Тема11. Створення невеликої мережі

Мета розділу: Реалізація схеми для невеликої мережі, що включає маршрутизатор, комутатор і кінцеві пристрої.

Заголовок таблиці	
Назва теми	**Мета вивчення теми**
11.1 **Пристрої у невеликій мережі**	Визначити пристрої, які використовуються в невеликій мережі.
Застосунки та протоколи невеликої мережі	Визначити протоколи і застосунки, які використовуються в невеликій мережі.
Масштабування до більших мереж	Пояснити, як невелика мережа створює основу для більших мереж.
Перевірка з'єднання	Використання результатів команд ping і tracert для перевірки з'єднання та встановлення відповідної працездатності мережі.
Команди вузла та IOS	Використання команд вузла та IOS для отримання інформації про пристрої в мережі.
Методи пошуку та усунення несправностей	Описати традиційні методи виявлення і усунення несправностей у мережі.
Сценарії пошуку та усунення несправностей	Усунення несправностей пристроїв у мережі.

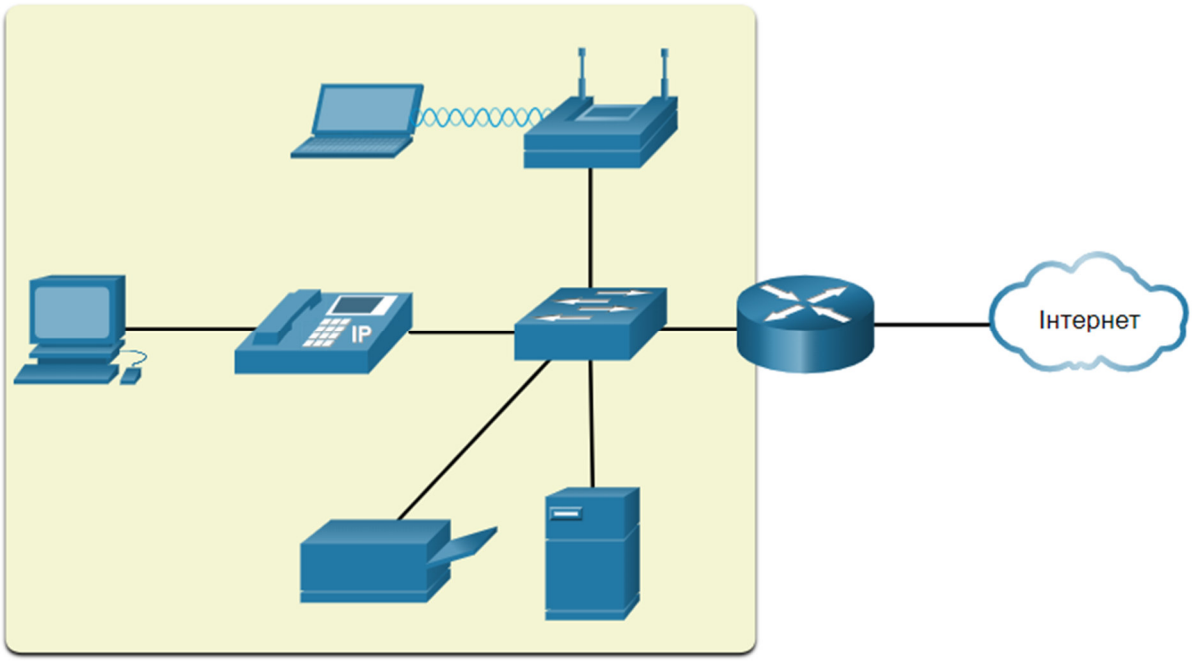
11.1. Пристрої у невеликій мережі

11.1.1. **Топології невеликої мережі**

Більшість підприємств невеликі, тому не дивно, що й більшість бізнес мереж також невеликі.

Архітектура невеликої мережі зазвичай проста. Кількість і тип під'єднаних пристроїв значно скорочується в порівнянні з більшою мережею.

Для прикладу розглянемо приклад мережі малого бізнесу, який показано на рисунку.



Ця невелика мережа потребує маршрутизатора, комутатора та точки бездротового доступу для з'єднання користувачів і WI-FI-користувачів, IP-телефону, принтера та сервера. Невеликі мережі зазвичай мають одне під'єднання WAN, що забезпечується DSL, кабелем або Ethernet з'єднанням.

Великі мережі потребують IT-відділу для підтримки, захисту та усунення несправностей мережних пристроїв і захисту організаційних даних. Керування невеликою мережею вимагає багатьох тих же навичок, що і ті, які необхідні для керування великою. Невеликими мережами керує місцевий IT-технік або нештатний фахівець (за контрактом).

11.1.2 **Вибір пристроїв для невеликої мережі**

Як і великі мережі, невеликі мережі вимагають планування та проектування, щоб відповідати вимогам користувачів. Планування забезпечує, що всі вимоги, фактори витрат та варіанти розгортання будуть належним чином враховані.

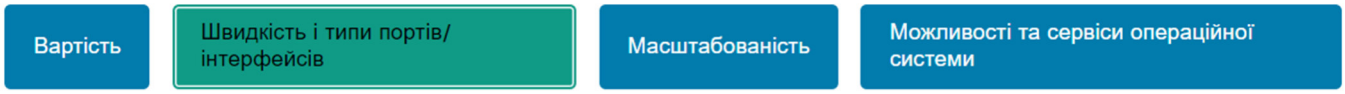
Одним з перших архітектурних рішень є тип проміжних пристроїв, які використовуватимуться для підтримки мережі.

Натисніть кожну кнопку для отримання додаткової інформації про фактори, які необхідно враховувати при виборі мережних пристроїв.

Вартість | Швидкість і типи портів/ інтерфейсів | Масштабованість | Можливості та сервіси операційної системи

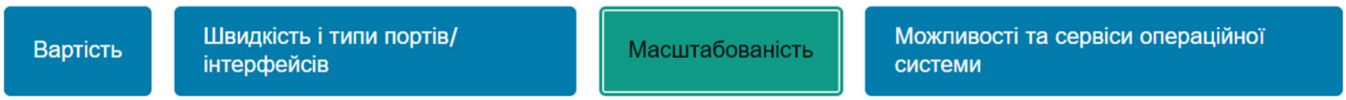
Вартість

Вартість комутатора або маршрутизатора визначається його потужністю і особливостями. Це включає в себе кількість і типи доступних портів і продуктивність внутрішньої шини. Іншими факторами, які впливають на вартість, є можливості керування мережею, вбудовані технології безпеки та додаткові передові технології комутації. Також необхідно враховувати витрати кабельних трас, необхідних для під'єднання кожного пристрою в мережі. Ще одним ключовим елементом, що впливає на витрати, є обсяг резервування, яким повинна володіти мережа.



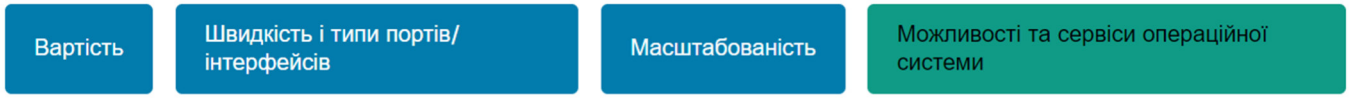
Швидкість і типи портів/інтерфейсів

Вибір кількості і типу портів на маршрутизаторі або комутаторі - критичне рішення. Новіші комп'ютери мають вбудовані NIC з пропускною здатністю 1 Гбіт/с. Деякі сервери можуть навіть мати порти з пропускною здатністю 10 Гбіт/с. Вибір пристроїв рівня 2, які можуть забезпечити збільшення швидкості, дозволяє мережі розвиватися без заміни центральних пристроїв.



Масштабованість

Мережні пристрої випускаються в фіксованій та модульній конфігурації. Фіксовані конфігурації мають певний тип і кількість портів або інтерфейсів. Модульні пристрої мають слоти розширення, які забезпечують гнучкість додавання нових модулів у міру необхідності. Комутатори поставляються з додатковими портами для високошвидкісних аплінків. Маршрутизатори можуть використовуватися для під'єднання різних типів мереж. Необхідно подбати про вибір відповідних модулів і інтерфейсів для конкретного носія.



Можливості та сервіси операційної системи

Мережні пристрої повинні мати операційні системи, які можуть виконувати вимоги організації, такі як:

- Комутація 3 рівня
- Технологія трансляції мережних адрес (NAT, Network Address Translation)
- Протокол динамічної конфігурації вузла (DHCP, Dynamic Host Configuration Protocol)
- Безпека
- Якість обслуговування (QoS)
- IP-телефонія (VoIP)

11.1.3 IP-адресація для невеликої мережі

При реалізації мережі створіть схему IP-адресації і використайте її. Усі вузли та пристрої в мережі Інтернет повинні мати унікальну адресу.

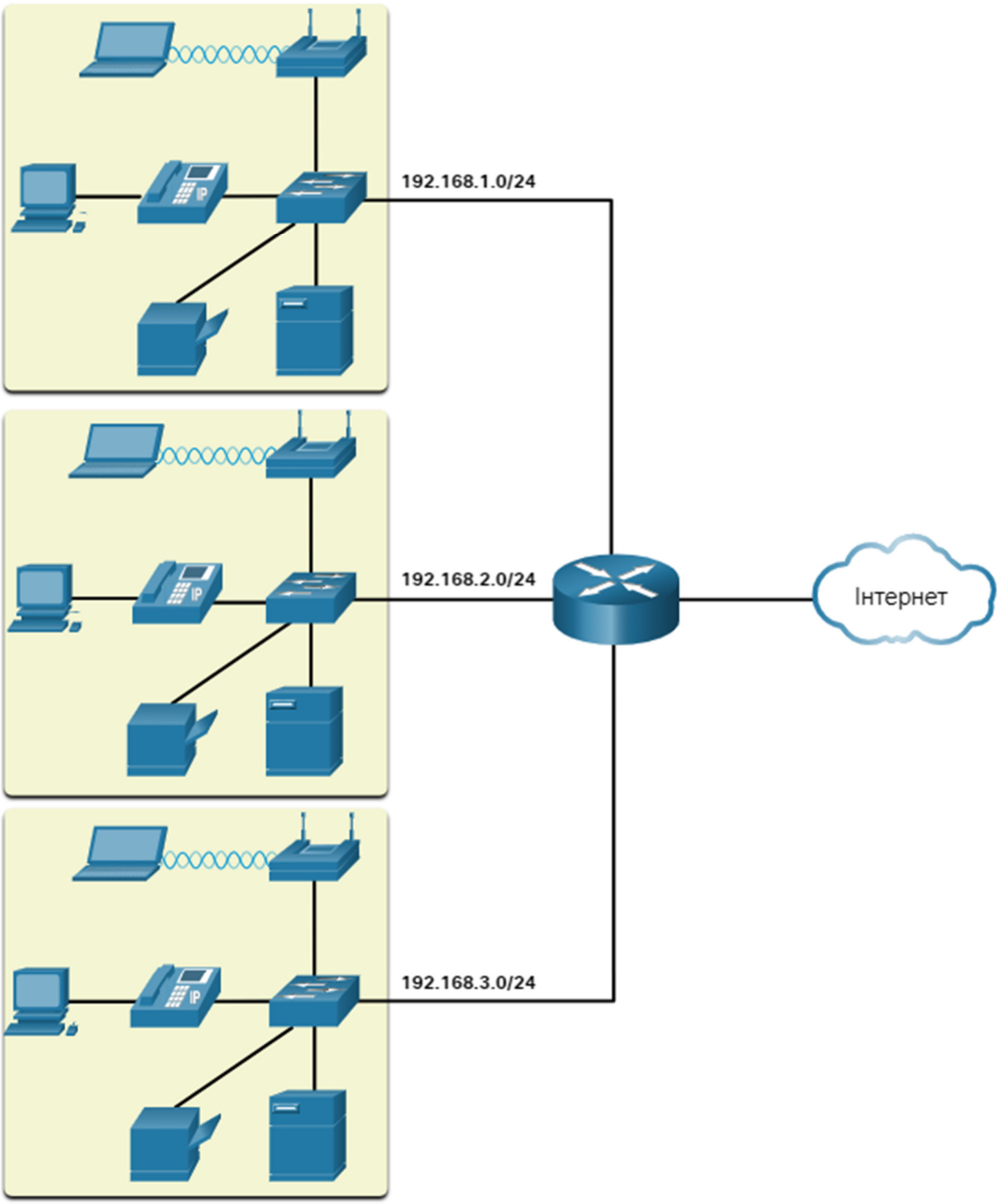
Пристрої, які будуть враховувати схему IP-адресації, включають наступне:

- Пристрої кінцевих користувачів - їх кількість і тип з'єднання (тобто дротове, бездротове, віддалений доступ)
- Сервери та периферійні пристрої (наприклад, принтери та камери безпеки)
- Проміжні пристрої, включаючи комутатори та точки доступу

Рекомендується планувати, документувати та підтримувати схему IP-адресації залежно від типу пристрою. Використання запланованої схеми IP-адресації полегшує виявлення типу пристрою і

усунення несправностей, як наприклад, при усуненні несправностей мережного трафіку за допомогою аналізатора протоколів.

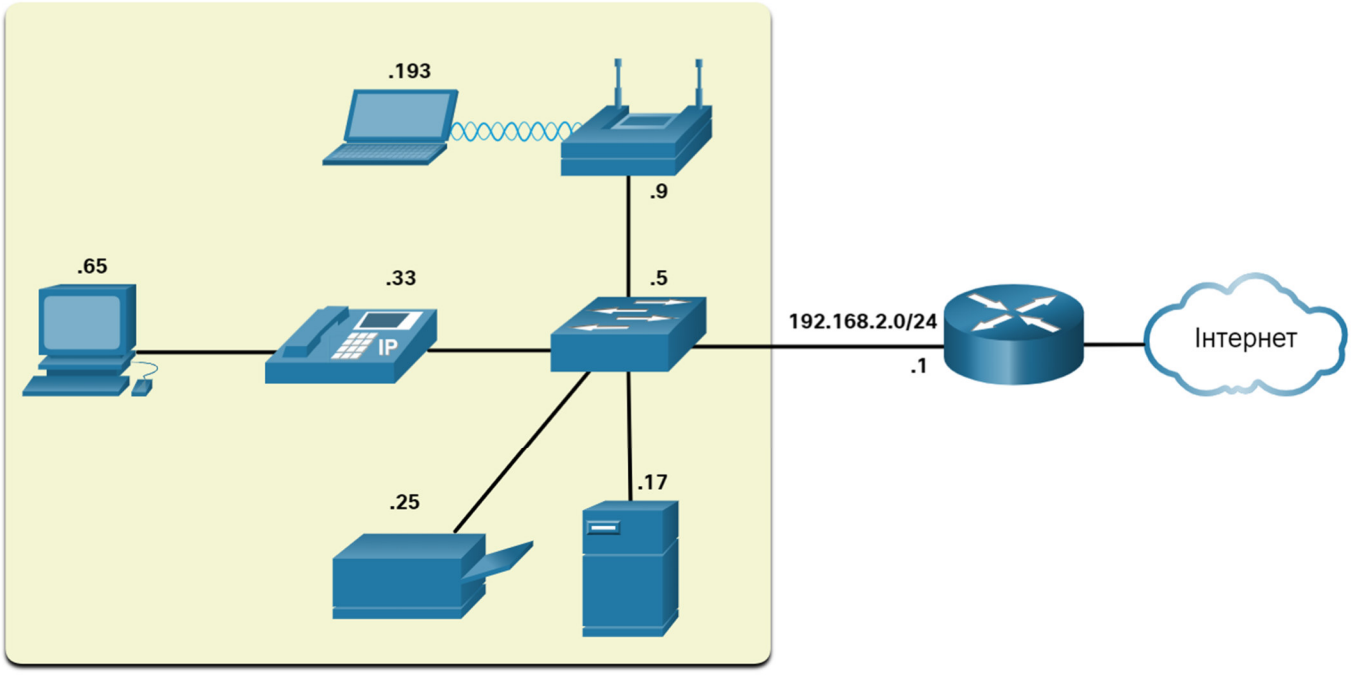
Наприклад, зверніться до топології організації малого та середнього розміру на рисунку.



Організації потрібно три LAN для користувачів (тобто 192.168.1.0/24, 192.168.2.0/24 і 192.168.3.0/24). Організація вирішила реалізувати послідовну схему IP-адресації для кожної локальної мережі 192.168.x.0/24, використовуючи наступний план:

Тип пристрою	Призначений діапазон IP-адрес	Підсумовано як.....
Основний шлюз (Маршрутизатор)	192.168.x.**1** - 192.168.x.**2**	192.168.x.**0/30**
Комутатори (макс. 2)	192.168.x.**5** - 192.168.x.**6**	192.168.x.**4/30**
Точки доступу (макс. 6)	192.168.x.**9** - 192.168.x.**14**	192.168.x.**8/29**
Сервери (макс. 6)	192.168.x.**17** - 192.168.x.**22**	192.168.x.**16/29**
Принтери (макс. 6)	192.168.x.**25** - 192.168.x.**30**	192.168.x.**24/29**
IP-телефони (макс. 6)	192.168.x.**33** - 192.168.x.**38**	192.168.x.**32/29**
Дротові пристрої (макс. 62)	192.168.x.**65** - 192.168.x.**126**	192.168.x.**64/26**
Бездротові пристрої (макс. 62)	192.168.x.**193** - 192.168.x.**254**	192.168.x.**192/26**

На рисунку показано приклад мережних пристроїв 192.168.2.0/24 з призначеними IP-адресами за заздалегідь визначеною схемою IP-адресації.



Наприклад, IP-адреса шлюзу за замовчуванням 192.168.2.1/24, комутатора 192.168.2.5/24, сервера 192.168.2.17/24 і т.д..

