

Комп'ютерні мережі

Матеріали для самостійного
вивчення (частина 2)

Створено на засадах курсів академії CISCO



Зміст

Визначення адрес

Адресація IPv4

Адресація IPv6

Протокол ICMP v4/v6

Транспортний рівень

Протоколи прикладного рівня

Створення невеликої мережі

Обладнання та приклади налаштування

Визначення адрес



Мета підтеми

Мета розділу: Пояснити, як ARP і ND дозволяють спілкуватися у мережі.

Назва теми	Мета вивчення теми
MAC- та IP-адреси	Порівняти ролі MAC-адрес та IP-адрес.
ARP	Описати призначення ARP.
Виявлення сусіда	Описати процес виявлення сусіда в IPv6.

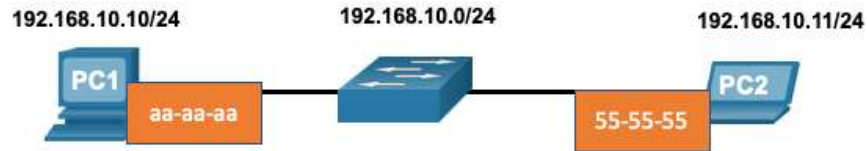
MAC- та IP-адреси

Пункт призначення у тій же мережі

Пристрою у локальній мережі Ethernet призначаються дві основні адреси:

- **Фізична адреса Рівня 2 (MAC-адреса)** – використовується для комунікації між мережними картами (NIC) в одній мережі Ethernet.
- **Логічна адреса Рівня 3 (IP-адреса)** – використовується для відправлення пакета від джерела до кінцевого пункту призначення.

Адреси Рівня 2 використовуються для доставки кадрів з одного мережного адаптера до іншого в одній мережі. Якщо IP-адреса призначення знаходиться у тій самій мережі, MAC-адресою призначення буде адреса пристрою-отримувача.

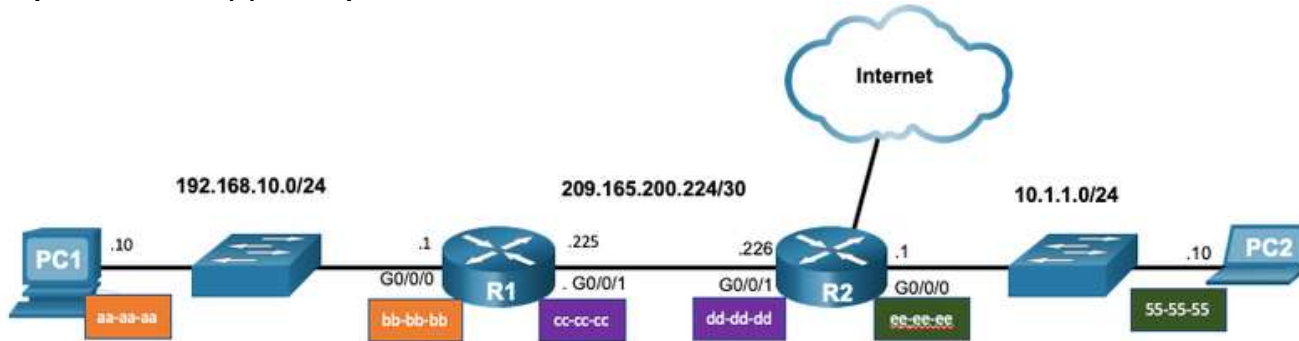


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Пункт призначення у віддаленій мережі

Якщо IP-адреса призначення знаходиться у віддаленій мережі, MAC-адресою призначення буде адреса шлюзу за замовчуванням.

- IPv4 використовує ARP, щоб пов'язати IPv4-адресу пристрою з MAC-адресою його мережного адаптера.
- IPv6 використовує ICMPv6, щоб пов'язати IPv6-адресу пристрою з MAC-адресою його мережного адаптера.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

