Лабораторна робота № 14
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ МЕРЕЖНОГО ЧАСУ NTP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи протоколу мережного часу NTP на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи протоколу NTP у мережі, побудованій на базі обладнання Cisco; дослідити процес роботи протоколу NTP та процеси передачі даних цього протоколу у побудованій мережі.

Теоретичні відомості

Загальні відомості про застосування протоколів мережного часу у локальних і глобальних мережах

Правильне представлення дати та часу є актуальним як для повсякденної діяльності людини, так і для функціонування будь-якої комп'ютерної системи. Загальними питаннями стандартизації часу займається Міжнародна організація зі стандартизації ISO. Основним документом, у якому наводиться опис рекомендованих для застосування форматів дати і часу, є стандарт ISO 8601:2004 „Data Elements and Interchange Formats – Information Interchange – Representation of Dates and Times". Питаннями стардартизації представлення дати і часу та протоколів передачі параметрів дати і часу у комп'ютерних та телекомунікаційних мережах займаються IETF, IEEE, ITU-T та деякі інші організації.

Серед найвідоміших та найуживаніших протоколів мережного часу, що застосовуються у сучасних мережах, слід згадати такі:

– DAYTIME, Daytime Protocol;
– TIME, Time Protocol;
– SNTP, Simple Network Time Protocol;
– NTP, Network Time Protocol;
– PTP, Precision Time Protocol;
– IRIG, Inter Range Instrumentation Group;
– AFNOR NFS 87-500, Association Français de Nermolisation;
– VINES Time Service, Virtual Integrated Network Service Time Service;
– HTP, HTTP Time Protocol.

Протоколи DAYTIME, TIME, SNTP, NTP – це відкриті протоколи стеку TCP/IP, які стандартизуються IETF і мають реалізації у більшості сучасних систем. Протоколи DAYTIME, TIME описуються у стандартах RFC-867 „Daytime Protocol" та RFC-868 „Time Protocol". Останні версії протоколів SNTP та NTP описані у стандарті RFC-5905 „Network Time Protocol Version 4: Protocol and Algorithms Specification". Протокол PTP стандартизується IEEE та описаний у стандарті IEEE 1588-2008, „Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems". Цей протокол має реалізації на обладнанні IP-мереж. Протокол IRIG стандартизується структурним підрозділом армії США Range Commanders Council, остання версія стандарту описана у документі IRIG STANDARD 200-04 „IRIG Serial Time Code Formats". Протокол AFNOR NFS 87-500 стандартизується Французькою асоціацією зі стандартизації (Association Française de Normalisation), описаний цей протокол в однойменному стандарті. Решта протоколів стандартизуються в ініціативному порядку відповідними групами або окремими розробниками.

Слід зазначити, що у будь-якій системі існує поняття апаратного і програмного годинника/календаря. Апаратний годинник (Hardware Clock, System Calendar) – це спеціальний енергонезалежний блок (пристрій) у складі системи, який веде відлік часу. Якщо вимкнено зовнішнє живлення, робота апаратного годинника забезпечується за рахунок внутрішнього джерела – батареї або акумулятора. Програмний годинник (Software Clock, Software-Based System Clock) – компонент ОС, що забезпечує відлік часу у процесі роботи системи. Часто застосовується термін „системний годинник/час" (System Clock/Time). Як правило, під терміном „системний годинник" розуміється саме програмний годинник.

Параметри часу апаратного годинника пристрою встановлюються через BIOS або за допомогою спеціальних засобів ОС. Параметри часу програмного годинника встановлюється під час завантаження ОС, як такі, що дорівнюють параметрам апаратного годинника. Надалі годинники працюють незалежно один від одного. ОС у своїй роботі застосовує параметри програмного годинника, оскільки для неї доступ до програмного годинника є набагато простішим і швидшим, ніж до апаратного. Існують механізми та засоби (команди, утиліти) обміну параметрами часу між апаратним і програмним годинниками.

Загальні відомості про протокол мережного часу NTP

Технологіям синхронізації параметрів дати та часу мережних вузлів почали приділяти увагу на початкових стадіях розробки та практичної реалізації багатьох мережних архітектур та стеків комунікаційних протоколів. Це стосувалося і стеку протоколів TCP/IP. Ще на початку 1981 року одна з технологій була описана у документі Internet Engineering Note 173 (IEN-173), що став основою опублікованого у квітні 1981 року першого стандарту IETF RFC-778 „DCNET Internet Clock Service", у якому описувалися принципи синхронізації часу між вузлами мережі DCNET. У травні 1983 року були прийняті стандарти IETF RFC-867 „Daytime Protocol" та RFC-868 „Time Protocol", які описували правила обміну параметрами дати та часу між вузлами IP-мережі. У вересні 1985 року був прийнятий розроблений фахівцем університету Делавер Девідом Л. Міллсом (David L. Mills) стандарт протоколу мережного часу NTP RFC-968 „Network Time Protocol (NTP)". Модифіковані версії цього протоколу і нині широко застосовуються у сучасних телекомунікаційних і комп'ютерних мережах для передачі високоточної часової інформації.

Протокол NTP постійно вдосконалювався, подальші його модифікації були описані у стандартах RFC-1059 „Network Time Protocol (Version 1). Specification and Implementation", RFC-1119 „Network Time Protocol (Version 2). Specification and Implementation", RFC-1305 „Network Time Protocol (Version 3). Specification, Implementation and Analysis". Остання версія протоколу описана у прийнятому у червні 2010 року стандарті RFC-5905 „Network Time Protocol Version 4: Protocol and Algorithms Specification".

Для передачі параметрів часу між пристроями, які не потребують високого ступеня точності (наприклад, вбудованими системами) був розроблений спрощений варіант протоколу NTP – протокол SNTP. Цей протокол початково був описаний у стандарті RFC-1361 „Simple Network Time Protocol (SNTP)". Наступні модифікації цього протоколу описані у стандартах RFC-1769 „Simple Network Time Protocol (SNTP)", RFC-1361 „Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC-4330 „Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI". Остання модифікація протоколу SNTP описана у загальному із протоколом NTP

стандарті RFC-5905 ,,Network Time Protocol Version 4: Protocol and Algorithms Specification".

Стосовно моделі OSI та стеку TCP/IP протокол NTP є протоколом прикладного рівня. Для транспортування повідомлень протоколу NTP початково передбачалося застосування протоколу UDP (порт сервера 123). Пізніше були запропоновані рішення із застосуванням протоколу TCP (порт сервера 123). Як адреси мережного рівня для передачі повідомлень протоколу NTP можуть застосовуватися як унікальні, так і групові IP-адреси. В IP-мережах версії 4 для протоколу NTP IANA призначила групову IP-адресу 224.0.1.1, в IP-мережах версії 6 – групову адресу, яка закінчується на :101.

У першу чергу протокол NTP був розроблений для синхронізації часових параметрів між вузлами, що підключені до мереж із комутацією пакетів, для яких характерна змінна латентність (змінна довжина затримки передачі даних). Можливе застосування протоколу і в мережах інших типів.

Протокол NTP базується на модифікованому алгоритмі Марзулло (Keith Marzullo), що дає змогу досягати точності в десятки мілісекунд при передачі часових параметрів через мережу Інтернет та точності менше однієї мілісекунди при передачі в локальній мережі. Обмін даними в протоколі NTP передбачається здійснювати на основі традиційної клієнт-серверної моделі, в якій чітко визначено ролі вузлів: роль NTP-сервера, який є джерелом, та роль NTP-клієнта, який є отримувачем часової інформації. У протоколі NTP також можливе використання однорівневих (P2P, Peer to Peer) відносин, коли NTP-вузол виступає як джерелом (сервером), так і отримувачем (клієнтом) часових параметрів. Для такого вузла у документації введено термін ,, NTP-пір" (NTP-Peer). Часто терміни NTP-клієнт та NTP-пір використовуються як синоніми.

Стандартом протоколу NTP передбачено виділення таких видів вузлів:

– первинний сервер NTP (NTP Primary Server);

– вторинний сервер NTP (NTP Secondary Server);

– клієнт NTP (NTP Client).

Взаємозв'язки між вузлами протоколу NTP організовані з використанням багаторівневої ієрархії (рис. 3.1). Рівні ієрархії протоколу називаються шарами або стратами (Stratum). Формально кількість страт становить 256 (від 0 до 255). Страта 0 містить пристрої, які є

високоточними джерелами часу, такі, як: атомні годинники, годинники систем GPS, Galileo тощо. Часто ці пристрої називають еталонними годинниками (Reference Clocks). Страта 1 містить первинні сервери NTP. Первинні сервери NTP отримують часові параметри безпосередньо від еталонних годинників. Страти з 2 по 15 містять вторинні сервери NTP, які отримують часові параметри або від первинних серверів NTP (страта 2), або від вторинних серверів NTP вищих страт (страти 3 – 15). Вторинні сервери NTP надають часові параметри вторинним серверам NTP поточної і нижчих страт та NTP-клієнтам. Страта 16 містить пристрої, які не виконують синхронізації часових параметрів. Страти з 17 до 255 зарезервовані для подальшого використання.

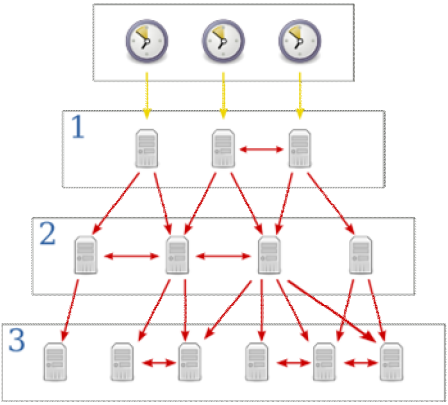

Рис. 3.1. Рівні ієрархії протоколу NTP

Топологія NTP-мережі повинна бути сформована таким чином, щоб були усунені часові петлі та мінімізована дистанція сихронізації. Для цього використовується один із варіантів алгоритму Беллмана-Форда, за допомогою якого розраховується найкоротший шлях до первинних серверів NTP. Як наслідок, на пристроях досягається можливість отримувати і встановлювати часові параметри, що більш точно відповідають еталонним параметрам.

Існує три варіанти функціонування протоколу NTP:

– симетричний NTP (Symmetric NTP);

– клієнт/серверний NTP (Client/Server NTP);

– широкомовний NTP (Broadcast NTP).

Кожен із зазначених варіантів протоколу пов'язаний із режимом асоціації (Association Mode), що описує відносини між двома NTP-вузлами. Існує шість режимів асоціації:

– режим 1 (Mode 1), симетричний активний режим, (Symmetric Active Mode);

– режим 2 (Mode 2), симетричний пасивний режим (Symmetric Passive Mode);

– режим 3 (Mode 3), клієнтський режим (Client Mode);

– режим 4 (Mode 4), серверний режим (Server Mode);

– режим 5 (Mode 5), широкомовний серверний режим (Broadcast Server Mode);

– режим 6 (Mode 6), широкомовний клієнтський режим (Broadcast Client Mode).

Режими асоціаціації можуть бути стійкими (Persistent) та нестійкими, ефемерними (Ephemeral). Стійкий режим асоціації для NTP-вузла встановлється під час завантаження системи і ніколи не розривається. Нестійкий режим асоціації для NTP-вузла встановлюється після отримання NTP-повідомлень певних видів і може бути розірваний унаслідок появи помилки або спливання відповідного таймера існування асоціації.