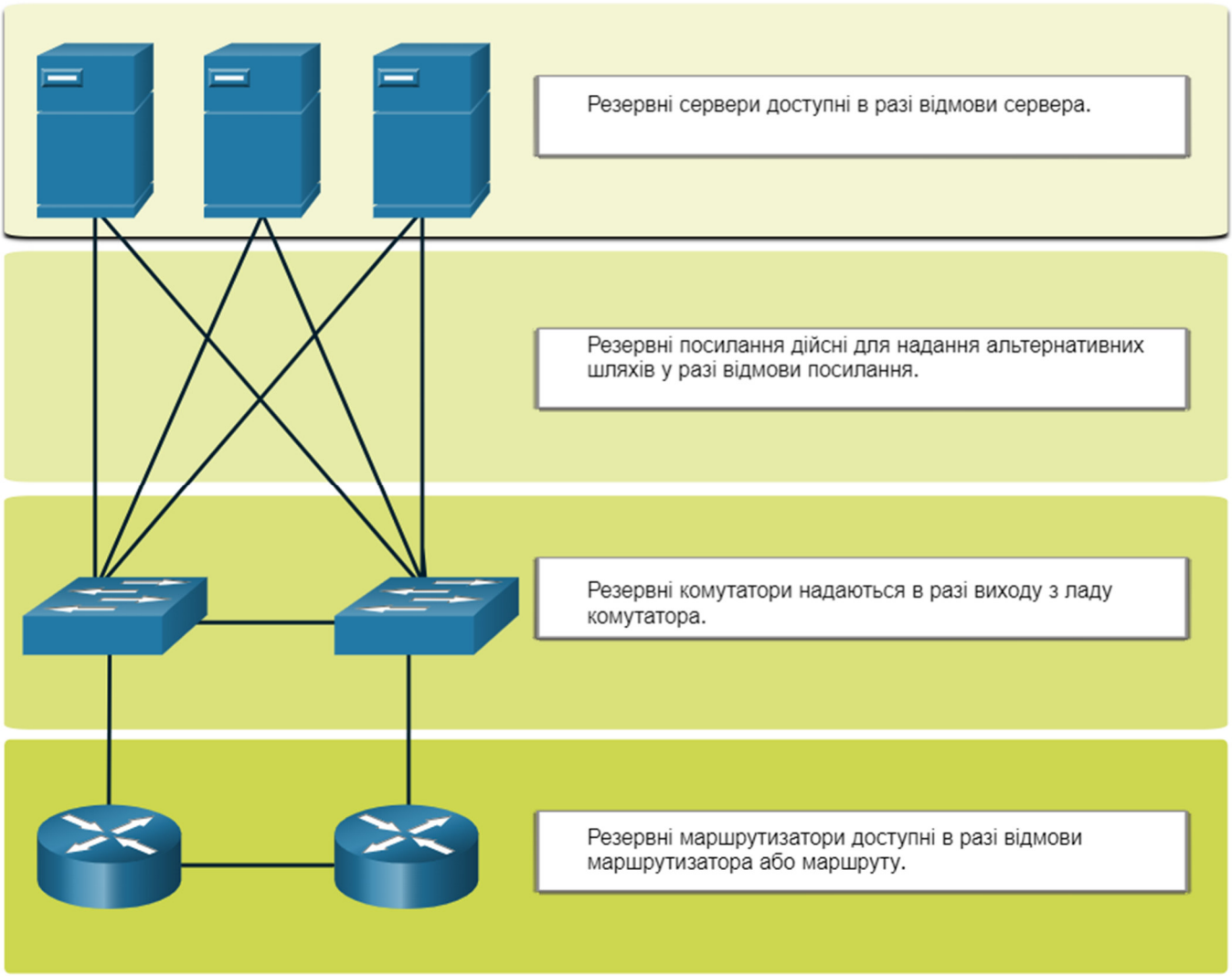
Зауважте, що діапазони IP-адрес, що присвоюються, були навмисно розподілені за межами підмереж, щоб спростити підсумовування типу групи. Наприклад, припустимо, що в мережу додано ще один комутатор з IP-адресою 192.168.2.6. Щоб ідентифікувати всі комутатори в мережній політиці, адміністратор може вказати узагальнену мережну адресу 192.168.x.4 / 30.

11.1.4 **Резервування в невеликій мережі**

Ще однією важливою частиною проектування мережі є надійність. Навіть малі підприємства занадто сильно покладаються на свою мережу для ведення бізнесу. А вихід з ладу мережі може виявитися дуже витратним.

Для того, щоб підтримувати високий ступінь надійності, в проектуванні мережі необхідне резервування. Резервування допомагає усунути окремі точки відмови.

Існує багато способів виконання резервування в мережі. Резервування може здійснюватися шляхом встановлення дублювального обладнання, але це також можна вирішити шляхом надання повторюваних мережних зв'язків для критичних областей, як показано на рисунку.

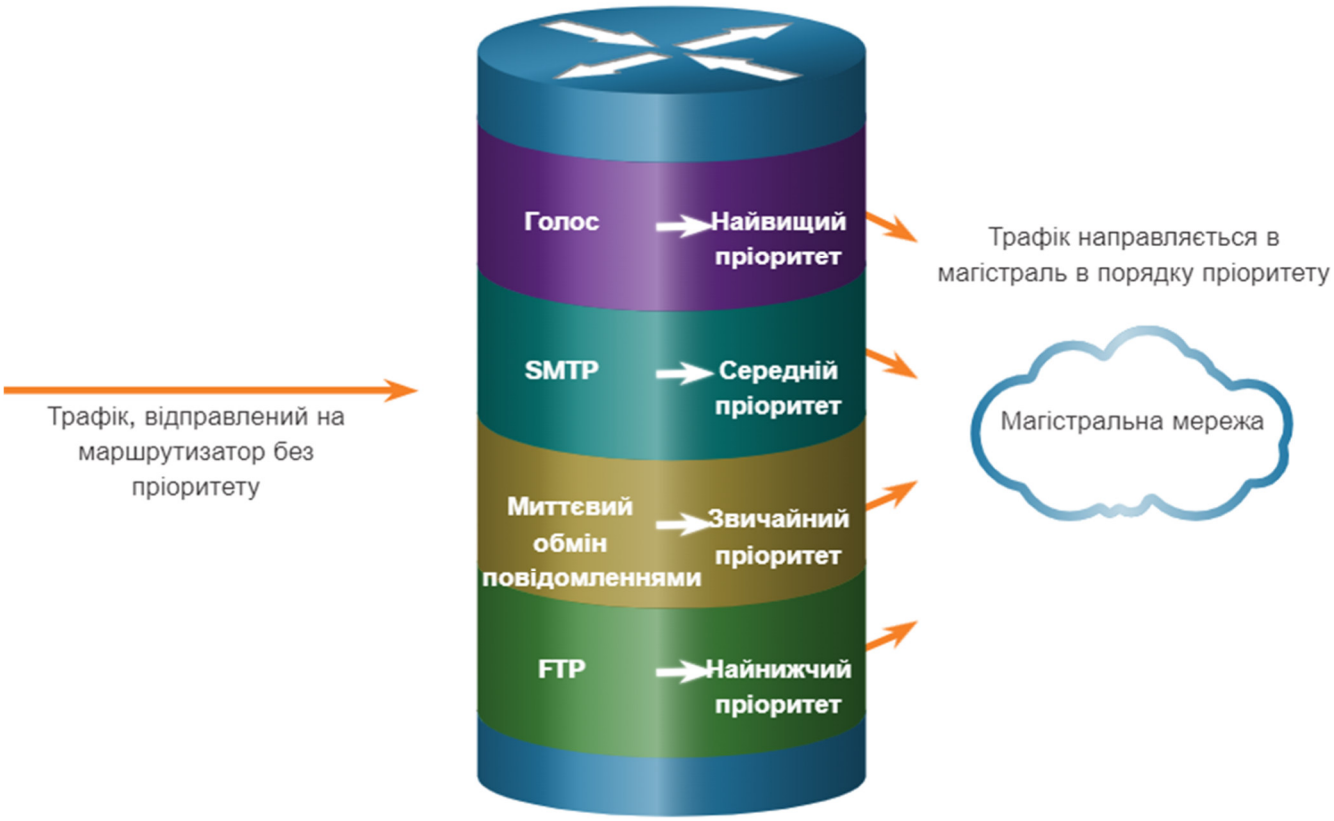


Невеликі мережі зазвичай забезпечують єдину точку виходу в Інтернет через один або кілька шлюзів за замовчуванням. Якщо маршрутизатор вийшов з ладу, вся мережа втрачає під'єднання до Інтернету. З цієї причини для малого бізнесу може бути доцільним сплатити за другого постачальника послуг в якості резервного.

11.1.5 **Керування трафіком**

Метою проектування мережі, навіть невеликої, є підвищення продуктивності співробітників і мінімізація простоїв мережі. Адміністратор мережі повинен враховувати різні типи трафіку і їх обробку в архітектурі мережі.

Маршрутизатори та комутатори в невеликій мережі повинні бути налаштовані на підтримку трафіку в режимі реального часу, наприклад голосового та відео, відповідно до іншого трафіку даних. Насправді, вдалий дизайн мережі дозволить реалізувати якість обслуговування (QoS), щоб ретельно класифікувати трафік за пріоритетом, як показано на рисунку.



Пріоритетна черга включає в себе чотири види. Черга з високим пріоритетом завжди порожніє першою.

11.1.6 **Питання для самоперевірки - Пристрої в невеликій мережі**

1. Яке твердження коректно описує невелику мережу?

- ◯ Невеликі мережі складні.
- ◯ Для невеликих мереж потрібен IT-відділ для обслуговування.
- ◯ Більшість підприємств невеликі.

2. Який фактор необхідно враховувати при виборі мережних пристроїв?

- ◯ колір
- ◯ консольні під'єднання
- ◯ вартість
- ◯ гнучкість

3. Що необхідно спланувати і використовувати при реалізації мережі?

- ◯ назви пристроїв
- ◯ схему IP-адресації
- ◯ схему адресації MAC
- ◯ розташування принтера

4. Що потрібно для підтримки високого ступеня надійності та усунення одиничних точок відмови?

- ◯ Доступність (accessibility)
- ◯ масштабованість
- ◯ цілісність
- ◯ надмірність

5. Що необхідно для класифікації трафіку за пріоритетом?

- ◯ схема IP-адресації
- ◯ якість обслуговування (QoS)
- ◯ маршрутизація
- ◯ комутація

1. Яке твердження коректно описує невелику мережу?

- ◯ Невеликі мережі складні.
- ◯ Для невеликих мереж потрібен IT-відділ для обслуговування.
- ◉ Більшість підприємств невеликі.

2. Який фактор необхідно враховувати при виборі мережних пристроїв?

- ◯ колір
- ◯ консольні під'єднання
- ◉ вартість
- ◯ гнучкість

3. Що необхідно спланувати і використовувати при реалізації мережі?

- ◯ назви пристроїв
- ◉ схему IP-адресації
- ◯ схему адресації MAC
- ◯ розташування принтера

4. Що потрібно для підтримки високого ступеня надійності та усунення одиничних точок відмови?

- ◯ Доступність (accessibility)
- ◯ масштабованість
- ◯ цілісність
- ◉ надмірність

5. Що необхідно для класифікації трафіку за пріоритетом?

- ◯ схема IP-адресації
- ◉ якість обслуговування (QoS)
- ◯ маршрутизація
- ◯ комутація

11.2 Застосунки та протоколи невеликої мережі

11.2.1 **Загальні застосунки**

У попередній темі обговорювалися компоненти невеликої мережі, а також деякі міркування щодо проектування. Ці міркування необхідні, коли ви лише налаштовуєте мережу. Після того, як ви налаштували мережу, їй все ще необхідні певні типи застосунків і протоколів для роботи.

Мережа корисна настільки, наскільки корисні використовувані в ній застосунки. Існує дві форми програм або процесів, що забезпечують доступ в мережу: мережні застосунки і сервіси прикладного рівня.

Мережні застосунки

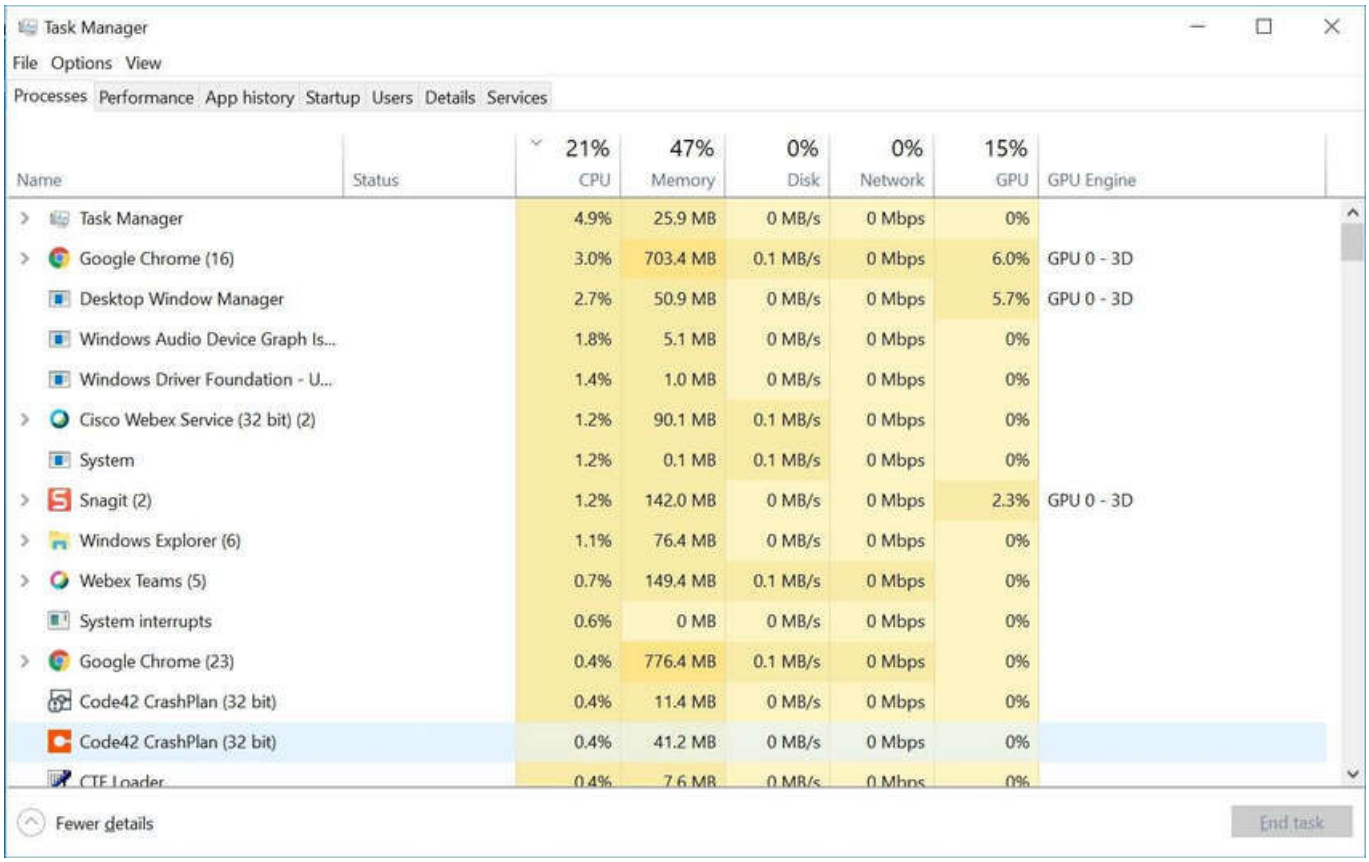
Застосунки - це програмне забезпечення, яке використовується для спілкування по мережі. Деякі застосунки кінцевих користувачів реалізують протоколи прикладного рівня та мають можливість безпосередньо встановлювати зв'язок з нижніми рівнями стеку протоколів. Поштові клієнти та веб-браузери є прикладами цього типу застосунків.

Застосунки прикладного рівня

Інші програми можуть потребувати допомоги сервісів прикладного рівня для використання мережних ресурсів, таких як передача файлів і тимчасове зберігання даних мережного друку. Прозорі для співробітника, ці сервіси є програмами, які взаємодіють з мережею і готують дані до передачі. Різні типи даних, будь то текстові, графічні чи відео, вимагають різних мережних служб, щоб забезпечити їх належну підготовку до обробки функціями, що виникають на нижніх рівнях моделі OSI.

Кожна програма або мережна служба використовує протоколи, які визначають стандарти та формати даних, які будуть використовуватися. Без протоколів мережа передачі даних не мала б спільного способу форматування і направлення даних. Для того, щоб розібратися в функціях різних мережних служб, необхідно ознайомитися з базовими протоколами, які регулюють їх роботу.

Використовуйте диспетчер завдань для перегляду поточних програм, процесів та служб, що працюють на ПК з Windows, як показано на рисунку.



11.2.2 **Загальні протоколи**

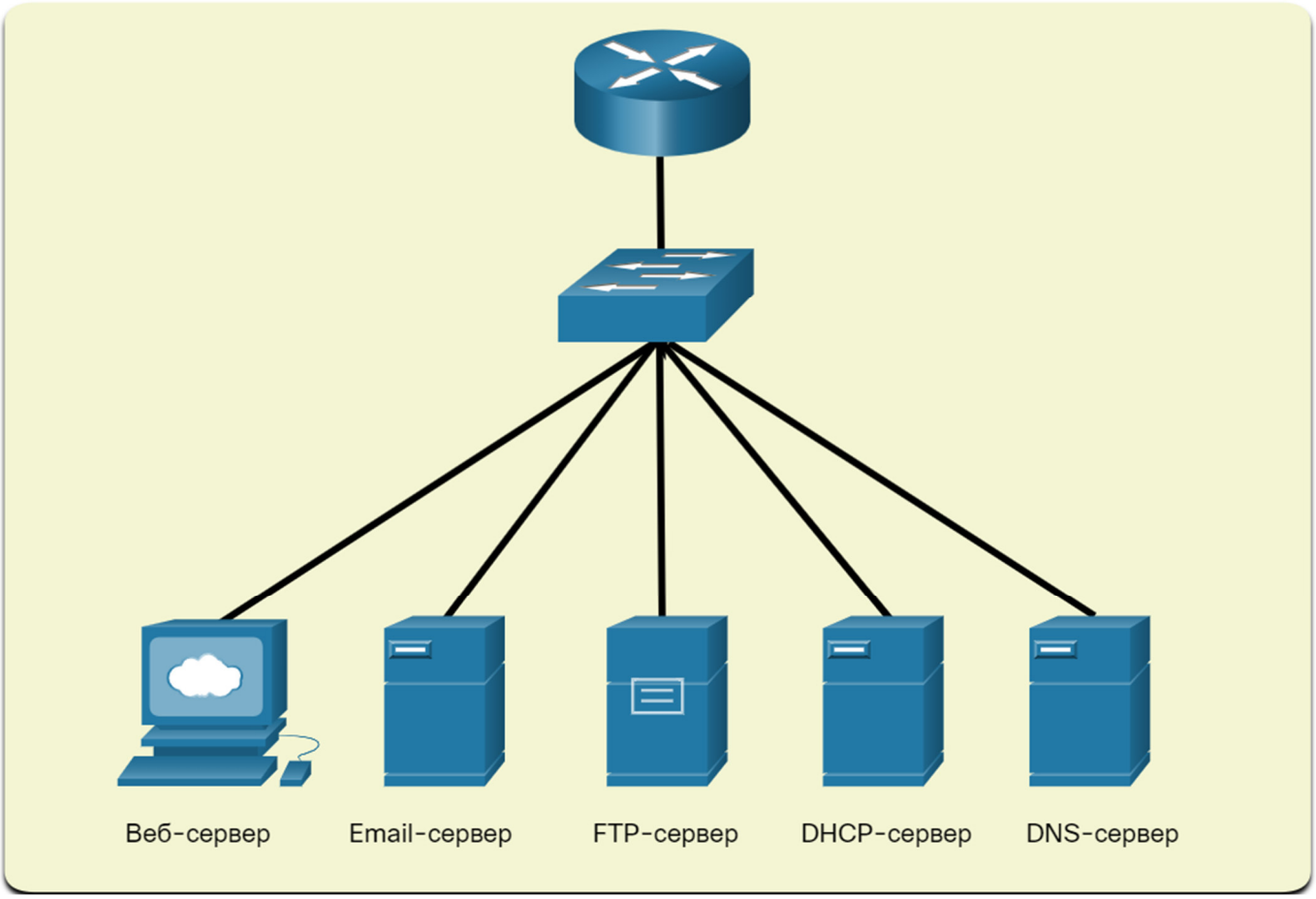
Більша частина роботи технічного персоналу, як в невеликій, так і в великій мережі, в певній мірі буде пов'язана з мережними протоколами. Мережні протоколи підтримують застосунки і служби, що використовуються співробітниками в невеликій мережі.