ARP

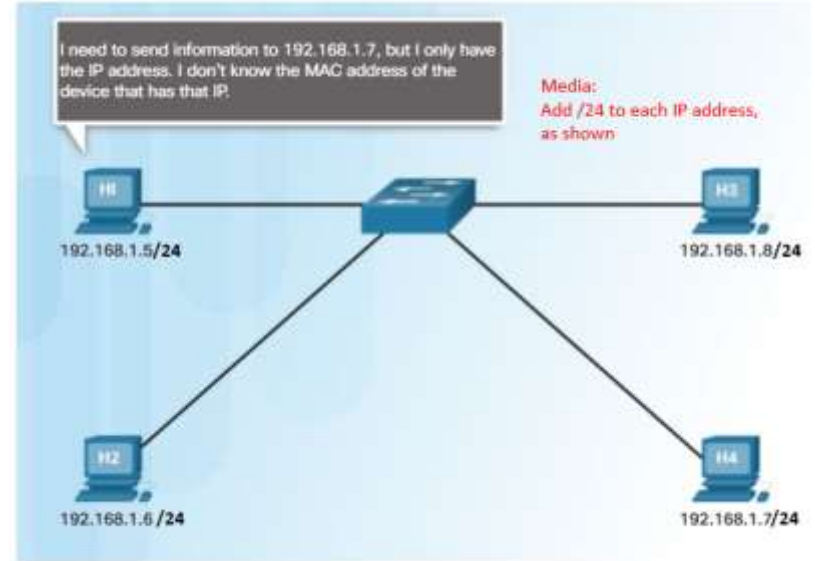
ARP

Огляд ARP

Пристрій використовує ARP для визначення MAC-адреси призначення локального пристрою, коли відома його IPv4-адреса.

ARP забезпечує дві основні функції:

- Перетворення IPv4-адреси у MAC-адресу
- Ведення ARP-таблиці відповідності між адресами IPv4 і MAC-адресами.



ARP

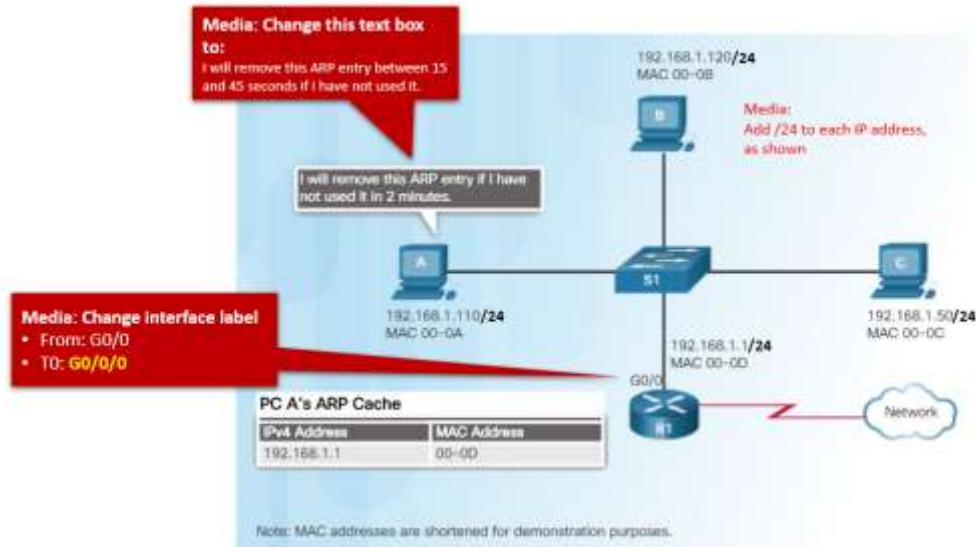
Функції ARP

Для надсилання кадру пристрій шукатиме в ARP-таблиці MAC-адресу, що відповідає IPv4-адресі призначення.

- Якщо IPv4-адреса призначення пакета знаходиться у тій самій мережі, що і IPv4 адреса джерела, пристрій буде шукати в ARP-таблиці запис для IPv4-адреси призначення.
- Якщо IPv4-адреса призначення знаходиться в іншій мережі, пристрій визначатиме за таблицею ARP IPv4-адресу шлюзу за замовчуванням.
- Якщо пристрій знаходить IPv4-адресу, то відповідна їй MAC-адреса використовується у кадрі як MAC-адреса призначення.
- Якщо жодного запису в ARP-таблиці не знайдено, пристрій надсилає ARP-запит.

ARP Видалення записів з ARP-таблиці

- Записи в ARP-таблиці не є постійними і видаляються, коли таймер ARP-кешу обнуляється після вказаного періоду часу.
- Цей період може бути різним і залежить від операційної системи пристрою.
- Записи ARP-таблиці також можуть видалятися вручну адміністратором.



ARP

ARP таблиці на мережних пристроях

- Команда `show ip arp` виводить ARP-таблицю на маршрутизаторі Cisco.
- Команда `arp -a` відображає ARP-таблицю на ПК під керуванням Windows 10.

