *hostname* | *IP-address* },

де ***hostname*** – текстова назва Syslog-сервера, яка або попередньо зазначена за допомогою команди **ip host**, або визначається з використанням засобів DNS;

IP-address – IP-адреса Syslog-сервера, у десятковому записі.

Синтаксис команди **logging alarm** (режим глобального конфігурування):

logging alarm [*severity_level_value*],

де ***severity_level_value*** – рівень важливості повідомлення, може набувати значень Critical (1), Major (2), Minor (3), Informational (4); за замовчуванням не встановлено.

Синтаксис команди **logging buffered** (режим глобального конфігурування):

logging buffered [discriminator *discriminator_name*] [*buffer_size*] [*severity_level_number* | *severity_level_name*],

де **discriminator** – службова конструкція, за допомогою якої специфікується використання визначених користувачем фільтрів;

discriminator_name – текстова назва фільтра, рядок довжиною до 8 символів, регістр символів впливає на трактування назви;

buffer_size – розмір буфера для повідомлень (байтів), може змінюватися у межах від 4096 до 2147483647; за замовчуванням дорівнює 4096 байтів; межі можуть змінюватися залежно від моделі пристрою та версії IOS;

severity_level_number – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC –Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging buffered filtered** (режим глобального конфігурування):

logging buffered filtered [***buffer_size*** **] [***severity_level_number*** **|** ***severity_level_name*****]**,

де ***buffer_size*** – розмір буфера для повідомлень (байтів), може змінюватися у межах від 4096 до 2147483647; за замовчуванням дорівнює 4096 байтів; межі можуть змінюватися залежно від моделі пристрою та версії IOS;

severity_level_number – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно RFC –Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging buffered xml** (режим глобального конфігурування):

logging buffered xml [***xml_buffer_size*** **]**,

де ***xml_buffer_size*** – розмір буфера для XML-повідомлень (байтів), може змінюватися у межах від 4096 до 2147483647; за замовчуванням дорівнює 4096 байтів; межі можуть змінюватися залежно від моделі пристрою та версії IOS;

Синтаксис команди **logging buginf** (режим глобального конфігурування):

logging buginf.

Команда не має параметрів.

Синтаксис команди **logging cns-events** (режим глобального конфігурування):

logging cns-events [***severity_level_number*** **|** ***severity_level_name*** **]**,
де ***severity_level_number*** – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC – Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging console** (режим глобального конфігурування):

logging console [discriminator ***discriminator_name*** **] [** ***severity_level_number*** **|** ***severity_level_name*** **]**,
де **discriminator** – службова конструкція, за допомогою якої специфікується використання визначених користувачем фільтрів;

discriminator_name – текстова назва фільтра, рядок довжиною до 8 символів, регістр символів впливає на трактування назви;

severity_level_number – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно RFC –Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3);

warnings (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging console filtered** (режим глобального конфігурування):

logging console filtered [***severity_level_number*** **|** ***severity_level_name*** **]**,

де ***severity_level_number*** – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC – Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging console guaranteed** (режим глобального конфігурування):

logging count guaranteed.

Команда не має параметрів.

Синтаксис команди **logging console xml** (режим глобального конфігурування):

logging console xml [***severity_level_number*** **|** ***severity_level_name*** **]**,

де ***severity_level_number*** – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC –Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging count** (режим глобального конфігурування):

logging count.

Команда не має параметрів.

Синтаксис команди **logging delimiter tcp** (режим глобального конфігурування):

logging delimiter tcp.

Команда не має параметрів.

Синтаксис команди **logging discriminator** (режим глобального конфігурування):

logging discriminator ***discriminator_name*** **[[facility] [mnemonics] [msg-body] { drops** ***string*** **| includes** ***string*** **}] [severity { drops** ***severity_level_numbers*** **| includes** ***severity_level_numbers*** **}] [rate-limit** ***msg_limit_value*** **],**

де ***discriminator_name*** – текстова назва фільтра, рядок довжиною до 8 символів, регістр символів впливає на трактування назви;

facility – службова конструкція, за допомогою якої зазначається підфільтр повідомлення для шаблона об'єкта в повідомленні про подію;

mnemonics – службова конструкція, за допомогою якої зазначається підфільтр повідомлення для мнемонічного шаблона в повідомленні про подію;

msg-body – службова конструкція, за допомогою якої зазначається підфільтр повідомлення для шаблона msg-body у повідомленні про подію;

drops – службова конструкція, за допомогою якої активується функція відкидання повідомлень, які збігаються із шаблоном;

includes – службова конструкція, за допомогою якої активується функція доставки повідомлень, які співпадають з шаблоном;

string – текстовий рядок, який містить вираз для фільтрації повідомлень;

severity – службова конструкція, за допомогою якої активується використання підфільтра повідомлень для рівня важливості або групи;

severity_level_numbers – одне числове значення рівня або кілька числових значень рівнів важливості повідомлення, одне значення змінюється у межах від 0 до 7;

rate-limit – службова конструкція, за допомогою якої зазначається максимальна кількість повідомлень, які можуть бути опрацьовані за одиницю часу;

msg_limit_value– кількість повідомлень, значення може змінюватися у межах від 1 до 10000.

Синтаксис команди **logging esm config** (режим глобального конфігурування):

logging esm config.

Команда не має параметрів.

Синтаксис команди **logging exception** (режим глобального конфігурування):

logging exception ***excep_size***,

де ***excep_size*** – числове значення граничного розміру буфера (байтів), може змінюватися у межах від 4096 до 2147483647; за замовчуванням дорівнює 4096.

Синтаксис команди **logging facility** (режим глобального конфігурування):

logging facility ***facility_type_value***,

де ***facility_type_value*** – текстове позначення системного об'єкта, може набувати значень **auth**, **cron**, **daemon**, **kern**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**, **lpr**, **mail**, **news**, **sys9**, **sys10**, **sys11**, **sys12**, **sys13**, **sys14**, **user**, **uucp**; за замовчуванням встановлено значення **local7**.

Синтаксис команди **logging filter** (режим глобального конфігурування):

logging filter ***filter_url*** **[** ***position_value*** **] [args** ***filter_arguments*****]**,

де ***filter_url*** – текстовий рядок, який містить розміщення модуля фільтрації Syslog, записаний за синтаксичними правилами Cisco IOS; включає і назву файла, який містить модуль фільтрації;

position_value – число, яке вказує порядок, у якому повинні виконуватися модулі фільтрації Syslog ;

args – службова конструкція, за допомогою якої додаються значення для проходження ESM-фільтрації;

filter_arguments – значення аргументів для проведення ESM-фільтрації.