За умови застосування симетричного варіанта протоколу NTP-вузли є однорівневими вузлами, тобто функціонують і як клієнти, і як сервери з використанням або симетричного активного, або симетричного пасивного режимів асоціації. NTP-вузол, що знаходиться у стійкому симетричному активному режимі асоціації, надсилає свої повідомлення (повідомлення режиму 1) до NTP-вузла, що знаходиться у симетричному активному режимі асоціації. NTP-вузол, для якого не було встановлено жодного режиму асоціації, після отримання повідомлення симетричного активного режиму асоціації перейде до стійкого симетричного пасивного режиму асоціації. Потім NTP-вузол надсилає повідомлення симетричного пасивного режиму (повідомлення режиму 2) та знаходиться у стійкому стані до появи помилки або закінчення часу існування. Надалі NTP-вузли надсилають один одному повідомлення, що містять параметри синхронізації.

За умови застосування клієнт/серверного варіанта протоколу NTP стійкий NTP-клієнт надсилає повідомлення серверного режиму

(повідомлення режиму 4) до NTP-сервера, який відповідає повідомленнями клієнтського режиму (повідомлення режиму 3). NTP-сервери надають параметри синхронізації одному або більше NTP-клієнтам, але не приймають параметрів синхронізації від них. NTP-сервери також можуть містити засоби для безпосереднього отримання часових параметрів від еталонного годинника. У цьому випадку NTP-клієнти отримують параметри синхронізації від серверів

За умови застосування широкомовного варіанта протоколу NTP-вузол, що знаходиться у стійкому широкомовному серверному режимі асоціації, періодично надсилає свої повідомлення (повідомлення режиму 5) множині клієнтів. NTP-вузол (NTP-клієнт або NTP-сервер), для якого не було встановлено жодного режиму асоціації, після отримання повідомлення широкомовного серверного режиму (режиму 5) перейде до нестійкого широкомовного клієнтського режиму асоціації і буде знаходитися у цьому режимі до появи помилки або спливання відповідного таймера. Перед встановленням широкомовного клієнтського режиму асоціації NTP-клієнт обмінюється кількома повідомленнями з NTP-сервером із метою уточнення затримки та взаємної аутентифікації. Широкомовний NTP-сервер надсилає параметри синхронізації NTP-клієнтам або іншим NTP-серверам.

У протоколі NTP наявна можливість динамічного виявлення NTP-серверів. Для цього використовуються два спеціальних режими асоціації:

– багатомовний клієнтський режим (Manycast Client Mode);

– багатомовний серверний режим (Manycast Server Mode).

Багатомовний клієнтський режим асоціаціації може бути стійким (Persistent) та нестійким, ефемерним (Ephemeral). Деталі процедури динамічного виявлення NTP-серверів описані у RFC-5905.

Час у протоколі NTP може бути представлений у трьох форматах:

– короткий формат часу (NTP Short Format);

– формат мітки часу (NTP TimeStamp Format);

– формат дати (NTP Date Format).

Детальне представлення зазначених форматів часу наведене на рис. 3.2*а*, *б*, *в* відповідно. Для кожного із форматів характерний поділ загального поля часу на два однакових за розміром поля. Перше поле

Seconds містить значення часу в секундах, друге поле Fraction містить значення часу у долях секунд. Для зручності переходів між форматами часу у форматі дати поле Seconds розбите на два підполя – Номер ери (Era Number) та Зсув ери (Era Offset). Значення вищезгаданих підполів не продукуються засобами протоколу NTP, а отримуються із зовнішніх джерел (від апаратури або з файлової системи).

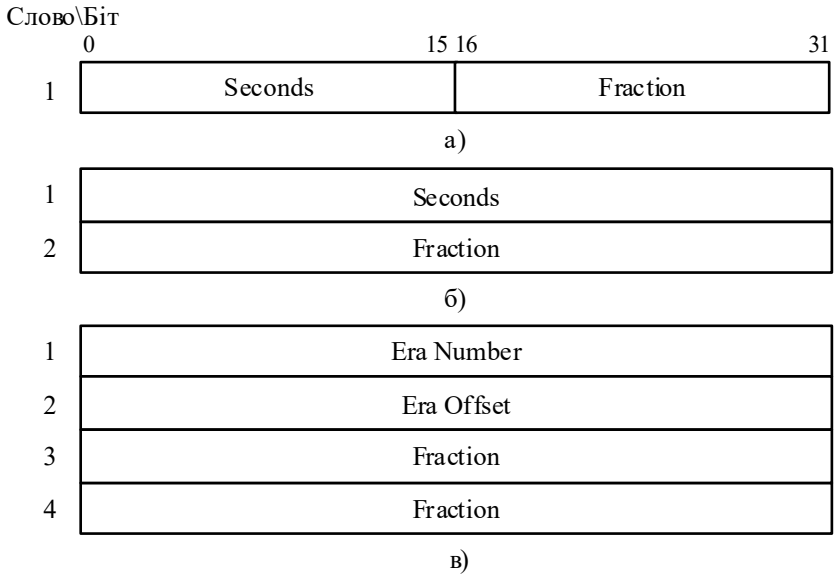

Рис. 3.2. Формати часу протоколу NTP

128-бітний формат дати використовується у системах, які мають можливість оперувати з даними такої довжини. У цьому форматі існує можливість відобразити часовий період тривалістю 584 мільярди років із точністю до 0,05 пс. 64-бітний формат мітки часу використовується у заголовках повідомлень протоколу NTP та в інших випадках, де у системи є можливість оперувати з даними такої довжини. У цьому форматі існує можливість відобразити часовий період тривалістю 136 років із точністю до 232 пс. 32-бітний короткий формат часу використовується у заголовках повідомлень протоколу NTP для формування полів затримки і дисперсії, в яких повне відображення часу з використанням інших форматів не доцільне. Пере-

ведення параметрів з одного формату в інший проводиться за спеціальними формулами.

Основним форматом відображення часу в протоколі NTP є формат мітки часу. Оскільки при його застосуванні шкала часу повторюється кожні 136 років, отримувач часових параметрів повинен знати приблизний поточний час. Для коректного суміщення часових параметрів серверів протоколу NTP із відповідними часовими параметрами систем Windows та Linux необхідно враховувати, що у протоколі NTP відлік часу починається з опівночі 1 січня 1900 року, а не з опівночі 1 січня 1970 року, як у системах Windows та Linux. Тому для коректного суміщення часових параметрів у цих системах слід віднімати майже 70 років (з урахуванням високосних років).

Структура повідомлення протоколу NTP наведена на рис. 3.3. Дані, що містяться у полях заголовку, можуть відрізнятися для різних режимів асоціацій.

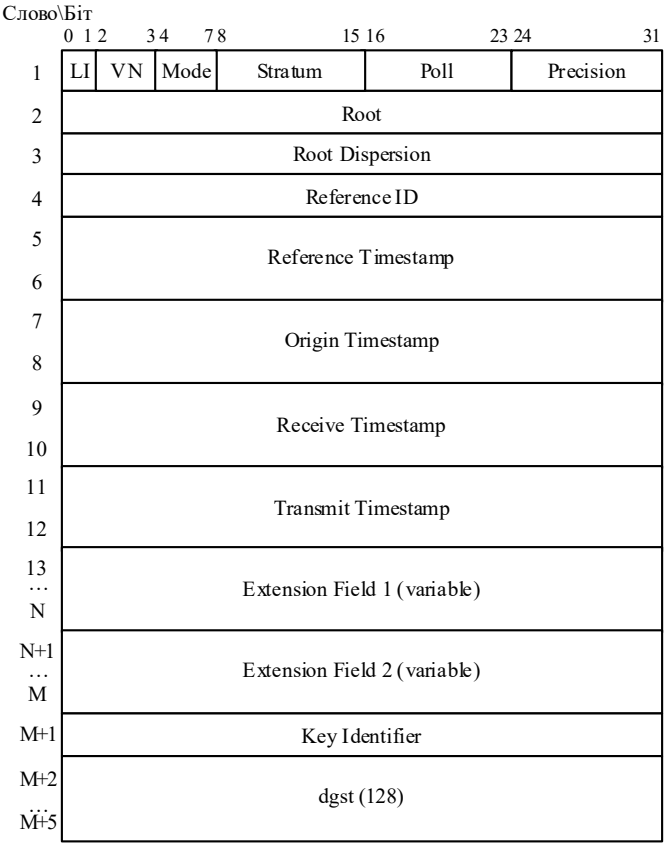

Рис. 3.3. Структура повідомлення протоколу NTP

Засоби синхронізації параметрів часу сучасних ОС Linux/Unix

Більшість сучасних клієнтських та серверних мережних ОС мають засоби синхронізації часових параметрів з еталонними джерелами часу. Для ОС Unix та Linux ці засоби розроблялися паралельно з розробкою самих систем і були орієнтовані на використання стандартних мережних протоколів, починаючи із застарілих сьогодні протоколів Daytime Protocol та Time Protocol і закінчуючи останньою версією сучасного протоколу мережного часу NTP.

Для забезпечення функціонування Linux/Unix-вузла як NTP-клієнта чи NTP-сервера в ОС необхідно встановити додаткові пакети, які підтримують функціонування модулів протоколу NTP в ОС: пакет **ntp** (демон **ntpd**), пакет **ntpdate** (утиліта для отримання і встановлення часових параметрів із віддаленого сервера часу), пакет **ntp-doc** (пакет документації). У деяких системах необхідно встановити додатковий пакет **ntp-utils** (набір утиліт діагностики роботи протоколу NTP).

Після встановлення пакетів у більшості дистрибутивів автоматично активується функціонування демона **ntpd**, для якого також автоматично створюються основні конфігураційні файли **/etc/ntp.conf** та **/var/lib/ntp/ntp.drift**. Файл **/etc/ntp.conf** містить параметри налагодження як NTP-клієнта, так і NTP-сервера. Файл **/var/lib/ntp/ntp.drift** містить параметри зсуву системного годинника. Вміст цих створених за замовчуванням файлів для ОС Linux Debian наведено відповідно на рис. 3.4, 3.5.

За замовчуванням у файлі **/etc/ntp.conf**, як правило, містяться записи про чотири сервери часу розробника дистрибутиву ОС. Для згаданої ОС Linux Debian (рис. 3.4) це сервери: 0.debian.pool.ntp.org, 1.debian.pool.ntp.org, 2.debian.pool.ntp.org, 3.debian.pool.ntp.org. Для прискорення отримання параметрів часу рекомендується замінити адреси серверів часу розробника ОС на адреси серверів, які є територіально ближчими. Перелік активних NTP-серверів можна отримати на сайті відкритого проекту www.ntp.org за посиланнями для серверів часу страти 1 та серверів часу страти 2 відповідно http://support.ntp.org/bin/view/Servers/StratumOneTimeServers та http://support.ntp.org/bin/view/Servers/StratumTwoTimeServers.