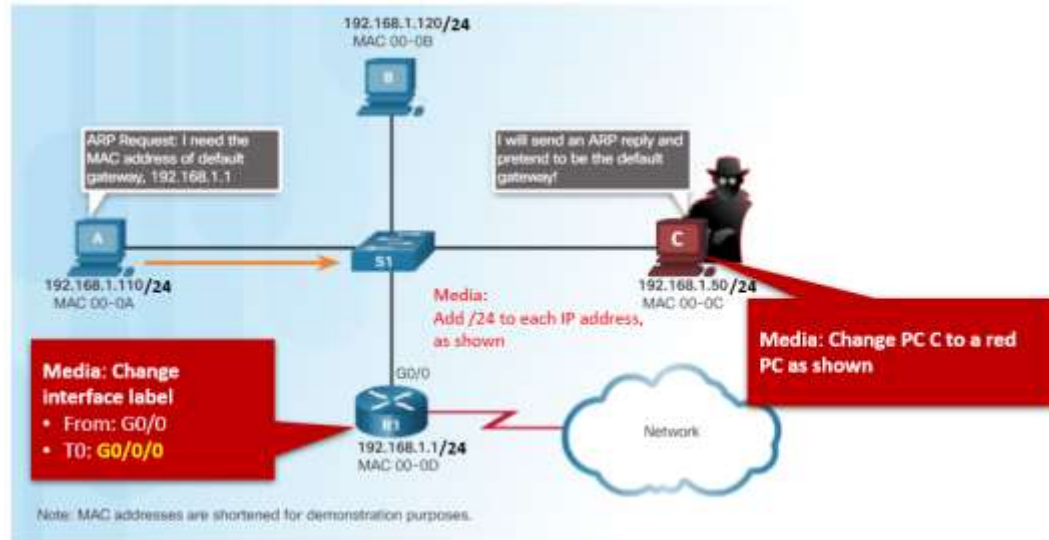
```
R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0
```