Синтаксис команди **logging history** (режим глобального конфігурування):

logging history [***severity_level_number*** **|** ***severity_level_name*** **],**

де ***severity_level_number*** – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC – Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging history size** (режим глобального конфігурування):

logging history size ***number*****,**

де ***number*** – число, за допомогою якого зазначається кількість повідомлень, про які повинен пам'ятати пристрій, за замовчуванням дорівнює 1.

Синтаксис команди **logging host** (режим глобального конфігурування):

logging host { { *ip-address* | *hostname* } [vrf *vrf_name*] | ipv6 { *ipv6-address* | *hostname* } } [discriminator *discriminator_name* | [filtered [stream *stream_id*] | xml]] [transport { [beep [audit] [channel *channel_number*] [sasl *profile_name*] [tls cipher [*cipher_number*] trustpoint *trustpoint_name*]] | tcp [audit] | udp } [port *port_number*]] [sequence-num-session] [session-id { hostname | ipv4 | ipv6 | string *custom_string* }],

де ***hostname*** – текстова назва Syslog-сервера, який буде отримувати Syslog-повідомлення; ця адреса або попередньо зазначається за допомогою команди **ip host**, або визначається з використанням засобів DNS;

IP-address **–** IP-адреса Syslog-сервера, який буде отримувати Syslog-повідомлення, у десятковому записі;

vrf – службова конструкція, за допомогою якої зазначається, що використовується технологія VRF (Virtual Routing and Forwarding);

vrf_name – назва об'єкта технології VRF;

ipv6 – службова конструкція, за допомогою якої зазначається, що використовується IP-адреса версії 6;

ipv6-address – IP-адреса версії 6 Syslog-сервера, який буде отримувати Syslog-повідомлення, у шістнадцятковому записі;

discriminator – службова конструкція, за допомогою якої специфікується використання визначених користувачем фільтрів;

discriminator_name – текстова назва фільтра, рядок довжиною до 8 символів, регістр символів впливає на трактування назви;

filtered – службова конструкція, за допомогою якої активується модуль фільтрації з використанням фільтра ESM перед відправкою повідомлення;

stream – службова конструкція, за допомогою якої вказується, необхідність відправки зазначеному вузлові повідомлень із певним ідетифікатором потоку, що відфільтровані за допомогою ESM;

stream_id – числове значення ідентифікатора потоку, може набувати значень у межах від 10 до 65535;

xml – службова конструкція, за допомогою якої активується використання тегів XML, які визначені Cisco, в результати журналювання;

transport – службова конструкція, за допомогою якої активується використання певного транспортного протоколу;

beep – службова конструкція, за допомогою якої активується використання транспортного протоколу BEEP (Blocks Extensible Exchange Protocol);

audit – службова конструкція, за допомогою якої активується ідентифікація вузла для журналювання міжмережних екранів, використовується лише для протоколів TCP та BEEP;

channel – службова конструкція, за допомогою якої вказується номер каналу протоколу BEEP;

channel_number – числове значення номера каналу BEEP, може набувати значень 1, 3, 5, 7, 9, 11, 13, 15; за замовчуванням дорівнює 1;

sasl – службова конструкція, за допомогою якої активується використання профілю BEEP SASL (Simple Authentication and Security Layer);

profile_name – текстова назва профілю SASL;

tls cipher – службова конструкція, за допомогою якої активується використання засобів шифрування для відповідного з'єднання;

cipher_number – числове значення, яке використовується для вибору способу шифрування, може набувати значень від 32 до 224 як сума – результат додавання чисел 32 (ENC_FLAG_TLS_RSA_WITH_ NULL_SHA), 64 (ENC_FLAG_TLS_RSA_ WITH_RC4_128_MD5) та 128 (ENC_FLAG_TLS_RSA_WITH_AES_128_CBC_SHA);

trustpoint – службова конструкція, за допомогою якої активується використання ,,точки довіри" для ідентифікаційної інформації та сертифікатів;

trustpoint_name – текстова назва ,,точки довіри";

tcp – службова конструкція, за допомогою якої активується використання транспортного протоколу TCP;

udp – службова конструкція, за допомогою якої активується використання транспортного протоколу UDP, даний протокол використовується за замовчуванням;

port – службова конструкція, за допомогою якої змінюється номер порта транспортного протоколу;

port_number – числове значення номера порта, може змінюватися у межах від 1 до 65535, за замовчуванням для протоколу TCP дорівнює 601, для протоколу BEPP – 601, для протоколу UDP – 514;

sequence-num-session – службова конструкція, за допомогою якої активується включення тегу номера сесійної послідовності у Syslog-повідомлення;

session-id – службова конструкція, за допомогою якої активується тегування сесій Syslog-повідомлень;

hostname – службова конструкція, за допомогою якої активується включення імені вузла у тег ідентифікатора сесії;

ipv4 – службова конструкція, за допомогою якої активується включення IP-адреси версії 4 відправника Syslog-повідомлення у тег ідентифікатора сесії;

ipv6 – службова конструкція, за допомогою якої активується включення IP-адреси версії 6 відправника Syslog-повідомлення у тег ідентифікатора сесії;

string – службова конструкція, за допомогою якої активується включення довільного текстового рядка у тег ідентифікатора сесії;

custom_string – довільний текстовий рядок.

Синтаксис команди **logging message-counter** (режим глобального конфігурування):

logging message-counter { debug | log | syslog },

де **debug** – службова конструкція, за допомогою якої активується лічильник діагностичних повідомлень;

log – службова конструкція, за допомогою якої активуються всі лічильники повідомлень;

syslog – службова конструкція, за допомогою якої активується лічильник Syslog-повідомлень; використання цього лічильника активовано за замовчуванням.

Синтаксис команди **logging monitor** (режим глобального конфігурування):

logging monitor [discriminator ***discriminator_name*** **] [** ***severity_level_number*** **|** ***severity_level_name*** **]**,

де **discriminator**, ***discriminator_name***, ***severity_level_number***, ***severity_level_name*** – параметри, що аналогічні відповідним параметрам команди **logging console**.

Синтаксис команди **logging monitor filtered** (режим глобального конфігурування):

logging monitor filtered [***severity_level_number*** **|** ***severity_level_name*** **]**,

де ***severity_level_number***, ***severity_level_name*** – параметри, що аналогічні відповідним параметрам команди **logging console filtered**.