Мережні адміністратори зазвичай вимагають доступу до мережних пристроїв і серверів. Два найпоширеніших рішення віддаленого доступу - Telnet та Secure Shell (SSH). Сервіс SSH є безпечною альтернативою Telnet. При під'єднанні адміністратори можуть отримати доступ до пристрою SSH сервера так, ніби вони були зареєстровані локально.

SSH використовується для встановлення безпечного з'єднання віддаленого доступу між SSH клієнтом та іншими пристроями, що підтримують SSH:

- **Мережний пристрій** - мережний пристрій (наприклад, маршрутизатор, комутатор, точка доступу тощо) має підтримувати SSH для надання клієнтам послуг віддаленого доступу SSH-сервера.
- **Сервер** - Сервер (наприклад, веб-сервер, сервер електронної пошти тощо) повинен підтримувати віддалений доступ до служб SSH сервера для клієнтів.

Адміністратори мережі також повинні підтримувати загальні мережні сервери та пов'язані з ними мережні протоколи, як показано на рисунку.



Натисніть кожну кнопку, щоб отримати додаткові відомості про загальні мережні сервери та пов'язані з ними мережні протоколи.

Веб-сервер | Email-сервер | FTP-сервер | DHCP-сервер | DNS Сервер

Веб-сервер

- Веб-клієнти та веб-сервери обмінюються веб-трафіком за допомогою протоколу передачі гіпертексту (HTTP).
- Hypertext Transfer Protocol Secure (HTTPS) використовується для безпечного веб-зв'язку.

Веб-сервер | Email-сервер | FTP-сервер | DHCP-сервер | DNS Сервер

Email-сервер

- Сервери електронної пошти та клієнти використовують Simple Mail Transfer Protocol (SMTP) для надсилання повідомлень електронної пошти.
- Поштові клієнти використовують протокол POP3 або протокол доступу до повідомлень Інтернету (IMAP) для отримання електронної пошти.
- Одержувачі вказуються за допомогою формату user@xyz.xxx.

FTP-сервер

- Служба File Transfer Protocol (FTP) дозволяє завантажувати та скачувати файли між клієнтом і FTP-сервером.
- Для безпечного обміну файлами FTP використовуються FTP Secure (FTPS) і Secure FTP (SFTP).

DHCP-сервер

Динамічний протокол конфігурації вузла (DHCP) використовується клієнтами для отримання IP-конфігурації (тобто IP-адреси, маски підмережі, шлюзу за замовчуванням і багато іншого) з DHCP-сервера.

DNS Сервер

- Служба доменних імен (DNS) надає доменне ім'я до IP-адреси (наприклад, cisco.com = 72.163.4.185)
- DNS надає IP-адресу веб-сайту (тобто доменне ім'я) для вузла, що запитує.

Примітка: Сервер може надавати кілька мережних служб. Наприклад, сервером може бути електронна пошта, FTP і SSH сервер.

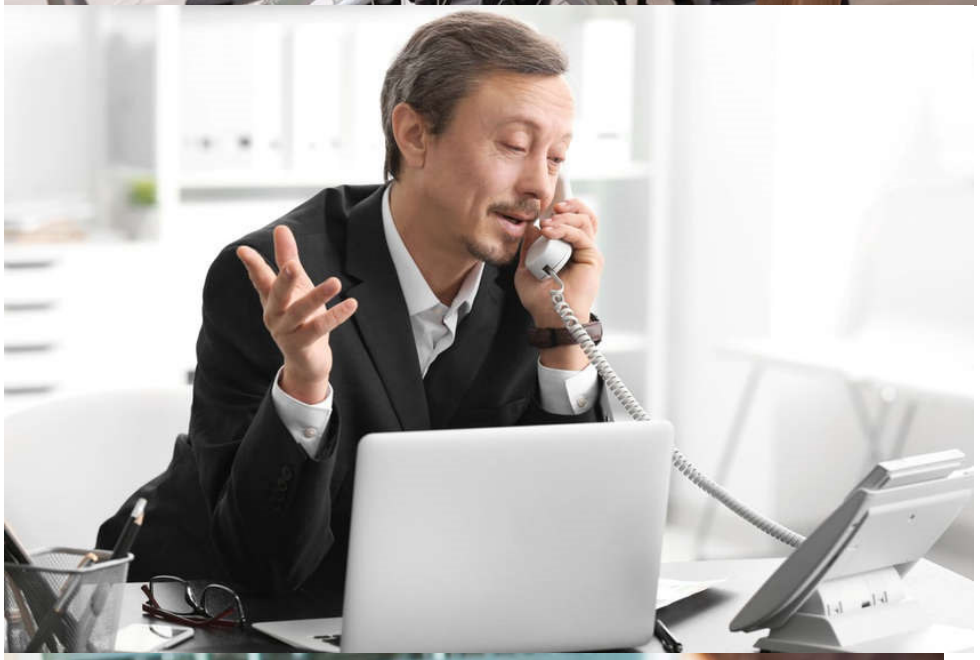
Ці мережні протоколи складають фундаментальний набір інструментів професійної мережі. Кожен з цих мережних протоколів визначає:

- Процеси на будь-якому кінці сеансу зв'язку
- Типи повідомлень
- Синтаксис повідомлень
- Значення інформаційних полів
- Способи відправлення повідомлення та очікувана відповідь
- Взаємодію з наступним нижчим рівнем

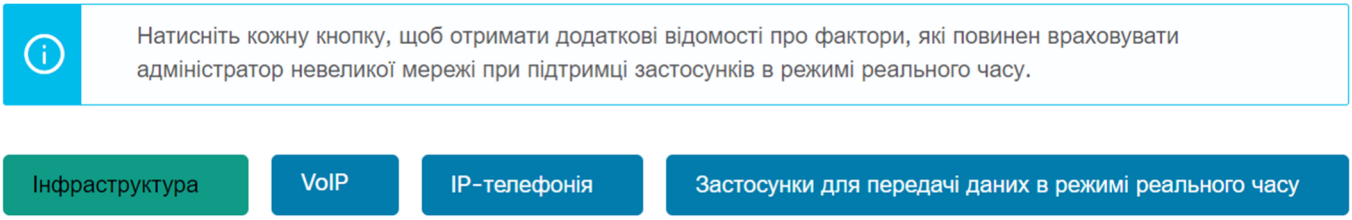
Багато компаній встановили політику використання захищених версій (наприклад, SSH, SFTP та HTTPS) цих протоколів, коли це можливо.

11.2.3 **Застосунки для передавання голосу та відео**

Сьогодні підприємства все частіше використовують IP-телефонію та потокове медіа для спілкування з клієнтами та діловими партнерами. Багато організацій надають можливість своїм співробітникам працювати віддалено. Як показано на рисунку, багато користувачів все ще потребують доступу до корпоративного програмного забезпечення та файлів, а також підтримки голосових та відео застосунків.



Адміністратор мережі повинен переконатися, що в мережі встановлено належне обладнання, і що мережні пристрої налаштовані для забезпечення пріоритетного доставлення.



Інфраструктура

- Мережна інфраструктура повинна підтримувати застосунки в режимі реального часу.
- Існуючі пристрої і прокладка кабелів повинні бути перевірені і протестовані.
- Можуть знадобитися новіші мережні продукти.

VoIP

- VoIP-пристрої перетворюють аналогові телефонні сигнали в цифрові IP-пакети.
- Як правило, VoIP дешевше, ніж рішення IP-телефонії, але якість зв'язку не відповідає тим же стандартам.
- Рішення для голосового зв'язку і відео по IP для невеликих мереж можуть бути вирішені за допомогою Skype або Cisco WebEx.

IP-телефонія

- IP-телефон виконує перетворення Voice-to-IP з використанням виділеного сервера для керування викликами і сигналізації.
- Багато постачальників надають рішення IP-телефонії для малого бізнесу, такі як продукти Cisco Business Edition 4000 Series.

Застосунки для передачі даних в режимі реального часу

- Мережа повинна підтримувати механізми якості обслуговування (QoS), щоб мінімізувати проблеми із затримкою для потокових програм у режимі реального часу.
- Транспортний протокол реального часу (RTP) і протокол керування транспортним протоколом реального часу (RTCP) - два протоколи, які підтримують цю вимогу.

11.2.4 **Питання для самоперевірки - Застосунки та протоколи невеликої мережі**

1. Які дві форми програм (ПЗ) або процесів забезпечують доступ до мережі? (Оберіть два варіанти.)

   - [ ] антивірусне ПЗ
   - [ ] сервіси прикладного рівня
   - [ ] ігрове програмне забезпечення
   - [ ] мережні програми
   - [ ] програмне забезпечення для підвищення продуктивності
   - [ ] програмне забезпечення віртуальної машини

2. Які два мережних протоколи використовуються для встановлення мережного під'єднання віддаленого доступу до пристрою? (Оберіть два варіанти.)

   - [ ] Протокол передавання файлів (FTP, File Transfer Protocol)
   - [ ] Протокол передавання гіпертексту (Hypertext Transfer Protocol, HTTP) :
   - [ ] Віддалене з' єднання (RC)
   - [ ] Захищена оболонка (Secure Shell, SSH)
   - [ ] Простий протокол передавання електронної пошти (Simple Mail Transfer Protocol, SMTP)
   - [ ] Telnet

1. Які дві форми програм (ПЗ) або процесів забезпечують доступ до мережі? (Оберіть два варіанти.)

- [ ] антивірусне ПЗ
- [x] сервіси прикладного рівня
- [ ] ігрове програмне забезпечення
- [x] мережні програми
- [ ] програмне забезпечення для підвищення продуктивності
- [ ] програмне забезпечення віртуальної машини

2. Які два мережних протоколи використовуються для встановлення мережного під'єднання віддаленого доступу до пристрою? (Оберіть два варіанти.)

- [ ] Протокол передавання файлів (FTP, File Transfer Protocol)
- [ ] Протокол передавання гіпертексту (Hypertext Transfer Protocol, HTTP) :
- [ ] Віддалене з' єднання (RC)
- [x] Захищена оболонка (Secure Shell, SSH)
- [ ] Простий протокол передавання електронної пошти (Simple Mail Transfer Protocol, SMTP)
- [x] Telnet

11.3 Масштабування до більших мереж

11.3.1 **Зростання невеликої мережі**

Якщо ваша мережа призначена для малого бізнесу, імовірно, ви хочете, щоб бізнес ріс, а ваша мережа зростала разом з ним. Це називається масштабуванням мережі, і є кілька найкращих практик для цього.

Зростання є природним процесом для багатьох малих підприємств, і їх мережі повинні рости відповідно. В ідеалі, у адміністратора мережі є достатньо часу для прийняття розумних рішень щодо розширення мережі відповідно до зростання компанії.

Для масштабування мережі потрібно кілька елементів:

- **Документація по мережі** - Фізична і логічна топологія
- **Інвентаризація пристроїв** - Список пристроїв, які використовуються або складають мережу
- **Бюджет** - деталізований IT-бюджет, включаючи бюджет на закупівлю обладнання на фінансовий рік

- **Аналіз трафіку** - Протоколи, застосунки та сервіси і відповідні вимоги до трафіку повинні бути задокументовані

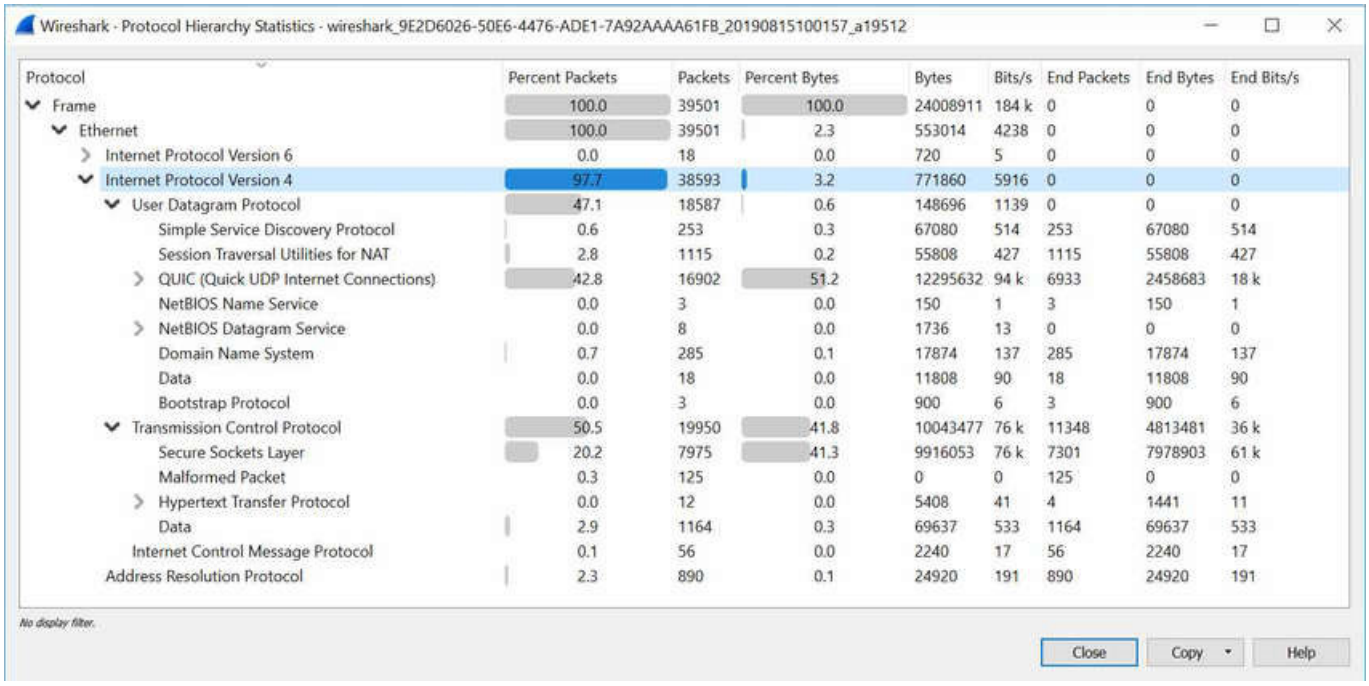
Ці елементи використовуються для інформування про прийняття рішень, що супроводжує масштабування невеликої мережі.

11.3.2 **Аналіз протоколів**

У міру зростання мережі стає важливим визначити, як керувати мережним трафіком. Важливо розуміти тип трафіку, який перетинає мережу, а також поточний трафік. Існує кілька інструментів керування мережею, які можна використовувати для цієї мети. Однак може бути використаний і простий аналізатор протоколів типу Wireshark.

Наприклад, запуск Wireshark на декількох ключових вузлах може виявити типи мережного трафіку, що проходить через мережу. На рисунку нижче наведено статистику ієрархії протоколів Wireshark для вузла з ОС Windows у невеликій мережі.

скріншот статистики ієрархії протоколів Wireshark для трафіку, захопленого вузлом



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	39501	100.0	24008911	184 k	0	0	0
Ethernet	100.0	39501	2.3	553014	4238	0	0	0
Internet Protocol Version 6	0.0	18	0.0	720	5	0	0	0
Internet Protocol Version 4	97.7	38593	3.2	771860	5916	0	0	0
User Datagram Protocol	47.1	18587	0.6	148696	1139	0	0	0
Simple Service Discovery Protocol	0.6	253	0.3	67080	514	253	67080	514
Session Traversal Utilities for NAT	2.8	1115	0.2	55808	427	1115	55808	427
QUIC (Quick UDP Internet Connections)	42.8	16902	51.2	12295632	94 k	6933	2458683	18 k
NetBIOS Name Service	0.0	3	0.0	150	1	3	150	1
NetBIOS Datagram Service	0.0	8	0.0	1736	13	0	0	0
Domain Name System	0.7	285	0.1	17874	137	285	17874	137
Data	0.0	18	0.0	11808	90	18	11808	90
Bootstrap Protocol	0.0	3	0.0	900	6	3	900	6
Transmission Control Protocol	50.5	19950	41.8	10043477	76 k	11348	4813481	36 k
Secure Sockets Layer	20.2	7975	41.3	9916053	76 k	7301	7978903	61 k
Malformed Packet	0.3	125	0.0	0	0	125	0	0
Hypertext Transfer Protocol	0.0	12	0.0	5408	41	4	1441	11
Data	2.9	1164	0.3	69637	533	1164	69637	533
Internet Control Message Protocol	0.1	56	0.0	2240	17	56	2240	17
Address Resolution Protocol	2.3	890	0.1	24920	191	890	24920	191

Скріншот показує, що вузол використовує протоколи IPv6 і IPv4. Специфічний висновок IPv4 також показує, що вузол використовував DNS, SSL, HTTP, ICMP та інші протоколи.