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

Interface: 192.168.1.124 --- 0x10
    Internet Address Physical Address Type
    192.168.1.1 c8-d7-19-cc-a0-86 dynamic
    192.168.1.101 08-3e-0c-f5-f7-77 dynamic
```

Проблеми ARP – Широкомовні розсилки ARP та ARP spoofing (підміна)

- ARP-запити отримують та обробляють всі пристрої в локальній мережі.
- Надмірні широкомовні розсилки ARP можуть викликати деяке зниження продуктивності.
- ARP-відповіді можуть бути підроблені зловмисником для здійснення атаки "отруєння" ARP (підробки ARP-кешу).
- Комутатори корпоративного рівня містять засоби пом'якшення наслідків для захисту від ARP-атак.



Packet Tracer – Дослідження ARP-таблиці

У Packet Tracer ви виконаєте такі завдання:

- Дослідження ARP-запитів
- Дослідження таблиці MAC-адрес комутатора
- Дослідження процесу ARP з віддаленим зв'язком

Виявлення сусіда

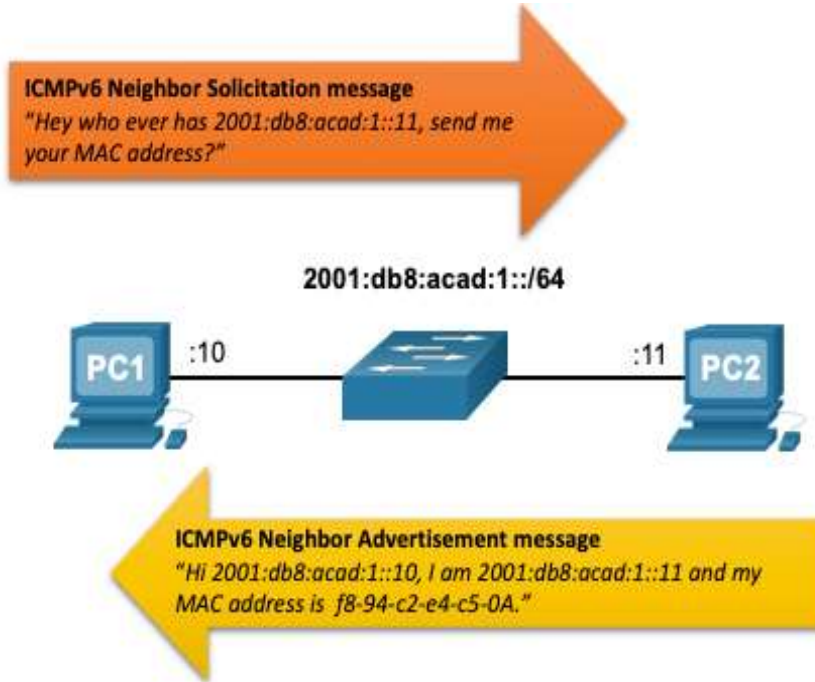
Повідомлення ND IPv6

Протокол IPv6 Виявлення сусіда (ND) забезпечує:

- Визначення адрес
- Виявлення маршрутизатора
- Послуги перенаправлення
- Повідомлення ICMPv6 Запит сусіда та Анонсування сусіда використовуються для обміну повідомленнями між пристроями, наприклад, для визначення адреси.
- Повідомлення ICMPv6 Запит маршрутизатора та Анонсування маршрутизатора призначені для обміну повідомленнями між пристроями та маршрутизаторами.
- Повідомлення переадресації ICMPv6 використовуються маршрутизаторами для кращого вибору наступного переходу.

Виявлення сусіда IPv6

ND IPv6 - Визначення адрес



- Пристрої IPv6 використовують Визначення сусіда (ND) для визначення MAC-адреси пристрою за відомою адресою IPv6.
- Повідомлення ICMPv6 Запит сусіда надсилаються за допомогою спеціальних групових Ethernet- і IPv6-адрес.

Що ми вивчили у цій підтемі?

- Фізичні адреси Рівня 2 (тобто, MAC-адреси Ethernet) використовуються для передавання кадру канального рівня з інкапсульованим IP-пакетом від однієї мережної карти до іншої в одній мережі.