Синтаксис команди **logging monitor xml** (режим глобального конфігурування):

logging monitor xml [***severity_level_number*** **|** ***severity_level_name*** **]**,

де ***severity_level_number***, ***severity_level_name*** – параметри, що аналогічні відповідним параметрам команди **logging console xml**.

Синтаксис команди **logging on** (режим глобального конфігурування):

logging on.

Команда не має параметрів.

Синтаксис команди **logging origin-id** (режим глобального конфігурування):

logging origin-id { hostname | ip | ipv6 | string ***user_defined_id*** **},**

де **hostname** – службова конструкція, за допомогою якої активується використання імені вузла для ідентифікації відправника повідомлення;

ip – службова конструкція, за допомогою якої активується використання IP-адреси версії 4 вихідного інтерфейсу для ідентифікації відправника повідомлення;

ipv6 – службова конструкція, за допомогою якої активується використання IP-адреси версії 6 вихідного інтерфейсу для ідентифікації відправника повідомлення;

string – службова конструкція, за допомогою якої активується використання текстового рядка, який зазначається адміністратором, для ідентифікації відправника повідомлення;

user_defined_id – текстовий рядок – ідентифікатор відправника повідомлення.

Синтаксис команди **logging persistent** (режим глобального конфігурування):

logging persistent [batch ***batch_size*** **] { filesize** ***logging_file_size*** **} [immediate] { notify } [protected] { size** ***filesystem_size*** **} [threshold** ***threshold_capacity*** **[alert]] [url { disk0:/***directory* **| disk1:/***directory* **}],**
де **batch** – службова конструкція, за допомогою якої змінюється розмір пакета.

batch_size – розмір пакета (байтів), може змінюватися у межах від 4096 до максимального розміру дискового простору; за замовчуванням дорівнює 4096;

filesize – службова конструкція, за допомогою якої змінюється розмір індивідуального файла журналювання;

logging_file_size – розмір файла (байтів), може змінюватися у межах від 8192 до максимального розміру дискового простору; за замовчуванням дорівнює 262144;

immediate – службова конструкція, за допомогою якої активується функція негайного внесення нового запису у файл журналювання;

notify – службова конструкція, за допомогою якої активується функція відправки повідомлення;

protected – службова конструкція, за допомогою якої активується заборона операцій над файлами журналювання;

size – службова конструкція, за допомогою якої зазначається розмір дискового простору, виділеного для Syslog-повідомлень;

filesystem_size – розмір дискового простору (байтів), може змінюватися у межах від 16384 до максимального розміру дискового простору; за замовчуванням дорівнює 10% від загального дискового простору;

threshold – службова конструкція, за допомогою якої зазначаються граничний розмір пристрою збереження журналу;

threshold_capacity – граничний розмір (%), може змінюватися у межах від 1 до 99; за замовчуванням дорівнює 95%;

alert – службова конструкція, за допомогою якої активується виведення звукового сигналу, коли граничний розмір перевищено;

url – службова конструкція, за допомогою якої зазначається розміщення будь-якої локальної підтримуваної файлової системи; за замовчуванням дорівнює disk0:/syslog;

disk0:/*directory*, **disk1:/*directory*** – повний шлях до каталогу, в якому зберігатимуться журнали.

Синтаксис команди **logging queue-limit** (режим глобального конфігурування):

logging queue-limit [*queue_size* | trap *queue_size* | esm *queue_size*], де ***queue_size*** – кількість повідомлень у відповідній черзі журналювання, може змінюватися у межах від 100 до 2147483647; за замовчуванням дорівнює 100;

trap – службова конструкція, за допомогою якої зазначається обмеження кількості повідомлень, які можуть бути розміщені у черзі для віддаленного Syslog-сервера, а також активується відправка повідомлення до засобу перехоплення;

esm – службова конструкція, за допомогою якої зазначається обмеження кількості повідомлень, які можубть бути розміщені у черзі підсистеми ESM.

Синтаксис команди **logging rate-limit** (режим глобального конфігурування):

logging rate-limit { *number* | all *number* | console { *number* | all *number* } } [except { *severity_level_number* | *severity_level_name* }], де ***number*** – кількість повідомлень, яка може бути зареєстрована у журналі за 1 с, може змінюватися у межах від 10 до 10000; за замовчуванням дорівнює 10;

all – службова конструкція, за допомогою якої встановлюється обмеження для всіх повідомлень про помилки та повідомлень про відлагодження, які виводяться на консоль та принтер;

console – службова конструкція, за допомогою якої встановлюється обмеження для всіх повідомлень про помилки та повідомлень про відлагодження, які виводяться на консоль;

except – службова конструкція, за допомогою якої виключаються повідомлення з рівнем важливості, який нижчий або дорівнює зазначеному;

severity_level_number – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 2;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно з RFC – Eme-rgency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2; встановлено за замовчуванням); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7).

Синтаксис команди **logging source-interface** (режим глобального конфігурування):

logging source-interface { ***interface_type interface_id*** **vrf** ***vrf_name*****}**,

де ***interface_type*** – тип інтерфейсу (порта), може набувати значень **Ethernet**, **FastEthernet**, **GigabitEthernet**, **Serial** тощо;

interface_id – ідентифікатор інтерфейсу, може мати одночислове позначення ***number*** (номер інтерфейсу), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейсу), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/ номер інтерфейсу);

vrf – службова конструкція, за допомогою якої зазначається, що використовується технологія VRF (Virtual Routing and Forwarding);

vrf_name – текстова назва об'єкта технології VRF.

Синтаксис команди **logging synchronous** (режим конфігурування лінії):

logging synchronous [level ***severity_level_number*** **|** ***severity_level_name*** **| all] [limit** ***number_of_lines*** **]**,

де **level** – службова конструкція, за допомогою якої активується використання певного рівня важливості повідомлень у ході організації асинхронного виведення;

severity_level_number – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 2;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно із RFC –Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2; встановлено за замовчуванням); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7).

all – службова конструкція, за допомогою якої активується виведення всіх повідомлень, незалежно від рівня важливості в асинхронному режимі;

limit – службова конструкція, за допомогою якої зазначається кількість рядків виведення, після якої нові повідомлення будуть відкидатися;

number_of_lines – кількість рядків виведення, за замовчуванням дорівнює 20.

