Лабораторна робота № 15

НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ДИНАМІЧНОГО КОНФІГУРУВАННЯ ВУЗЛІВ DHCP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи протоколу динамічного конфігурування вузлів DHCP на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи DHCP-сервера на базі маршрутизатора Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи DHCP-клієнтів різних ОС; дослідити процес роботи протоколу DHCP та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Загальні відомості про технології та протоколи логічної адресації в IP-мережах

Для забезпечення ефективного функціонування будь-якого вузла в IP-мережі його мережному адаптеру/інтерфейсу необхідно призначити такі параметри логічної адресації:

– IP-адреса адаптера/інтерфейсу;
– маска/префікс мережі (підмережі);
– IP-адреса шлюзу за замовчуванням;
– IP-адреса DNS-сервера;
– IP-адреса WINS-сервера.

Для функціонування вузла у локальній мережі, яка не має підключення до іншої мережі, достатньо призначати лише перші два параметри. Коли ж виникає потреба забезпечити міжмережний обмін між локальними мережами або підключення до глобальної мережі, необхідно встановлювати IP-адресу шлюзу за замовчуванням. У деяких випадках таких адрес може бути кілька. Для забезпечення доступу до ресурсів серверів з використанням символьних доменних імен вузлів необхідно встановлювати IP-адресу DNS-сервера. У більшості ОС передбачена можливість використання кількох IP-адрес DNS-серверів. IP-адреса WINS-сервера необхідна в ОС Windows для зіставлення NetBIOS-імен комп'ютерів з IP-адресами. Нині служба WINS майже не використовується: корпорація Microsoft оголосила її застарілою у Windows Server 2022 і вилучає з усіх випусків після

Windows Server 2025, рекомендуючи натомість засоби розрізнення імен на базі DNS.

Призначення параметрів IP-адресації може здійснюватися як статично адміністратором, так динамічно з використанням спеціальних технологій та протоколів. Статично параметри призначаються вузлам, які постійно знаходяться у мережі. Це можуть бути як кінцеві вузли (сервери, стаціонарні робочі станції, мережні принтери тощо), так і комунікаційні пристрої (комутатори, маршрутизатори, точки доступу, міжмережні екрани тощо). Динамічно параметри призначаються вузлам, які мігрують між мережами. Це можуть бути переносні робочі станції, планшети тощо.

Для статичного призначення параметрів IP-адресації використовуються як графічні засоби ОС, так і відповідні команди, що виконуються у командному рядку. Наприклад, в ОС Unix/Linux застосовується команда **ifconfig**. Серед засобів динамічного призначення у першу чергу необхідно згадати такі технології та протоколи:

– технологія автоматичного самопризначення адрес APIPA (Automatic Private IP Addressing) відома також як IPAC (Internet Protocol Automatic Configuration) для вузлів ОС Windows або Zeroconf (Zero Configuration Networking) для вузлів ОС Linux;

– протокол динамічного конфігурування вузлів DHCP (Dynamic Host Configuration Protocol);

– протокол віддаленого завантаження BOOTP (Bootstrap Protocol).

Технологія APIPA реалізована як для IP версії 4, так і для IP версії 6. У першому випадку передбачається самопризначення IP-адрес з адресного діапазону мережі 169.254.0.0/16, у другому – з адресного діапазону FE80::/10. Програмно технологія APIPA реалізована як складова DHCP-клієнта.

Протокол DHCP реалізовано за клієнт-серверною схемою. DHCP-клієнт звертається з запитами про надання адресної інформації до DHCP-сервера. DHCP-сервер обслуговує запити клієнтів, відстежує актуальність бази даних виданих і вільних адрес, контролює активність вузлів та виконує інші сервісні операції. Окрім сервера та клієнта в протоколі DHCP реалізується ще один вид вузла – агент ретрансляції, який використовується для пересилки запитів між клієнтами і серверами, що розташовані у різних IP-мережах.

Протокол DHCP визначено стандартом RFC 2131, перелік його опцій – RFC 2132, параметри агента ретрансляції (зокрема опцію 82) – RFC 3046, самопризначення адрес у IPv4 (APIPA) – RFC 3927, протокол-попередник BOOTP – RFC 951, а версію протоколу для IPv6 (DHCPv6) – RFC 8415.

Блок-схема алгоритму функціонування DHCP-клієнта сучасної ОС (з підтримкою технології APIPA) наведена на рис. 1.

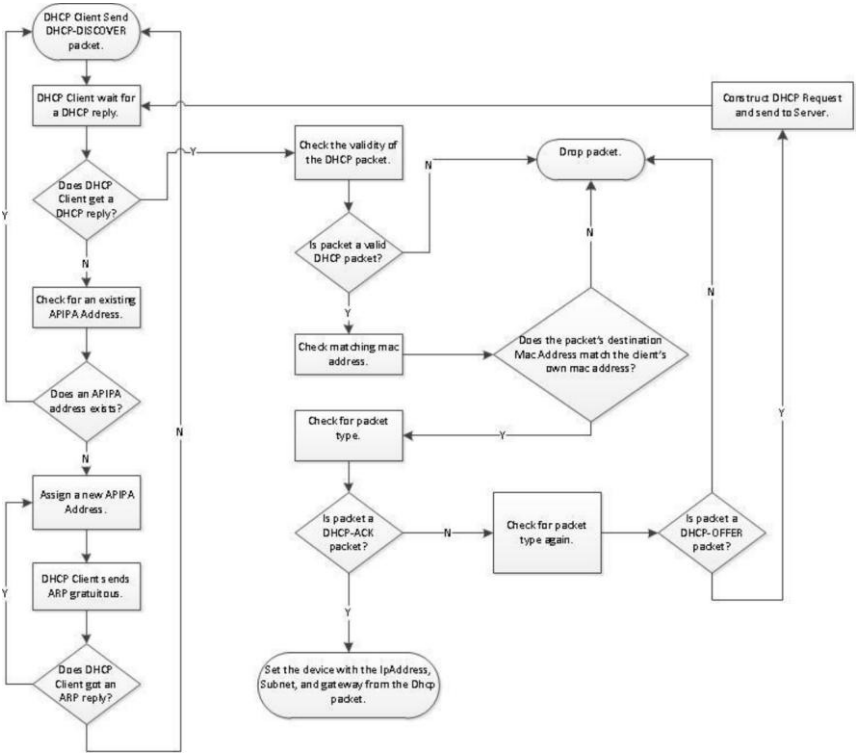


Рис. 1. Блок-схема алгоритму функціонування DHCP-клієнта

Призначення параметрів IP-адресації за допомогою засобів протоколу DHCP (надалі призначення IP-адрес) може бути виконано одним з трьох способів:

– динамічне призначення IP-адрес;

– автоматичне призначення IP-адрес;

– ручне призначення IP-адреси.