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift
# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example
# pool.ntp.org maps to about 1000 low-stratum NTP servers.  Your server will
# pick a different set every time it starts up.  Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#server ntp.your-provider.example
# pool.ntp.org maps to about 1000 low-stratum NTP servers.  Your server will
# pick a different set every time it starts up.  Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html for
# details.  The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1
# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1
# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
#restrict 192.168.123.0 mask 255.255.255.0 notrust
# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
#broadcast 192.168.123.255
# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines.  Please do this only if you trust everybody on the network!
#disable auth
#broadcastclient
```

Рис. 3.4. Вміст конфігураційного файла **/etc/ntp.conf** ОС Linux Debian

```
-13.430
```

Рис. 3.5. Вміст конфігураційного файла **/var/lib/ntp/ntp.drift** ОС Linux Debian

Після отримання загального переліку серверів часу рекомендується за допомогою утиліти **ntpdate** (**ntpdate -q**) визначити сервери з меншими затримками передачі NTP-повідомлень і внести їх до конфігураційного файла **/etc/ntp.conf**. Після внесення змін у конфігурацію слід перезапустити демон **ntpd**. Запуск, перезапуск та зупинка роботи цього демона здійснюються відповідно командами **ntpd start**, **ntpd restart**, **ntpd stop**.

Для контролю процесу отримання часових параметрів рекомендується застосовувати спеціалізовану утиліту **ntpq**, яка дає змогу отримати деталізовану інформацію стосовно характеристик серверів часу, що використовуються для синхронізації. Ця утиліта має великий набір ключів, які дозволяють отримувати та встановлювати різні параметри сеансів зв'язку поточного вузла з серверами часу.

Приклад використання цієї утиліти з ключем **-p** (**ntpq -p**), який активував виведення інформації про встановлені сеанси зв'язку з серверами часу та параметри цих сеансів, наведений на рис. 3.6.

```
ntp-server:~# ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
-n3.time1.d6.hsd .PPS.            1 u   34   64  177   70.162    2.375   8.618
+ntp1.vniiftri.r .PPS.            1 u   33   64  177   43.479   -0.020  10.198
*ntp2.vniiftri.r .PPS.            1 u    6   64  177   43.616   -0.192   0.688
+ntp4.vniiftri.r .PPS.            1 u    4   64  177   43.623    0.440   0.546
-n1.time1.d6.hsd .PPS.            1 u   53   64   77   92.865  -11.358  38.346
-n2.time1.d6.hsd .PPS.            1 u   33   64  177   70.161    2.375   8.620
-ns1.hsdn.org    .GPS.            1 u   40   64  177   78.057   -3.292  35.083
-ntp3.vniiftri.r .PPS.            1 u   44   64   77   47.667    2.292   2.611
-scylla-10.msk.c 192.43.244.18    2 u   62   64   77   41.565   -1.564  28.914
```

Рис. 3.6. Приклад використання утиліти **ntpq (ntpq -p)**

Існує можливість синхронізації параметрів часу поточного Linux вузла з параметрами часу віддаленого NTP-сервера у ручному режимі. Ця операція виконується за допомогою спеціальної утиліти **ntpdate**. У певних випадках для зменшення об'єму службового NTP-трафіка на робочих станціях ОС Linux локальної мережі рекомендують налагодити автоматичний періодичний запуск цієї утиліти з метою отримання параметрів часу від локального NTP-сервера.

Засоби синхронізації параметрів часу сучасних ОС Windows

У клієнтських і серверних ОС Windows наявні засоби, які дають змогу виконувати синхронізацію часових параметрів вузлів мережі з еталонним джерелом часу. У перших версіях Windows ці засоби насамперед були орієнтовані на використання фірмових розробок Microsoft, але з часом з'явилися можливості налагодження та використання стандартних протоколів часу. Саме в останніх версіях ОС Windows розробник забезпечив повноцінну підтримку протоколу NTP та його підмножини – протоколу SNTP.

За замовчуванням в ОС Windows використовуються власні реалізації протоколів часу Microsoft. Спосіб синхронізації параметрів часу Windows-вузлів залежить від схеми адміністрування мережі. Якщо мережа побудована з використанням концепції робочих груп Windows (тобто є одноранговою мережею), то кожен вузол (робоча станція Windows) повинен здійснювати синхронізацію параметрів часу з еталонним джерелом особисто і незалежно від інших вузлів. Якщо ж мережа побудована з використанням концепції доменів Windows (тобто є клієнт-серверною або гібридною мережею), то синхронізацію параметрів часу з еталонним джерелом здійснює лише сервер, який є первинним контролером домену (PDC, Primary Domain Controller). Решта серверів і робочих станцій здійснюють синхронізацію параметрів часу з первинним контролером домену, як правило, з використанням фірмового протоколу часуWindows.

Для забезпечення виконання операцій синхронізації часових параметрів в ОС Windows застосовується служба часу Windows (Windows Time Service), яка автоматично додається до списку служб і активується при інсталяції системи. Іноді службу часу Windows називають службою W32Time. Дана назва пов'язана з іменем виконуваного файла, що застосовується для керування параметрами функціонування цієї служби. Параметри, які необхідні для функціонування служби часу Windows (список серверів, періодичність проведення синхронізації тощо) зберігаються у реєстрі системи.

Типово синхронізація параметрів часу поточного вузла з віддаленим джерелом часу в ОС Windows здійснюється автоматично з періодичністю 20 хвилин. Для їх отримання за замовчуванням у системі використовується група серверів, до якої входить основний сервер часу фірми Microsoft (time.windows.com) та чотири додатко-

вих сервери часу Національного інституту стандартів і технологій США (time.nist.gov, time-nw.nist.gov, time-a.nist.gov, time-b.nist.gov). До цієї групи можуть бути додані й інші сервери. Для проведення позачергової синхронізації параметрів часу використовується стандартний додаток ОС Windows „Дата и время". За його допомогою можна переглянути і відредагувати список групи серверів часу. Для зміни додаткових параметрів роботи служби часу Windows необхідно або вручну редагувати реєстр, або скористатися відповідними командами редагування.

Виконати синхронізацію параметрів часу робочої станції ОС Windows XP із параметрами сервера – джерела часу можна за допомогою мережних команд групи **net**, зокрема команди **net time**. Сценарій, який виконує дану процедуру, наведений нижче. Особливістю даного сценарію є те, що використовується спрощений протокол мережного часу SNTP.

```
C:\>net stop w32time
C:\>net time /setsntp: srv1.my.net
C:\>net start w32time
C:\>net time /querysntp
C:\>
```

В останніх версіях ОС Windows команда **net time** була модифікована для використання виключно у доменній мережі Windows. Тому замість цієї команди рекомендується використовувати команду **w32tm**, яка, з одного боку, забезпечує функціонал, аналогічний команді **net time**, а з іншого – забезпечує підтримку роботи останніх версій протоколів SNTP та NTP. Сценарій синхронізації параметрів часу поточного вузла з параметрами, що надаються одним із групи NTP-серверів, наведено нижче.

```
C:\>w32tm /config /syncfromflags:manual /manualpeerlist:
"0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org"
C:\>
```

Приклад скрипту, який дозволяє здійснити автоматизоване налагодження взаємодії з сервером часу для Windows-клієнта наведений на рис. 3.7.

```
@echo off
Color f0
```

```
rem  Скрипт налагодження NTP-клієнта ОС Windows
echo Скрипт налагодження NTP-клієнта ОС Windows
echo.

rem Зазначення адреси NTP-сервера
set /p ntp_server="Зазначте адресу NTP-сервера: "
rem Зазначення періоду оновлення часу (хв)
set /p ntp_update="Зазначте період оновлення (хв): "
rem Зазначення як NTP-сервера за замовчуванням 0 елемент
echo.
echo ==========================================================
echo Зазначення як NTP-сервера за замовчуванням 0 елемента
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers /ve /t
REG_SZ /d 0 /f

rem Редагування значення NTP-сервера оновлень із списку під номером 0
echo.
echo ==========================================================
echo Зміна поточного значення сервера оновлень зі списку серверів на значення %ntp_server%
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers /v 0 /t
REG_SZ /d %ntp_server% /f

rem Вимкнення NTP-клієнта
echo.
echo ==========================================================
echo Вимкнення NTP-клієнта
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters /v Type /t
REG_SZ /d NTP /f

rem Зазначення поточного NTP-сервера оновлень
echo.
echo ==========================================================
echo Зазначення поточного NTP-сервера оновлень %ntp_server%
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters /v NtpServer /t
REG_SZ /d %ntp_server%,0x9 /f

rem Встановлення періоду оновлень
echo.
echo ==========================================================
echo Встановлення періоду оновлень %ntp_update% хв
rem Переведення часу в с
set /a ntp_update*=60
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient /v
SpecialPollInterval /t REG_DWORD /d %ntp_update% /f

rem Зазначення автоматичного запуску служби часу
echo.
echo ==========================================================
echo Зазначення автоматичного запуску служби часу
sc config w32time start= auto

rem -- Запуск/перезапус незапущеної/запущеної служби часу
echo. && echo========================================== && echo Спроба перезапуску
служби часу && echo. && sc stop w32time && PING -n 5 -w 1000 127.0.0.1 >nul && sc start w32time
|| echo. && echo ========================================================== && echo Спроба переза-
пуску служби часу && echo. && sc start w32time