Щоб визначити закономірності руху трафіку, важливо зробити наступне:

- Захопити трафік під час пікового використання, щоб отримати повне уявлення про різні типи трафіку.
- Виконати захоплення на різних сегментах мережі та пристроях, оскільки деякий трафік буде локальним для певного сегмента.

Інформація, зібрана аналізатором протоколу, оцінюється на основі джерела і призначення трафіку, а також типу відправленого трафіку. Цей аналіз може бути використаний для прийняття рішень про те, як ефективніше керувати трафіком. Це можна зробити, зменшивши непотрібні потоки трафіку або змінивши схеми потоку, наприклад, перемістивши сервер.

Іноді просто переміщення сервера або служби в інший сегмент мережі покращує продуктивність мережі і задовольняє зростаючі потреби в трафіку. В інший час оптимізація продуктивності мережі вимагає великого редизайну мережі і втручання.

11.3.3 **Використання службової мережі**

Окрім розуміння тенденцій зміни трафіку, адміністратор мережі повинен знати, як змінюється використання мережі. Багато операційних систем надають вбудовані засоби для відображення такої інформації. Наприклад, вузол з ОС Windows надає такі інструменти, як диспетчер завдань, засіб перегляду подій і використання даних.

Ці інструменти можна використовувати для захоплення «знімка» інформації, наприклад:

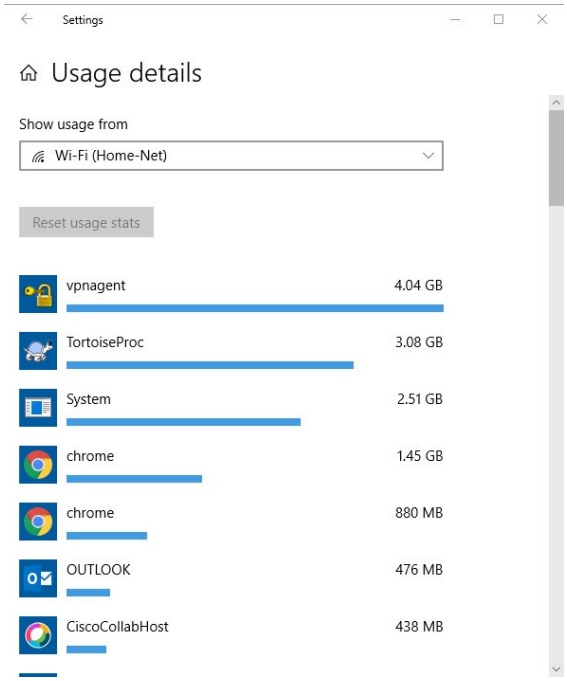
- Версія ОС
- Використання процесора
- Використання оперативної пам'яті
- Використання дискового простору
- Немережні програми
- Мережні програми

Документування знімків для співробітників у невеликій мережі протягом певного періоду часу дуже корисно для визначення вимог до протоколів і пов'язаних з ними потоків трафіку. Зміна використання ресурсів може вимагати від адміністратора мережі відповідно коригувати розподіл мережних ресурсів.

Інструмент використання даних Windows 10 особливо корисний для визначення, які програми використовують мережні послуги на вузлі. Доступ до інструменту використання даних здійснюється за допомогою **Settings > Network & Internet > Data usage > network interface** (за останніх 30 днів).

Приклад на рисунку - це відображення програм, що працюють на віддаленому вузлі користувача з Windows 10 за допомогою локального під'єднання до мережі Wi-Fi.

захоплення екрана інструментом користування даними Windows 10, що показує використання з локального з'єднання Wi-Fi



11.3.4 **Питання для самоперевірки - Масштабування до більших мереж**

1. Які елементи необхідні для масштабування в більшу мережу? (Оберіть два варіанти.)

- [ ] бюджет
- [ ] конфігурація пристроїв
- [ ] збільшена пропускна здатність
- [ ] документація мережі
- [ ] вузли Windows

2. Яке програмне забезпечення, встановлене на ключових вузлах, може виявити типи мережного трафіку, що проходить через мережу?

- ◯ Linux
- ◯ MacOS
- ◯ SSH
- ◯ Windows
- ◯ Wireshark

3. Який інструмент Windows 10 придатний для визначення програм, які використовують мережні сервіси на вузлі?

- ◯ Панель керування (Control Panel)
- ◯ Використання даних
- ◯ Файловий менеджер
- ◯ Брандмауер Захисника Windows
- ◯ Windows Explorer

1. Які елементи необхідні для масштабування в більшу мережу? (Оберіть два варіанти.)

- [x] бюджет
- [ ] конфігурація пристроїв
- [ ] збільшена пропускна здатність
- [x] документація мережі
- [ ] вузли Windows

2. Яке програмне забезпечення, встановлене на ключових вузлах, може виявити типи мережного трафіку, що проходить через мережу?

- ( ) Linux
- ( ) MacOS
- ( ) SSH
- ( ) Windows
- (•) Wireshark

3. Який інструмент Windows 10 придатний для визначення програм, які використовують мережні сервіси на вузлі?

- ( ) Панель керування (Control Panel)
- (•) Використання даних
- ( ) Файловий менеджер
- ( ) Брандмауер Захисника Windows
- ( ) Windows Explorer

11.4 Перевірка з'єднання

11.4.1 **Перевірка з'єднання за допомогою команди Ping**

Незалежно від того, чи ваша мережа невелика та нова, чи ви масштабуєте існуючу мережу, ви завжди захочете переконатися у тому, що ваші компоненти належним чином під'єднані один до одного та до Інтернету. У цьому розділі розглядаються деякі утиліти, які можна використовувати для забезпечення під'єднання мережі.

Команда **ping** є найефективнішим способом швидко перевірити зв'язок рівня 3 між IP-адресою джерела та призначення. Команда також відображає різні статистичні дані часу в обидва кінці.

Зокрема, команда **ping** використовує у протоколі Internet Control Message (ICMP) echo-запити (ICMP Type 8) та echo-запити відповіді (ICMP Type 0). Команда **ping** доступна в більшості операційних систем, включаючи Windows, Linux, macOS і Cisco IOS.

На вузлі з ОС Windows 10 команда **ping** надсилає чотири послідовні ICMP ехо-повідомлення і очікує чотири послідовні ICMP ехо-відповіді від місця призначення.

Наприклад, припустимо, що PC A пінгує PC B. Як показано на рисунку, вузол PC A з ОС Windows надсилає чотири послідовні ICMP ехо-повідомлення на PC B (тобто 10.1.1.10).

На схемі показаний вузол PC A, з адресою 192.168.10.10, за допомогою команди ping 10.1.10 з командного рядка для відправки чотирьох ICMP ехо-повідомлень з IP джерела 198.168.10.10 (слід прочитати 192.168.10.10) і цільовий IP 10.1.10 10.10, який є вузлом PC B в іншій мережі.

192.168.10.10PC APC BC:\>ping 203.0.113.8203.0.113.8

IP джерела	**IP призначення**	**ICMP**
192.168.10.10	10.1.1.10	**Echo**

Інтернет

Вузол призначення отримує і обробляє ICMP ехо-запити. Як показано на рисунку, PC B відповідає, надсилаючи чотири ICMP ехо-відповіді на PC A.

На схемі вказано вузол PC B, за адресою 10.1.1.0, що відправляє чотири ICMP ехо-відповіді з джерелом IP 10.1.1.10 і цільовий IP 198.168.10.10 (слід читати 192.168.10.10) у відповідь на пінг з вузла PC A за адресою 192.168.10.10.

PC APC BC:\>ping 203.0.113.8203.0.113.8192.168.10.10

IP джерела	**IP призначення**	**ICMP**
10.1.1.10	192.168.10.10	**Ехо-відповідь**

Інтернет

Як показано у вихідних даних команди, PC A отримав ехо-відповіді від PC B, що підтверджує мережне з'єднання рівня 3.

```
C:\Users\PC-A> ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time=47ms TTL=51

Reply from 10.1.1.10: bytes=32 time=60ms TTL=51

Reply from 10.1.1.10: bytes=32 time=53ms TTL=51

Reply from 10.1.1.10: bytes=32 time=50ms TTL=51

Ping statistics for 10.1.1.10:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
```

```
    Minimum = 47ms, Maximum = 60ms, Average = 52ms
```

```
C:\Users\PC-A>
```

Вихідні дані показують зв'язок рівня 3 між PC A та PC B.

Вихідні дані команди **ping** Cisco IOS залежать від вузла Windows. Наприклад, ping IOS надсилає п'ять ICMP ехо-повідомлень, як показано у прикладі.

```
R1# ping 10.1.1.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
R1#
```

Зверніть увагу на символи **!!!!!** у виводі команди. Команда IOS **ping** відображає індикатор для кожної отриманої ехо-відповіді ICMP. У таблиці перелічено найпоширеніші символи виводу з команди **ping**.

Індикатори команди ping в IOS

Заголовок таблиці	
Елемент	**Опис**
!	• Знак оклику вказує на успішне отримання ехо-відповіді повідомлення. • Він перевіряє зв'язок рівня 3 між джерелом та пунктом призначення.
.	• Період означає, що минув час очікування ехо-відповіді. • Це вказує на те, що проблема з під'єднанням сталася десь уздовж шляху.
U	• U у верхньому регістрі вказує на те, що маршрутизатор вздовж шляху відповів повідомленням про помилку ICMP типу 3 «пункт призначення недоступний». повідомлення про помилку. • До можливих причин можна віднести те, що маршрутизатор не знає напрямку до мережі призначення або не вдалося знайти вузол в мережі призначення.

Примітка: Інші можливі відповіді на ping включають Q, M,? або &. Однак, їх значення поза рамками даного модуля.

11.4.2 **Розширена команда Ping**

Стандартна команда **ping** використовує IP-адресу інтерфейсу найближчого до мережі призначення як джерело **ping**. IP-адресою джерела команди **ping 10.1.1.10** на R1 буде вказаний інтерфейс G0/0/0 (тобто 209.165.200.225), як показано в прикладі.

На діаграмі показано, як маршрутизатор використовує стандартний ping вузлу, надсилаючи чотири послідовних ехо-повідомлення ICMP, отримані з інтерфейсу, найближчого до пункту призначення. Маршрутизатор R1 під'єднаний до двох мереж: ліворуч знаходиться 192.168.10.0/24 на інтерфейсі G0/0/1 з адресою .1 і праворуч мережа 209.165.200.224/30 на інтерфейсі G0/0/0 з адресою .225. Остання мережа з'єднана з R2, яка з'єднана з мережею 10.1.1.0/24, на якій вузол PC B має адресу .10. R1 надсилає PC B чотири ICMP ехо-повідомлень з джерелом IP 209.165.200.225 і призначення IP 10.1.10.

R2.10.1G0/0/0.10209.165.200.224 /30192.168.10.0 /2410.1.1.0/24.225G0/0/1PC APC BR1

IP джерела	**IP призначення**	**ICMP**
209.165.200.225	10.1.1.10	**Echo**

Cisco IOS пропонує розширений режим команди **ping**. Цей режим дозволяє користувачеві створювати особливий тип пінгів шляхом налаштування параметрів, пов'язаних з командною операцією.

Розширена команда ping вводиться в привілейованому режимі EXEC шляхом введення **ping** без IP-адреси призначення. Згодом вам буде надано кілька підказок, щоб налаштувати розширену команду **ping**.

Примітка: Натискання **Enter** приймає вказані значення за замовчуванням.

Наприклад, припустимо, що ви хотіли перевірити з'єднання локальної мережі R1 (тобто 192.168.10.0/24) з локальною мережою 10.1.1.0. Це можна перевірити на PC A. Проте, розширена команда **ping** може бути налаштована на R1 для вказівки іншої адреси джерела.

Як показано у прикладі, IP-адреса джерела розширеної команди **ping** на R1 може бути налаштована на використання IP-адреси інтерфейсу G0/0/1 (тобто 192.168.10.1).

На схемі показано, як маршрутизатор використовує розширену команду ping для пінгування вузла, надсилаючи чотири послідовні ICMP echo-повідомлення з вказаною IP-адресою джерела. Маршрутизатор R1 під'єднаний до двох мереж: ліворуч знаходиться 192.168.10.0/24 на інтерфейсі G0/0/1 з адресою .1 і праворуч мережа 209.165.200.224/30 на інтерфейсі G0/0/0 з адресою .225. Остання мережа з'єднана з R2, яка під'єднана до мережі 10.1.1.0/24, на якій вузол PC B має адресу .10. R1 надсилає PC B чотири ICMP ехо-повідомлення з джерелом IP 192.168.10.1 і IP призначенням 10.1.10.

R2.10.1G0/0/0.10209.165.200.224 /30192.168.10.0 /2410.1.1.0/24.225G0/0/1PC APC BR1

IP джерела	**IP призначення**	**ICMP**
192.168.10.1	10.1.1.10	**Echo**

Наступні вихідні дані команди налаштовують розширену команду **ping** на R1 і вказує IP-адресу джерела такою, як на інтерфейсі G0/0/1 (тобто 192.168.10.1).

```
R1# ping
```

```
Protocol [ip]:
```

```
Target IP address: 10.1.1.10
```

```
Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Ingress ping [n]:

Source address or interface: 192.168.10.1

DSCP Value [0]:

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0x0000ABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.10.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#
```

Примітка: Команда **ping ipv6** використовується для розширеної команди ping для IPv6.

11.4.3 Перевірка з'єднання за допомогою команди Traceroute

Команда **ping** корисна, щоб швидко визначити, чи є проблема з'єднання на рівні 3. Однак вона не визначає, де знаходиться проблема.

Traceroute може допомогти знайти проблемні зони рівня 3 в мережі. Трасування повертає список хопів, коли пакет направляється через мережу. Вона може бути використана для визначення точки на шляху, де проблема може бути знайдена.

Синтаксис команди трасування різниться між операційними системами, як показано на рисунку.

На схемі показано різницю між командою трасування, як видається з вузла Windows до маршрутизатора Cisco IOS. Топологія мережі складається з вузла PC A, з'єднаного з комутатором, під'єднаного до маршрутизаторів R1, R2, R3, з'єднаних з комутатором, що під'єднаний до вузла PC B. PC A, з IP-адресою 192.168.10.10, видає наступну команду з командного рядка Windows: C:\ >:tracert 10.1.1.10. R1 видає наступну команду від Cisco IOS CLI: R#traceroute 10.1.10.

Команди трасування Windows і Cisco IOS

PC APC B10.1.1.10192.168.10.10.1R3R2R1

Трасування від вузла Windows

```
C:\ >:tracert 10.1.1.10
```

Трасування від маршрутизатора Cisco IOS

```
R# traceroute 10.1.1.10
```

Нижче наведено приклад вихідних даних команди **tracert** на вузлі з ОС Windows 10.

```
C:\Users\PC-A> tracert 10.1.1.10

Tracing route to 10.1.10 over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms  192.168.10.1

  2    *       *       *     Request timed out.

  3    *       *       *     Request timed out.

  4    *       *       *     Request timed out.

^C

C:\Users\PC-A>
```

Примітка: Використовуйте **Ctrl-C**, щоб перервати трасування у Windows**.

Єдина успішна відповідь була від шлюзу на R1. Запити трасування до наступного хопу вичерпано, як зазначено зірочкою (*), що означає, що наступний маршрутизатор-хоп не відповів. Запити тайм-аута вказують на те, що в

мережі Інтернет поза локальною мережею є збій або що ці маршрутизатори налаштовані не відповідати на ехо-запити, які використовуються в трасуванні. У цьому прикладі виникає проблема між R1 і R2.

Вихідні дані команди **traceroute** Cisco IOS відрізняється від команди **tracert** Windows. Наприклад, розглянемо наведену нижче топологію.

На схемі показана топологія мережі з IP-адресацією інтерфейсів маршрутизатора і командою traceroute, виданої з маршрутизатора Cisco IOS. Топологія складається з наступних пристроїв і мереж, зліва направо. Комутатор мережі 192.168.10.0/24 під'єднаний до маршрутизатора R1 на інтерфейсі з адресою .1. R1 під'єднується до маршрутизатора R2 по мережі 209.165.200.224/30. Інтерфейс на R1 має адресу .225, а інтерфейс на R2 має адресу .226. R2 під'єднується до маршрутизатора R3 по мережі 209.165.200.228/30. Інтерфейс на R2 має адресу .229, а інтерфейс на R3 має адресу .230. R3 під'єднується до комутатора, який з'єднаний з вузлом PC B з адресою 10.1.1.10. R1 видає таку команду трасування з CLI: R1# traceroute 10.1.1.10.

PC B10.1.1.10192.168.10.0 /24.1R3R1.225.226.229R2.230209.165.200.224 /30209.165.200.228 /30R1

Трасування від маршрутизатора Cisco IOS

```
R1# traceroute 10.1.1.10
```

Нижче наведено приклад вихідних даних команди traceroute з R1.

```
R1# traceroute 10.1.1.10

Type escape sequence to abort.

Tracing the route to 10.1.1.10

VRF info: (vrf in name/id, vrf out name/id)

  1 209.165.200.226 1 msec 0 msec 1 msec

  2 209.165.200.230 1 msec 0 msec 1 msec

  3 10.1.1.10 1 msec 0 msec

R1#
```

У цьому прикладі трасування підтверджено: воно може успішно досягти PC B.

Тайм-аути вказують на потенційну проблему. Наприклад, якщо вузол 10.1.1.10 був недоступний, команда **traceroute** буде відображати такі результати.

```
R1# traceroute 10.1.1.10

Type escape sequence to abort.

Tracing the route to 10.1.1.10
```

```
VRF info: (vrf in name/id, vrf out name/id)

  1 209.165.200.226 1 msec 0 msec 1 msec

  2 209.165.200.230 1 msec 0 msec 1 msec

  3 * * *

  4 * * *

  5 *
```

Використовуйте **Ctrl-Shift-6** для переривання **traceroute** в Cisco IOS.

Примітка: Реалізація traceroute (tracert) в Windows надсилає ICMP exo-запити. Cisco IOS і Linux використовують UDP з неприпустимим номером порту. Кінцеве місце призначення поверне ICMP-порту недоступне повідомлення.