- Якщо IP-адреса призначення знаходиться в тій самій мережі, MAC-адресою призначення буде адреса пристрою-отримувача.
- Якщо IP-адреса (IPv4 чи IPv6) призначення перебуває у віддаленій мережі, MAC-адресою призначення буде адреса шлюзу за замовчуванням (тобто інтерфейс маршрутизатора).
- Пристрій IPv4 використовує ARP для визначення MAC-адреси призначення локального пристрою, коли відома його IPv4 -адреса.
- ARP забезпечує дві основні функції: зіставлення IPv4-адрес із MAC-адресами і ведення таблиці відповідності IPv4- до MAC-адрес.
- Після отримання ARP-відповіді, пристрій додає IPv4-адресу та відповідну MAC-адресу до своєї ARP-таблиці.
- На кожному пристрої є таймер кешу ARP, який видаляє з таблиці ARP записи, що не використовувались протягом зазначеного періоду часу.
- Для визначення MAC-адрес IPv6 не замість ARP використовує протокол ND.
- Зокрема, пристрій IPv6 використовує ND протоколу ICMPv6 для визначення MAC-адреси призначення локального пристрою, коли відома його IPv6-адреса.

Нові терміни та команди

- Address Resolution Protocol (ARP)
- ARP-таблиця
- show ip arp
- arpr -a
- Протокол виявлення сусідів (ND або NDP - Neighbor Discovery Protocol)
- Повідомлення ICMPv6 Запит сусіда (NS - Neighbor Solicitation)
- Повідомлення ICMPv6 Анонсування сусіда (NA - Neighbor Advertisement)
- Повідомлення ICMPv6 Запит маршрутизатора (RS - Router Solicitation)
- Повідомлення ICMPv6 Анонсування маршрутизатора (RA - Router Advertisement)
- Повідомлення ICMPv6 перенаправлення

Адресація IPv4



Завдання

Завдання підтеми: Обчислити схему підмережі IPv4, щоб ефективно сегментувати мережу.

Назва теми	Мета вивчення теми
Структура адреси IPv4	Описати структуру адреси IPv4, включаючи мережну частину, вузлову частину та маску підмережі.
Одноадресна, широкомовна та групова розсилки IPv4	Порівняти характеристики та способи використання одноадресних, широкомовних і групових адрес IPv4.
Типи IPv4 адрес	Пояснити публічні, приватні та зарезервовані IPv4-адреси.
Сегментація мережі	Пояснити як підмережі сегментують мережу для забезпечення кращої комунікації.