Синтаксис команди **logging trap** (режим глобального конфігурування):

logging trap [***severity_level_number*** **|** ***severity_level_name*** **]**,

де ***severity_level_number*** – числове значення рівня важливості повідомлення, може змінюватися у межах від 0 до 7; для більшості систем за замовчуванням дорівнює 7;

severity_level_name – текстове значення рівня важливості повідомлення, може набувати значень: **emergencies** (назва згідно з RFC – Emergency, рівень важливості – 0); **alerts** (Alert, 1); **critical** (Critical, 2); **errors** (Error, 3); **warnings** (Warning, 4); **notifications** (Notice, 5); **informational** (Informational, 6); **debugging** (Debug, 7; встановлено за замовчуванням).

Синтаксис команди **logging userinfo** (режим глобального конфігурування):

logging userinfo.

Команда не має параметрів.

Синтаксис команди **service timestamps** (режим глобального конфігурування):

service timestamps [**debug** | **log**] [**uptime** | **datetime** [**msec**]] [**localtime**] [**show-timezone**] [**year**],

де **debug** – службова конструкція, за допомогою якої зазначається необхідність використання часових міток для повідомлень відлагодження;

log – службова конструкція, за допомогою якої зазначається необхідність використання міток часу для повідомлень журналювання;

uptime – службова конструкція, за допомогою якої зазначається необхідність включення до мітки часу інтервалу часу після завантаження системи;

datetime – службова конструкція, за допомогою якої зазначається необхідність включення до мітки часу поточної дати і часу;

msec – службова конструкція, за допомогою якої зазначається необхідність включення до мітки часу значень часу поточної дати і часу у більш точному вимірюванні, з додаванням мілісекунд;

localtime – службова конструкція, за допомогою якої зазначається необхідність формування мітки часу відповідно до локальної часової зони;

show-timezone – службова конструкція, за допомогою якої зазначається необхідність включення до мітки часу часової зони;

year – службова конструкція, за допомогою якої зазначається необхідність включення до мітки часу значення поточного року.

Синтаксис команди **service sequence-numbers** (режим глобального конфігурування):

service sequence-numbers.

Команда не має параметрів.

Синтаксис команди **login on-failure log** (режим глобального конфігурування):

login on-failure log [every *login_value*],

де **every** – службова конструкція, за допомогою якої зазначається необхідність виконання журналювання неуспішних спроб входу в систему;

login_value – числове значення кількості спроб підключення, може змінюватися у межах від 1 до 65535.

Синтаксис команди **login on-success log** (режим глобального конфігурування):

login on-success log [every *login_number*],

де **every** – службова конструкція, за допомогою якої зазначається необхідність виконання журналювання успішних спроб входу в систему;

login_value – числове значення кількості спроб підключення, може змінюватися у межах від 1 до 65535.

Команди моніторингу та діагностики роботи системи журналювання подій на пристроях Cisco

Для моніторингу та діагностики функціонування системи журналювання подій на пристроях використовуються як команди загального призначення, так і спеціалізовані команди. Перелік спеціалізованих команд є відносно невеликим і включає такі команди як: **show logging**, **show logging count**, **show logging history**, **show logging xml**. Доцільним є також застосування додаткових команд **show facility-alarm status**, **show login**, **show login failure** та їх модифікацій.

Узагальнений перелік команд моніторингу та діагностики роботи системи журналювання подій на пристроях Cisco наведений у табл. 4.5.

Таблиця 4.5

Перелік команд моніторингу та діагностики роботи системи журналювання на пристроях Cisco

Команда	Призначення
Команди **show logging**	
show logging	Виведення загальної інформації про роботу підсистеми журналювання пристрою
show logging count	Виведення кількості повідомлень журналювання за типами
show logging history	Виведення інформації про стан заповнення таблиці історії подій підсистеми журналювання
show logging xml	Виведення загальної інформації про роботу підсистеми журналювання пристрою у форматі розширюваної мови розмітки XML (Extensible Markup Language)
Додаткові команди	

show facility-alarm status	Виведення інформації про стан згенерованих попереджувальних повідомлень
show login	Виведення загальної інформації про підключення до пристрою
show login failure	Виведення інформації про невдалі підключення до пристрою

Модельний приклад налагодження функціонування протоколу журналювання подій Syslog у мережі на базі обладнання Cisco

Розглянемо специфіку налагодження роботи протоколу журналювання подій Syslog для комунікаційних пристроїв мережі, схема якої наведена на рис. 4.4. У даному випадку Syslog-сервером є сервер Serv_A_1, а Syslog-клієнтами – маршрутизатор R_1 і комутатор SW_1. Як сервер журналювання застосовується програмний продукт SysRose Syslog Desktop.

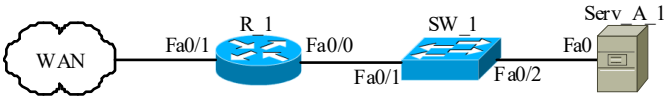

Рис. 4.4. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 4.6. Для налагодження параметрів адресації пристроїв використано дані табл. 4.7.

Таблиця 4.6

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Fa0/0	Комутатор SW_1	Fa0/1
	Fa0/1	WAN	WAN Interface
Комутатор SW_1	Fa0/1	Маршрутизатор R_1	Fa0/0
	Fa0/2	Сервер Serv_A_1	Fa0
Сервер Serv_A_1	Fa0	Комутатор SW_1	Fa0/2

Таблиця 4.7

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.10.1.0	255.255.255.0	/24
WAN	–	196.10.1.0	255.255.255.252	/30
Маршрутизатор R_1	Інтерфейс Fa0/0	195.10.1.254	255.255.255.0	/24
	Інтерфейс Fa0/1	196.10.1.2	255.255.255.252	/30
Комутатор SW_1	Інтерфейс Vlan 1	195.10.1.250	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Сервер	Мережний адаптер	195.10.1.1	255.255.255.0	/24

Serv_A_1	Шлюз за замовчуванням	195.10.1.254	–	–

Для налагодження параметрів комунікаційних пристроїв як Syslog-клієнтів мережі використано дані табл. 4.8.