11.4.4 **Розширена команда Traceroute**

Як і розширена команда **ping**, існує ще й розширена команда **traceroute**. Вона дозволяє адміністратору налаштовувати параметри, пов'язані з командною операцією. Це корисно для пошуку проблеми під час виправлення несправностей циклів маршрутизації, визначення точного маршрутизатора наступного переходу або визначення місця, де пакети потрапляють або забороняються маршрутизатором чи брандмауером.

Команда Windows **tracert** дозволяє введення декількох параметрів через опції в командному рядку. Однак, в ній необхідно керувати інакше, ніж у розширеній команді IOS traceroute. У наведеному нижче прикладі відображаються доступні параметри команди Windows **tracert**.

```
C:\Users\PC-A> tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
```

```
-R                Trace round-trip path (IPv6-only).

-S srcaddr        Source address to use (IPv6-only).

-4                Force using IPv4.

-6                Force using IPv6.

C:\Users\PC-A>
```

Цей режим Cisco IOS дозволяє створювати спеціальний запит **traceroute**, налаштовуючи параметри, пов'язані з роботою команди. Для переходу в цей режим необхідно ввести текст **traceroute** в привілейованому режимі EXEC, не вказуючи IP-адресу призначення. IOS допоможе налаштувати параметри команд, представивши ряд підказок, пов’язаних із встановленням усіх різних параметрів.

Примітка: Натискання **Enter** приймає вказані значення за замовчуванням.

Наприклад, припустимо, що потрібно перевірити під'єднання до PC B з локальної мережі R1. Хоча, це може бути перевірено на PC A, розширена команда **traceroute** може бути налаштована на R1 для визначення іншої вихідної адреси.

На схемі показана топологія мережі з IP-адресацією інтерфейсів маршрутизатора і розширеною командою traceroute, виданої з маршрутизатора Cisco IOS. Топологія складається з наступних пристроїв і мереж, зліва направо. Комутатор мережі 192.168.10.0/24 під'єднаний до маршрутизатора R1 в інтерфейсі з адресою .1. R1 під'єднується до маршрутизатора R2 по мережі 209.165.200.224/30. Інтерфейс на R1 має адресу .225, а інтерфейс на R2 має адресу .226. R2 під'єднується до маршрутизатора R3 по мережі 209.165.200.228/30. Інтерфейс на R2 має адресу .229, а інтерфейс на R3 має адресу .230. R3 під'єднується до комутатора, який з'єднаний з вузлом PC B з адресою 10.1.1.10. R1 видає наступну команду трасування з CLI: R1# traceroute.

PC B192.168.10.0/24209.165.200.224/30209.165.200.228/3010.1.1.10R1R3R2.1.225.226.229.230

Розширене трасування з маршрутизатора Cisco IOS

```
R1# traceroute
```

Як показано в прикладі, IP-адреса джерела розширеної команди **traceroute** на R1 може бути налаштована на використання IP-адреси інтерфейсу LAN R1 (тобто 192.168.10.1).

```
R1# traceroute

Protocol [ip]:

Target IP address: 10.1.1.10

Ingress traceroute [n]:

Source address: 192.168.10.1

DSCP Value [0]:
```

```
Numeric display [n]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]:

Port Number [33434]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.

Tracing the route to 192.168.10.10

VRF info: (vrf in name/id, vrf out name/id)

 1 209.165.200.226 1 msec 1 msec 1 msec

 2 209.165.200.230 0 msec 1 msec 0 msec

 3  *

   10.1.1.10 2 msec 2 msec

R1#
```

11.4.5 **Базовий рівень мережі**

Одним з найбільш ефективних інструментів для моніторингу та усунення несправностей продуктивності мережі є створення базового рівня мережі. Створення ефективного базового рівня продуктивності мережі здійснюється протягом певного періоду часу. Вимірювання продуктивності в різний час і навантаження допоможе створити краще уявлення про загальну продуктивність мережі.

Вихідні дані, отримані в результаті використання мережних команд, надають дані для внесення в базовий рівень мережі. Одним із способів запуску базового рівня є копіювання та вставлення результатів виконання **ping**, **trace** або інших відповідних команд у текстовий файл. Ці текстові файли можуть бути позначені часом з датою і збережені до архіву для подальшого пошуку та порівняння.

Серед елементів, які слід розглянути, є повідомлення про помилки та значення часу відповіді між вузлами. Якщо є значне збільшення часу відповіді, може бути проблема, яка пов'язана із затримкою.

Наприклад, наступні вихідні дані команди **ping** були захоплені і вставлені в текстовий файл.

August 19, 2019 at 08:14:43

C:\Users\PC-A> **ping 10.1.1.10**

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.1.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\PC-A>

Зверніть увагу, що час команди **ping** в обидва кінці менше 1 мс.

Через місяць пінг повторюється і захоплюється.

September 19, 2019 at 10:18:21

C:\Users\PC-A> **ping 10.1.1.10**

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time=50ms TTL=64

Reply from 10.1.1.10: bytes=32 time=49ms TTL=64

Reply from 10.1.1.10: bytes=32 time=46ms TTL=64

Reply from 10.1.1.10: bytes=32 time=47ms TTL=64

```
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 50ms, Average = 48ms
C:\Users\PC-A>
```

Зверніть увагу, що на цей раз проміжок часу для передавання **ping** в обидва кінці набагато довший, що вказує на потенційну проблему.

Корпоративні мережі повинні мати великі базові рівні; більш широкі, ніж ми можемо описати в цьому курсі. Професійні програмні засоби доступні для зберігання та підтримки базового рівня. В рамках даного курсу розглядається кілька основних прийомів базових рівнів і обговорюється їх призначення.

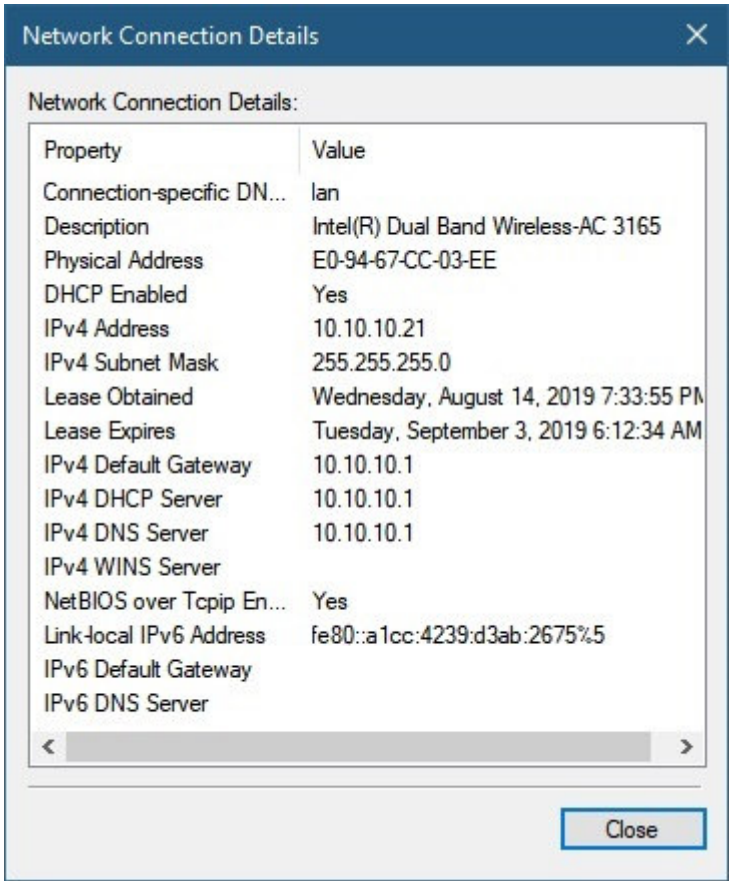
Найкращі практики Cisco для базових процесів можна знайти в Інтернеті за допомогою пошуку «Найкращі практики базового процесу».

11.5 Команди вузла та IOS

11.5.1 **Налаштування IP-конфігурації на вузлі з ОС Windows**

Якщо ви використовували будь-який з інструментів у попередньому розділі, щоб перевірити під'єднання і виявили, що якась частина вашої мережі не працює належним чином, зараз настав час використати певні команди для усунення несправностей на ваших пристроях. Команди вузла і IOS можуть допомогти вам визначити, чи є проблема з IP-адресацією ваших пристроїв, що є поширеною проблемою мережі.

Перевірка IP-адресації на вузлах є поширеною практикою для перевірки та усунення несправностей наскрізного з'єднання в мережі. У Windows 10 ви можете отримати доступ до деталей IP-адреси з **Network and Sharing Center**, як показано на рисунку, для швидкого перегляду чотирьох важливих параметрів: адреси, маски, шлюзу та DNS.



Однак адміністратори мережі зазвичай переглядають інформацію про IP-адресацію на вузлі з ОС Windows, видаючи команду **ipconfig** в командному рядку комп'ютера з ОС Windows, як показано у прикладі.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Використовуйте команду **ipconfig /all** для перегляду MAC-адреси, а також низки деталей щодо адресації 3 рівня для пристрою, як показано у прикладі.

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
```

```
   Host Name . . . . . . . . . . . . : PC-A-00H20
   Primary Dns Suffix  . . . . . . . : cisco.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cisco.com
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Якщо вузол налаштований як клієнт DHCP, конфігурацію IP-адреси можна поновити за допомогою команд **ipconfig /renew** і **ipconfig /release** , як показано у прикладі.

```
C:\Users\PC-A> ipconfig /release
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
```

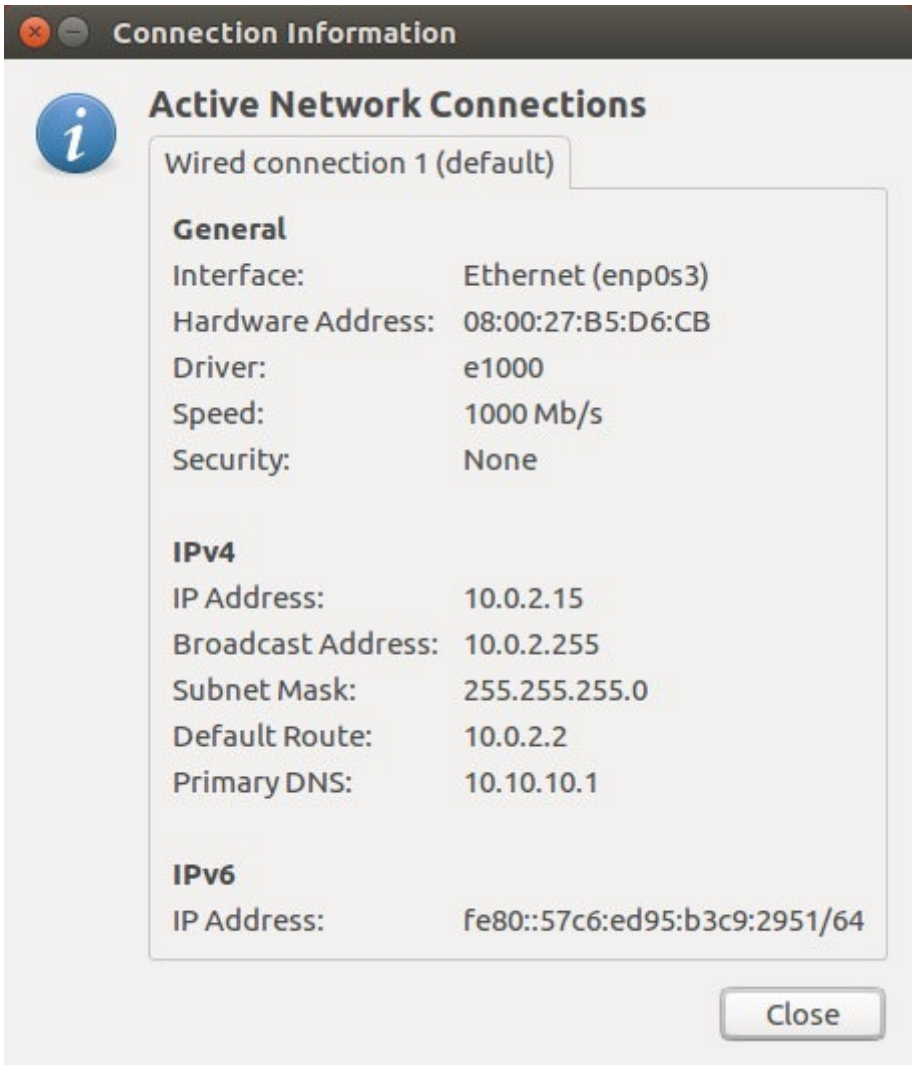
```
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   Default Gateway . . . . . :
(Output omitted)
C:\Users\PC-A> ipconfig /renew
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
(Output omitted)
C:\Users\PC-A>
```

Служба DNS-клієнта на комп'ютерах з ОС Windows також оптимізує продуктивність вирішення імен DNS, зберігаючи раніше перетворені імена в пам'яті. На ПК з ОС Windows команда **ipconfig /displaydns** відображає на екрані всі кешовані записи DNS, як показано в прикладі.

```
C:\Users\PC-A> ipconfig /displaydns
Windows IP Configuration
(Output omitted)
    netacad.com
    ----------------------------------------
    Record Name . . . . . : netacad.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 602
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 54.165.95.219
(Output omitted)
```

11.5.2 **Налаштування IP-конфігурації на вузлі з ОС Linux**

Перевірка параметрів IP за допомогою графічного інтерфейсу на ПК з Linux буде відрізнятися залежно від дистрибутива Linux та інтерфейсу робочого столу. На рисунку показано діалогове вікно **Connection Information** дистрибутива Ubuntu під керуванням робочого стола Gnome.



У командному рядку мережні адміністратори використовують команду **ifconfig** для відображення стану активних в даний момент інтерфейсів та їх IP-конфігурації, як показано у прикладі.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

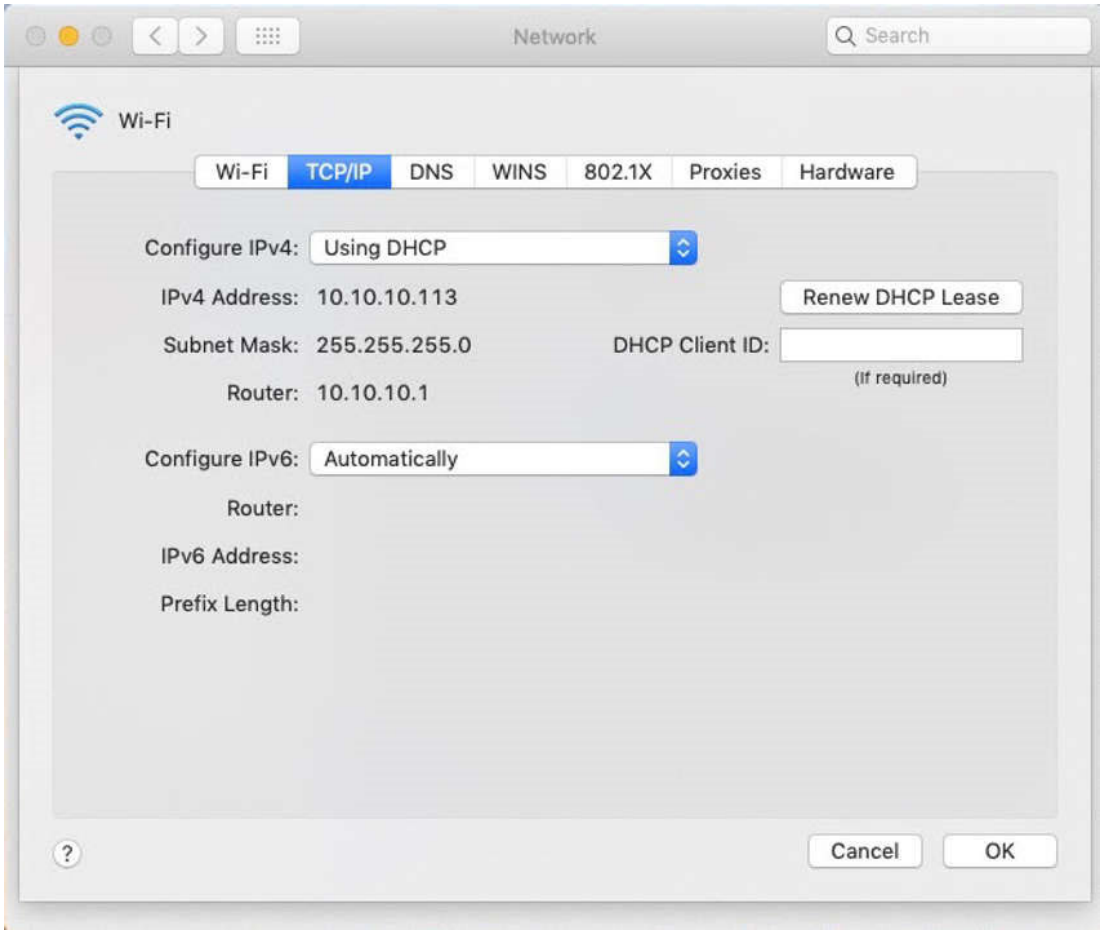
```
        RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Команда Linux **ip address** використовується для відображення адрес і їх властивостей. Її також можна використовувати для додавання або видалення IP-адрес.

Примітка: Виведені дані можуть відрізнятися в залежності від дистрибутива Linux.

11.5.3 **Налаштування IP-конфігурації на вузлі з macOS**

У графічному інтерфейсі вузла з macOS відкрийте **Network Preferences > Advanced** для отримання інформації щодо IP-адресації, як показано на рисунку.



Однак, команда **ifconfig** також може бути використана для перевірки IP -конфігурації інтерфейсу, показаного у прикладі.