При динамічному призначенні IP-адрес DHCP-сервер видає DHCP-клієнту будь-яку вільну IP-адресу на обмежений час. При автоматичному призначенні IP-адрес DHCP-сервер спочатку видає DHCP-клієнту будь-яку вільну IP-адресу, запам'ятовує параметри клієнта (фізичну, MAC-адресу) і при наступних спробах отримання адреси цим клієнтом видає лише її. При ручному призначенні IP-адреса призначається адміністратором DHCP-клієнту по його MAC-адресі, відповідність IP-адреса-MAC-адреса зберігається у відповідній базі даних чи файлі, а DHCP-сервер використовується лише для передачі IP-адреси. Якщо MAC-адреса вузла відсутня, то IP-адреса не видається.

Кожен із способів має свої переваги і недоліки. Динамічне призначення IP-адрес з одного боку забезпечує можливість швидкого призначення параметрів IP-адресації великій кількості клієнтів, а з іншого – дає можливість вузлу зловмисника безпроблемно отримати IP-адресу, визначити всі параметри адресації мережі і на основі отриманої інформації надалі виконувати атаки на певні вузли чи групи вузлів мережі. Ручне призначення IP-адрес з одного боку вимагає володіння повною інформацією про фізичні та логічні адреси вузлів та вимагає набагато більше часу на налагодження DHCP-сервера, з іншого – забезпечує вищий рівень захисту, тобто ускладнює завдання зловмисникові.

Повідомлення протоколу DHCP

Обмін даними у протоколі DHCP здійснюється повідомленнями, які передаються за протоколом UDP: клієнт використовує порт 68, сервер – порт 67. Основний цикл отримання адреси складається з чотирьох повідомлень, які за першими літерами їх назв позначають абревіатурою DORA (рис. 2).

DHCPDISCOVER – клієнт, який ще не має IP-адреси, надсилає широкомовний запит на пошук DHCP-серверів. **DHCPOFFER** – сервер пропонує клієнтові вільну адресу та супутні параметри. **DHCPREQUEST** – клієнт широкомовно повідомляє, яку саме з отриманих пропозицій він приймає (широкомовно – щоб решта серверів звільнили свої пропозиції). **DHCPACK** – сервер підтверджує оренду; від цього моменту клієнт може користуватися адресою.

Окрім перелічених, у протоколі застосовуються повідомлення DHCPNAK (сервер відхиляє запит, наприклад, коли клієнт просить

адресу з іншої мережі), DHCPDECLINE (клієнт виявив, що запропонована адреса вже зайнята), DHCPRELEASE (клієнт достроково звільняє адресу) та DHCPINFORM (клієнт уже має адресу і потребує лише додаткових параметрів).

Оренда поновлюється повторним повідомленням DHCPREQUEST, яке клієнт надсилає безпосередньо своєму серверу після спливання половини її строку (стан RENEWING). Якщо відповіді немає, після 87,5 % строку клієнт переходить до широкомовних спроб поновлення (стан REBINDING), а після закінчення оренди припиняє користуватися адресою.



Рис. 2. Обмін повідомленнями протоколу DHCP (цикл DORA)

Елементи захисту при використанні протоколу DHCP

Протокол DHCP не передбачає взаємної автентифікації клієнта і сервера, тому у мережі можливі дві типові атаки. Перша – несанкціонований (rogue) DHCP-сервер, який відповідає на запити швидше за легітимний і видає клієнтам свою адресу як шлюз за замовчуванням, перехоплюючи увесь їхній трафік. Друга – вичерпання пулу (DHCP starvation), коли зловмисник надсилає велику кількість запитів з різними MAC-адресами, після чого легітимні клієнти не можуть отримати адресу.

Основним засобом протидії на комутаторах Cisco є механізм інспекції DHCP (DHCP snooping, рис. 3). Він вмикається командою **ip dhcp snooping** (режим глобального конфігурування) та **ip dhcp**

snooping vlan *vlan-id* для потрібних VLAN. Порти, за якими розташовані легітимні сервери або шлях до них, позначаються як довірені командою **ip dhcp snooping trust** (режим конфігурування інтерфейсу); решта портів залишаються недовіреними, і відповіді DHCP, отримані з них, відкидаються.

Комутатор при цьому веде таблицю прив'язок (DHCP snooping binding table) відповідностей «MAC-адреса – IP-адреса – порт – VLAN», яку використовують також механізми динамічної інспекції ARP (DAI) та перевірки джерела IP (IP Source Guard). Обмежити кількість запитів з одного порту дає змогу команда **ip dhcp snooping limit rate**.

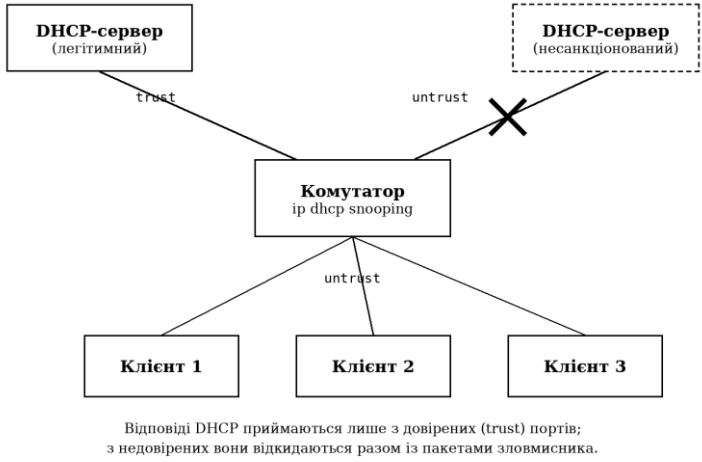


Рис. 3. Інспекція DHCP: довірені та недовірені порти

Усі сучасні мережні серверні ОС, зокрема і ОС Windows Server, мають у своєму складі реалізовані розробниками DHCP-сервери. Усі сучасні мережні клієнтські ОС мають у своєму складі DHCP-клієнти. У багатьох ОС існує можливість встановлювати DHCP-сервери сторонніх виробників. Перелік популярних реалізацій DHCP-серверів для різних ОС наведений у табл. 1.