echo.
pause
```

Рис. 3.7. Скрипт автоматизованого налагодження NTP-клієнта ОС Windows

Засоби встановлення та синхронізації параметрів часу Cisco IOS

Операційна система Cisco IOS, як і решта ОС цього виробника, таких як Cisco IOS XR, Cisco IOS XE, Cisco NX-OS, на всіх пристроях Cisco забезпечує функціонування програмного годинника/календаря. У деяких моделях пристроїв також наявний і апаратний годинник/календар. Відповідно існують механізми обміну даними між цими годинниками.

Параметри програмного годинника пристрою Cisco можуть встановлюватися як за допомогою команд локального застосування, так і з використанням мережного джерела часу. У першому випадку, за умови відсутності апаратного годинника, параметри програмного годинника зберігаються лише в оперативній пам'яті пристрою і є актуальними лише на період його роботи. Після перезавантаження пристрою їх необхідно встановлювати заново. Якщо ж апаратний годинник наявний і виконана синхронізація параметрів апаратного годинника з параметрами попередньо налагодженого програмного годинника, то після перезавантаження пристрою апаратний годинник отримає параметри від програмного й отримані параметри часу будуть актуальними. У другому випадку програмний годинник після завантаження пристрою синхронізується з годинником сервера часу за відповідним мережним протоколом. Надалі операція синхронізації періодично повторюється. Це дає змогу мати більш точні параметри часу на пристрої. Звичайно, що такі операції вимагають певних специфічних налагоджень пристрою.

Всі версії ОС Cisco для всіх пристроїв Cisco підтримують можливість обміну параметрами часу за допомогою протоколів DAYTIME, TIME та NTP. Протоколи DAYTIME та TIME належать до групи протоколів, відомих як TCP/UDP Small Services, які з точки зору безпеки рекомендується відключати. Основним протоколом для обміну параметрами дати та часу є протокол NTP. У деяких версіях Cisco IOS підтримуються робота спрощеного протоколу SNTP, більш сучасного протоколу PTP та застарілого протоколу VINES Time Service. Певні спеціалізовані моделі пристроїв підтримують роботу інших мережних протоколів часу.

Порядок налагодження функціонування протоколу мережного часу NTP на пристроях Cisco

Більшість комунікаційних пристроїв Cisco (комутаторів, маршрутизаторів, точок доступу, контролерів доступу безпровідних мереж, міжмережних екранів, систем виявлення втручань тощо) можуть бути налагодженими як клієнти, так і як сервери протоколу мережного часу NTP. Досить часто пристрій виконує функції і клієнта, і сервера одночасно. Деякі з пристроїв (наприклад, IP-телефони Cisco) можуть бути налагоджені лише як клієнти.

Налагодження пристроїв, як NTP-вузлів передбачає як виконання певних однакових дій, так і дій, які характерні лише для NTP-клієнта чи NTP-сервера. Варіантів налагодження NTP-сервера є більше, оскільки існує досить багато схем і режимів його роботи.

Налагодження засобів протоколу NTP, як правило, здійснюється на пристрої Cisco в цілому. Існує можливість і більш точного налагодження, за рахунок встановлення параметрів роботи протоколу на певних фізичних інтерфейсах.

Налагодження функціонування NTP-клієнта на пристроях Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Налагодити детальні параметри часових міток для повідомлень відлагодження (рекомендовано).
2. Налагодити детальні параметри часових міток для повідомлень журналювання подій (рекомендовано).
3. Налагодити параметри часового поясу (обов'язково).
4. Налагодити параметри переходу на літній/зимовий час (обов'язково).
5. Активувати аутентифікацію протоколу NTP (рекомендовано).
6. Зазначити IP-адресу основного NTP-сервера – джерела часу для даного пристрою (обов'язково).
7. Зазначити IP-адресу(-и) допоміжного(-них) NTP-сервера(-ів) – джерела часу для даного пристрою (рекомендовано).
8. Зазначити IP-адресу(-и) NTP-Peer(s) (рекомендовано).

Якщо виникає потреба налагодити додаткові параметри протоколу, то даний перелік доповнюється необхідними етапами.

Налагодження функціонування NTP-сервера на пристроях Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Налагодити детальні параметри часових міток для повідомлень відлагодження (рекомендовано).
2. Налагодити детальні параметри часових міток для повідомлень журналювання подій (рекомендовано).
3. Налагодити параметри часового поясу (обов'язково).
4. Налагодити параметри переходу на літній/зимовий час (обов'язково).
5. Активувати аутентифікацію протоколу NTP (рекомендовано).
6. Зазначити IP-адресу NTP-сервера – джерела часу для даного пристрою (обов'язково).
7. Зазначити IP-адресу(-и) пристрою(-їв) NTP-Peer(-s), з якими буде взаємодіяти даний пристрій (рекомендовано).
8. Зазначити роль (та страту) даного пристрою як головного NTP-сервера (обов'язково).
9. Зазначити інтерфейс, IP-адреса якого буде встановлюватися як адреса джерела NTP-повідомлення (рекомендовано).
10. Обмежити (за допомогою списку доступу) IP-адреси пристроїв, яким буде дозволено взаємодіями з даним пристроєм як NTP-сервером (рекомендовано).
11. Обмежити (за допомогою списку доступу) IP-адреси пристроїв, з якими даному пристрою буде дозволено взаємодіяти як NTP-серверу або NTP-Peer(-s) (рекомендовано).
12. Активувати оновлення апаратного годинника (рекомендовано).

Якщо виникає потреба налагодити додаткові параметри протоколу, то даний перелік доповнюється додатковими етапами. Необхідно зазначити, що функціонування NTP-сервера на маршрутизаторі Cisco активоване за замовчуванням.

Часто налагодження протоколу NTP на пристрої є необхідним для функціонування інших мережних протоколів та технологій. Слід зазначити, що особливо важливим є коректне функціонування серверів та клієнтів протоколу NTP для протоколу журналювання подій Syslog та протоколу мережного керування SNMP, технології Voice IP.

Команди налагодження функціонування протоколу мережного часу NTP на пристроях Cisco

Налагодження функціонування протоколу мережного часу NTP може здійснюватися на більшості пристроїв, виготовлених фірмою Cisco. Деякі відмітності у процесі налагодження можуть виникати через особливості синтаксису команд та версій Cisco IOS. Слід пам'ятати, що налагодження функціонування протоколу NTP на маршрутизаторі здійснюється як на пристрої в цілому, так і на певних його інтерфейсах, на комутаторі – тільки на пристрої в цілому.

Серед команд, які тісно пов'язані з налагодженням параметрів функціонування протоколу NTP, слід згадати команди налагодження параметрів часу пристроїв Cisco такі, як: **clock set**, **clock read-calendar, clock update-calendar**, **clock calendar-valid**, **clock summertime**, **clock timezone**.

Основною командою, від якої походить решта команд для налагодження засобів протоколу NTP у Cisco IOS, є однойменна команда **ntp**. Перелік похідних команд протоколу NTP містить такі команди, як: **ntp access-group**, **ntp allow mode private**, **ntp authenticate**, **ntp authentication-key**, **ntp broadcast**, **ntp broadcast client**, **ntp broadcastdelay**, **ntp clear drift**, **ntp clock-period**, **ntp disable**, **ntp logging**, **ntp master**, **ntp max-associations**, **ntp maxdistance**, **ntp multicast**, **ntp multicast client**, **ntp orphan**, **ntp panic update**, **ntp passive**, **ntp peer**, **ntp refclock**, **ntp server**, **ntp source**, **ntp trusted-key**, **ntp update-calendar**. Призначення та синтаксис усіх вищезгаданих команд наведено нижче.

Основними командами, які застосовуються для налагодження загальних параметрів функціонування NTP-вузлів є команди **ntp server**, **ntp peer**, **ntp master**, **ntp source**, **ntp logging**. Команда **ntp server** застосовується для налагодження синхронізації часових параметрів поточного вузла із зазначеним NTP-сервером. Команда **ntp peer** застосовується для налагодження синхронізації часових параметрів між однорівневими NTP-вузлами. Команда **ntp master** застосовується для налагодження головного джерела часу, з яким NTP-вузли здійснюють синхронізацію параметрів часу у разі, коли зовнішні NTP-сервери недоступні. У разі активації цієї команди за замовчуванням встановлюється страта 8. Команда **ntp source** застосовується для встановлення постійної IP-адреси відправника в IP-

пакетах, що містять повідомлення протоколу NTP. Активація виведення повідомлень журналювання подій протоколу NTP здійснюється за допомогою команди **ntp logging**.

Частина команд NTP застосовується для налагодження специфічних параметрів функціонування протоколу. Це команди: **ntp clear drift**, **ntp clock-period**, **ntp max-associations**, **ntp maxdistance**, **ntp orphan**, **ntp refclock**, **ntp update-calendar**, **ntp panic update**, **ntp passive**, **ntp allow mode private**.

Команда **ntp clear drift** застосовується для обнулення значення зміщення часу локального годинника у конфігураційному файлі. Команда **ntp clock-period** застосовувалася для компенсації помилок у програмних годинниках пристроїв. У Cisco IOS версій 15.0(1)M і вище ця команда усунута, її функції виконуються модулями NTP-вузла автоматично. Команда **ntp max-associations** відповідає за обмеження кількості встановлених відносин з іншими NTP-вузлами. Команда **ntp maxdistance** застосовується для встановлення значення граничної кількості NTP-повідомлень, необхідних для синхронізації однорівневих вузлів у протоколі NTP версії 4. Команда **ntp orphan** призначена для активації групи NTP-вузлів для вибору одного з них для симуляції джерела універсального глобального часу (UTC, Coordinated Universal Time) у випадку, коли реальне джерело стає недоступним. Команда **ntp refclock** застосовується для налагодження зовнішніх джерел часу, які будуть використовуватися NTP-вузлами. Команда **ntp update-calendar** відповідає за періодичне оновлення апаратного годинника (календаря) на основі даних, що отримані від джерела протоколу NTP. Команда **ntp panic update** призначена для активації функції відкидання оновлень часових параметрів, які містять значення більші, ніж встановлене аварійне („панічне") граничне значення (1000 с). Команда **ntp passive** призначена для встановлення пасивних режимів асоціації на NTP-вузлі. За замовчуванням дані режими не налагоджені. Для активації дозволу опрацювання повідомлень приватного режиму NTP в деяких версіях Cisco IOS застосовується команда **ntp allow mode private**. У сучасних версіях Cisco IOS її усунуто.

Окремі групи команд застосовуються для налагодження параметрів широкомовної і групової передачі повідомлень у різних режимах для окремих інтерфейсів. До цих команд належать команди: **ntp broadcast**, **ntp broadcast client**, **ntp broadcastdelay**, **ntp multicast**, **ntp multicast client**, **ntp disable**.

Для забезпечення передачі широкомовних повідомлень протоколу NTP у Cisco IOS наявні команди **ntp broadcast**, **ntp broadcast client**, **ntp broadcastdelay**. Команда **ntp broadcast** застосовується для налагодження параметрів передачі широкомовного трафіка протоколу NTP на певному інтерфейсі. Окремо виділяється команда **ntp broadcast client**, що застосовується для активації приймання широкомовних повідомлень протоколу NTP на певному інтерфейсі. Команда **ntp broadcastdelay** призначена для встановлення фіксованого значення зворотної затримки між поточним NTP-вузлом та NTP-сервером.

Для забезпечення передачі групових повідомлень протоколу NTP у Cisco IOS наявні команди **ntp multicast** та **ntp multicast client**. Команда **ntp multicast** застосовується для налагодження параметрів передачі групових повідомлень протоколу NTP на певному інтерфейсі. Окремо виділяється команда **ntp multicast client**, що застосовується для активації приймання групових повідомлень протоколу NTP на певному інтерфейсі. Команда **ntp disable** призначена для відключення приймання повідомлень протоколу NTP на певному інтерфейсі.

У протоколі NTP наявні засоби забезпечення безпечного обміну параметрами часу між вузлами – засоби аутентифікації та засоби контролю доступу. З цією метою використовуються команди **ntp authenticate**, **ntp authentication-key**, **ntp trusted-key**, **ntp access-group**. Команда **ntp authenticate** застосовується для активації засобів аутентифікації протоколу на NTP-вузлах. За допомогою команди **ntp authentication-key** зазначається ключ аутентифікації протоколу. Команда **ntp trusted-key** відповідає за встановлення меж діапазону довірених ключів аутентифікації протоколу NTP. Налагодження параметрів контролю доступу до служб протоколу NTP у системі Cisco IOS здійснюється із застосуванням команди **ntp access-group**.

Синтаксис команди **ntp access-group** (режим глобального конфігурування):

ntp access-group [ipv4 | ipv6] { peer | query-only | serve | serve-only } ***{access_list_number | access_list_number_expanded | access_list_name}*** **[kod]**,

де **ipv4** – службова конструкція, за допомогою якої зазначається використання списку доступу IP-мереж версії 4;

ipv6 – службова конструкція, за допомогою якої зазначається використання списку доступу IP-мереж версії 6;

peer – службова конструкція, за допомогою якої дозволяється можливість пересилання запитів часу та керуючих запитів протоколу NTP, а також синхронізація параметрів часу локальної системи з параметрами часу віддаленої системи;

query-only – службова конструкція, за допомогою якої дозволяється лише пересилання керуючих запитів протоколу NTP;

serve – службова конструкція, за допомогою якої дозволяється можливість пересилання запитів часу та керуючих запитів протоколу NTP, але не дозволяється синхронізація параметрів часу локальної системи з параметрами часу віддаленої системи;

serve-only – службова конструкція, за допомогою якої зазначається лише можливість пересилання запитів часу;

access_list_number – номер стандартного списку доступу IP-мереж версії 4; може набувати значень від 1 до 99;

access_list-number_expanded – номер розширеного списку доступу IP-мереж версії 4; може набувати значень від 1300 до 1999;

access_list_name – текстова назва списку доступу;

kod – службова конструкція, за допомогою якої активується надсилання повідомлення KOD („Kiss-O-Death”) будь-якому вузлу, що намагається надсилати повідомлення, які не відповідають параметрам групи контролю доступу.

Синтаксис команди **ntp allow mode private** (режим глобального конфігурування):

ntp allow mode private.

Команда не має параметрів.

Синтаксис команди **ntp authenticate** (режим глобального конфігурування):

ntp authenticate.

Команда не має параметрів.

Синтаксис команди **ntp authentication-key** (режим глобального конфігурування):

ntp authentication-key ***key_number*** **md5** ***key_string*** **[*encryption_type*]**, де ***key_number*** – номер ключа аутентифікації; може набувати значень від 1 до 4294967295;

md5 – службова конструкція, за допомогою якої зазначається використання функції хешування MD5 для забезпечення аутентифікації;

key_string – текстовий рядок довжиною до 32 символів, що містить значення ключа MD5;

encryption_type – тип ключа аутентифікації; може набувати значень від 1 до 4294967295.

Синтаксис команди **ntp broadcast** (режим конфігурування інтерфейсу):

ntp broadcast [client | [destination { *IP_address* | *hostname* }] [key [*broadcast_key_id*]] [version *number_value*]],

де **client** – службова конструкція, за допомогою якої активується режим прослуховування широкомовних повідомлень протоколу NTP;