```
MacBook-Air:~ Admin$ ifconfig en0
en0: flags=8863 mtu 1500
        ether c4:b3:01:a0:64:98
        inet6 fe80::c0f:1bf4:60b1:3adb%en0 prefixlen 64 secured scopeid 0x5
        inet 10.10.10.113 netmask 0xffffff00 broadcast 10.10.10.255
        nd6 options=201
        media: autoselect
        status: active
MacBook-Air:~ Admin$
```

Інші корисні команди macOS для перевірки параметрів IP вузла включають **networksetup -listallnetworkservices** і **networksetup -getinfo <***network service***>,** як показано в наступному прикладі.

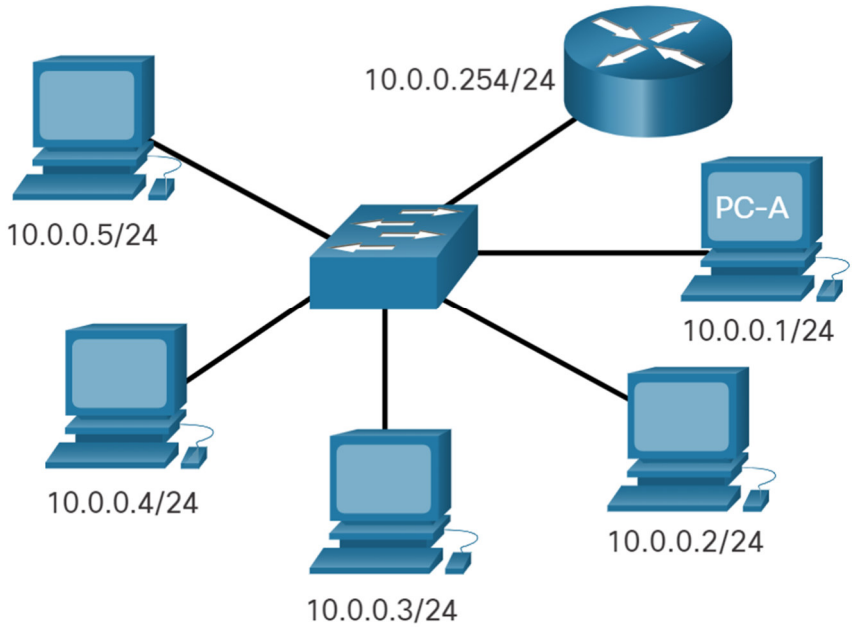
```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
```

```
MacBook-Air:~ Admin$
```

11.5.4 Команда ARP

Команда **arp** виконується з командного рядка Windows, Linux або Mac. Команда надає можливість отримати перелік всіх пристроїв, які на даний час є в ARP-кеші вузла, а також адресу IPv4, фізичну адресу і тип адресації (статичний/динамічний) для кожного пристрою.

Наприклад, розглянемо наведену нижче топологію.



п'ять вузлів з IP-адресами 10.0.0.1/24, 10.0.0.2/24, 10.0.0.3/24, 10.0.0.4/24 і 10.0.0.5/24, під'єднані до комутатора, який з'єднаний з маршрутизатором з IP-адресою 10.0.0.254/24

10.0.0.254/2410.0.0.1/2410.0.0.2/2410.0.0.3/2410.0.0.4/2410.0.0.5/24PC-A

Відображаються вихідні дані команди **arp -a** на вузлі PC-A з ОС Windows.

```
C:\Users\PC-A> arp -a
```

```
Interface: 192.168.93.115 --- 0xc
```

```
  Internet Address      Physical Address      Type
```

```
  10.0.0.2              d0-67-e5-b6-56-4b     dynamic
```

```
  10.0.0.3              78-48-59-e3-b4-01     dynamic
```

```
  10.0.0.4              00-21-b6-00-16-97     dynamic
```

```
10.0.0.254            00-15-99-cd-38-d9     dynamic
```

Команда **arp -a** відображає відому IP-адресу та прив'язку MAC-адреси. Зверніть увагу, що IP-адреса 10.0.0.5 не включена до переліку. Це пов'язано з тим, що ARP-кеш відображає інформацію тільки з пристроїв, до яких було нещодавно отримано доступ.

Щоб переконатися, що кеш ARP заповнений, слід виконати команду **ping** для перевірки зв'язку з пристроєм, щоб для нього було створено запис у таблиці ARP. Наприклад, якщо PC-A пропінгував 10.0.0.5, то ARP-кеш буде містити запис для цієї IP-адреси.

Кеш можна очистити за допомогою команди **netsh interface ip delete arpcache** в тому випадку, якщо адміністратор мережі захоче заповнити кеш оновленою інформацією.

Примітка: Вам може знадобитися доступ адміністратора на вузлі, щоб мати можливість використовувати команду **netsh interface ip delete arpcache**.

11.5.5 Повторний розгляд команди show

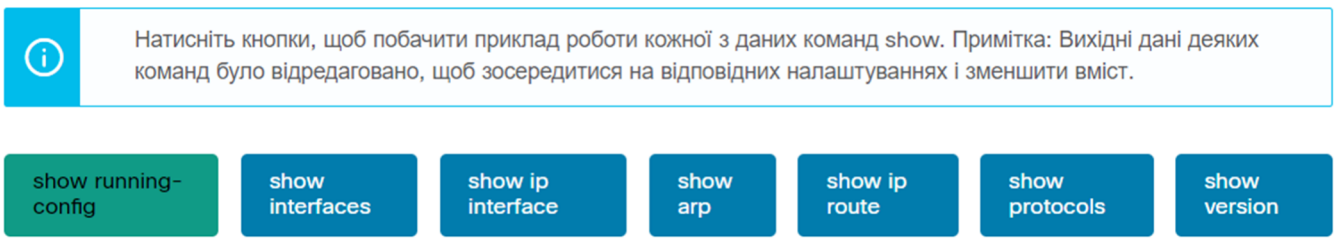
Таким же чином, як команди та утиліти використовуються для перевірки конфігурації вузла, команди можуть бути використані для перевірки інтерфейсів проміжних пристроїв. Cisco IOS надає команди для перевірки роботи інтерфейсів маршрутизатора і комутатора.

Команди **show** Cisco IOS CLI відображають актуальну інформацію про конфігурацію і роботу пристрою. Спеціалісти мережі широко використовують команди **show** для перегляду конфігураційних файлів, перевірки стану інтерфейсів і процесів пристрою, а також перевірки стану роботи пристрою. Статус майже кожного процесу або функції маршрутизатора можна відобразити за допомогою команди **show**.

Загальновживані команди **show** та коли їх використовувати, наведені в таблиці.

Команда	Корисно для …
show running-config	Для перевірки поточної конфігурації та налаштувань
show interfaces	Для перевірки стану інтерфейсу та наявності повідомлень про помилки
show ip interface	Для перевірки інформації рівня 3 для інтерфейсу
show arp	Для перевірки списку відомих хостів у локальних мережах Ethernet
show ip route	Для перевірки інформації про маршрутизацію 3 рівня
show protocols	Для перевірки, які протоколи працюють
show version	Для перевірки пам’яті, інтерфейсів та ліцензії пристрою

Натисніть кнопки, щоб побачити приклад роботи кожної з даних команд show. Примітка: Вихідні дані деяких команд було відредаговано, щоб зосередитися на відповідних налаштуваннях і зменшити вміст.



show running-config

Перевіряє поточні налаштування та параметри

```
R1# show running-config
(Output omitted)
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0/0
 description Link to R2
 ip address 209.165.200.225 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 description Link to LAN
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
!
router ospf 10
 network 192.168.10.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.3 area 0
!
banner motd ^C Authorized access only! ^C
!
line con 0
 password 7 14141B180F0B
```

```
 login
line vty 0 4
 password 7 00071A150754
 login
 transport input telnet ssh
!
end
R1#
```

show interfaces
Перевіряє стан інтерфейсу і відображає будь-які повідомлення про помилки

```
R1# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Description: Link to R2
  Internet address is 209.165.200.225/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:21, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5127 packets input, 590285 bytes, 0 no buffer
```

```
Received 29 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 5043 multicast, 0 pause input
1150 packets output, 153999 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
1 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up
(Output omitted)
```

show ip interface
Перевіряє інформацію 3 рівня для інтерфейсу

```
R1# show ip interface
GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 209.165.200.225/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5 224.0.0.6
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound  access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
```

Split horizon is enabled

ICMP redirects are always sent

ICMP unreachables are always sent

ICMP mask replies are never sent

IP fast switching is enabled

IP Flow switching is disabled

IP CEF switching is enabled

IP CEF switching turbo vector

IP Null turbo vector

Associated unicast routing topologies:

    Topology "base", operation state is UP

IP multicast fast switching is enabled

IP multicast distributed fast switching is disabled

IP route-cache flags are Fast, CEF

Router Discovery is disabled

IP output packet accounting is disabled

IP access violation accounting is disabled

TCP/IP header compression is disabled

RTP/IP header compression is disabled

Probe proxy name replies are disabled

Policy routing is disabled

Network address translation is disabled

BGP Policy Mapping is disabled

Input features: MCI Check

IPv4 WCCP Redirect outbound is disabled

IPv4 WCCP Redirect inbound is disabled

IPv4 WCCP Redirect exclude is disabled

GigabitEthernet0/0/1 is up, line protocol is up

(Output omitted)

show arp

Перевіряє список відомих вузлів на локальних мережах Ethernet

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  192.168.10.10          95   c07b.bcc4.a9c0  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.225          -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.226        138   a03d.6fe1.9d90  ARPA   GigabitEthernet0/0/0
R1#
```

show ip route

Перевіряє відомості про маршрутизацію 3 рівня

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O        209.165.200.228/30
```

```
      [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

show protocols
Перевіряє, які протоколи працюють

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 209.165.200.225/30
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
Serial0/1/0 is down, line protocol is down
Serial0/1/1 is down, line protocol is down
GigabitEthernet0 is administratively down, line protocol is down
R1#
```

show version
Перевіряє пам'ять, інтерфейси та ліцензії пристрою

```
R1# show version
Cisco IOS XE Software, Version 03.16.08.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(3)S8, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 08-Aug-18 10:48 by mcpre
(Output omitted)
ROM: IOS-XE ROMMON
R1 uptime is 2 hours, 25 minutes
Uptime for this control processor is 2 hours, 27 minutes
System returned to ROM by reload
System image file is "bootflash:/isr4300-universalk9.03.16.08.S.155-3.S8-ext.SPA.bin"
Last reload reason: LocalSoft
```

```
(Output omitted)
Technology Package License Information:
------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------
appxk9        appxk9        RightToUse    appxk9
uck9          None          None          None
securityk9    securityk9    Permanent     securityk9
ipbase        ipbasek9      Permanent     ipbasek9
cisco ISR4321/K9 (1RU) processor with 1647778K/6147K bytes of memory.
Processor board ID FLM2044W0LT
2 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
978928K bytes of USB flash at usb0:.
Configuration register is 0x2102
R1#
```

11.5.6 **Команда show cdp neighbors**

Є кілька інших команд IOS, які стануть в нагоді. Cisco Discovery Protocol (CDP) — це пропрієтарний протокол Cisco, який працює на канальному рівні. Оскільки CDP працює на канальному рівні, два або більше мережних пристроїв Cisco, таких як маршрутизатори, які підтримують різні протоколи мережного рівня, можуть дізнатися один про одного, навіть якщо під'єднання рівня 3 не існує.

Коли пристрій Cisco завантажується, CDP запускається за замовчуванням. CDP автоматично виявляє сусідні пристрої Cisco, на яких працює протокол CDP, незалежно від того, який протокол або комплекси рівня 3 запущено. CDP обмінюється інформацією про апаратне та програмне забезпечення з його безпосередньо під'єднаними сусідами CDP.

CDP надає такі відомості про кожний пристрій сусіда CDP:

- **Ідентифікатори пристрою** - налаштоване ім'я комутатора, маршрутизатора або іншого пристрою
- **Список адрес** - не більше однієї адреси мережного рівня для кожного підтримуваного протоколу

- **Ідентифікатор порту** - Ім'я локального та віддаленого порту у вигляді рядка символів ASCII, наприклад FastEthernet 0/0
- **Список можливостей** - Наприклад, чи є конкретний пристрій комутатором Рівня 2 або комутатором Рівня 3
- **Платформа** - Апаратна платформа пристрою, наприклад, маршрутизатор Cisco серії 1841.

Зверніться до топології та вихідних даних команди **show cdp neighbor**.


```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

Вихідні дані показують, що інтерфейс R3 GigabitEthernet 0/0/1 під'єднаний до інтерфейсу FastEthernet 0/5 S3, який є комутатором Cisco Catalyst 2960+. Зверніть увагу, що R3 не зібрав інформацію про S4. Це пов'язано з тим, що CDP може виявити лише безпосередньо під'єднані пристрої Cisco. S4 не під'єднано безпосередньо до R3 і тому не вказано у вихідних даних.

Команда **show cdp neighbors detail** розкриває IP-адресу сусіднього пристрою, як показано у прикладі. CDP виявить IP-адресу сусіда незалежно від того, чи можете ви пінгувати даного сусіда. Ця команда дуже корисна, коли два маршрутизатори Cisco не можуть маршрутизуватися через спільне посилання для передачі даних. Команда **show cdp neighbors detail** допоможе визначити, чи є у одного з сусідів CDP помилка IP-конфігурації.

Незважаючи на корисність, CDP також може становити загрозу безпеці, оскільки може надати корисну інформацію про мережну інфраструктуру суб'єктам загрози. Наприклад, за замовчуванням багато версій IOS відправляють анонси CDP з усіх включених портів. Однак найкращі практики передбачають, що CDP слід включати лише на інтерфейсах, що під'єднуються до інших інфраструктурних пристроїв Cisco. CDP реклами слід вимкнути на користувацьких портах.

Оскільки деякі версії IOS за замовчуванням надсилають анонси CDP, важливо знати, як відключити CDP. Щоб відключити CDP глобально, використовуйте команду глобальної конфігурації **no cdp run**. Щоб відключити CDP на інтерфейсі, скористайтеся командою інтерфейсу **no cdp enable**.

11.5.7 Команда show ip interface brief

Однією з найчастіше використовуваних команд є команда **show ip interface brief**. Ця команда надає більш скорочені вихідні дані, ніж команда **show ip interface**. Вона надає зведену ключову інформацію для всіх мережних інтерфейсів на маршрутизаторі.

Наприклад, у виходних даних команди **show ip interface brief** відображаються всі інтерфейси на маршрутизаторі, IP-адреси, які присвоєні кожному інтерфейсу (якщо такі є) і робочий стан інтерфейсу.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

Перевірка інтерфейсу комутатора

Команда **show ip interface brief** також може бути використана для перевірки стану інтерфейсів комутатора, як показано у прикладі.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

Інтерфейсу VLAN1 призначено адресу IPv4 192.168.254.250, яку увімкнено та яка працює.

У прикладі також видно, що інтерфейс FastEthernet0/1 не працює. Це вказує на те, що до інтерфейсу не під'єднано жодного пристрою, або пристрій, який під'єднано, має неробочий мережний інтерфейс.

На відміну від цього, на виході видно, що інтерфейси FastEthernet0/2 і FastEthernet0/3 працюють. Про це зазначено станом up у стовпцях Status (Стан) та Protocol (Протокол).

11.5.8 **Команда show version**

Команда **show version** може бути використана для перевірки і усунення несправностей деяких базових апаратних і програмних компонентів, що використовуються в процесі завантаження. Натисніть кнопку Відтворити, щоб переглянути відео з більш ранніх курсів, в якому показано пояснення команди **show version**.

11.5.9 **Packet Tracer — Інтерпретація вихідних даних команди show**

Це завдання призначено для закріплення знань про використання команд **show** маршрутизатора. Вам не потрібно буде виконувати конфігурування, але вам необхідно проаналізувати вихідні дані декількох команд show.

Packet Tracer — Інтерпретація результату виконання команди show

Цілі та задачі

Частина 1: Аналіз результату виконання команди show

Частина 2: Питання для самоперевірки

Довідкова інформація

Це завдання призначене для закріплення використання команд **show** на маршрутизаторі. Налаштування виконувати не потрібно, але вам необхідно проаналізувати результати виконання декількох команд **show**. В цьому завданні бали не нараховуються автоматично.

Інструкції

Частина 1: Аналіз результату виконання команди show

a. Для під'єднання до ISPRouter, натисніть на **ISP PC**, потім на вкладку **Desktop**, а потім - **Terminal**.

b. Увійдіть в привілейований режим EXEC.

c. Використовуйте наступні команди **show**, щоб відповісти на запитання для самоперевірки в частині 2.

Примітка: Якщо результат завершується запитом - –More— обов'язково натисніть пробіл, поки не з'явиться рядок **ISPRouter#** для отримання всіх вихідних даних команди.

```
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
```

11.6 Методи пошуку та усунення несправностей

11.6.1 **Основні підходи до пошуку та усунення несправностей**

У попередніх двох темах ви дізналися про деякі утиліти і команди, які можна використовувати для визначення проблемних ділянок у вашій мережі. Це важлива частина усунення несправностей. Існує безліч способів усунення несправностей в мережі. У цій темі детально описаний структурований процес усунення несправностей, який допоможе вам стати кращим мережним адміністратором. Також передбачено ще кілька команд, які допоможуть вирішити проблеми. Проблеми з мережею можуть бути простими або складними і можуть виникнути в результаті поєднання проблем з обладнанням, програмним забезпеченням і під'єднанням. Техніки повинні вміти аналізувати проблему та визначати причину помилки, перш ніж вони зможуть вирішити проблему в мережі. Цей процес називається пошуком і усуненням несправностей.

Загальна та ефективна методологія пошуку та усунення несправностей базується на науковому методі.

У таблиці наведено шість основних кроків у процесі пошуку та усунення несправностей.

Заголовок таблиці	
Крок	**Опис**
Крок 1. Визначення проблеми.	• Це перший крок у процесі усунення несправностей. • Хоча на цьому кроці можна використовувати інструменти, розмова з користувачем часто дуже корисна.
Крок 2. Формування припущень щодо можливої причини несправності.	• Після того, як проблема виявлена, спробуйте сформувати припущення щодо ймовірних причин. • Цей крок часто призводить до більшої кількості можливих причин проблеми.
Крок 3. Перевірка припущень щодо визначення причини несправності	• Виходячи з ймовірних причин, перевірте свої припущення, щоб визначити яка одна з них є причиною проблеми. • Технік часто застосовує швидку процедуру для тестування і перевіряє, чи вирішує вона проблему. • Якщо швидка процедура не виправляє проблему, можливо, знадобиться подальше дослідження проблеми для встановлення точної причини.
Крок 4. Розроблення плану дій та реалізація рішення	Після того, як ви визначили точну причину проблеми, розробіть план дій для вирішення проблеми і реалізуйте рішення.
Крок 5. Перевірка рішення та впровадження превентивних заходів	• Після того, як ви виправили проблему, перевірте повну функціональність. • За необхідності застосуйте профілактичні заходи.
Крок 6. Документування отриманих даних, вжитих заходів та результатів	• На завершальному етапі процесу усунення несправностей задокументуйте свої висновки, дії та результати. • Це дуже важливо для подальшого використання.