Таблиця 4.8

Параметри налагодження комунікаційних пристроїв як Syslog-клієнтів

Параметр	Значення
Системний час	Поточний (включає поточні час та дату)
Часовий пояс	EET, Eastern European Time
Перехід на літній час	Активовано
Часові мітки	Активовані (зазначається час, мс та рік)
Нумерація Syslog-повідомлень	Активована
IP-адреса Syslog-сервера	195.10.1.1
Назва пристрою	Додається у Syslog-повідомлення
Ім’я користувача	Додається у Syslog-повідомлення
Рівень важливості повідомлень	Informational
Швидкість генерації Syslog-повідомлень, повідомлень/с	12
Консольне журналювання	Відключено
Локальне журналювання	Активовано
Розмір буфера локального журналювання, кБайт	64
Рівень важливості повідомлень у локальному журналюванні	Debug
Журналювання успішних віддалених підключень до пристрою	Активовано
Журналювання невдалих віддалених підключень до пристрою	Активовано
Період, на який блокуються підключення, с	10
Кількість послідовних невдалих підключень за період	3
Період для послідовних невдалих підключень, с	3

Сценарій налагодження часових параметрів, параметрів адресації інтерфейсів, можливості консольного підключення та віддаленого підключення за протоколом SSH (з використанням локальної аутентифікації на базі механізму користувачів) та параметрів блокування і журналювання невдалих спроб підключення для маршрутизатора мережі R_1 наведений нижче. Сценарій налагодження пара-

метрів комутатора мережі SW_1 подібний до сценарію для маршрутизатора R_1.

```
…
R_1>enable
R_1#clock set 10:04:00 11 dec 2016
R_1#configure terminal
R_1(config)#clock timezone EET 2
R_1(config)#clock summertime EET reccuring last monday october 3:00 last monday march 3:00
R_1(config)#interface FastEthernet 0/0
R_1(config-if)#description LINK_TO_LAN_A
R_1(config-if)#ip address 195.10.1.254 255.255.255.0
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#interface FastEthernet 0/1
R_1(config-if)#description LINK_TO_WAN
R_1(config-if)#ip address 196.10.1.2 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#banner motd # Connection to router R_1
                                    For legal users only #
R_1(config)#username adminer privilege 15 secret adminerpass
R_1(config)#username technic privilege 1 secret technicpass
R_1(config)#enable secret adminerpass2
R_1(config)#ip domain-name mynet.net
R_1(config)#crypto key generate rsa general-keys modulus 1024
R_1(config)#ip ssh version 2
R_1(config)#ip ssh time-out 60
R_1(config)#ip ssh authentication-retries 5
R_1(config)#ip ssh maxstartups 5
R_1(config)#ip ssh logging events
R_1(config)#line console 0
R_1(config-line)#logout-warning 30
R_1(config-line)#absolute-timeout 10
R_1(config-line)#logging synchronous
R_1(config-line)#login local
```

R_1(config-line)#exit
R_1(config)#line vty 0 4
R_1(config-line)#transport input ssh
R_1(config-line)#transport output ssh
R_1(config-line)#logout-warning 30
R_1(config-line)#absolute-timeout 10
R_1(config-line)#logging synchronous
R_1(config-line)#login local
R_1(config-line)#exit
R_1(config)#login block-for 10 attempts 3 within 3
R_1(config)#login on-failure log
R_1(config)#login on-success log
R_1(config)#login delay 5
R_1(config)#exit
R_1#
…

Сценарій налагодження параметрів протоколу журналювання подій Syslog для маршрутизатора мережі R_1 наведений нижче. Параметри журналювання, що пов'язані із підключеннями, були налагоджені у попередньому сценарії (команди **ip ssh logging events**, **login on-failure log**, **login on-success log**).

…
R_1>enable
R_1#configure terminal
R_1(config)#service timestamps log datetime msec year
R_1(config)#service timestamps debug datetime msec year
R_1(config)#service sequence-numbers
R_1(config)#logging on
R_1(config)#logging 195.10.1.1
R_1(config)#logging origin-id hostname
R_1(config)#logging userinfo
R_1(config)#logging trap informational
R_1(config)#logging rate-limit 12 except 2
R_1(config)#logging buffered 64000 debugging
R_1(config)#exit

R_1#exit
R_1>
…

Результати виконання команд моніторингу та діагностики роботи протоколу журналювання подій Syslog для розглянутого прикладу

З метою перегляду інформації про роботу протоколу журналювання подій Syslog для розглянутого прикладу використано команди **show logging**, **show logging count**, **show logging history**. Також використано додаткові команди **show login**, **show login failure**. Результати роботи цих команд для маршрутизатора R_1 наведено відповідно на рис. 4.5 – 4.9. Результати журналювання на сервері Serv_A_1 показані на рис. 4.10.

```
R_1#show logging
Syslog logging: enabled (12 messages dropped, 2 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 25 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
No active filter modules.
    Trap logging: level informational, 29 message lines logged
        Logging to 195.10.1.1(global) (udp port 514, audit disabled,   link up), 29
message lines logged, xml disabled,
              filtering disabled

Log Buffer (64000 bytes):
sslinit fn

*Mar   1 00:00:05.343: %SW_VLAN-4-IFS_FAILURE: VLAN manager encountered file operation
error: call = ifs_open/read / code = 3588 (No device available)
    / bytes transfered = 0
...

000028: * Jan 31 2017 07:04:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:00:49 EET Fri Mar 1 2002 to 10:04:00 EET Tue Jan 31 2017, configured from
console by console.
000029: Jan 31 2017 07:05:00.159: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: adm]
[Source: 196.10.1.1] [localport: 23] [Reason: Login Authentication Failed - BadUser] at
10:05:00 EET Tue Jan 31 2017
000030: Jan 31 2017 07:05:08.415: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user:
admin] [Source: 196.10.1.1] [localport: 23] at 10:05:08 EET Tue Jan 31 2017
000031: Jan 31 2017 07:05:32.827: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down
000032: Jan 31 2017 07:05:33.827: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
000033: Jan 31 2017 07:06:27.239: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
000034: Jan 31 2017 07:06:28.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
000035: Jan 31 2017 07:06:28.867: %SYS-5-CONFIG_I: Configured from console by admin on
vty0 (196.10.1.1)
000036: Jan 31 2017 07:07:39.699: %SYS-5-CONFIG_I: Configured from console by console
R_1#
```

Рис. 4.5. Результат роботи команди **show logging** для маршрутизатора R_1

```
R_1#show logging count
Facility       Message Name                      Sev Occur      Last Time
================================================================================
R_1#
```

Рис. 4.6. Результат роботи команди **show logging count** для маршрутизатора R_1

```
R_1#show logging history
Syslog History Table:1 maximum table entries,
saving level warnings or higher
 43 messages ignored, 12 dropped, 0 recursion drops
 8 table entries flushed
 SNMP notifications not enabled
   entry number 9 : LINK-3-UPDOWN
    Interface FastEthernet0/1, changed state to up
    timestamp: 181448
R_1#
```