Розподіл мережі IPv4 на підмережі	Обчислити підмережі IPv4 для префікса /24.

Завдання розділу (Продовж.)

Назва розділу: Адресація IPv4

Завдання розділу: Обчислити схему підмережі IPv4, щоб ефективно сегментувати мережу.

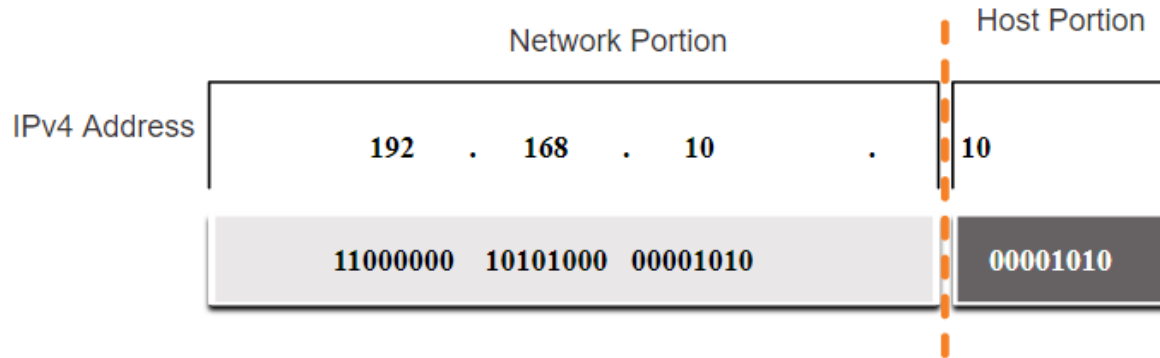
Назва теми	Мета вивчення теми
Розподіл на підмережі з префіксом /16 і /8	Обчислити підмережі IPv4 для префікса /16 і /8.
Розподіл на підмережі відповідно до вимог	Враховуючи набір вимог до підмережі, реалізувати схему адресації IPv4.
Маска підмережі змінної довжини	Пояснити, як створити гнучку схему адресації за допомогою маски підмережі змінної довжини (VLSM).
Структуроване проектування	Реалізувати схему адресації VLSM.

Структура адреси IPv4

Структура адреси IPv4

Мережна та вузлова частини

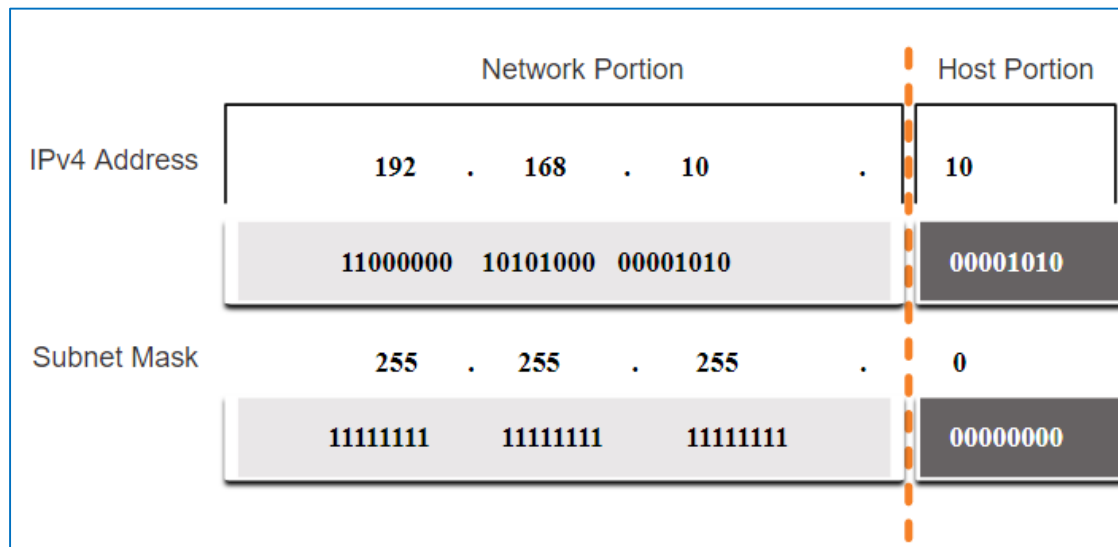
- Адреса IPv4 - це 32-розрядна ієрархічна адреса, яка складається з мережної частини та вузлової частини.
- Визначаючи мережну частину чи вузлову частину, необхідно звернути увагу не на десяткове значення, а на 32-бітну послідовність, яку показано на рисунку.
- Маска підмережі використовується для визначення мережної та вузлової частини.



Структура адреси IPv4

Маска підмережі

- Для ідентифікації мережної і вузлової частини IPv4-адреси маска підмережі побітово порівнюється з IPv4-адресою зліва направо, як показано на рисунку.
- На практиці процес, який використовується для визначення мережної частини та вузлової частини називається логічною операцією І (AND).



Структура адреси IPv4

Довжина префікса

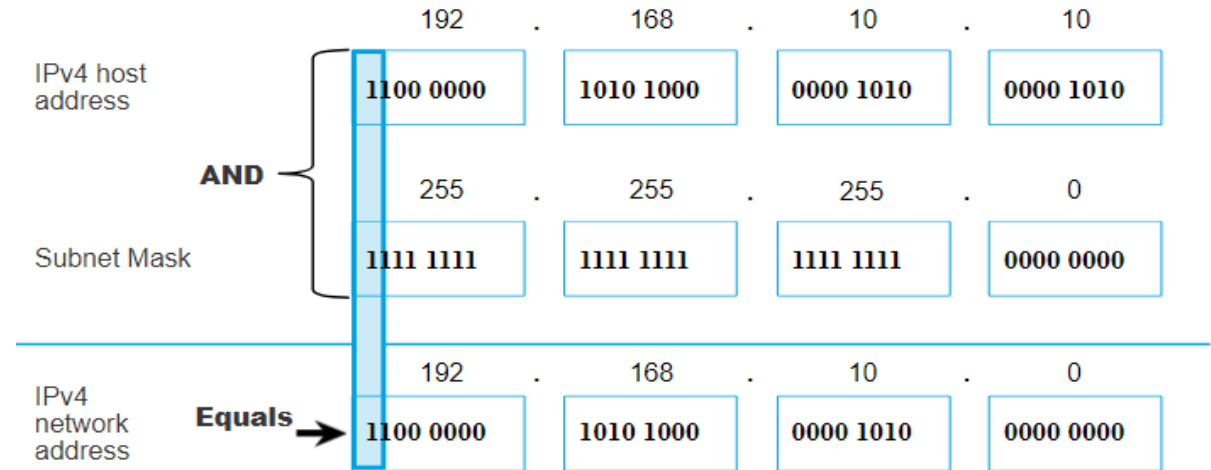
- Довжина префікса - це простіший метод, який використовується для визначення адреси маски підмережі.
- Довжина префікса - це кількість бітів, встановлених в одиницю (1) у масці підмережі.
- Маска підмережі позначається скісною рисою («/»), за якою вказується кількість бітів, встановлених в 1.

Маска підмережі	32-бітна IP-адреса	Префікс Довжина
255.0.0.0	11111111.00000000.00000000.0000000000	/8