Таблиця 1

Перелік популярних реалізацій DHCP-серверів

Назва сервера	ОС BSD	ОС Solaris	ОС Linux	ОС macOS ОС	Windows

dnsmasq	+	–	+	+	–
ISC DHCP (підтримку припинено)	+	+	+	–	–
Kea DHCP	+	+	+	+	–
udhcpd (BusyBox)	+	+	+	+	–
odhcpd (OpenWrt)	–	–	+	–	–
dhcpy6d (лише DHCPv6)	+	–	+	+	–
systemd-networkd	–	–	+	–	–
Windows Server DHCP	–	–	–	–	+

Більшість сучасних виробників маршрутизаторів (зокрема Cisco, Huawei, Juniper) реалізують підтримку функціонування як DHCP-серверів, так і DHCP-клієнтів та агентів ретрансляції на своїх пристроях.

Слід зазначити, що підтримку реалізації ISC DHCP припинено наприкінці 2022 року; її наступником є сервер Kea DHCP того самого розробника. Сервер FreeRADIUS, який інколи згадують у цьому переліку, є насамперед сервером RADIUS із допоміжними засобами DHCP, а не повноцінною реалізацією DHCP-сервера.

Порядок налагодження DHCP-сервера на базі маршрутизатора Cisco

У практиці побудови мереж маршрутизатор Cisco у більшості випадків налагоджується як DHCP-сервер, у деяких випадках – як агент ретрансляції DHCP і досить рідко – як DHCP-клієнт. Налагодження функціонування DHCP-сервера на базі маршрутизатора Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Включити функціонування DHCP-сервера на маршрутизаторі (залежно від ситуації, за замовчуванням запускається автоматично).

2. Налагодити DHCP Database Agent або відключити DHCP Conflict Logging (обов'язково).

3. Виключити IP-адреси, які не будуть призначатися DHCP-клієнтам (обов'язково).

4. Створити та налагодити набір (набори) IP-адрес, які будуть призначатися DHCP-клієнтам (обов'язково).

5. Налагодити ручне призначення IP-адрес (необов'язково).

6. Налагодити параметри завантажувального файла для даного DHCP-сервера (необов'язково).

7. Зазначити кількість перевірочних запитів протоколу ICMP (необов'язково).

8. Встановити значення тайм-ауту для перевірочних запитів протоколу ICMP (необов'язково).

При налагодженні агента ретрансляції DHCP для даного порядку додаються наступні етапи :

1. Активувати Cisco IOS DHCP-клієнта на інтерфейсах Ethernet/Fast Ethernet ... (необов'язково).

2. Налагодити параметри імпорту опцій DHCP-сервера та автоконфігурування (необов'язково).

3. Налагодити параметри опцій агента ретрансляції DHCP в повідомленнях BOOTREPLY (необов'язково).

4. Налагодити параметри політики передачі для агента ретрансляції DHCP (необов'язково).

5. Активувати додаткові можливості агента ретрансляції DHCP (необов'язково).

На практиці можливе застосування іншого порядку.

Команди налагодження DHCP-сервера на базі маршрутизатора Cisco

Включення функціонування DHCP-сервера на маршрутизаторі Cisco виконується командою **service dhcp**. Виключення — командою **no service dhcp**. За замовчуванням на маршрутизаторі Cisco DHCP-сервер є включеним. Якщо використання DHCP-сервера не планується, то з метою підвищення рівня захисту пристрою рекомендується даний функціонал відключати.

Основною командою, від якої походить більшість команд для налагодження засобів протоколу DHCP у Cisco IOS є команда **ip dhcp**. Перелік та призначення похідних команд можна отримати за допомогою інтерактивної довідки командного рядка. Слід зауважити, що для різних моделей маршрутизаторів, версій IOS та наборів властивостей, переліки можуть відрізнятися. У більшості випадків у режимі глобального конфігурування доступними є такі команди **ip**

dhcp aaa, **ip dhcp binding**, **ip dhcp bootp**, **ip dhcp class**, **ip dhcp compatibility**, **ip dhcp conflict**, **ip dhcp database**, **ip dhcp excluded-address**, **ip dhcp limit**, **ip dhcp limited-broadcast-address**, **ip dhcp ping**, **ip dhcp pool**, **ip dhcp relay**, **ip dhcp smart-relay**, **ip dhcp update**, **ip dhcp use**. У деяких випадках використовуються і інші команди. Призначення та синтаксис основних команд наведено нижче.

Створення або редагування набору (пулу) адрес, які будуть видаватися DHCP-клієнтам, виконується командою **ip dhcp pool**. Після виконання даної команди здійснюється перехід до режиму налагодження протоколу DHCP. У цьому режимі наявно більше ніж 25 команд, які стосуються різних аспектів налагодження пулу адрес протоколу DHCP.

Після переходу до режиму налагодження протоколу DHCP наступним кроком є зазначення IP-адреси та маски (префікса) мережі, адреси якої будуть призначатися DHCP-клієнтам. Для цього використовується команда **network**. Ще одним важливим кроком є зазначення IP-адреси шлюзу за замовчуванням для даної мережі. Для цього використовується команда **default-router**. Можливе використання до 8 шлюзів. На практиці достатньо одного. Наступними (необов'язковими) кроками є зазначення сервера (серверів) служб DNS, WINS, а також типу вузлів NetBIOS для WINS. Для цього виконуються відповідно команди **dns-server**, **netbios-name-server**, **netbios-node-type**. IP-адреси, що вказуються як параметри цих команд, можуть належати іншим мережам. DHCP-сервер може також видавати назву домену. Для цього використовується команда **domain-name**. Важливим параметром налагодження DHCP-маршрутизатора є час, на який виділяється IP-адреса, відомий також як час оренди адреси. Для його налагодження використовується команда **lease**.

Для вилучення з пулу IP-адрес, які не будуть призначатися, використовується команда **ip dhcp excluded-address**. Цією командою можна вилучити як одну адресу, так і певний діапазон адрес. З метою усунення конфліктів вилучення IP-адрес рекомендується виконувати перед створенням пулу.

Перед виділенням IP-адреси з пулу алгоритмом роботи DHCP-сервера передбачена попередня перевірка, чи дійсно дана адреса є вільною. Для цього DHCP-сервер двічі посилає ICMP-запит за даною адресою. Якщо відповіді на запит немає, то DHCP-сервер вважає, що

адреса є вільною і надає її клієнтові. Параметри даної перевірки (кількість запитів, інтервал між ними) можна змінити. Для цього використовуються команди **ip dhcp ping packets** та **ip dhcp ping timeout**. Для активації/деактивації журналювання конфліктів адрес використовується команда **ip dhcp conflict logging**.

Одним з режимів роботи DHCP є ручне призначення IP-адрес. У цьому випадку для кожного клієнта формується окремий пул і в цьому пулі за допомогою спеціалізованих команд проводиться налагодження призначення адреси. Для налагодження ручного призначення IP-адрес використовуються спеціальні команди **host**, **client-identifier**, **client-name**. Для зазначення IP-адреси шлюзу за замовчуванням, IP-адрес DNS-сервера та WINS-сервера використовуються вищезгадані команди **default-router**, **dns-server**, **netbios-name-server** та деякі інші.