Щоб оцінити проблему, визначте, скільки пристроїв в мережі зазнали проблеми. Якщо виникла проблема з одним пристроєм у мережі, запустіть процес виправлення несправностей на цьому пристрої. Якщо виникла проблема з усіма пристроями в мережі, запустіть процес усунення несправностей на пристрої, до якого під'єднані всі інші пристрої. Слід розробити логічний і послідовний метод діагностики мережних проблем шляхом усунення однієї проблеми за раз.

11.6.2 **Вирішення проблеми або її ескалація?**

У деяких ситуаціях неможливо негайно вирішити проблему. Проблему слід загострити, коли вона потребує рішення менеджера, певного досвіду або потрібного рівня доступу до мережі, недоступного фахівцю з усунення несправностей.

Наприклад, після усунення несправностей фахівець робить висновок, що модуль маршрутизатора повинен бути замінений. Цю проблему слід загострити для затвердження менеджером. Менеджеру, можливо, доведеться ще більше загострити проблему, оскільки це може вимагати схвалення фінансового відділу, перш ніж можна придбати новий модуль.

Політика компанії повинна чітко вказати, коли і як фахівець повинен загострити проблему.

11.6.3 **Команда debug**

Процеси ОС, протоколи, механізми і події генерують повідомлення для показу їх статусу. Ці повідомлення можуть надавати цінну інформацію під час виправлення несправностей або перевірки системних операцій. Команда IOS **debug** дозволяє адміністратору відображати ці повідомлення в режимі реального часу для аналізу. Це дуже важливий інструмент для моніторингу подій на пристрої Cisco IOS.

Всі команди **debug** вводяться в привілейованому режимі EXEC. Cisco IOS дозволяє звужувати вихідні дані **debug**, включаючи до них лише відповідну функцію або підфункцію. Це дуже важливо, оскільки налагодженню присвоюється високий пріоритет серед процесів ЦП, і це може зробити систему непридатною для використання. З цієї причини використовуйте команди **debug** тільки для усунення конкретних проблем.
Наприклад, для відстеження стану повідомлень ICMP в маршрутизаторі Cisco використовуйте **debug ip icmp**, як показано в прикладі.

```
R1# debug ip icmp
ICMP packet debugging is on
R1#
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
R1#
```

Щоб переглянути короткий опис всіх параметрів команди налагодження, використовуйте команду **debug ?** в привілейованому режимі EXEC у командному рядку.
Щоб вимкнути певну функцію налагодження, додайте ключове слово **no** перед командою **debug**:

```
Router# no debug ip icmp
```

Крім того, ви можете ввести форму команди **undebug** в привілейованому режимі EXEC:

```
Router# undebug ip icmp
```

Щоб відключити відразу всі активні команди debug, використовуйте команду **undebug all**:

```
Router# undebug all
```

Будьте обережні, використовуючи деякі команди **debug**. Такі команди, як **debug all** і **debug ip packet** генерують значний обсяг вихідних даних і можуть використовувати велику частину системних ресурсів. Маршрутизатор може настільки зайнятись відображенням повідомлень **debug**, що у нього не буде достатньої потужності для

виконання своїх мережних функцій або навіть прослуховування команд, щоб вимкнути налагодження. З цієї причини використання цих параметрів команд не рекомендується, і їх слід уникати.

11.6.4 **Команда terminal monitor**

Під'єднання для надання доступу до інтерфейсу командного рядка IOS можна встановити двома способами:

- **Локально** - локальні під'єднання (тобто консольне під'єднання) вимагають фізичного доступу до консольного порту маршрутизатора або комутатора за допомогою консольного (rollover) кабелю.
- **Віддалено** - віддалені під'єднання вимагають використання Telnet або SSH для встановлення під'єднання до пристрою з налаштованою IP-конфігурацією.

Певні повідомлення IOS автоматично відображаються на консольному під'єднанні, але не на віддаленому під'єднанні. Наприклад, вихідні дані **debug** за замовчуванням відображаються на консольних з'єднаннях. Однак, вихідні дані **debug** не відображаються автоматично на віддалених під'єднаннях. Це пояснюється тим, що повідомлення **debug** - це повідомлення журналу, які не можуть відображатися на vty-лініях.
Наприклад, у наведених нижче вихідних даних, користувач встановив віддалене під'єднання за допомогою Telnet від R2 до R1. Після цього користувач видав команду **debug ip icmp**. Однак команда не змогла відобразити вихідні дані **debug**.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
! No debug output displayed>
```

Щоб відобразити повідомлення журналу на терміналі (віртуальній консолі), використовуйте команду привілейованого режиму EXEC **terminal monitor**. Щоб зупинити реєстрацію повідомлень на терміналі, використовуйте команду привілейованого режиму EXEC **terminal no monitor**.
Наприклад, зверніть увагу, як було введено команду **terminal monitor**, і як команда **ping** відображає вихідні дані **debug**.

```
R1#  terminal monitor
R1# ping 10.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

Примітка: Мета команди **debug** полягає в тому, щоб захопити прямий вихід протягом короткого проміжку часу (тобто від декількох секунд до хвилини або наближено до цього часу). Завжди відключати **debug**, коли не потрібно.

11.6.5 **Питання для самоперевірки - Методи пошуку та усунення несправностей**

1. Технічний фахівець вирішує проблеми з мережею та щойно розробив теорію ймовірних причин. Яким буде наступний крок в процесі усунення несправностей?

   - ◯ Документування отриманих даних, вжитих дій та результатів.
   - ◯ Розроблення плану дій та реалізація рішення
   - ◯ Визначення проблеми.
   - ◯ Перевірка припущень щодо визначення причини несправності
   - ◯ Перевірка рішення та впровадження превентивних заходів

2. Технічний фахівець вирішує проблеми з мережею. Після усунення несправностей, фахівець робить висновок про необхідність заміни комутатора. Що повинен робити фахівець далі?

   - ◯ Надіслати електронною поштою всім користувачам повідомлення про те, що вони замінюють комутатор.
   - ◯ Передати заявку на усунення несправності менеджеру для затвердження змін.
   - ◯ Придбати новий комутатор і замінити несправний.
   - ◯ Вирішити проблему.

3. Технік використовує команду **debug ip icmp** привілейованого режиму EXEC для захоплення вихідних даних маршрутизатора. Які команди будуть зупиняти цю команду **debug** на маршрутизаторі Cisco? (Оберіть два варіанти.)

- [ ] **debug ip icmp off**
- [ ] **no debug debug ip icmp**
- [ ] **no debug ip icmp**
- [ ] **undebug all**
- [ ] **undebug debug ip icmp**

4. Технік встановив віддалене під'єднання до маршрутизатора R1 для спостереження за вихідними даними команди **debug**. Технік вводить команду **debug ip icmp**, після чого пінгує віддалений пункт призначення. Однак, вихідні дані не відображаються. Яку команду потрібно ввести техніку для відображення повідомлень журналу на віддаленому під'єднанні?

- ◯ **monitor debug output**
- ◯ **monitor terminal**
- ◯ **terminal monitor**
- ◯ **terminal monitor debug**

1. Технічний фахівець вирішує проблеми з мережею та щойно розробив теорію ймовірних причин. Яким буде наступний крок в процесі усунення несправностей?

- ◯ Документування отриманих даних, вжитих дій та результатів.
- ◯ Розроблення плану дій та реалізація рішення
- ◯ Визначення проблеми.
- ◉ Перевірка припущень щодо визначення причини несправності
- ◯ Перевірка рішення та впровадження превентивних заходів

2. Технічний фахівець вирішує проблеми з мережею. Після усунення несправностей, фахівець робить висновок про необхідність заміни комутатора. Що повинен робити фахівець далі?

- ◯ Надіслати електронною поштою всім користувачам повідомлення про те, що вони замінюють комутатор.
- ◉ Передати заявку на усунення несправності менеджеру для затвердження змін.
- ◯ Придбати новий комутатор і замінити несправний.
- ◯ Вирішити проблему.

3. Технік використовує команду **debug ip icmp** привілейованого режиму EXEC для захоплення вихідних даних маршрутизатора. Які команди будуть зупиняти цю команду **debug** на маршрутизаторі Cisco? (Оберіть два варіанти.)

- ☐ **debug ip icmp off**
- ☐ **no debug debug ip icmp**
- ☑ **no debug ip icmp**
- ☑ **undebug all**
- ☐ **undebug debug ip icmp**

4. Технік встановив віддалене під'єднання до маршрутизатора R1 для спостереження за вихідними даними команди **debug**. Технік вводить команду **debug ip icmp**, після чого пінгує віддалений пункт призначення. Однак, вихідні дані не відображаються. Яку команду потрібно ввести техніку для відображення повідомлень журналу на віддаленому під'єднанні?

- ◯ **monitor debug output**
- ◯ **monitor terminal**
- ◉ **terminal monitor**
- ◯ **terminal monitor debug**

11.7 Сценарії пошуку та усунення несправностей

11.7.1 Проблеми з дуплексною експлуатацією та невідповідністю налаштувань

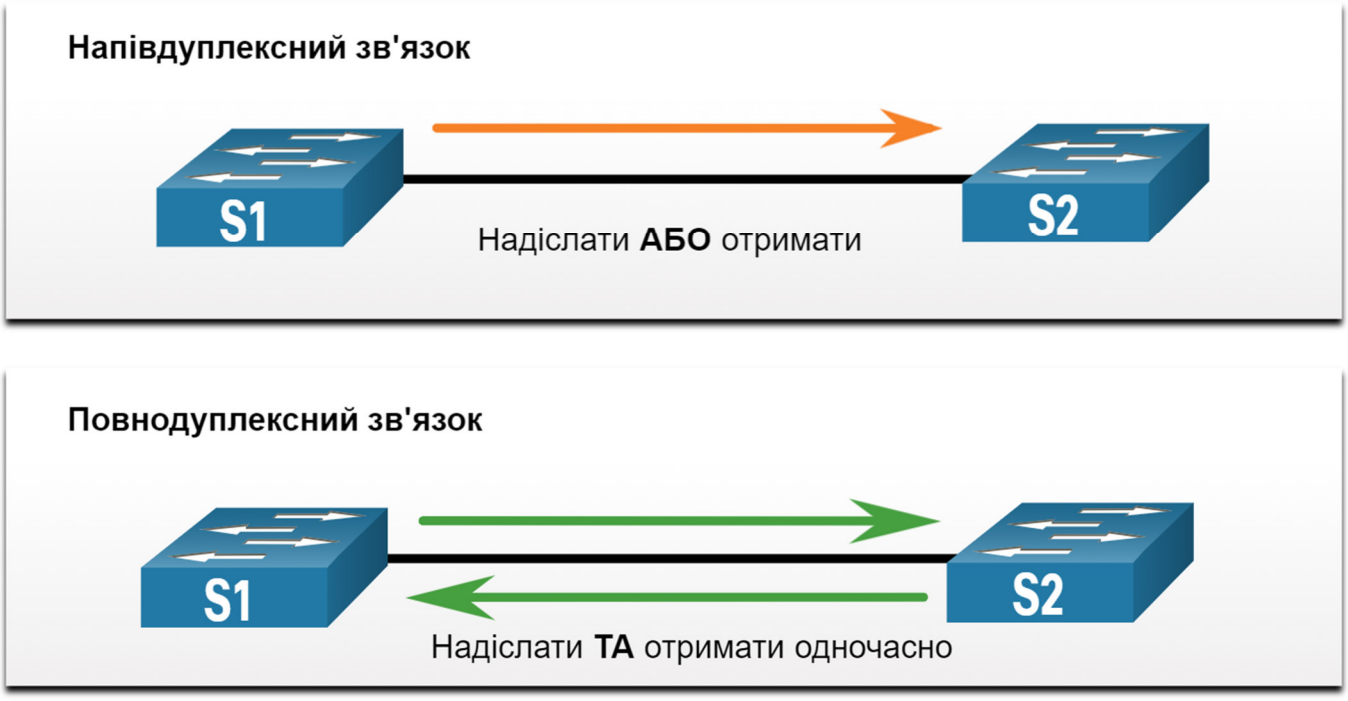
Багато поширених мережних проблем можна виявити та вирішити з невеликими зусиллями. Тепер, коли у вас є інструменти та процес виправлення несправностей мережі, цей розділ розглядає деякі поширені проблеми мережі, які ви, ймовірно, зустрінете у якості адміністратора мережі.

У передачі даних *duplex* посилається на напрямок передачі даних між двома пристроями.

Існує два режими дуплексного зв'язку:

- **Напівдуплекс** - зв'язок обмежений обміном даними одночасно тільки в одному напрямку.
- **Повнодуплексний зв'язок** - зв'язок дозволяє надсилати та отримувати дані одночасно.

На рисунку показано, як працює кожен дуплексний метод.



Інтерфейси Ethernet, що з'єднуються між собою, повинні працювати в одному і тому ж дуплексному режимі, щоб забезпечити найкращу ефективність зв'язку та уникнути неефективності та затримки по лінії зв'язку.

Функція Autonegotation Ethernet полегшує конфігурацію, мінімізує проблеми та максимально збільшує продуктивність зв'язку між двома з'єднувальними мережами Ethernet. Під'єднані пристрої спочатку оголошують підтримувані можливості, а потім обирають режим найвищої продуктивності, підтримуваний обома кінцями. Наприклад, комутатор та маршрутизатор на рисунку успішно автоматично налагодили режим повного дуплексу.

Якщо один з двох під'єднаних пристроїв працює в режимі повного дуплексу, а інший працює в напівдуплексі, виникає невідповідність дуплексу. У той час як передача даних відбуватиметься за допомогою дуплексної невідповідності, продуктивність зв'язку буде дуже низькою.

Дуплексні невідповідності зазвичай викликані неправильно налаштованим інтерфейсом або, в рідкісних випадках, через невдале автоматичне налаштування. Невідповідність дуплексу може бути складно усунути, оскільки зв’язок між пристроями все ще відбувається.

11.7.2 Проблеми з IP-адресацією на пристроях IOS

Проблеми, пов'язані з IP-адресами, швидше за все, не дадуть віддаленим мережним пристроям встановити зв'язок. Оскільки IP-адреси ієрархічні, будь-яка IP-адреса, яка призначена мережному пристрою, має відповідати цьому діапазону адрес у цій мережі. Неправильно призначені IP-адреси створюють різні проблеми, зокрема конфлікти IP-адрес і проблеми маршрутизації.

Двома поширеними причинами неправильного призначення IPv4 є помилки призначення вручну або проблеми, пов'язані з DHCP.

Мережним адміністраторам часто доводиться вручну призначати IP-адреси таким пристроям, як сервери і маршрутизатори. Якщо під час призначення допущена помилка, то є велика ймовірність виникнення проблеми зв'язку з пристроєм.

На пристрої IOS використовуйте команди **show ip interface** або **show ip interface brief**, щоб перевірити, що IPv4-адреси призначені для мережних інтерфейсів. Наприклад, виконання команди **show ip interface brief**, як показано, перевірить стан інтерфейсу на R1.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

11.7.3 Проблеми з IP-адресацією на кінцевих пристроях

У комп'ютерах під керуванням ОС Windows, коли пристрій не може зв'язатися з DHCP-сервером, Windows автоматично призначає адресу, що належить діапазону 169.254.0.0/16. Ця функція називається автоматичним приватним IP-адресуванням (APIPA) і призначена для полегшення зв'язку в локальній мережі. Уявіть, що Windows говорить: "Я буду використовувати цю адресу з діапазону 169.254.0.0/16, тому що я не міг отримати жодної іншої адреси".

Часто комп'ютер з адресою APIPA не зможе спілкуватися з іншими пристроями в мережі, оскільки ці пристрої, швидше за все, не належать до мережі 169.254.0.0/16. Ця ситуація вказує на автоматичну проблему призначення адреси IPv4, яку слід виправити.

Примітка: Інші операційні системи, такі як Linux і OS X, не будуть привласнювати мережному інтерфейсу IPv4-адресу, якщо зв'язок з DHCP-сервером завершиться невдало.

Більшість кінцевих пристроїв налаштовано на сервер DHCP для автоматичного призначення адрес IPv4. Якщо пристрою не вдається зв'язатися з DHCP-сервером, то сервер не може призначити IPv4 адресу для конкретної мережі, і пристрій не зможе встановити зв'язок.

Щоб перевірити IP-адреси, призначені комп'ютеру під керуванням ОС Windows, використовуйте команду **ipconfig**, як показано у прикладі.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

11.7.4 Несправності, пов'язані зі шлюзом за замовчуванням

Шлюз за замовчуванням для кінцевого пристрою - це найближчий мережний пристрій, який може пересилати трафік до інших мереж. Якщо пристрій має неправильну або неіснуючу адресу шлюзу за замовчуванням, він не зможе встановлювати зв'язок з пристроями у віддалених мережах. Оскільки шлюзом за замовчуванням є шлях до віддалених мереж, його адреса повинна належати тій самій мережі, що і кінцевий пристрій.

Адресу шлюзу за замовчуванням можна встановити вручну або отримати з DHCP-сервера. Подібно до проблем з вирішенням IPv4, проблеми шлюзу за замовчуванням можуть бути пов'язані з неправильною конфігурацією (у випадку призначення вручну) або проблемами DHCP (якщо використовується автоматичне призначення).

Щоб вирішити неправильно налаштовані проблеми шлюзу, переконайтеся, що на пристрої налаштовано правильний шлюз за замовчуванням. Якщо адреса за замовчуванням була встановлена вручну, але неправильно, просто замініть її відповідною адресою. Якщо адреса шлюзу за замовчуванням була встановлена автоматично, переконайтеся, що пристрій може встановлювати зв'язок з DHCP-сервером. Важливо також перевірити, чи правильно IPv4-адреса і маска підмережі були налаштовані на інтерфейсі маршрутизатора і що інтерфейс активний.

Щоб перевірити шлюз за замовчуванням на комп'ютерах під керуванням Windows, використовуйте команду **ipconfig**, як показано.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

На маршрутизаторі використовуйте команду **show ip route**, щоб переглянути таблицю маршрутизації та переконатися, що шлюз за замовчуванням, відомий як маршрут за замовчуванням, встановлений. Цей маршрут використовується, коли адреса призначення пакету не відповідає жодним іншим маршрутам у таблиці маршрутизації.