Рис. 4.7. Результат роботи команди **show logging history** для маршрутизатора R_1

```
R_1#show login
     A login delay of 5 seconds is applied.
     No Quiet-Mode access list has been configured.
     All successful login is logged.
     All failed login is logged.

     Router enabled to watch for login Attacks.
     If more than 3 login failures occur in 3 seconds or less,
     logins will be disabled for 10 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 2 seconds.
         Login failures for current window: 0.
     Total login failures: 4.

R_1#
```

Рис. 4.8. Результат роботи команди **show login** для маршрутизатора R_1

```
R_1#show login failures
Total failed logins: 4
Detailed information about last 50 failures

Username        SourceIPAddr    lPort Count TimeStamp
adminer         196.10.1.1      22    4     20:46:29 EET Tue Jan 31 2017

R_1#
```

Рис. 4.9. Результат роботи команди **show login failure** для маршрутизатора R_1

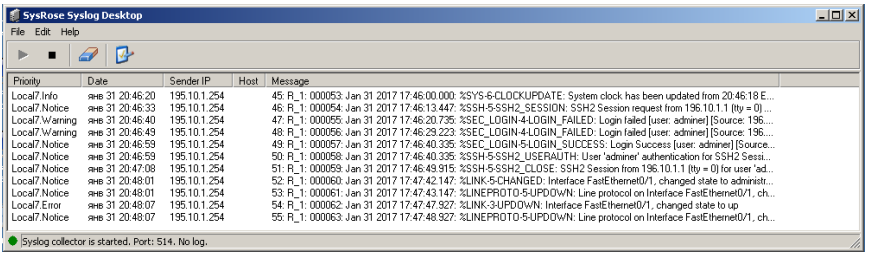

Рис. 4.10. Результати журналювання на сервері Serv_A_1

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 4.11). Під час побудови звернути увагу на вибір моделей комутаторів та маршрутизаторів, мережних модулів та адаптерів, а також мережних з'єднань. Різновиди технологій Ethernet для підмереж A, B, C, D, H, O, P обираються довільно. Під час формування каналів E, F, G скористатися даними табл. 4.9. Підключені локальні мережі (A, B, D, H, O, P) можна показувати як за допомогою одного вузла, так і за допомогою повноцінної мережі на базі окремого комутатора з кількома вузлами. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 4.6.

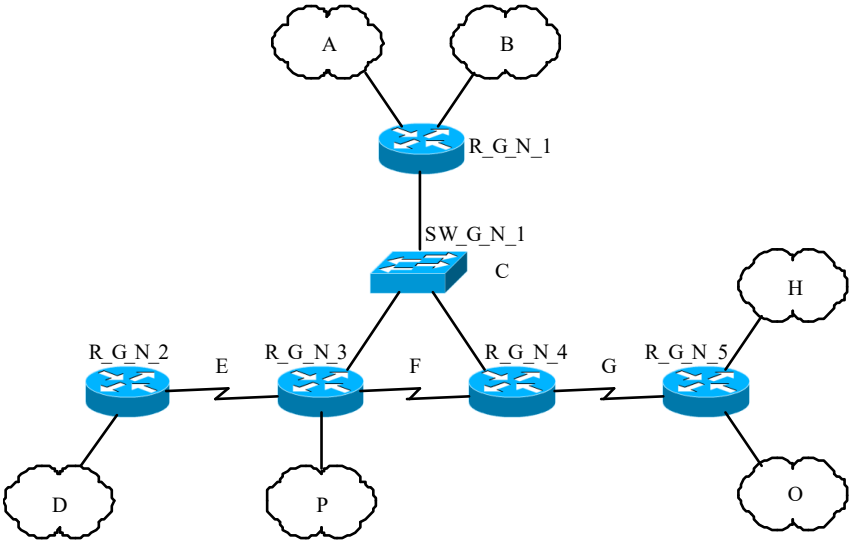

Рис. 4.11. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані табл. 4.10, 4.11. Результати навести у вигляді таблиці, яка аналогічна табл. 4.7.

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку (за даними табл. 4.9). Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевірити наявність зв'язку між сусідніми парами пристроїв мережі.

4. Налагодити маршрутизацію на кожному із маршрутизаторів мережі. Протокол/метод маршрутизації обирається довільно. Перевірити доступність вузлів віддалених мереж.

5. Налагодити функціонування сервера часу у відповідній локальній мережі (за даними табл. 4.12).

6. Налагодити параметри системного часу (за рахунок налагодження засобів протоколу NTP) та параметри часових міток на основних комунікаційних пристроях мережі.

7. Налагодити функціонування основного да допоміжного Syslog-серверів у відповідних локальних мережах (за даними табл. 4.12). Вибір програмного продукту для організації Syslog-сервера виконується довільно.

8. Налагодити функціонування як Syslog-клієнтів основних комунікаційних пристроїв мережі (за даними табл. 4.12).

9. Дослідити процес передачі даних протоколу Syslog між Syslog-клієнтами та Syslog-серверами. У разі відсутності зв'язку визначити проблеми та усунути їх.

10. Виконати операції віддаленого підключення до комунікаційних пристроїв за допомогою протоколів Telnet або SSH, операції відключення або зміни параметрів інтерфейсів чи каналів зв'язку цих пристроїв тощо.

11. Дослідити та проаналізувати результати журналювання подій, що збережені у відповідних системних журналах/базах даних Syslog-серверів до та після виконання операції п. 10.

Таблиця 4.9

Параметри підмереж (каналів зв'язку)