Завантаження конфігурації для DHCP-сервера можливе з внутрішнього (Flash-пам'ять) або зовнішнього джерела (FTP, TFTP, RCP-сервери). Для цього використовуються команди **bootfile** та **ip dhcp database**.

Синтаксис команди **ip dhcp pool** (режим глобального конфігурування):

ip dhcp pool *name*,

де ***name*** – текстова назва (англійською мовою) набору IP-адрес, які будуть призначатися.

Синтаксис команди **network** (режим конфігурування протоколу DHCP):

network *network_IP-address* [*network_mask* | /*prefix-length*],

де ***network_IP-address*** – IP-адреса мережі, з якої призначаються IP-адреси вузлам;

network_mask – маска мережі для IP-адреси, що призначається, записана у звичайній формі (необов'язково, може вказуватися префікс);

prefix-length – довжина префікса для IP-адреси, що призначається (необов'язково, може вказуватися маска).

Синтаксис команди **domain-name** (режим конфігурування протоколу DHCP):

domain-name *domain_name*,

де ***domain_name*** – текстова назва домену для клієнта.

Синтаксис команди **default-router** (режим конфігурування протоколу DHCP):

default-router *IP-address* [*IP-address2 ... IP-address8*],

де ***IP-address*** – IP-адреса першого шлюзу за замовчуванням;

IP-address2 ... **–** IP-адреса наступного шлюзу за замовчуванням.

Синтаксис команд **dns-server**, **netbios-name-server** аналогічний синтаксису команди **default-router**.

Синтаксис команди **netbios-node-type** (режим конфігурування протоколу DHCP):

netbios-node-type *type*,

де ***type*** – тип вузла NetBIOS (може набувати значень **b-node**, **pnode**, **m-node**, **h-node**); рекомендоване значення **h-node**.

Синтаксис команди **lease** (режим конфігурування протоколу DHCP):

lease {*days* [*hours*][*minutes*] | infinite},

де ***days*** – кількість днів оренди;

hours – кількість годин оренди (необов'язково);

minutes – кількість хвилин оренди (необов'язково);

infinite – час оренди необмежений.

Синтаксис команди **host** (режим конфігурування протоколу DHCP):

host *IP-address* [*network_mask* | /*prefix-length*],

де ***IP-address*** – IP-адреса, яка виділяється вузлові;

network_mask – маска мережі для IP-адреси, що призначається, записана у звичайній формі (необов'язково, може вказуватися префікс);

prefix-length – довжина префікса для IP-адреси, що призначається (необов'язково, може вказуватися маска).

Синтаксис команди **client-identifier** (режим конфігурування протоколу DHCP):

client-identifier *unique-identifier*,

де ***unique-identifier*** – унікальний семибайтний ідентифікатор клієнта записаний у шістнадцятковій формі; формується як байт, що позначає середовище (для Ethernet – 01h) та фізична (MAC) адреса клієнта.

Синтаксис команди **client-name** (режим конфігурування протоколу DHCP):

client-name *client_name*,

де ***client_name*** – текстовий ідентифікатор клієнта.

Синтаксис команди **ip dhcp excluded-address** (режим глобального конфігурування):

ip dhcp excluded-address *low_IP_address* [*high_IP_address*],

де ***low_IP_address*** – початкова IP-адреса діапазону (вона вказується також у випадку, якщо вилучається одна адреса);

high_IP_address – кінцева IP-адреса діапазону.

Синтаксис команди **ip dhcp ping packets** (режим глобального конфігурування):

ip dhcp ping packets *number*,

де ***number* –** кількість перевірочних запитів, за замовчуванням – 2.

Синтаксис команди **ip dhcp ping timeout** (режим глобального конфігурування):

ip dhcp ping timeout *interval*,

де ***interval* –** час очікування відповіді на перевірочний запит; зазначається у мілісекундах; за замовчуванням – 500 мс.

Синтаксис команди **ip dhcp conflict logging** (режим глобального конфігурування):

ip dhcp conflict logging.

Команда не має параметрів.

З синтаксисом та особливостями використання решти команд можна ознайомитися у технічній документації.

Команди моніторингу, діагностики та керування процесом роботи складових протоколу DHCP на маршрутизаторі Cisco

Для моніторингу та діагностики роботи протоколу DHCP на маршрутизаторах Cisco використовуються як команди загального призначення, так і спеціалізовані команди. Серед команд загального призначення можна виділити такі команди: **show running-config**, **show startup-config**, **show interface *interface-type interface-id***. Остання команда дає змогу визначити яким чином призначена IP-адреса відповідному інтерфейсу. Перелік спеціалізованих команд є відносно невеликим і включає такі команди як: **show ip dhcp binding**, **show ip dhcp conflict**, **show ip dhcp database**, **show ip dhcp import**, **show ip dhcp pool**, **show ip dhcp relay**, **show ip dhcp server statistics**.

Важливими командами, які допомагають зрозуміти процеси передачі повідомлень протоколу є команди трасування такі як: **debug ip dhcp server class**, **debug ip dhcp server events**, **debug ip dhcp server**

linkage, **debug ip dhcp server packet**. Також важливими є команди, які дають змогу впливати на процес роботи складових протоколу такі як: **clear ip dhcp binding**, **clear ip dhcp conflict**, **clear ip dhcp pool**, **clear ip dhcp server statistics**, **clear ip dhcp subnet**.

Узагальнений перелік команд моніторингу, діагностики та керування процесом роботи складових протоколу DHCP на маршрутизаторі Cisco наведений у табл. 2.

Агент ретрансляції DHCP

Коли DHCP-сервер і клієнти перебувають у різних IP-мережах, широкомовний запит DHCPDISCOVER не проходить через маршрутизатор. У такому разі інтерфейс маршрутизатора, до якого підключені клієнти, налагоджується як агент ретрансляції: він приймає широкомовний запит, вписує у поле giaddr адресу свого інтерфейсу і пересилає повідомлення на зазначену адресу сервера як одноадресне. За значенням giaddr сервер визначає, з якого саме пулу виділити адресу, і повертає відповідь тому самому агентові, який передає її клієнтові.

Синтаксис команди **ip helper-address** (режим конфігурування інтерфейсу):

ip helper-address IP-address,

де IP-address – IP-адреса DHCP-сервера; команда може зазначатися кілька разів, якщо серверів декілька.

Зазначена адреса може належати як маршрутизатору, що виконує роль DHCP-сервера, так і окремому серверу. Окрім DHCP, агент ретрансляції за замовчуванням пересилає ще низку широкомовних службових протоколів (зокрема TFTP, DNS, NetBIOS); перелік змінюється командою ip forward-protocol udp.