destination – службова конструкція, за допомогою якої активується режим адресного надсилання широкомовних NTP-повідомлень;

IP_address – IP-адреса пристрою, якому надсилаються широкомовні NTP-повідомлення;

hostname – текстова назва пристрою, якому надсилаються широкомовні NTP-повідомлення;

key – службова конструкція, за допомогою якої активується використання ключа аутентифікації для широкомовних NTP-повідомлень;

broadcast_key_id – номер ключа аутентифікації для широкомовних повідомлень протоколу NTP; може набувати значень від 1 до 4294967295;

version – службова конструкція, за допомогою якої зазначається версія протоколу NTP, що використовується на NTP-вузлі;

number_value – номер версії протоколу NTP; може набувати значень від 2 до 4.

Синтаксис команди **ntp broadcast client** (режим конфігурування інтерфейсу):

ntp broadcast client.

Команда не має параметрів.

Синтаксис команди **ntp broadcastdelay** (режим глобального конфігурування):

ntp broadcastdelay ***broadcast_delay_value***,

де ***broadcast_delay_value*** – значення зворотної затримки (мкс); може набувати значень від 1 до 999999 мкс; за замовчуванням становить 3000 мкс.

Синтаксис команди **ntp clear drift** (режим глобального конфігурування):

ntp clear drift.

Команда не має параметрів.

Синтаксис команди **ntp clock-period** (режим глобального конфігурування):

ntp clock-period ***clock_period_value*****,**

де ***clock_period_value*** – значення часового періоду (мс), що повинен додаватися до часу програмного годинника за кожен такт роботи апаратного годинника; за замовчуванням дорівнює 4 мс.

Синтаксис команди **ntp disable** (режим конфігурування інтерфейсу):

ntp disable [**ip** | **ipv6**],

де **ip** – службова конструкція, за допомогою якої здійснюється відключення приймання повідомлень протоколу NTP для IP-трафіка;

ipv6 – службова конструкція, за допомогою якої здійснюється відключення приймання повідомлень протоколу NTP для трафіка IP версії 6.

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

ntp logging.

Команда не має параметрів.

Синтаксис команди **ntp master** (режим глобального конфігурування):

ntp master [*stratum_value*],

де ***stratum_value*** – номер страти, може набувати значень від 1 до 15; якщо команда активована, то за замовчуванням номер страти дорівнює 8.

Синтаксис команди **ntp max-associations** (режим глобального конфігурування):

ntp max-associations ***number_value*****,**

де ***number_value*** – максимальна кількість встановлених відносин на пристрої; може набувати значень від 1 до 4294967295; за замовчуванням дорівнює 100.

Синтаксис команди **ntp maxdistance** (режим глобального конфігурування):

ntp maxdistance ***threshold_value***,

де ***threshold_value*** – значення граничної кількості NTP-повідомлень; може змінюватися у межах від 1 до 16; за замовчуванням дорівнює 8.

Синтаксис команди **ntp multicast** (режим конфігурування інтерфейсу):

ntp multicast [***IP address*** **|** ***IPv6 address*** **] [key** ***multicast_key_id*****] [ttl** ***ttl value*** **] [version** ***version_number*** **]**,

де ***IP_address*** – IP-адреса версії 4, що використовується для групової розсилки NTP-повідомлень; за замовчуванням дорівнює 224.0.1.1;

IPv6_address – IP-адреса версії 6, що використовується для групової розсилки NTP-повідомлень; це може бути адреса FF02::1, що використовується для групової розсилки всім вузлам мережі або будь-яка інша групова IP-адреса версії 6;

key – службова конструкція, за допомогою якої активується використання ключа аутентифікації для групових NTP-повідомлень;

multicast_key_id – номер ключа аутентифікації для групових NTP-повідомлень; може набувати значень від 1 до 4294967295;

ttl – службова конструкція, за допомогою якої встановлюється значення часу існування IP-пакета, що містить групове NTP-повідомлення;

ttl_value – значення часу існування IP-пакета, що містить групове NTP-повідомлення; може набувати значень від 1 до 255; за замовчуванням дорівнює 16;

version – службова конструкція, за допомогою якої зазначається версія протоколу NTP, що використовується на NTP-вузлі;

version_number – номер версії протоколу NTP; може набувати значень від 2 до 4; за замовчуванням для IP-мереж версії 4 дорівнює 3, для IP-мереж версії 6 дорівнює 4.

Синтаксис команди **ntp multicast client** (режим конфігурування інтерфейсу):

ntp multicast client [***IP_address*** **|** ***IPv6_address*** **]**,

де ***IP_address*** – IP-адреса версії 4, що використовується для групової розсилки NTP-повідомлень; за замовчуванням дорівнює 224.0.1.1;

IPv6_address – IP-адреса версії 6, що використовується для групової розсилки NTP-повідомлень; це може бути адреса FF02::1, що використовується для групової розсилки всім вузлам мережі або будь-яка інша групова IP-адреса версії 6.

Синтаксис команди **ntp orphan** (режим глобального конфігурування):

ntp orphan ***stratum_value***,

де ***stratum_value*** – номер страти, може набувати значень від 1 до 15; якщо команда активована, то за замовчуванням номер страти дорівнює 0.

Синтаксис команди **ntp panic update** (режим глобального конфігурування):

ntp panic update,

Команда не має параметрів.

Синтаксис команди **ntp passive** (режим глобального конфігурування):

ntp passive.

Команда не має параметрів.

Синтаксис команди **ntp peer** (режим глобального конфігурування):

ntp peer [vrf ***vrf_name*** **] {** ***IP_address*** **|** ***IPv6_address*** **| [ip | ipv6]** ***hostname*** **} [normal-sync] [version** ***version_number*** **] [key** ***key_id*** **] [source** ***interface_type interface_id*** **] [prefer] [maxpoll** ***maxpoll_number*** **] [minpoll** ***minpoll_number*** **] [burst] [iburst]**,

де **vrf** – службова конструкція, за допомогою якої створюється об'єкт технології VRF (VPN Routing and Forwarding), що буде використовуватися NTP-вузлом для маршрутизації до NTP-сервера замість глобальної таблиці маршрутизації ;

vrf_name – текстова назва об'єкта VRF;

IP_address – IP-адреса версії 4 віддаленого NTP-вузла, який надає параметри часу для синхронізації;

IPv6_address – IP-адреса версії 6 віддаленого NTP-вузла, який надає параметри часу для синхронізації;;

ip – службова конструкція, за допомогою якої активується використання засобів системи DNS в адресному просторі IP версії 4;

ipv6 – службова конструкція, за допомогою якої активується використання засобів системи DNS в адресному просторі IP версії 6;

hostname – текстова назва віддаленого NTP-вузла, який надає параметри часу для синхронізації;

normal-sync – службова конструкція, за допомогою якої відключається режим швидкої синхронізації часових параметрів NTP-вузла з програмним годинником при завантаженні;

version – службова конструкція, за допомогою якої зазначається версія протоколу NTP, що використовується на NTP-вузлі;

version_number – номер версії протоколу NTP; може набувати значень від 2 до 4;

key – службова конструкція, за допомогою якої активується використання ключа аутентифікації при обміні NTP-повідомленнями;

key id – номер ключа аутентифікації повідомлень протоколу NTP;

source – службова конструкція, за допомогою якої зазначається, що як адреса NTP-сервера застосовується адреса вказаного вихідного інтерфейсу;

interface_type – тип інтерфейсу (порту), 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);

prefer – службова конструкція, за допомогою якої зазначається, що обраний NTP-вузол має переваги перед іншими вузлами при отриманні параметрів синхронізації часу;

maxpoll – службова конструкція, за допомогою якої встановлюється максимальне значення інтервалу між запитами NTP-клієнта до NTP-сервера;

maxpoll_number – максимальне значення інтервалу (с) між NTP-запитами; може змінюватися у межах від 4 до 17; за замовчуванянм дорівнює 10;

minpoll – службова конструкція, за допомогою якої встановлюється мінімальне значення інтервалу між запитами NTP-клієнта до NTP-сервера;

minpoll_number – мінімальне значення інтервалу (с) між NTP-запитами; може змінюватися у межах від 4 до 17; за замовчуванянм дорівнює 6;

burst – службова конструкція, за допомогою якої активується використання пульсуючого режиму обміну NTP-повідомленнями (8 замість 2) з метою зменшення ефекту пульсацій;

iburst – службова конструкція, за допомогою якої активується використання стартового пульсуючого режиму обміну NTP-повідомленнями.

Синтаксис команди **ntp refclock** (режим глобального конфігурування):

ntp refclock { trimble | telecom-solutions } pps { cts | ri | none } [inverted] [pps-offset *pps offset value*] [stratum *stratum_value*] [timestamp-offset *timestamp_offset_number*],

де **trimble** – службова конструкція, за допомогою якої активується використання драйвера еталонного годинника для Trimble Palisade NTP Synchronization Kit;

telecom-solutions – службова конструкція, за допомогою якої активується використання драйвера еталонного годинника для пристрою, на якому функціонує система GPS;

pps – службова конструкція, за допомогою якої активується сигнальна лінія PPS (Pulse Per Second);

cts – службова конструкція, за допомогою якої активується PPS на лінії CTS (Clear To Send);

ri – службова конструкція, за допомогою якої активується PPS на лінії RI (Ring Indicator);

none – службова конструкція, за допомогою якої зазначається, що сигнал PPS недоступний;

inverted – службова конструкція, за допомогою якої зазначається, що сигнал PPS передається в інвертованому вигляді;

pps-offset – службова конструкція, за допомогою якої вказується зсув сигналу PPS;

pps offset_value – тривалість сигналу зсуву (мс);

stratum – службова конструкція, за допомогою якої зазначається номер страти, на яку система може претендувати;

stratum_value – номер страти, може набувати значень від 0 до 14;

timestamp-offset – службова конструкція, за допомогою якої зазначається зсув мітки часу;

timestamp_offset_number – значення зсуву мітки часу (мс);

Синтаксис команди **ntp server** (режим глобального конфігурування):

ntp server [vrf *vrf name*] { *ip-address* | *ipv6-address* | [ip | ipv6] *hostname* } [normal-sync] [version *number*] [key *key-id*] [source *interface-type interface-number*] [prefer] [maxpoll *number*] [minpoll *number*] [burst] [iburst],

Параметри команди **ntp server** аналогічні параметрам команди **ntp peer**.

Синтаксис команди **ntp source** (режим глобального конфігурування):

ntp source *interface_type interface_number*,

де ***interface_type*** – тип інтерфейсу (порту), 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), тричис-

лове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/ номер інтерфейсу).

Синтаксис команди **ntp trusted-key** (режим глобального конфігурування):

ntp trusted-key ***key_number*** **[-** ***end_key_number*** **]**,

де ***key_number*** – початкове значення діапазону довірених ключів аутентифікації; може набувати значень від 0 до 65535;

end_key_number – кінцеве значення діапазону довірених ключів аутентифікації; може набувати значень від 0 до 65535.

Синтаксис команди **ntp update-calendar** (режим глобального конфігурування):

ntp update-calendar.

Команда не має параметрів.

Команди моніторингу та діагностики часових параметрів та параметрів роботи протоколу мережного часу NTP на пристроях Cisco

Для моніторингу та діагностики поточних параметрів програмного годинника на пристроях Cisco застосовуються команди **show clock**, **show clock detail**, **show calendar**. Для моніторингу та діагностики функціонування засобів протоколу NTP застосовуються як команди загального призначення, так і спеціалізовані команди. Перелік спеціалізованих команд є відносно невеликим і включає такі команди як: **show ntp associations**, **show show ntp associations detail**, **show ntp status**. Важливими командами, які допомагають зрозуміти процеси передачі повідомлень протоколу NTP є команди трасування, такі як: **debug ntp adjust**, **debug ntp all**, **debug ntp core**, **debug ntp events**, **debug ntp packet**, **debug ntp refclock**.

Узагальнений перелік команд моніторингу та діагностики поточних параметрів програмного годинника та параметрів функціонування протоколу NTP на пристроях Cisco наведений у табл. 3.1.

Таблиця 3.1

Перелік команд моніторингу та діагностики поточних параметрів програмного годинника та параметрів функціонування протоколу NTP на пристроях Cisco

Команда	Призначення
Команди **show clock, show calendar** та **show ntp**	
show clock	Виведення поточних дати та часу пристрою
show clock detail	Виведення поточних дати та часу пристрою та джерела їх отримання
show calendar	Виведення поточних дати та часу пристрою
show ntp associations	Виведення інформації про встановлені асоціації протоколу NTP
show ntp associations detail	Виведення деталізованої інформації про встановлені асоціації протоколу NTP
show ntp status	Виведення інформації про стан поточних часових параметрів пристрою
Команди **ntp debug**	
debug ntp adjust	Активація виведення інформації про коригування часових параметрів із використанням протоколу NTP
debug ntp all	Активація виведення всієї інформації про функціонування протоколу NTP
debug ntp core	Активація виведення інформації про передачу повідомлень типу Core протоколу NTP
debug ntp events	Активація виведення інформації про події протоколу NTP
debug ntp packet	Активація виведення інформації про передачу повідомлень протоколу NTP
debug ntp refclock	Активація виведення інформації про передачу повідомлень типу Refclock протоколу NTP.

Модельний приклад налагодження функціонування протоколу мережного часу NTP у мережі на базі обладнання Cisco

Розглянемо специфіку налагодження функціонування протоколу мережного часу NTP для мережі, схема якої наведена на рис. 3.8. Джерелом часу (NTP-сервером) для пристроїв даної мережі є сервер Serv_A_1. Решта пристроїв мережі є NTP-клієнтами.

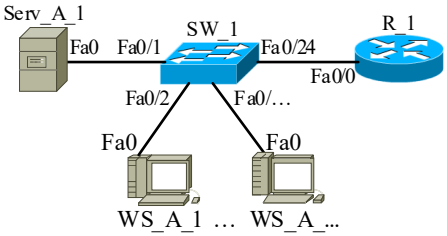

Рис. 3.8. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3.2. Для налагодження параметрів адресації пристроїв мережі використано дані табл. 3.3. Для налагодження параметрів протоколу NTP на NTP-сервері і NTP-клієнтах використано дані табл. 3.4.

Таблиця 3.2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Fa0/0	Комутатор SW_1	Fa0/24
Комутатор SW_1	Fa0/1	Сервер Serv_A_1	Fa0/0
	Fa0/2	Робоча станція WS_A_1	Fa0
	…	…	…
	Fa0/…	Робоча станція WS_A_…	Fa0
	Fa0/24	Маршрутизатор R_1	Fa0/0
Сервер Serv_A_1	Fa0	Комутатор SW_1	Fa0/1
Робоча станція WS_A_1	Fa0	Комутатор SW_1	Fa0/2
…	…	…	…
Робоча станція WS_A_…	Fa0	Комутатор SW_1	Fa0/…

Таблиця 3.3

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
Маршрутизатор R_1	Інтерфейс Fa0/0	195.10.1.254	255.255.255.0	/24
Комутатор SW_1	Інтерфейс Vlan 1	195.10.1.252	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Сервер Serv_A_1	Мережний адаптер	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS_A_1	Мережний адаптер	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
…	…	…	…	…
Робоча станція WS_A_...	Мережний адаптер	195.10.1….	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–

Таблиця 3.4

Параметри для налагодження функціонування протоколу NTP на пристроях мережі

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)
IP-адреса NTP-сервера	195.10.1.1
Аутентифікація NTP	Активована
Номер ключа аутентифікації NTP	1
Ключ аутентифікації	mypass

Сценарії налагодження параметрів адресації інтерфейсів маршрутизатора R_1 та комутатора SW_1 наведені нижче.