255.255.0.0	11111111.11111111.00000000.0000000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.1111100	/30

Визначення мережі: Логічна операція I

- Операція I використовується для визначення адреси мережі.
- Логічна операція I (AND) - це порівняння двох бітів, де тільки 1 I 1 призведе до 1, а будь-яка інша комбінація - до 0.
- Логічна операція I $1 I 1 = 1$, $0 I 1 = 0$, $1 I 0 = 0$, $0 I 0 = 0$, де 1 = Правда (True) і 0 = Неправда (False).

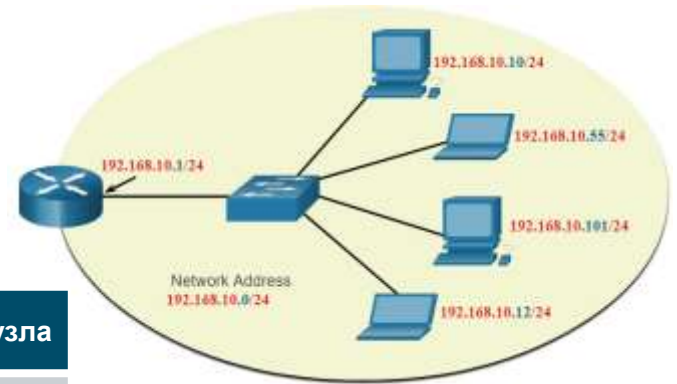
- Щоб визначити мережну IPv4-адресу вузла для IPv4-адреси та маски підмережі побітово виконується логічна операція I.



Структура адреси IPv4

Адреса мережі, адреса вузла та широкомовна адреса.

- У межах кожної мережі є три типи IP-адрес:
 - Адреса мережі
 - Адреса вузла
 - Широкомовна адреса



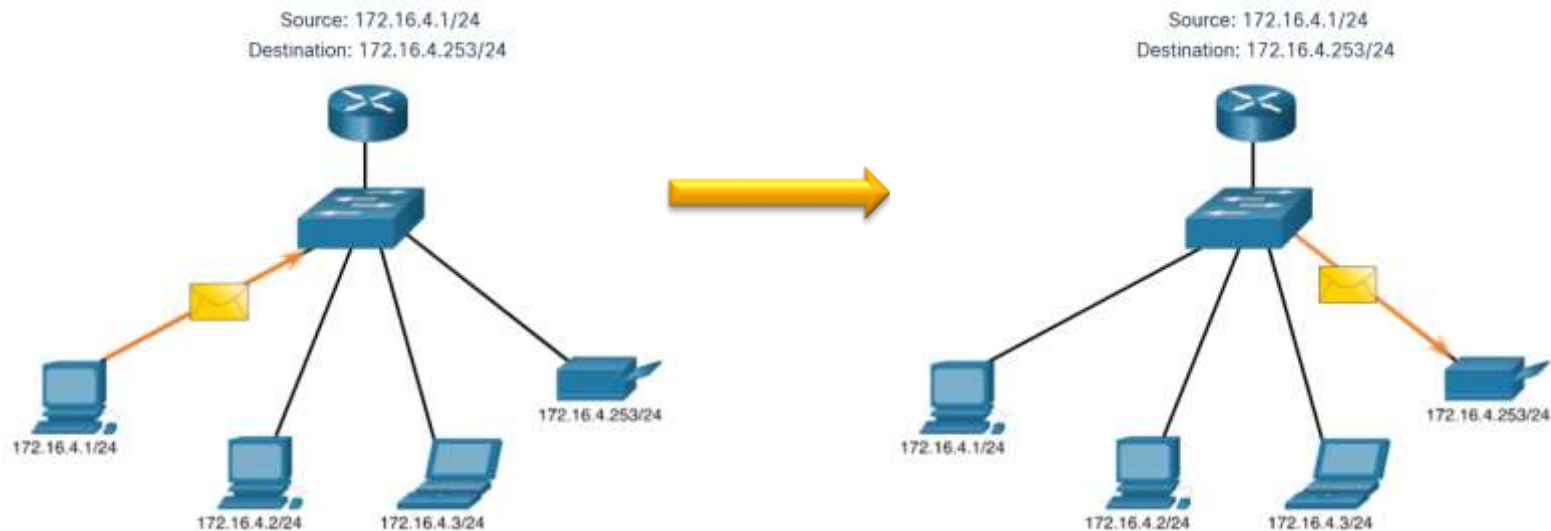
	Мережна частина	Вузлова частина	Біти вузла
Маска мережі 255.255.255.0 або /24	255 255 255 11111111 111111 111111 111111	0 00000000	
Адреса мережі 192.168.10.0 або /24	192 168 10 11000000 10100000 00001010	0 00000000	Всі 0
Перша адреса 192.168.10.1 або /24	192 168 10 11000000 10100000 00001010	1 00000001	Всі 0 і 1
Остання адреса 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 1111110	Всі 1 і 0
Широкомовна адреса 192.168.10.255 or /24	192 168 10 11000000 10100000 00001010	255 1111111	Всі 1

Одноадресна,
широкомовна та групова
розсилки IPv4

Одноадресна, широкомовна та групова розсилки IPv4

Одноадресна розсилка

- Одноадресна розсилка (Unicast) - це відправлення пакета на одну IP-адресу призначення.
- Наприклад, ПК з адресою 172.16.4.1 відправляє одноадресний пакет на принтер з адресою 172.16.4.253.



Одноадресна, широкомовна та групова розсилка IPv4

Широкомовна розсилка

- Широкомовна розсилка IPv4 (Broadcast) – це відправлення пакета усім вузлам у мережі.
- Наприклад, ПК з адресою 172.16.4.1 відправляє широкомовний пакет усім вузлам IPv4.



Одноадресна, широкомовна та групова розсилка IPv4

Групова розсилка

- Групова розсилка (Multicast) – це відправлення пакета обраній групі вузлів, які підписані на групову розсилку.