Таблиця 2

Перелік команд моніторингу, діагностики та керування процесом роботи складових протоколу DHCP на маршрутизаторі Cisco

Команда	Призначення
Команди show ip dhcp	
show ip dhcp binding	Виведення інформації про видані вузлам IP-адреси
show ip dhcp conflict	Виведення інформації про конфлікти при виділенні IP-адрес
show ip dhcp database	Виведення інформації про розміщення та стан бази даних DHCP
show ip dhcp import	Виведення інформації про імпортовані параметри протоколу

show ip dhcp pool	Виведення інформації про параметри та стан використання пулів IP-адрес
show ip dhcp relay	Виведення інформації про роботу агента ретрансляції DHCP
show ip dhcp server statistics	Виведення статистичної інформації про роботу DHCP-сервера
Команди debug ip dhcp	
debug ip dhcp server class	Активувати виведення інформації, пов'язаної з класовою адресацією
debug ip dhcp server events	Активувати виведення інформації про події, пов'язані з роботою DHCP-сервера
debug ip dhcp server linkage	Активувати виведення інформації, пов'язаної з операціями з базою даних DHCP-сервера
debug ip dhcp server packet	Активувати декодування інформації з отриманих і відправлених повідомлень
Команди clear ip dhcp	
clear ip dhcp binding	Очистити інформацію про автоматичне призначення IP-адрес у базі даних протоколу DHCP
clear ip dhcp conflic	Очистити інформацію про конфлікти в базі даних DHCP
clear ip dhcp pool	Очистити пул IP-адрес
clear ip dhcp server statistics	Очистити лічильники DHCP-сервера
clear ip dhcp subnet	Очистити інформацію про підмережі

Налагодження, моніторинг та діагностика роботи DHCP-клієнтів сучасних мережних ОС

Більшість сучасних мережних клієнтських ОС мають вбудовані засоби динамічного отримання параметрів IP-адресації. В ОС Windows наявний реалізований у вигляді служби DHCP-клієнт, який дає змогу вирішувати питання призначення адрес як за допомогою технології APIPA, так і за допомогою протоколу DHCP. Окрім цього, на нього покладаються завдання по реєстрації і оновленню DNS-записів. За замовчуванням служба DHCP-клієнта ОС Windows запускається автоматично. При потребі можливе її відключення стандартними засобами.

Визначити актуальні параметри IP-адресації певного мережного адаптера чи підключення в ОС Windows можна як за допомогою засобів графічного інтерфейсу, так і з використанням командного рядка. Основним засобом в останньому випадку є команда **ipconfig**. Найбільш інформативним варіантом команди є використання з

параметром **/all** – команда **ipconfig /all**. Для керування процесом модифікації параметрів IP-адресації мережного адаптера/підключення також використовується команда **ipconfig** з відповідними параметрами: параметр **/release** призначений для вивільнення адреси, параметр **/renew** – для отримання нових параметрів IP-адресації або їх оновлення. Більш детальну інформацію про застосування команди можна отримати за допомогою довідки ОС.

Для ОС Unix/Linux реалізовано кілька програмних реалізацій DHCP-клієнтів. Для ОС, які орієнтовані на використання мінімуму обчислювальних ресурсів (наприклад, вбудованих систем), розроблено DHCP-клієнт Udhcpc (μDHCPc, Micro DHCP Client). Цей клієнт застосовується у таких відомих системах як Busybox, Linux MicroCore, Linux TinyCore. Програмно DHCP-клієнт Udhcpc реалізований у вигляді однойменної утиліти. Параметри роботи **udhcpc** зберігаються у відповідних конфігураційних файлах. Для багатьох популярних ОС Linux, наприклад, ОС Debian, розроблена стандартна утиліта **dhclient**. Запуск DHCP-клієнта у більшості випадків в ОС Linux виконується автоматично.

Визначити актуальні параметри IP-адресації певного мережного адаптера чи підключення в ОС Linux, як і в ОС Windows можна як за допомогою засобів графічного інтерфейсу (якщо він підтримується), так і з використанням командного рядка. Основним засобом в останньому випадку є команда **ifconfig**. На відміну від утиліти ОС Windows **ipconfig** ця команда не така інформативна, тому доводиться використовувати інші команди, наприклад, для виведення маршруту за замовчуванням – команду **route**. Функціональні можливості **ifconfig** теж відрізняються від **ipconfig**. За допомогою **ifconfig** неможливо керувати процесом вивільнення чи оновлення параметрів IP-адресації – для цього необхідно скористатися утилітою **dhclient** з відповідними параметрами: параметр **-r** призначений для вивільнення адреси, а повторний запуск утиліти без параметрів – для отримання нових параметрів IP-адресації або їх оновлення. Для отримання повної інформації стосовно параметрів IP-адресації для різновидів ОС Unix/Linux рекомендується використовувати технічну документацію.

Слід зазначити, що команди ifconfig та route належать до застарілого пакета net-tools, який у сучасних дистрибутивах Linux за замовчуванням не встановлюється. Їх відповідниками з пакета iproute2 є команди **ip addr** (перегляд та налагодження параметрів

адресації) і **ip route** (перегляд таблиці маршрутизації). Утиліта dhclient входить до складу ISC DHCP, підтримку якого припинено, тому в сучасних системах роль DHCP-клієнта виконують dhcpcd, вбудований клієнт NetworkManager або systemd-networkd.

Мережний пристрій Cisco (маршрутизатор, комутатор тощо) в певних випадках теж може бути DHCP-клієнтом. Найпростіший спосіб у такому разі налагодити динамічне отримання параметрів IP-адресації – на обраному інтерфейсі у режимі конфігурування інтерфейсу виконати команду **ip address dhcp**. Можливі і інші способи, особливості їх використання описані у технічній документації.

Модельний приклад налагодження функціонування DHCP-сервера на базі маршрутизатора Cisco

Розглянемо специфіку налагодження роботи протоколу DHCP для мережі, схема якої наведена на рис. 4. Параметри IP-адресації комутатора та маршрутизатора призначені статично. У даній мережі передбачається функціонування одного сервера та одного мережного принтера, параметри IP-адресації яких призначені статично та 7 робочих станцій, параметри IP-адресації яких призначаються динамічно.