```
…
R_1>enable
R_1#configure terminal
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)#exit
R_1#
…
```

```
…
SW_1#configure terminal
SW_1(config)#interface vlan 1
SW_1(config-if)#ip address 195.10.1.252 255.255.255.0
SW_1(config-if)#no shutdown
SW_1(config)#ip default-gateway 195.10.1.254
SW_1(config-if)#exit
SW_1(config)#exit
SW_1#
…
```

Сценарії налагодження маршрутизатора R_1 та комутатора SW_1 як NTP-клієнтів наведені нижче.

```
…
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)#clock timezone EET 2
R_1(config)#clock summertime EET reccuring last monday
october 3:00 last monday march 3:00
R_1(config)#ntp server 195.10.1.1 key 1
R_1(config)#ntp authentificate
R_1(config)#ntp authentication-key 1 md5 mypass
R_1(config)#ntp trusted-key 1
R_1(config)#ntp update-calendar
R_1(config)#
…

…
SW_1#configure terminal
SW_1(config)#service timestamps log datetime msec year
SW_1(config)#service timestamps debug datetime msec year
SW_1(config)#clock timezone EET 2
SW_1(config)#clock summertime EET reccuring last monday
october 3:00 last monday march 3:00
SW_1(config)#ntp server 195.10.1.1 key 1
SW_1(config)#ntp authentificate
SW_1(config)#ntp authentication-key 1 md5 mypass
SW_1(config)#ntp trusted-key 1
SW_1(config)#ntp update-calendar
SW_1(config)#
…
```

Результати виконання команд моніторингу та діагностики роботи протоколу мережного часу NTP для розглянутого прикладу

З метою перегляду інформації про роботу протоколу мережного часу NTP для розглянутого прикладу використано команди **show clock detail, show ntp status**, **show ntp associations**, **show ntp associations detail**. Результати роботи цих команд для маршрутизатора R_1 наведено відповідно на рис. 3.9 – 3.12.

```
R_1#show clock detail
20:55:02.177 EET Sun Jan 22 2017
Time source is NTP
Summer time starts 03:00:00 EET Mon Oct 31 2016
Summer time ends 03:00:00 EET Mon Mar 27 2017
R_1#
```

Рис. 3.9. Результати виконання команди **show ntp status** на маршрутизаторі R_1

```
R_1#show ntp status
Clock is synchronized, stratum 5, reference is 195.10.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is DC2F9D60.19167F84 (21:06:40.097 EET Sun Jan 22 2017)
clock offset is 3.9775 msec, root delay is 11.75 msec
root dispersion is 6.15 msec, peer dispersion is 2.15 msec
R_1#
```

Рис. 3.10. Результати виконання команди **show ntp status** на маршрутизаторі R_1

```
R_1#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
*~195.10.1.1       127.127.7.1       4    13    64  377    11.7    7.30     5.3
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R_1#
```

Рис. 3.11. Результати виконання команди **show ntp associations** на маршрутизаторі R_1

```
R_1#show ntp associations detail
195.10.1.1 configured, authenticated, our_master, sane, valid, stratum 4
ref ID 127.127.7.1, time DC2F9D61.F3B1BF20 (21:06:41.951 EET Sun Jan 22 2017)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 11.246
delay 11.75 msec, offset 7.3015 msec, dispersion 5.34
precision 2**18, version 3
org time DC2F9DA0.189695E8 (21:07:44.096 UTC Sun Jan 22 2017)
rcv time DC2F9DA0.18396480 (21:07:44.094 UTC Sun Jan 22 2017)
xmt time DC2F9DA0.152EC34A (21:07:44.082 UTC Sun Jan 22 2017)
filtdelay =    11.75   15.73   15.73   15.73   15.75   15.75   15.75   15.73
filtoffset =    7.30    1.92    1.93    1.93    1.95    1.96    1.97    1.99
filterror =     0.02    0.99    1.01    1.02    1.04    1.05    1.07    1.08