№ варіанта	Канал E		Канал F		Канал G	
	Clock rate, біт/с	DCE	Clock rate, біт/с	DCE	Clock rate, біт/с	DCE
1	9600	R_G_N_2	500000	R_G_N_3	72000	R_G_N_4
2	1000000	R_G_N_2	800000	R_G_N_3	500000	R_G_N_5
3	38400	R_G_N_2	1000000	R_G_N_4	64000	R_G_N_5
4	250000	R_G_N_2	1300000	R_G_N_4	128000	R_G_N_4
5	64000	R_G_N_3	2000000	R_G_N_3	250000	R_G_N_4
6	128000	R_G_N_3	1000000	R_G_N_3	800000	R_G_N_5
7	125000	R_G_N_3	19200	R_G_N_4	128000	R_G_N_4
8	128000	R_G_N_3	2000000	R_G_N_4	19200	R_G_N_5
9	148000	R_G_N_2	56000	R_G_N_3	2000000	R_G_N_4
10	250000	R_G_N_2	19200	R_G_N_3	1000000	R_G_N_5
11	500000	R_G_N_2	9600	R_G_N_4	500000	R_G_N_5
12	800000	R_G_N_2	1000000	R_G_N_4	800000	R_G_N_4
13	1000000	R_G_N_3	38400	R_G_N_3	1000000	R_G_N_4
14	1300000	R_G_N_3	250000	R_G_N_3	1300000	R_G_N_5
15	2000000	R_G_N_3	64000	R_G_N_4	2000000	R_G_N_4
16	1000000	R_G_N_3	128000	R_G_N_4	1000000	R_G_N_5
17	19200	R_G_N_2	125000	R_G_N_3	19200	R_G_N_4
18	2000000	R_G_N_2	128000	R_G_N_3	2000000	R_G_N_5
19	56000	R_G_N_2	148000	R_G_N_4	56000	R_G_N_5
20	19200	R_G_N_2	250000	R_G_N_4	19200	R_G_N_4
21	72000	R_G_N_3	72000	R_G_N_3	9600	R_G_N_4
22	500000	R_G_N_3	500000	R_G_N_3	1000000	R_G_N_5
23	64000	R_G_N_3	64000	R_G_N_4	38400	R_G_N_4
24	128000	R_G_N_3	128000	R_G_N_4	250000	R_G_N_5
25	250000	R_G_N_2	250000	R_G_N_3	64000	R_G_N_4
26	800000	R_G_N_2	800000	R_G_N_3	128000	R_G_N_5
27	128000	R_G_N_2	128000	R_G_N_4	125000	R_G_N_5
28	19200	R_G_N_2	19200	R_G_N_4	128000	R_G_N_4
29	2000000	R_G_N_3	2000000	R_G_N_3	148000	R_G_N_4

30	1000000	R_G_N_3	1000000	R_G_N_3	250000	R_G_N_5

Таблиця 4.10

Дані для адресації підмереж

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
1	193.G.N.0	/25	193.G.N.128	/25	194.G.N.0	/29	195.G.N.0	/24	196.G.N.0	/30
2	193.G.N.0	/26	193.G.N.64	/26	194.G.N.8	/29	195.G.N.0	/25	196.G.N.4	/30
3	193.G.N.128	/26	193.G.N.192	/26	194.G.N.16	/29	195.G.N.0	/26	196.G.N.8	/30
4	193.G.N.0	/27	193.G.N.32	/27	194.G.N.24	/29	195.G.N.0	/27	196.G.N.12	/30
5	193.G.N.64	/27	193.G.N.96	/27	194.G.N.32	/29	195.G.N.0	/28	196.G.N.16	/30
6	193.G.N.128	/27	193.G.N.160	/27	194.G.N.40	/29	195.G.N.0	/24	196.G.N.20	/30
7	193.G.N.192	/27	193.G.N.224	/27	194.G.N.48	/29	195.G.N.0	/25	196.G.N.24	/30
8	193.G.N.0	/28	193.G.N.16	/28	194.G.N.56	/29	195.G.N.0	/26	196.G.N.28	/30
9	193.G.N.32	/28	193.G.N.48	/28	194.G.N.64	/29	195.G.N.0	/27	196.G.N.32	/30
10	193.G.N.64	/28	193.G.N.80	/28	194.G.N.72	/29	195.G.N.0	/28	196.G.N.36	/30
11	193.G.N.96	/28	193.G.N.112	/28	194.G.N.0	/28	195.G.N.0	/24	196.G.N.40	/30
12	193.G.N.128	/28	193.G.N.144	/28	194.G.N.16	/28	195.G.N.0	/25	196.G.N.44	/30
13	193.G.N.160	/28	193.G.N.176	/28	194.G.N.32	/28	195.G.N.0	/26	196.G.N.48	/30
14	193.G.N.192	/28	193.G.N.208	/28	194.G.N.48	/28	195.G.N.0	/27	196.G.N.52	/30
15	193.G.N.224	/28	193.G.N.240	/28	194.G.N.64	/28	195.G.N.0	/28	196.G.N.56	/30
16	193.G.N.0	/25	193.G.N.128	/25	194.G.N.80	/28	195.G.N.0	/24	196.G.N.60	/30
17	193.G.N.0	/26	193.G.N.64	/26	194.G.N.96	/28	195.G.N.0	/25	196.G.N.64	/30
18	193.G.N.128	/26	193.G.N.192	/26	194.G.N.112	/28	195.G.N.0	/26	196.G.N.68	/30
19	193.G.N.0	/27	193.G.N.32	/27	194.G.N.128	/28	195.G.N.0	/27	196.G.N.72	/30
20	193.G.N.64	/27	193.G.N.96	/27	194.G.N.0	/27	195.G.N.0	/28	196.G.N.76	/30
21	193.G.N.128	/27	193.G.N.160	/27	194.G.N.32	/27	195.G.N.0	/24	196.G.N.80	/30
22	193.G.N.192	/27	193.G.N.224	/27	194.G.N.64	/27	195.G.N.0	/25	196.G.N.84	/30
23	193.G.N.0	/28	193.G.N.16	/28	194.G.N.96	/27	195.G.N.0	/26	196.G.N.88	/30
24	193.G.N.32	/28	193.G.N.48	/28	194.G.N.128	/27	195.G.N.0	/27	196.G.N.92	/30
25	193.G.N.64	/28	193.G.N.80	/28	194.G.N.160	/27	195.G.N.0	/28	196.G.N.96	/30
26	193.G.N.96	/28	193.G.N.112	/28	194.G.N.192	/27	195.G.N.0	/24	196.G.N.4	/30
27	193.G.N.128	/28	193.G.N.144	/28	194.G.N.224	/27	195.G.N.0	/25	196.G.N.24	/30
28	193.G.N.160	/28	193.G.N.176	/28	194.G.N.0	/26	195.G.N.0	/26	196.G.N.44	/30
29	193.G.N.192	/28	193.G.N.208	/28	194.G.N.64	/26	195.G.N.0	/27	196.G.N.64	/30
30	193.G.N.224	/28	193.G.N.240	/28	194.G.N.128	/26	195.G.N.0	/28	196.G.N.84	/30