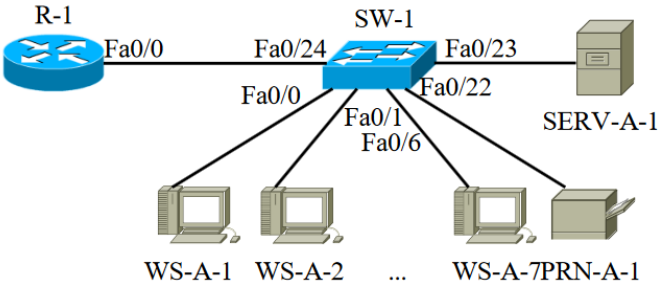


Рис. 4. Приклад мережі

При побудові даної мережі для з'єднання пристроїв використано дані табл. 3.

Таблиця 3

Параметри з'єднань пристроїв та каналів для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Комутатор SW-1	Fa0/24

Комутатор SW-1	Fa0/0	Робоча станція WS-A-1	Fa0
	Fa0/1	Робоча станція WS-A-2	Fa0
	...	...	...
	Fa0/6	Робоча станція WS-A-7	Fa0
	...	...	...
	Fa0/22	Принтер PRN-A-1	Fa0
	Fa0/23	Сервер SERV-A-1	Fa0
	Fa0/24	Маршрутизатор R-1	Fa0/0
Робоча станція WS-A-1	Fa0	Комутатор SW-1	Fa0/0
Робоча станція WS-A-2	Fa0	Комутатор SW-1	Fa0/1
...	...	...	...
Робоча станція WS-A-7	Fa0	Комутатор SW-1	Fa0/6
Принтер PRN-A-1	Fa0	Комутатор SW-1	Fa0/22
Сервер SERV-A-1	Fa0	Комутатор SW-1	Fa0/23

Загальна кількість IP-адрес, які передбачається використовувати у мережі становить 11. Зокрема, це 4 статичні IP-адреси (IP-адреси маршрутизатора, комутатора, сервера та мережного принтера) та 7 динамічних IP-адрес (IP-адреси робочих станцій). Як IP-адресу мережі оберемо адресу 195.1.1.0. З метою економного використання адресного простору для даної мережі оберемо маску 255.255.255.240. За такої маски у мережі можливе використання лише 14 IP-адрес (діапазон 195.1.1.1–195.1.1.14), що цілком задовольняє умовам прикладу.

Виконаємо узагальнений розподіл IP-адрес за використанням для DHCP-сервера. Результати розподілу наведені у табл. 4.

Таблиця 4

Узагальнений розподіл IP-адрес мережі за використанням

Вид адрес	Кіль-кість	Діапазони IP-адрес/ Окремі IP-адреси	Адреси DHCP-сервером
Підмережа A			
Динамічні IP-адреси	7	195.1.1.2–195.1.1.8	призначаються
Статичні IP-адреси	4	195.1.1.1, 195.1.1.12 – 195.1.1.14	не призначаються
Адреси, що не використовуються	3	195.1.1.9 – 195.1.1.11	

Для налагодження параметрів адресації пристроїв використано дані табл. 5.

Таблиця 5

Параметри IP-адресації мережі

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Підмережа A	–	195.1.1.0	255.255.255.240	/28
Маршрутизатор R-1	Інтерфейс Fa0/0	195.1.1.1	255.255.255.240	/28
Комутатор SW-1	Інтерфейс Vlan 1	195.1.1.14	255.255.255.240	/28
	Шлюз за замовчуванням	195.1.1.1	–	–
Сервер SERV-A-1	Мережний адаптер	195.1.1.13	255.255.255.240	/28
	Шлюз за замовчуванням	195.1.1.1	–	–
Принтер PRN-A-1	Інтерфейс	195.1.1.12	255.255.255.240	/28
	Шлюз за замовчуванням	195.1.1.1	–	–
Робоча станція WS-A-1 (Linux)	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Робоча станція WS-A-2 (Windows)	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
...	...	...		
Робоча станція WS-A-7 (...)	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			

Сценарій налагодження параметрів статичної адресації комутатора SW-1 та сценарій налагодження маршрутизатора R-1 як DHCP-сервера наведені нижче.

```
…
SW-1>enable
SW-1(config)#interface Vlan 1
SW-1(config-if)#ip address 195.1.1.14 255.255.255.240
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 195.1.1.1
SW-1(config)#ip name-server 196.1.1.10
SW-1(config)#ip domain-name my.net
SW-1(config)#no ip domain-lookup
SW-1(config)#exit
SW-1#
…
…
```

```
R-1>enable
R-1#configure terminal
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LAN_A
R-1(config-if)#ip address 195.1.1.1 255.255.255.240
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#service dhcp
R-1(config)#ip dhcp excluded-address 195.1.1.1
R-1(config)#ip dhcp excluded-address 195.1.1.9 195.1.1.14
R-1(config)#ip dhcp pool LAN_A
R-1(dhcp-config)#network 195.1.1.0 255.255.255.240
R-1(dhcp-config)#default-router 195.1.1.1
R-1(dhcp-config)#domain-name my.net
R-1(dhcp-config)#dns-server 196.1.1.10
R-1(dhcp-config)#exit
R-1(config)#exit
R-1#
…
```

Результати виконання команд моніторингу та діагностики роботи протоколу DHCP для розглянутого прикладу

З метою перегляду інформації про роботу протоколу DHCP на маршрутизаторі Cisco для розглянутого прикладу використано команди **show ip dhcp pool**, **show ip dhcp binding**, **show ip dhcp server statistics**. Результати роботи цих команд для маршрутизатора R-1 наведено відповідно на рис. 5–7.

```
R-1#show ip dhcp pool
Pool LAN_A :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 195.1.1.5            195.1.1.1        - 195.1.1.14        3
R-1#
```

Рис. 5. Результат виконання команди show ip dhcp pool на маршрутизаторі R-1

```
R-1#show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
195.1.1.2           0108.0027.7f91.0a       Nov 14 2015 9:50 AM    Automatic
195.1.1.3           0108.0027.c9c8.30       Nov 14 2015 9:51 AM    Automatic
195.1.1.4           0100.5079.6668.01       Nov 14 2015 9:56 AM    Automatic
R-1#
```

Рис. 6. Результати виконання команди show ip dhcp binding на маршрутизаторі R-1

```
R-1#show ip dhcp server statistics
Memory usage         24463
Address pools        1
Database agents      0
Automatic bindings   3
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         9
DHCPREQUEST          10
DHCPDECLINE          0
DHCPRELEASE          1
DHCPINFORM           0
Message              Sent
BOOTREPLY            0
DHCPOFFER            9
DHCPACK              3
DHCPNAK              0
R-1#
```

Рис. 7. Результат виконання команди show ip dhcp server statistics на маршрутизаторі R-1