R_1#
```

Рис. 3.12. Результати виконання команди **show ntp associations detail** на маршрутизаторі R_1

Модельний приклад налагодження функціонування протоколу мережного часу NTP у мережі на базі обладнання Cisco

Розглянемо специфіку налагодження роботи протоколу мережного часу NTP для мережі, схема якої наведена на рис. 3.13. Еталонні джерела часу знаходяться у глобальній мережі (WAN). Джерелом часу для пристроїв даної мережі є маршрутизатор R_1. NTP-клієнтами виступають решта пристроїв мережі.

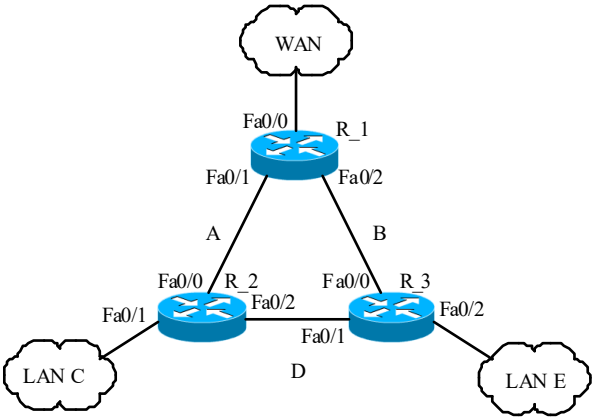

Рис. 3.13. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3.5. Для налагодження параметрів адресації пристроїв використано дані табл. 3.6. Для налагодження параметрів протоколу NTP на NTP-сервері і NTP-клієнтах використано дані табл. 3.7.

Таблиця 3.5

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Fa0/0	WAN	WAN Interface
	Fa0/1	Маршрутизатор R_2	Fa0/0
	Fa1/0	Маршрутизатор R_3	Fa0/0
Маршрутизатор R_2	Fa0/0	Маршрутизатор R_1	Fa0/1
	Fa0/1	LAN A	LAN A Interface
	Fa1/0	Маршрутизатор R_3	Fa0/1
Маршрутизатор R_3	Fa0/0	Маршрутизатор R_1	Fa1/0
	Fa0/1	Маршрутизатор R_2	Fa1/0
	Fa1/0	LAN B	LAN B Interface

Таблиця 3.6

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
WAN	–	195.10.1.0	255.255.255.252	/30
Підмережа A	–	195.20.1.0	255.255.255.252	/24
Підмережа B	–	195.30.1.0	255.255.255.252	/30
Підмережа C	–	195.40.1.0	255.255.255.0	/24
Підмережа D	–	195.50.1.0	255.255.255.252	/30
Підмережа E	–	195.60.1.0	255.255.255.0	/24
WAN	WAN Interface	195.10.1.1	255.255.255.252	/30
Маршрутизатор R_1	Інтерфейс Fa0/0	195.10.1.2	255.255.255.252	/30
	Інтерфейс Fa0/1	195.20.1.1	255.255.255.252	/30
	Інтерфейс Fa1/0	195.30.1.1	255.255.255.252	/30
Маршрутизатор R_2	Інтерфейс Fa0/0	195.20.1.2	255.255.255.252	/30
	Інтерфейс Fa0/1	195.40.1.254	255.255.255.0	/24
	Інтерфейс Fa1/0	195.50.1.1	255.255.255.252	/30
Маршрутизатор R_3	Інтерфейс Fa0/0	195.30.1.2	255.255.255.252	/30
	Інтерфейс Fa0/1	195.50.1.2	255.255.255.252	/30
	Інтерфейс Fa1/0	195.60.1.254	255.255.255.0	/24

Таблиця 3.7

Параметри для налагодження функціонування протоколу NTP на пристроях мережі

Параметр	Значення
Загальні параметри	
Системний час	Поточний (включає поточні час та дату)
Часовий пояс	EET, Eastern European Time
Перехід на літній час	Активовано
Часові мітки	Активовані
Аутентифікація NTP	Активована
Номер ключа аутентифікації NTP	1
Ключ аутентифікації	mypass
Параметри для маршрутизатора R_1	
IP-адреса еталонного джерела часу 1	195.10.1.1
Страта еталонного джерела часу 1	3
IP-адреса еталонного джерела часу 2	198.13.15.200
Страта еталонного джерела часу 1	3
Параметри для маршрутизатора R_2	
IP-адреса основного NTP-сервера	195.20.1.1
IP-адреса допоміжного NTP-сервера	195.10.1.1
IP-адреса NTP-Peer	195.50.1.2
Параметри для маршрутизатора R_3	
IP-адреса основного NTP-сервера	195.30.1.1
IP-адреса допоміжного NTP-сервера	195.10.1.1
IP-адреса NTP-Peer	195.50.1.1

Сценарії налагодження параметрів адресації пристроїв мережі та протоколу маршрутизації EIGRP наведені нижче.

```
…
R_1>enable
R_1#configure terminal
R_1(config)#interface FastEthernet 0/0
R_1(config-if)#description LINK_TO_WAN
R_1(config-if)#ip address 195.10.1.2 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#interface FastEthernet 0/1
R_1(config-if)#description LINK_TO_R_2
R_1(config-if)#ip address 195.20.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#interface FastEthernet 1/0
R_1(config-if)#description LINK_TO_R_3
R_1(config-if)#ip address 195.30.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#router eigrp 100
R_1(config-router)#network 195.10.1.0 0.0.0.3
R_1(config-router)#network 195.20.1.0 0.0.0.3
R_1(config-router)#network 195.30.1.0 0.0.0.3
R_1(config- router)#exit
R_1(config)#exit
R_1#
…
```

```
…
R_2>enable
R_2#configure terminal
R_2(config)#interface FastEthernet 0/0
R_2(config-if)#description LINK_TO_ R_1
R_2(config-if)#ip address 195.20.1.2 255.255.255.252
R_2(config-if)#no shutdown
R_2(config-if)#interface FastEthernet 0/1
R_2(config-if)#description LINK_TO_LAN_C
R_2(config-if)#ip address 195.40.1.254 255.255.255.0
R_2(config-if)#no shutdown
```

R_2(config-if)#interface FastEthernet 1/0
R_2(config-if)#description LINK_TO_R_3
R_2(config-if)#ip address 195.50.1.1 255.255.255.252
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#router eigrp 100
R_2(config-router)#network 195.20.1.0 0.0.0.3
R_2(config-router)#network 195.40.1.0 0.0.0.255
R_2(config-router)#network 195.50.1.0 0.0.0.3
R_2(config-router)#exit
R_2(config)#exit
R_2#
…

…
R_3>enable
R_3#configure terminal
R_3(config)#interface FastEthernet 0/0
R_3(config-if)#description LINK_TO_ R_1
R_3(config-if)#ip address 195.30.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#interface FastEthernet 0/1
R_3(config-if)#description LINK_TO_R_2
R_3(config-if)#ip address 195.50.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#interface FastEthernet 1/0
R_3(config-if)#description LINK_TO_ LAN_E
R_3(config-if)#ip address 195.60.1.254 255.255.255.0
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#router eigrp 100
R_3(config-router)#network 195.30.1.0 0.0.0.3
R_3(config-router)#network 195.50.1.0 0.0.0.3
R_3(config-router)#network 195.60.1.0 0.0.0.255
R_3(config-router)#exit
R_3(config)#exit
R_3#
…

Сценарій налагодження маршрутизатора R_1, як NTP-клієнта еталонного джерела часу та NTP-сервера (за даними табл. 3.7) для побудованої мережі, наведений нижче.

```
…
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)#clock timezone EET 2
R_1(config)#clock summertime EET reccuring last monday october 3:00 last monday march 3:00
R_1(config)#ntp authentificate
R_1(config)#ntp authentication-key 1 md5 mypass
R_1(config)#ntp trusted-key 1
R_1(config)#ntp server 195.10.1.1 key 1 prefer
R_1(config)#ntp server 198.13.15.200 key 1
R_1(config)#ntp update-calendar
R_1(config)#exit
R_1#
…
```

Сценарії налагодження маршрутизаторів R_2 та R_3 як NTP-клієнтів та встановлення однорівневих зв'язків між ними (за даними табл. 3.7) наведені нижче.

```
…
R_2>enable
R_2#configure terminal
R_2(config)#service timestamps log datetime msec year
R_2(config)#service timestamps debug datetime msec year
R_2(config)#clock timezone EET 2
R_2(config)#clock summertime EET reccuring last monday october 3:00 last monday march 3:00
R_2(config)#ntp authentificate
R_2(config)#ntp authentication-key 1 md5 mypass
R_2(config)#ntp trusted-key 1
R_2(config)#ntp server 195.20.1.1 key 1 prefer
```

R_1(config)#ntp server 195.10.1.1 key 1
R_2(config)#ntp peer 195.50.1.2 key 1
R_2(config)#ntp update-calendar
R_2(config)#exit
R_2#
…

…
R_3>enable
R_3#configure terminal
R_3(config)#service timestamps log datetime msec year
R_3(config)#service timestamps debug datetime msec year
R_3(config)#clock timezone EET 2
R_3(config)#clock summertime EET reccuring last monday october 3:00 last monday march 3:00
R_3(config)#ntp authentificate
R_3(config)#ntp authentication-key 1 md5 mypass
R_3(config)#ntp trusted-key 1
R_3(config)#ntp server 195.30.1.1 key 1 prefer
R_1(config)#ntp server 195.10.1.1 key 1
R_3(config)#ntp peer 195.50.1.1 key 1
R_3(config)#ntp update-calendar
R_3(config)#exit
R_3#
…

Сценарій налагодження маршрутизатора R_2 як широкомовного NTP-сервера для підключеної локальної мережі С наведений нижче.

…
R_2>enable
R_2#configure terminal
R_2(config-if)#interface FastEthernet 0/1
R_2(config-if)#ntp broadcast
R_2(config-if)#exit
R_3(config)#exit
R_3#
…

Результати виконання команд моніторингу та діагностики роботи протоколу мережного часу NTP для розглянутого прикладу

З метою перегляду інформації про роботу протоколу мережного часу NTP для розглянутого прикладу використано команди **show clock detail, show ntp status**, **show ntp associations**, **show ntp associations detail**. Результати роботи цих команд для маршрутизаторів R_1, R_2, R_3 наведено відповідно на рис. 3.14 – 3.23.