Наприклад, вихідні дані показують, що R1 має шлюз за замовчуванням (тобто шлюз останньої інстанції) налаштований на IP-адресу 209.168.200.226.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
```

```
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
O        209.165.200.228/30
         [110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0
R1#
```

Перший виділений рядок говорить про те, що це шлюз (тобто 0.0.0.0) і будь який пакет повинен бути відправлений на IP-адресу 209.165.200.226. Другий виділений рядок відображає, як R1 дізнався про шлюз за замовчуванням. В цьому випадку R1 отримав інформацію від іншого маршрутизатора з підтримкою OSPF.

11.7.5 Пошук та усунення несправностей, пов'язаних з DNS

Служба доменних імен (DNS) - це автоматизована служба, яка співставляє імена, наприклад www.cisco.com з IP-адресами. Хоча перетворення імен DNS не має вирішального значення для зв'язку пристрою, це дуже важливо для кінцевого користувача.

Для користувачів прийнято помилково пов'язувати роботу інтернет-посилання з доступністю DNS. Скарги користувачів, такі як «мережа не працює» або «Інтернет не працює», часто викликані недоступним DNS-сервером. Хоча маршрутизація пакетів і всі інші мережні служби все ще працюють, DNS-збої часто призводять користувача до неправильного висновку. Якщо користувач вводить доменне ім’я, наприклад www.cisco.com у веб-браузері, і DNS-сервер недоступний, ім'я не буде переведено на IP-адресу та веб-сайт не відображатиметься.

Адреси DNS-серверів можуть бути призначені вручну або автоматично. Мережні адміністратори часто відповідають за ручне призначення адрес DNS-серверів на серверах і інших пристроях, в той час як DHCP використовується для автоматичного призначення адрес DNS-серверів клієнтам.

Хоча для компаній і організацій це звичайне керування власними DNS-серверами, для розпізнавання імен можна використовувати будь-який доступний DNS-сервер. Користувачі малого офісу та домашнього офісу (SOHO) часто розраховують на DNS-сервер, який підтримує їх Інтернет-провайдер для вирішення імен. DNS-сервери, підтримувані ISP, призначаються клієнтам SOHO через DHCP. Крім того, Google підтримує публічний DNS-сервер, який може бути використаний будь-ким, і це дуже корисно для тестування. Адреса IPv4 публічного DNS-сервера Google становить 8.8.8.8 і 2001:4860:4860:: 8888 для DNS-адреси IPv6.

Cisco пропонує OpenDNS, який забезпечує захищену службу DNS, фільтруючи фішингові та деякі сайти шкідливих програм. Ви можете змінити адресу DNS на 208.67.222.222 і 208.67.220.220 в полях "Бажаний DNS-сервер" і "Альтернативний DNS-сервер". Для домашнього та корпоративного використання доступні розширені функції, такі як фільтрування веб-вмісту та безпека.

Використовуйте команду **ipconfig /all** як показано, щоб перевірити, який DNS-сервер використовується на комп'ютері з ОС Windows.

```
C:\Users\PC-A> ipconfig /all
(Output omitted)
Wireless LAN adapter Wi-Fi:
```

```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 208.67.222.222
   NetBIOS over Tcpip. . . . . . . . : Enabled
(Output omitted)
```

Команда **nslookup** є ще одним корисним інструментом усунення несправностей DNS для ПК. За допомогою команди **nslookup** користувач може вручну відправляти DNS-запити і аналізувати DNS-відповіді.
Команда **nslookup** показує вихідні дані запиту для www.cisco.com. Зверніть увагу, що ви також можете просто ввести IP-адресу і команда **nslookup** поверне ім'я.

```
C:\Users\PC-A> nslookup
Default Server:  Home-Net
Address:  192.168.1.1
> cisco.com
Server:  Home-Net
Address:  192.168.1.1
Non-authoritative answer:
Name:    cisco.com
Addresses:  2001:420:1101:1::185
          72.163.4.185
```

```
> 8.8.8.8
Server:  Home-Net
Address:  192.168.1.1
Name:    dns.google
Address:  8.8.8.8
>
> 208.67.222.222
Server:  Home-Net
Address:  192.168.1.1
Name:    resolver1.opendns.com
Address:  208.67.222.222
>
```

Лабораторна робота - Проектування та побудова мережі невеликого підприємства

Цілі та задачі

Пояснити, як створюється, налаштовується та перевіряється невелика мережа безпосередньо пов'язаних сегментів.

Довідкова інформація /Сценарій

Примітка: Це завдання найкраще виконувати в групах по 2-3 студенти.

Проектування і побудова мережі з нуля.

- Ваш дизайн повинен включати мінімум один маршрутизатор Cisco 4321, два комутатори Cisco 2960 і два ПК.
- Повністю налаштуйте мережу і використовуйте IPv4 або IPv6 (підмережа повинна бути включена як частина вашої схеми адресації).
- Перевірте мережу за допомогою принаймні п'яти команд show.
- Захистіть мережу за допомогою SSH, захищених паролів і паролів на консольній лінії (мінімум).

Створіть критерії, які будуть використовуватися для неформального оцінювання колегами. Представте свій Capstone Project на заняттях та дайте відповідь на запитання колег та інструктора!

Необхідні ресурси

- Packet Tracer
- Критерії, створені студентом / групою, для оцінки завдання

Запитання для самоперевірки

1. Що було найважчою частиною цього завдання?

2. Чому, на вашу думку, мережна документація настільки важлива у цьому завданні і в реальному світі?

11.8.4 **Що ми вивчили у цьому розділі?**

Пристрої у невеликій мережі

Невеликі мережі зазвичай мають одне під'єднання WAN, що забезпечується DSL, кабелем або Ethernet з'єднанням. Невеликими мережами керує місцевий IT-фахівець або нештатний фахівець (за контрактом). Факторами, які слід враховувати при виборі мережних пристроїв для невеликої мережі, є вартість, швидкість і типи портів/інтерфейсів, масштабованість, а також функції і сервіси ОС. При реалізації мережі створіть схему IP-адресації і використовуйте її на кінцевих пристроях, серверах і периферійних пристроях, а також на проміжних пристроях. Резервування може здійснюватися шляхом установки дублювального обладнання, але це також можна вирішити шляхом надання повторюваних мережних зв'язків для критичних областей. Маршрутизатори та комутатори в невеликій мережі повинні бути налаштовані на підтримку трафіку в режимі реального часу, наприклад голосового та відео, відповідно до іншого трафіку даних. Насправді, вдала побудова мережі дозволить реалізувати якість обслуговування (QoS), щоб ретельно класифікувати трафік за пріоритетом.

Застосунки та протоколи невеликої мережі

Існує дві форми програм або процесів, що забезпечують доступ в мережу: мережні застосунки і сервіси прикладного рівня. Деякі застосунки кінцевих користувачів реалізують протоколи прикладного рівня та мають можливість безпосередньо встановлювати зв'язок з нижніми рівнями стеку протоколів. Поштові клієнти та веб-браузери є прикладами цього типу застосунків. Інші програми можуть потребувати допомоги сервісів прикладного рівня для використання мережних ресурсів, таких як передача файлів і тимчасове зберігання даних мережного друку. Це програми, які взаємодіють з мережею і готують дані до передачі. Два найпоширеніших рішення віддаленого доступу - Telnet та Secure Shell (SSH). Сервіс SSH є безпечною альтернативою Telnet. Адміністратори мережі також повинні підтримувати загальні мережні сервери та необхідні пов'язані з ними мережні протоколи, такі як веб-сервер, сервер електронної пошти, сервер FTP, DHCP-сервер і DNS-сервер. Сьогодні підприємства все частіше використовують IP-телефонію та потокове медіа для спілкування з клієнтами та діловими партнерами. Це застосунки для передачі даних в режимі реального часу Мережна інфраструктура повинна підтримувати VoIP, IP-телефонію та інші програми в режимі реального часу.

Масштабування до більших мереж

Для масштабування мережі потрібно кілька елементів: документація мережі, інвентаризація пристроїв, бюджет і аналіз трафіку. Важливо розуміти тип трафіку, який перетинає мережу, а також поточний трафік. Захоплення трафіку під час пікового використання, щоб отримати гарне уявлення про різні типи трафіку і виконати захоплення на різних сегментах мережі і пристроях, оскільки деякий трафік буде локальним для певного сегмента. Адміністратори мережі повинні знати, як змінюється використання мережі. Інформація про використання комп’ютерів працівників може бути захоплено в 'знімок' за допомогою таких інструментів, як диспетчер завдань Windows, Переглядач подій та Використання даних.

Перевірка з'єднання

Команда **ping** є найефективнішим способом швидко перевірити зв'язок рівня 3 між IP-адресою джерела та призначення. Команда також відображає різні статистичні дані часу в обидва кінці. Cisco IOS пропонує розширений режим команди ping, який дозволяє користувачеві створювати спеціальні типи пінгів шляхом налаштування параметрів, пов'язаних з командною операцією. Розширена команда ping вводиться в привілейованому режимі EXEC шляхом введення ping без IP-адреси призначення. Команда Traceroute може допомогти знайти проблемні зони рівня 3 в мережі. trace повертає список хопів, коли пакет направляється через мережу. Воно може бути використано для визначення точки на шляху, де проблема може бути знайдена. У Windows команда **tracert**. У Cisco IOS команда **traceroute**. Також існує розширена команда **traceroute**. Вона дозволяє адміністратору налаштовувати параметри, пов'язані з командною операцією. Вихідні дані, отримані в результаті використання мережних команд, надають дані для внесення в базовий рівень мережі. Одним із способів запуску базового рівня є копіювання та вставлення результатів виконання команди ping, trace або інших відповідних команд у текстовий файл. Ці текстові файли можуть бути позначені часом з датою і збережені до архіву для подальшого пошуку та порівняння.

Команди вузла та IOS

Адміністратори мережі переглядають інформацію про IP-адресацію (адресу, маску, маршрутизатор та DNS) на вузлі з ОС Windows, видаючи команду **ipconfig**. Інші необхідні команди **ipconfig /all**, **ipconfig /release** і **ipconfig /renew**, і **ipconfig /displaydns**. Перевірка параметрів IP за допомогою графічного інтерфейсу на комп'ютері з Linux буде відрізнятися залежно від дистрибутива Linux і інтерфейсу робочого столу. Необхідні команди **ifconfig**, і **ip address**. У графічному інтерфейсі вузла з MacOS відкрийте Network Preferences > Advanced, щоб отримати інформацію про IP-адресацію. Інші команди IP-адресації для Mac **ifconfig**, **networksetup -listallnetworkservices** і **networksetup -getinfo** <*network service*>.
Команда **arp** виконується з командного рядка Windows, Linux або Mac. Команда надає можливість отримати перелік всіх пристроїв, які на даний час є в ARP-кеші вузла, а також адресу IPv4, фізичну адресу і тип адресації (статичний/динамічний) для кожного пристроїв. Команда **arp -a** відображає відому IP-адресу та прив'язку MAC-адреси. Загальні команди **show show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, і **show version**. Команда **show cdp neighbor** надає такі відомості про кожний пристрій CDP сусіда: ідентифікатори, список адрес, ідентифікатор порту, список можливостей і платформи. **Команда show cdp neighbors detail допоможе визначити, чи є у одного з сусідів CDP помилка конфігурації IP. Вихідні дані команди show ip interface brief** відображають всі інтерфейси на маршрутизаторі, IP-адреси, присвоєні кожному інтерфейсу, якщо такі є, і стан інтерфейсів.

Методи пошуку та усунення несправностей

Крок 1. Визначення проблеми.

Крок 2. Формування припущень щодо можливої причини несправності.

Крок 3. Перевірка припущень щодо визначення причини несправності.

Крок 4. Розроблення плану дій та реалізація рішення

Крок 5. Перевірка рішення та впровадження превентивних заходів

Крок 6. Документування отриманих даних, вжитих дій та результатів.

Проблему слід загострити, коли вона потребує рішення менеджера, певного досвіду або потрібного рівня доступу до мережі, недоступного фахівцю з усунення несправностей. Процеси ОС, протоколи, механізми і події генерують повідомлення для передачі їх статусу. Команда IOS **debug** дозволяє адміністратору відображати ці повідомлення в режимі реального часу для аналізу. Щоб відобразити повідомлення журналу на терміналі (віртуальній консолі), використовуйте команду привілейованого режиму EXEC **terminal monitor**.

Сценарії пошуку та усунення несправностей

Існує два режими дуплексного режиму зв'язку: напівдуплексний і повнодуплексний. Якщо один з двох під'єднаних пристроїв працює в режимі повного дуплексу, а інший працює в напівдуплексі, виникає невідповідність дуплексу. У той час як передача даних відбуватиметься за допомогою дуплексної невідповідності, продуктивність зв'язку буде дуже низькою.

Неправильно призначені IP-адреси створюють різні проблеми, зокрема конфлікти IP-адрес і проблеми маршрутизації. Двома поширеними причинами неправильного призначення IPv4 є помилки призначення вручну або пов'язані з DHCP проблеми. Більшість кінцевих пристроїв налаштовано на сервер DHCP для автоматичного призначення адрес IPv4. Якщо пристроїв не вдається зв'язатися з DHCP-сервером, то сервер не може призначити IPv4 адресу для конкретної мережі, і пристрій не зможе встановити зв'язок.

Шлюз за замовчуванням для кінцевого пристроїв - це найближчий мережний пристрій, який може пересилати трафік до інших мереж. Якщо пристрій має неправильну або неіснуючу адресу шлюзу за замовчуванням, він не зможе встановлювати зв'язок з пристроями у віддалених мережах. Оскільки шлюзом за замовчуванням є шлях до віддалених мереж, його адреса повинна належати тій самій мережі, що і кінцевий пристрій.

Збої DNS часто приводять користувача до висновку, що мережа не працює. Якщо користувач вводить доменне ім’я, наприклад www.cisco.com у веб-браузері, і DNS-сервер недоступний, ім'я не буде переведено на IP-адресу та веб-сайт не відображатиметься.

11.8 Контрольна робота

11.8.5 **Контрольна робота з розділу - Створення невеликої мережі**

1. Яке рішення проектування мережі було б більш важливішим для великої корпорації, ніж для малого бізнесу?

   - ◯ міжмережний екран (firewall)
   - ◯ надмірність
   - ◯ комутатор портів низької концентрації
   - ◯ Інтернет-маршрутизатор

2. Нещодавно найнятому мережному технікові доручено замовити нове обладнання для малого бізнесу з великим прогнозом зростання. Яким першочерговим фактором повинен перейматися технік при виборі нових пристроїв?

   - ◯ резервні пристрої
   - ◯ пристрої, які мають підтримку моніторингу мережі
   - ◯ пристрої з підтримкою модульності
   - ◯ пристрої з фіксованим числом і типом інтерфейсів

3. Який тип трафіку, найімовірніше, матиме найвищий пріоритет в мережі?

- ◯ FTP
- ◯ Миттєвий обмін повідомленнями
- ◯ SNMP
- ◯ голос

4. Мережний спеціаліст вивчає мережне з'єднання ПК з віддаленим вузлом з адресою 10.1.1.5. Яка команда, видана ПК з ОС Windows, відобразить шлях до віддаленого вузла?

- ◯ **trace 10.1.1.5**
- ◯ **tracert 10.1.1.5**
- ◯ **traceroute 10.1.1.5**
- ◯ **ping 10.1.1.5**

5. Користувач не може отримати доступ до веб-сайту під час набору тексту **ht tp://www.cisco.com** у веб-браузері, але може досягти того самого сайту, ввівши **http://72.163.4.161**. В чому проблема?

- ◯ Стек протоколів TCP/IP
- ◯ DNS
- ◯ DHCP
- ◯ шлюз по замовчуванню (default gateway)

6. Куди за замовчуванням надсилаються вихідні повідомлення про налагодження Cisco IOS?

- буфери пам'яті
- консольна лінія
- vty лінії
- Syslog сервер

7. Який елемент масштабування мережі передбачає виявлення фізичних і логічних топологій?

- аналіз трафіку
- інвентаризація пристрою
- документація мережі
- аналіз витрат

8. Який механізм можна реалізувати в невеликій мережі, щоб зменшити затримку мережі для потокових програм у режимі реального часу?

- ICMP
- AAA
- QoS
- PoE

9. Який процес завершився невдало, якщо комп'ютер не має доступу до Інтернету та отримав IP-адресу 169.254.142.5?

- ◯ IP
- ◯ DNS
- ◯ HTTP
- ◯ DHCP

10. Невелика компанія має в якості точки виходу до свого провайдера всього один маршрутизатор. Яке рішення може бути прийняте для підтримання під'єднання , якщо сам маршрутизатор або його з'єднання з провайдером не вдається?

- ◯ Активуйте інший інтерфейс маршрутизатора, який під'єднаний до провайдера, щоб трафік міг проходити через нього.
- ◯ Майте другий маршрутизатор, під'єднаний до іншого провайдера.
- ◯ Придбайте другий канал з мінімальною вартістю у іншого провайдера, щоб під'єднатися до цього маршрутизатора.
- ◯ Додайте більше інтерфейсів до маршрутизатора, який під'єднаний до внутрішньої мережі.

11. Коли адміністратор повинен встановити базовий рівень мережі?

- ◯ через певні проміжки часу
- ◯ в найнижчій точці трафіку в мережі
- ◯ при різкому падінні трафіку
- ◯ коли трафік знаходиться на піку в мережі

12. Які два типи трафіку вимагають чутливої до затримки доставки? (Оберіть два варіанти.)

- ☐ голос
- ☐ Електронна пошта (Email)
- ☐ FTP
- ☐ web
- ☐ відео

13. Мережний спеціаліст підозрює, що певне мережне з'єднання між двома комутаторами Cisco має дуплексну невідповідність. Яку команду спеціаліст використає для перегляду деталей рівня 1 та рівня 2 щодо порту комутатора?

- ◯ **show running-config**
- ◯ **show interfaces**
- ◯ **show mac-address-table**

14. Яке твердження вірне і стосується CDP на пристрої Cisco?

- ◯ Щоб відключити CDP глобально, потрібно використовувати команду **no cdp enable** в режимі конфігурації інтерфейсу.
- ◯ Оскільки він працює на канальному рівні, протокол CDP може бути реалізований тільки на комутаторах.
- ◯ Команда **show cdp neighbor detail** виявить IP-адресу сусіда тільки при наявності під'єднання рівня 3.
- ◯ CDP можна відключити глобально або на певному інтерфейсі.

15. Який фактор слід враховувати при проектуванні невеликої мережі при виборі пристроїв?

- ◯ аналіз трафіку
- ◯ надмірність
- ◯ вартість приладів
- ◯ ISP (провайдер послуг Інтернет)