З метою перегляду інформації про роботу протоколу DHCP на робочих станціях WS-A-1 (Linux) та WS-A-2 (Windows) відповідно використано команди **ifconfig** та **ipconfig** з необхідними параметрами. Результати їх виконання наведено на рис. 8, 9 відповідно.

```
root@WS-A-1:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:7F:91:0A
          inet addr:195.1.1.2  Bcast:195.1.1.15  Mask:255.255.255.240
          inet6 addr: fe80::a00:27ff:fe7f:910a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26368 (25.7 KiB)  TX bytes:4014 (3.9 KiB)
          Interrupt:10 Base address:0xd020
root@WS-A-1:~#
```

Рис. 8. Результат виконання команди ifconfig eth0 на робочій станції WS-A-1

```
C:\Documents and Settings\Admin>ipconfig /all
Налаштування протоколу IP для Windows
        Ім’я комп’ютера . . . . . : WS-A-2
        Основний DNS-суфікс . . . . . :
        Тип вузла . . . . . : невідомий
        IP-маршрутизацію увімкнено  . . . : ні
        WINS-проксі увімкнено . . . . . : ні
        Порядок перегляду суфіксів DNS  . : my.net
Підключення по локальній мережі – адаптер Ethernet:
        DNS-суфікс цього підключення  . . : my.net
        Опис  . . . . . : AMD PCNET Family Ethernet Adapter
(PCI)
        Фізична адреса  . . . . . : 08-00-27-C9-C8-30
        DHCP увімкнено  . . . . . : так
        Автоналаштування увімкнено  . . . : так
        IP-адреса . . . . . : 195.1.1.3
        Маска підмережі . . . . . : 255.255.255.240
        Основний шлюз . . . . . : 195.1.1.1
        DHCP-сервер . . . . . : 195.1.1.1
        DNS-сервери . . . . . : 196.1.1.10
        Оренду отримано . . . . . : 14 листопада 2015 р. 9:50:46
        Оренда спливає  . . . . . : 15 листопада 2015 р. 9:50:46
C:\Documents and Settings\Admin>
```

Рис. 9. Результат виконання команди ipconfig /all на робочій станції WS-A-2

Для дослідження поведінки DHCP-сервера при виявлені конфліктів змодельовано ситуацію, коли одній із робочих станцій (WS_C) параметри IP-адресації призначено статично. Сервером виявлено конфлікт адрес та виведено системне повідомлення-попередження. Для виведення детальної інформації про конфлікт використано команду **show ip dhcp conflict**. Результат виконання даної команди наведено на рис. 10.

```
R-1#show ip dhcp conflict
IP address        Detection method   Detection time          VRF
195.1.1.2         Ping               Nov 14 2015 10:50 AM
R-1#
```

Рис. 10. Результат виконання команди show ip dhcp conflict на маршрутизаторі R-1

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 11). При побудові звернути увагу на вибір моделей мережних пристроїв, мережних модулів та адаптерів, а також мережних з'єднань. Різновиди технологій Ethernet для підмереж A, B, C обираються довільно. Кожну з підключених локальних мереж A та B показати за допомогою комутаторів та точок доступу. Для вибору кількості серверів, комутаторів, точок доступу скористатися даними табл. 6. Один із серверів мережі A виконує роль виділеного DHCP-сервера для мережі B (рис. 11). Кількість підключених робочих станцій та мережних принтерів для кожної мережі – довільна, але не менше 2-х пристроїв одного типу на один комутатор або одну точку доступу. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 3.

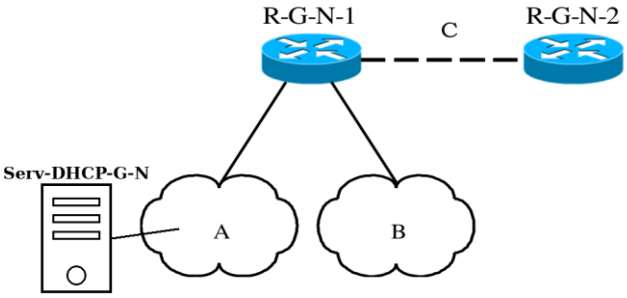


Рис. 11. Проект мережі

2. Розробити узагальнену схему адресації пристроїв мережі. Для цього скористатися даними табл. 6, 7. При виконанні розрахунків звернути увагу на те, що динамічне призначення параметрів IP-адресації буде застосовуватися на робочих станціях мереж A та B та інтерфейсі маршрутизатора R-G-N-2, через яких здійснено підключення до маршрутизатора R-G-N-1. На всіх інтерфейсах маршрутизатора R-G-N-1, комутаторах, точках доступу, серверах та мережних принтерах параметри IP-адресації зазначаються статично. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

3. З урахуванням даних п. 2. провести розподіл IP-адрес. Дані розподілу навести у вигляді таблиці, яка аналогічна табл. 5.

Таблиця 6

Кількість пристроїв для побудови мережі

№ варіанта	Мережа А – Кількість					Мережа В – Кількість				
	Робочих станцій	Серверів	Мережних принтерів	Комутаторів	Точок доступу	Робочих станцій	Серверів	Мережних принтерів	Комутаторів	Точок доступу
1	50	3	5	2	1	40	2	4	2	2
2	65	3	6	2	2	20	1	3	2	1
3	13	2	2	3	1	50	2	5	3	2
4	122	2	8	3	2	22	1	2	3	1
5	50	2	5	2	1	40	2	4	3	2
6	240	5	12	2	2	30	5	3	3	1
7	140	3	10	3	1	20	2	2	2	2
8	220	4	15	3	2	58	3	5	2	1
9	144	3	13	2	0	140	4	14	2	3
10	20	2	2	2	3	120	3	12	2	0
11	51	3	3	3	0	80	3	8	3	3
12	192	4	18	3	3	14	1	2	3	0
13	232	5	16	2	0	80	3	10	2	2
14	100	3	10	2	0	50	2	10	2	1
15	200	4	20	2	2	100	4	15	2	0
16	26	1	4	2	1	14	1	2	2	0
17	24	3	6	3	1	30	2	5	3	2
18	28	2	8	3	2	62	3	6	3	1
19	62	2	8	2	0	126	3	13	2	3
20	126	3	15	2	3	255	5	25	2	0
21	50	2	5	2	0	70	2	7	2	2
22	140	5	12	2	0	28	1	3	2	1
23	200	5	28	2	1	50	2	5	2	2
24	50	1	5	2	2	100	2	12	2	1
25	40	2	4	2	1	80	3	10	3	2
26	90	3	9	2	2	110	3	11	3	1
27	120	5	12	2	0	240	4	28	2	3
28	50	2	5	2	3	120	2	10	2	0
29	240	3	24	3	1	150	3	15	3	2
30	42	2	4	3	2	24	2	3	3	1
31	50	3	5	2	1	22	1	2	3	1
32	65	3	6	2	2	40	2	4	3	2
33	13	2	2	3	1	30	5	3	3	1