```
R_1#show clock detail
15:42:16.483 EET Tue Jan 24 2017
Time source is NTP
Summer time starts 03:00:00 EET Mon Oct 31 2016
Summer time ends 03:00:00 EET Mon Mar 27 2017
R_1#
```

Рис. 3.14. Результати виконання команди **show ntp clock detail** на маршрутизаторі R_1

```
R_2#show clock detail
15:43:47.248 EET Tue Jan 24 2017
Time source is NTP
Summer time starts 03:00:00 EET Mon Oct 31 2016
Summer time ends 03:00:00 EET Mon Mar 27 2017
R_2#
```

Рис. 3.15. Результати виконання команди **show ntp clock detail** на маршрутизаторі R_2

```
R_3#show clock detail
15:43:50.248 EET Tue Jan 24 2017
Time source is NTP
Summer time starts 03:00:00 EET Mon Oct 31 2016
Summer time ends 03:00:00 EET Mon Mar 27 2017
R_3#
```

Рис. 3.16. Результати виконання команди **show ntp clock detail** на маршрутизаторі R_3

```
R_1#show ntp status
Clock is synchronized, stratum 4, reference is 195.10.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0004 Hz, precision is 2**18
reference time is DC31CA9D.7BA902BA (15:44:13.483 EET Tue Jan 24 2017)
clock offset is -6.2031 msec, root delay is 7.72 msec
root dispersion is 73.81 msec, peer dispersion is 67.57 msec
R_1#
```

Рис. 3.17. Результати виконання команди **show ntp status** на маршрутизаторі R_1

```
R_2#show ntp status
Clock is synchronized, stratum 5, reference is 195.20.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0280 Hz, precision is 2**18
reference time is DC31CB81.D46D1FC2 (15:48:01.829 EET Tue Jan 24 2017)
clock offset is -10.5119 msec, root delay is 35.45 msec
root dispersion is 8001.19 msec, peer dispersion is 7905.21 msec
R_2#
```

Рис. 3.18. Результати виконання команди **show ntp status** на маршрутизаторі R_2

```
R_3#show ntp status
Clock is synchronized, stratum 5, reference is 195.30.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0067 Hz, precision is 2**18
reference time is DC31CBD5.2A5F5E34 (15:49:25.165 EET Tue Jan 24 2017)
clock offset is -194.8043 msec, root delay is 55.42 msec
root dispersion is 567.14 msec, peer dispersion is 137.76 msec
R_3#
```

Рис. 3.19. Результати виконання команди **show ntp status** на маршрутизаторі R_3

```
R_1#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
*~195.10.1.1       127.127.7.1      3    32   128  377     7.7   -6.20    67.6
 ~198.13.15.200    0.0.0.0         16     -  1024    0     0.0    0.00  16000.
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R_1#
```

Рис. 3.20. Результати виконання команди **show ntp associations** на маршрутизаторі R_1

```
R_2#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
+~195.20.1.1       195.10.1.1       4    59    64  377    19.6    2.94    26.5
*~195.10.1.1       127.127.7.1      3    56    64    3    71.8    7.47  7893.3
 ~195.50.1.2       195.10.1.1       4   122   256  377    27.5   22.26    11.1
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R_2#
```

Рис. 3.21. Результати виконання команди **show ntp associations** на маршрутизаторі R_2

```
R_3#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
+~195.30.1.1       195.10.1.1       4    68   128  377    11.7   29.82    29.8
 ~195.50.1.1       195.10.1.1       4    91  1024  376    61.1   26.87    34.4
*~195.10.1.1       127.127.7.1      3    22   128  177    27.7   41.86   159.2
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R_3#
```

Рис. 3.22. Результати виконання команди **show ntp associations** на маршрутизаторі R_3

```
R_1#show ntp associations detail
195.10.1.1 configured, authenticated, our_master, sane, valid, stratum 3
ref ID 127.127.7.1, time DC31CBF0.69556CC3 (15:49:52.411 EET Tue Jan 24 2017)
our mode client, peer mode server, our poll intvl 256, peer poll intvl 256
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 84.076
delay 75.68 msec, offset -7.0707 msec, dispersion 46.20
precision 2**24, version 3
org time DC31CC1B.45846B58 (15:50:35.271 EET Tue Jan 24 2017)
rcv time DC31CC1B.51041811 (15:50:35.316 EET Tue Jan 24 2017)
xmt time DC31CC1B.3D9B847E (15:50:35.240 EET Tue Jan 24 2017)
filtdelay =    75.68  115.69  215.71  227.69   35.69   79.71    7.72   99.70
filtoffset =   -7.07  -31.62   85.32  -33.47 -114.40  -21.15   -6.20   39.61
filterror =     0.02    1.94    3.89    5.84    7.80    8.77    9.69   10.67

198.13.15.200 configured, insane, invalid, unsynced, stratum 16
ref ID 0.0.0.0, time 00000000.00000000 (02:00:00.000 eet Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 1024, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 50.690
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**5, version 3
org time 00000000.00000000 (02:00:00.000 eet Mon Jan 1 1900)
rcv time 00000000.00000000 (02:00:00.000 eet Mon Jan 1 1900)
xmt time DC31CB32.4104FB96 (15:46:42.253 EET Tue Jan 24 2017)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0

R_1#
```

Рис. 3.23. Результати виконання команди **show ntp associations detail** на маршрутизаторі R_1

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 3.24). 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. 3.8. 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. 3.5.

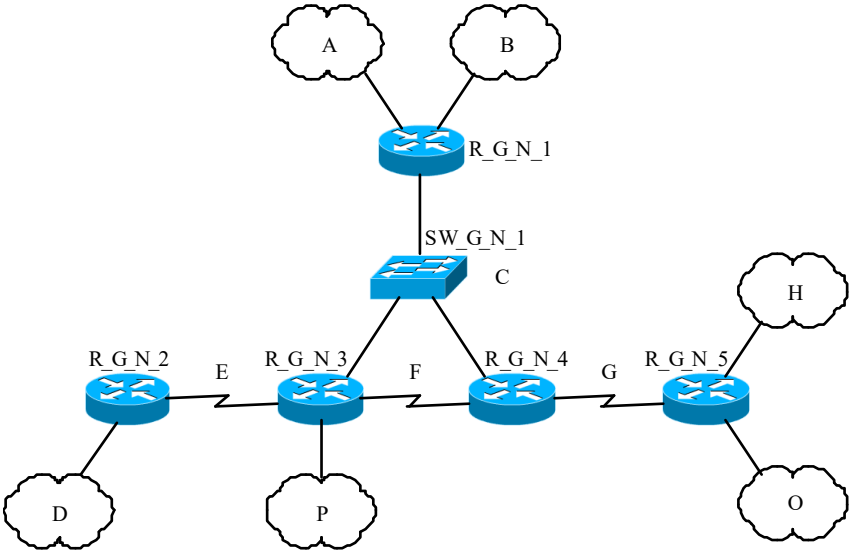

Рис. 3.24. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані табл. 3.9, 3.10. Результати навести у вигляді таблиці, яка аналогічна табл. 3.6.

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку (за даними табл. 3.8). 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. Розробити схему NTP-ролей комунікаційних пристроїв та кінцевих вузлів (за можливості) мережі та зв'язків між ними. Враховувати, що еталонне джерело часу знаходиться у відповідній локальній мережі (за даними табл. 3.11). Результати подати у вигляді таблиці.

6. Налагодити функціонування еталонного джерела/джерел часу у відповідній локальній мережі (за даними табл. 3.11). За потреби для еталонного джерела часу налагодити параметри часового поясу (за даними табл. 3.11) та переходу на літній/зимовий час. Вибір засобів для організації еталонного джерела часу виконується довільно.

7. Налагодити параметри часового поясу (за даними табл. 3.11) та переходу на літній/зимовий час на комунікаційних пристроях мережі.

8. Налагодити функціонування протоколу NTP для комунікаційних пристроїв та кінцевих вузлів (за можливості) мережі з урахуванням визначених у п. 5 NTP-ролей. Дані для налагодження параметрів аутентифікації обирати за даними табл. 3.11.

9. Дослідити процес передачі даних протоколу NTP між пристроями мережі. У разі відсутності зв'язку між NTP-вузлами визначити проблеми та усунути їх.

10. Налагодити функціонування одного з маршрутизаторів мережі як NTP-сервера, що функціонує у режимі широкомовної (або групової) розсилки для підключеної локальної мережі. Маршрутизатор та мережа зазначені у табл. 3.11. Налагодити функціонування пристроїв мережі як NTP-клієнтів даного сервера (за можливості).

11. Дослідити процес передачі даних протоколу NTP між налагодженим у п. 10 NTP-сервером та комунікаційними пристроями локальної мережі (за можливості).

Таблиця 3.8

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 3.9

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 3.10

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 3.11

Дані для налагодження протоколу NTP

№ варіанта	Мережа розміщення еталонного джерела часу	Основний сервер часу	Часовий пояс	Години	Кількість ключів аутентифікації	Номери ключів аутентифікації	Сервер часу (широкомовна розсилка)	Мережа (клієнти широкомовної або групової розсилки)
1	A	R_G_N_1	GMT	0	2	GN01X	R_G_N_5	H
2	B	R_G_N_1	BST	+1	3	GN02X	R_G_N_5	O
3	H	R_G_N_5	IST	+1	4	GN03X	R_G_N_1	A
4	O	R_G_N_5	WET	0	4	GN04X	R_G_N_1	B
5	D	R_G_N_2	WEST	+1	3	GN05X	R_G_N_1	A
6	P	R_G_N_3	CET	+1	2	GN06X	R_G_N_1	B
7	A	R_G_N_1	CEST	+2	2	GN07X	R_G_N_2	D
8	B	R_G_N_1	EET	+2	4	GN08X	R_G_N_3	P
9	H	R_G_N_5	EEST	+3	3	GN09X	R_G_N_2	D
10	O	R_G_N_5	MSK	+4	3	GN10X	R_G_N_3	P
11	D	R_G_N_2	GMT	0	4	GN11X	R_G_N_5	H
12	P	R_G_N_3	BST	+1	2	GN12X	R_G_N_5	O
13	A	R_G_N_1	IST	+1	3	GN13X	R_G_N_5	H
14	B	R_G_N_1	WET	0	2	GN14X	R_G_N_2	D
15	H	R_G_N_5	WEST	+1	4	GN15X	R_G_N_1	A
16	O	R_G_N_5	CET	+1	4	GN16X	R_G_N_1	B
17	D	R_G_N_2	CEST	+2	2	GN17X	R_G_N_1	A
18	P	R_G_N_3	EET	+2	3	GN18X	R_G_N_1	B
19	A	R_G_N_1	EEST	+3	3	GN19X	R_G_N_3	P
20	B	R_G_N_1	MSK	+4	4	GN20X	R_G_N_5	H
21	H	R_G_N_5	GMT	0	2	GN21X	R_G_N_2	D
22	O	R_G_N_5	BST	+1	2	GN22X	R_G_N_3	P
23	D	R_G_N_2	IST	+1	4	GN23X	R_G_N_5	H
24	P	R_G_N_3	WET	0	3	GN24X	R_G_N_5	O
25	A	R_G_N_1	WEST	+1	4	GN25X	R_G_N_5	H
26	B	R_G_N_1	CET	+1	2	GN26X	R_G_N_2	D
27	H	R_G_N_5	CEST	+2	3	GN27X	R_G_N_1	A
28	O	R_G_N_5	EET	+2	3	GN28X	R_G_N_1	B
29	D	R_G_N_2	EEST	+3	2	GN29X	R_G_N_5	H
30	P	R_G_N_3	MSK	+4	4	GN30X	R_G_N_5	O

Примітка: X – число (1, 2, 3, 4), яке застосовується для формування номера ключа; залежить від необхідної кількості ключів.

Контрольні питання

1. Передумови та проблеми розробки засобів та протоколів мережного часу.
2. Загальна характеристика протоколу NTP.
3. Сфера застосування протоколу NTP.
4. Стандартизація протоколу NTP.
5. Характеристики протоколу NTP стосовно моделі OSI та стеку TCP/IP.
6. Види вузлів протоколу NTP.
7. Варіанти та режими функціонування протоколу NTP.
8. Формати часу протоколу NTP.
9. Структура повідомлення протоколу NTP.
10. Безпека протоколу NTP.
11. Основні реалізації компонентів протоколу NTP у сучасних мережних ОС.
12. Реалізація протоколу NTP провідними виробниками мережного обладнання.
13. Особливості реалізації протоколу NTP на мережному обладнанні фірми Cisco.
14. Перелік та призначення основних команд для налагодження протоколу NTP на пристроях Cisco.
15. Перелік та призначення основних команд моніторингу роботи протоколу NTP на пристроях Cisco.