Таблиця 4.11

Дані для адресації підмереж

№ варіанта	Підмережа F		Підмережа G		Підмережа H		Підмережа O		Підмережа P	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
1	197.G.N.0	/30	198.G.N.8	/30	199.G.N.0	/27	199.G.N.32	/27	200.G.N.0	/24
2	197.G.N.20	/30	198.G.N.28	/30	199.G.N.64	/27	199.G.N.96	/27	200.G.N.0	/25
3	197.G.N.40	/30	198.G.N.48	/30	199.G.N.128	/27	199.G.N.160	/27	200.G.N.0	/26
4	197.G.N.60	/30	198.G.N.68	/30	199.G.N.192	/27	199.G.N.224	/27	200.G.N.0	/27
5	197.G.N.80	/30	198.G.N.88	/30	199.G.N.0	/28	199.G.N.16	/28	200.G.N.0	/28
6	197.G.N.4	/30	198.G.N.12	/30	199.G.N.32	/28	199.G.N.48	/28	200.G.N.0	/24
7	197.G.N.24	/30	198.G.N.32	/30	199.G.N.64	/28	199.G.N.80	/28	200.G.N.0	/25
8	197.G.N.44	/30	198.G.N.52	/30	199.G.N.96	/28	199.G.N.112	/28	200.G.N.0	/26
9	197.G.N.64	/30	198.G.N.72	/30	199.G.N.128	/28	199.G.N.144	/28	200.G.N.0	/27
10	197.G.N.84	/30	198.G.N.92	/30	199.G.N.160	/28	199.G.N.176	/28	200.G.N.0	/28
11	197.G.N.8	/30	198.G.N.16	/30	199.G.N.192	/28	199.G.N.208	/28	200.G.N.0	/24
12	197.G.N.28	/30	198.G.N.36	/30	199.G.N.224	/28	199.G.N.240	/28	200.G.N.0	/25
13	197.G.N.48	/30	198.G.N.56	/30	199.G.N.0	/25	199.G.N.128	/25	200.G.N.0	/26
14	197.G.N.68	/30	198.G.N.76	/30	199.G.N.0	/26	199.G.N.64	/26	200.G.N.0	/27
15	197.G.N.88	/30	198.G.N.96	/30	199.G.N.128	/26	199.G.N.192	/26	200.G.N.0	/28
16	197.G.N.12	/30	198.G.N.16	/30	199.G.N.0	/27	199.G.N.32	/27	200.G.N.0	/24
17	197.G.N.32	/30	198.G.N.36	/30	199.G.N.64	/27	199.G.N.96	/27	200.G.N.0	/25
18	197.G.N.52	/30	198.G.N.56	/30	199.G.N.128	/27	199.G.N.160	/27	200.G.N.0	/26
19	197.G.N.72	/30	198.G.N.76	/30	199.G.N.192	/27	199.G.N.224	/27	200.G.N.0	/27
20	197.G.N.92	/30	198.G.N.96	/30	199.G.N.0	/26	199.G.N.64	/26	200.G.N.0	/28
21	197.G.N.16	/30	198.G.N.0	/30	199.G.N.32	/28	199.G.N.48	/28	200.G.N.0	/24
22	197.G.N.36	/30	198.G.N.20	/30	199.G.N.64	/28	199.G.N.80	/28	200.G.N.0	/25
23	197.G.N.56	/30	198.G.N.40	/30	199.G.N.96	/28	199.G.N.112	/28	200.G.N.0	/26
24	197.G.N.76	/30	198.G.N.60	/30	199.G.N.128	/28	199.G.N.144	/28	200.G.N.0	/27
25	197.G.N.96	/30	198.G.N.80	/30	199.G.N.160	/28	199.G.N.176	/28	200.G.N.0	/28
26	197.G.N.16	/30	198.G.N.4	/30	199.G.N.192	/28	199.G.N.208	/28	200.G.N.0	/24
27	197.G.N.36	/30	198.G.N.24	/30	199.G.N.224	/28	199.G.N.240	/28	200.G.N.0	/25
28	197.G.N.56	/30	198.G.N.44	/30	199.G.N.0	/25	199.G.N.128	/25	200.G.N.0	/26
29	197.G.N.76	/30	198.G.N.64	/30	199.G.N.0	/26	199.G.N.64	/26	200.G.N.0	/27
30	197.G.N.96	/30	198.G.N.84	/30	199.G.N.128	/26	199.G.N.192	/26	200.G.N.0	/28

Таблиця 12

Дані для налагодження підсистеми журналювання подій Syslog

№ варіанта	Мережа розміщення			Розмір буфера локального журналювання, Кбайт	Граничний рівень важливості повідомлень	Швидкість розсилки Syslog-повідомлень, повідомл./с
	NTP-сервера	основного Syslog-сервера	допоміжного Syslog-сервера			
1	A	A	A	8	5	12
2	B	A	B	16	6	15
3	H	A	P	24	7	18
4	O	A	H	32	7	21
5	D	A	O	40	6	24
6	P	B	A	48	5	24
7	A	B	B	64	5	21
8	B	B	P	8	6	18
9	H	B	H	12	7	15
10	O	B	O	16	7	12
11	D	P	A	20	6	10
12	P	P	B	24	5	15
13	A	P	P	28	5	20
14	B	P	H	32	6	25
15	H	P	O	36	7	30
16	O	H	A	40	7	30
17	D	H	B	44	6	25
18	P	H	P	48	5	20
19	A	H	H	52	5	15
20	B	H	O	56	6	10
21	H	O	A	60	7	11
22	O	O	B	64	7	13
23	D	O	P	16	6	15
24	P	O	H	32	5	17
25	A	O	O	48	5	19
26	B	O	A	64	6	19
27	H	H	B	24	7	17
28	O	P	P	48	7	15
29	D	B	H	64	6	13
30	P	A	O	32	5	11

Контрольні питання

1. Передумови та проблеми розробки засобів та протоколів журналювання подій.
2. Загальна характеристика протоколу Syslog.
3. Сфера застосування протоколу Syslog.
4. Стандартизація протоколу Syslog.
5. Характеристики протоколу Syslog стосовно моделі OSI та стеку TCP/IP.
6. Ролі пристроїв (процесів) у протоколі Syslog.
7. Структура повідомлення протоколу Syslog.
8. Рівні важливості повідомлень протоколу Syslog.
9. Кодування суб'єктів, що формують повідомлення протоколу Syslog.
10. Безпека протоколу Syslog.
11. Основні реалізації компонентів протоколу Syslog у сучасних мережних ОС.
12. Реалізація протоколу Syslog провідними виробниками мережного обладнання.
13. Особливості реалізації протоколу Syslog на мережному обладнанні фірми Cisco.
14. Перелік та призначення основних команд для налагодження протоколу Syslog на пристроях Cisco.
15. Перелік та призначення основних команд моніторингу роботи протоколу Syslog на пристроях Cisco.