Таблиця 7

IP-адреси підмереж та параметри налагодження DHCP-пулів

№ з/п	IP-адреси мереж			Інтервал перевірки		Час оренди		
	Мережа A	Мережа B	Мережа C	К-ть спроб	Таймаут, мс	Дні	Години	Хвилини
1	191.G.N.0	192.G.N.0	193.G.N.N/30	3	350	0	6	30
2	192.G.N.0	193.G.N.0	194.G.N.N/30	4	450	0	8	30
3	193.G.N.0	194.G.N.0	195.G.N.N/30	5	550	0	10	30
4	194.G.N.0	195.G.N.0	196.G.N.N/30	5	550	0	12	30
5	195.G.N.0	196.G.N.0	197.G.N.N/30	4	450	0	14	30
6	196.G.N.0	197.G.N.0	198.G.N.N/30	3	600	0	16	30
7	197.G.N.0	198.G.N.0	199.G.N.N/30	3	600	0	6	30
8	198.G.N.0	199.G.N.0	200.G.N.N/30	5	550	0	12	30
9	199.G.N.0	200.G.N.0	201.G.N.N/30	4	450	0	16	30
10	200.G.N.0	201.G.N.0	202.G.N.N/30	4	450	0	18	30
11	201.G.N.0	202.G.N.0	203.G.N.N/30	5	550	1	4	0
12	202.G.N.0	203.G.N.0	204.G.N.N/30	3	350	1	8	0
13	203.G.N.0	204.G.N.0	205.G.N.N/30	3	350	1	12	0
14	204.G.N.0	205.G.N.0	206.G.N.N/30	3	600	1	16	0
15	205.G.N.0	206.G.N.0	207.G.N.N/30	4	600	1	20	0
16	206.G.N.0	207.G.N.0	208.G.N.N/30	4	700	1	20	30
17	207.G.N.0	208.G.N.0	209.G.N.N/30	5	700	1	16	30
18	208.G.N.0	209.G.N.0	210.G.N.N/30	5	450	1	12	30
19	209.G.N.0	210.G.N.0	211.G.N.N/30	5	350	1	8	30
20	210.G.N.0	211.G.N.0	212.G.N.N/30	5	550	1	4	30
21	211.G.N.0	212.G.N.0	213.G.N.N/30	4	450	0	4	0
22	212.G.N.0	213.G.N.0	214.G.N.N/30	4	350	0	8	0
23	213.G.N.0	214.G.N.0	215.G.N.N/30	3	600	0	12	0
24	214.G.N.0	215.G.N.0	216.G.N.N/30	3	650	0	16	0
25	215.G.N.0	216.G.N.0	217.G.N.N/30	3	250	0	20	0
26	216.G.N.0	217.G.N.0	218.G.N.N/30	4	350	0	20	0
27	217.G.N.0	218.G.N.0	219.G.N.N/30	4	450	0	16	0
28	218.G.N.0	219.G.N.0	220.G.N.N/30	3	350	0	12	0
29	219.G.N.0	220.G.N.0	221.G.N.N/30	5	550	0	8	0
30	220.G.N.0	221.G.N.0	222.G.N.N/30	5	600	0	4	0
31	221.G.N.0	222.G.N.0	223.G.N.0/30	3	350	0	6	30
32	222.G.N.0	223.G.N.0	191.G.N.0/30	4	450	0	8	30
33	223.G.N.0	191.G.N.0	192.G.N.0/30	5	550	0	10	30

4. Провести базове налагодження пристроїв, інтерфейсів та каналів зв’язку побудованої мережі. При налагодженні пристроїв

безпровідних сегментів локальної мережі А використовувати унікальні ідентифікатори (SSID) вигляду SSID-A-G-N-X, локальної мережі В – вигляду SSID-B-G-N-X. Для пристроїв мережі, що використовують статичне призначення, виконати налагодження параметрів IP-адресації відповідно до даних, які отримані у п. 2, 3. Перевірити наявність зв'язку між сусідніми парами пристроїв.

5. Провести налагодження функціонування DHCP-сервера на маршрутизаторі R-G-N-1 для мережі А та для каналу до маршрутизатора R-G-N-2 з урахуванням даних розрахунку п. 2, 3 та даних табл. 7. Налагодження перевірочного інтервалу та часу оренди виконати за можливості (якщо відповідні команди підтримуються симулятором/емулятором).

6. Для мережі В налагодити окремий (виділений) DHCP-сервер на базі пристрою Server, розміщеного у мережі А (рис. 11). Налагодити на ньому пул адрес мережі В з відповідними шлюзом за замовчуванням та адресою DNS-сервера. Оскільки сервер і клієнти мережі В перебувають у різних IP-мережах, на інтерфейсі маршрутизатора R-G-N-1, до якого підключено мережу В, налагодити агент ретрансляції командою ip helper-address із зазначенням адреси цього сервера.

7. Провести налагодження функціонування маршрутизатора R-G-N-2 та робочих станцій як DHCP-клієнтів.

8. Дослідити особливості отримання службової та діагностичної інформації протоколу DHCP за допомогою відповідних команд.

9. Дослідити процеси передачі даних між DHCP-клієнтами та DHCP-сервером. У разі появи конфліктів визначити та усунути їх джерела.

Контрольні питання

1. Наведіть перелік параметрів IP-адресації вузла.

2. Технології та протоколи динамічного призначення параметрів IP-адресації.

3. Технологія APIPA.

4. Загальна характеристика протоколу DHCP.

5. Ролі пристроїв у протоколі DHCP.

6. Наведіть характеристики протоколу DHCP стосовно моделі OSI та стеку TCP/IP.

7. Наведіть основні параметри адресації, які надаються мережному вузлу за протоколом DHCP.

8. Наведіть перелік та призначення способів призначення параметрів IP-адресації у протоколі DHCP.

9. Наведіть перелік та призначення основних повідомлень протоколу DHCP.

10. Які механізми (елементи) захисту мережі може надати протокол DHCP?

11. Наведіть перелік та призначення основних команд для налагодження DHCP-сервера на маршрутизаторі Cisco при умові динамічного призначення адрес.

12. Наведіть перелік та призначення основних команд для налагодження DHCP-сервера на маршрутизаторі Cisco при умові статичного призначення адрес.

13. Наведіть перелік та призначення основних команд моніторингу роботи протоколу DHCP на маршрутизаторі Cisco.

14. Застосування протоколу DHCP у сучасних мережних ОС.

15. Діагностика та керування процесом роботи DHCP-клієнта в ОС Windows та ОС Unix/Linux.