- Наприклад, ПК з адресою 172.16.4.1 відправляє пакет з адресою групової розсилки 224.10.10.10.5.



Типи адрес IPv4

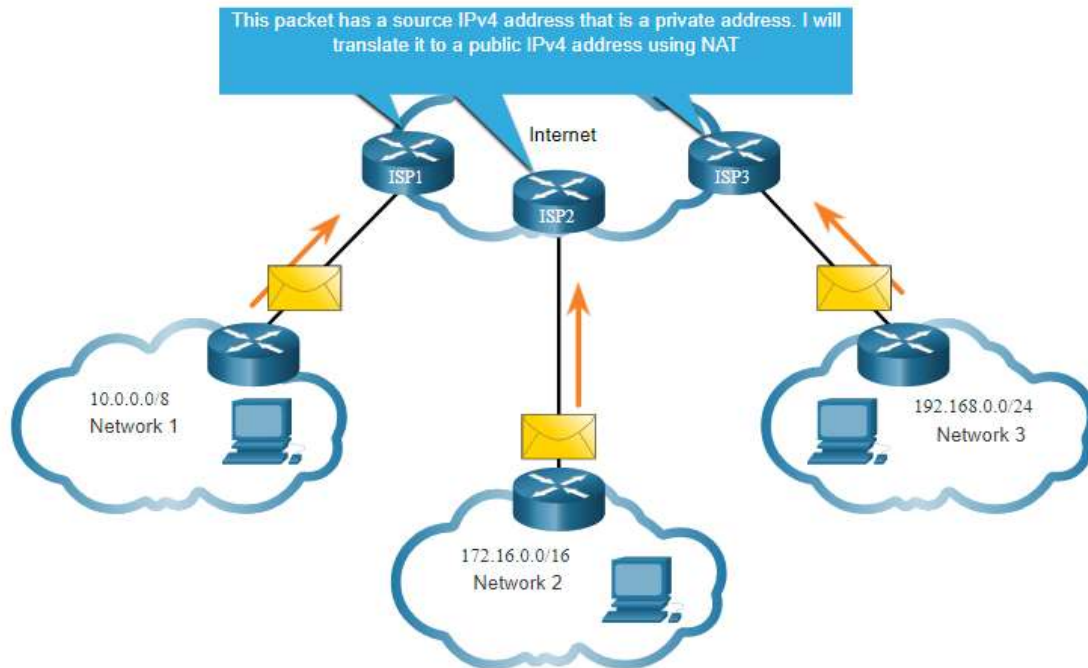
Публічні та приватні адреси IPv4

- Як визначено в RFC 1918, публічні адреси IPv4 глобально маршрутизуються між маршрутизаторами постачальника послуг Інтернету (ISP).
- Однак, приватні адреси не є глобально маршрутизованими.
- Приватні адреси - це загальні блоки адрес, які використовуються більшістю організацій для призначення IPv4-адрес внутрішнім вузлам.
- Приватні IPv4-адреси не є унікальними і можуть використовуватися всередині будь-якої мережі.

Адреса мережі та префікс	Діапазон приватних адрес RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Маршрутизація в Інтернеті

- Трансляція мережних адрес (NAT, Network Address Translation) використовується для перетворення приватних IPv4-адрес на публічні IPv4-адреси, і навпаки.
- Зазвичай NAT активується на граничному маршрутизаторі, що під'єднується до Інтернету.
- Він перетворює внутрішню приватну адресу на публічну (глобальну) IP-адресу.



Публічні та приватні адреси IPv4

Адреси (loopback)

- 127.0.0.0 /8 (від 127.0.0.1 до 127.255.255.254)
- Зазвичай ідентифікуються як 127.0.0.1
- Використовуються вузлом, щоб перевірити, чи працює TCP/IP.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Локальна адреса каналу (LLA)

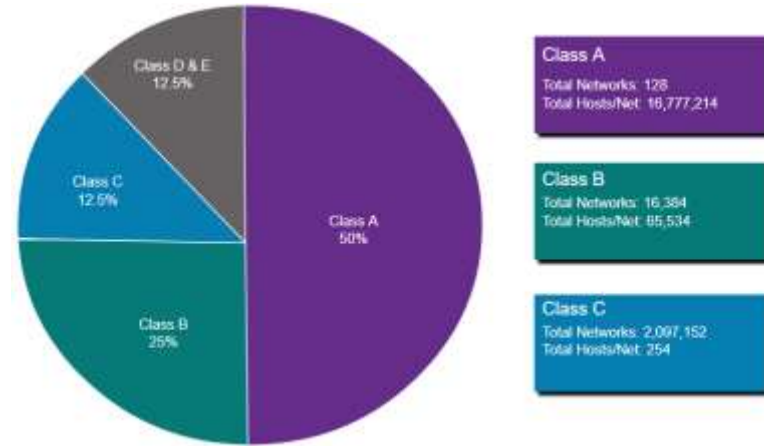
- 169.254.0.0 /16 (від 169.254.0.1 до 169.254.255.254)
- Більш відомі як автоматична приватна IP-адресація (APIPA, Automatic Private IP Addressing) або самопризначені адреси.
- Вони використовуються Windows DHCP-клієнтом для самостійної конфігурації у випадку, якщо ні один DHCP-сервер не доступний.

Застаріла класова адресація

Відповідно до стандарту RFC одноадресні діапазони поділяються на наступні класи:

- Клас А (0.0.0/8 — 127.0.0.0/8)
 - Клас В (128.0.0.0 /16 — 191.255.0.0 /16)
 - Клас С (192,0.0.0 /24 — 223.255.255.0 /24)
 - Клас D (224.0.0.0 — 239.0.0.0)
 - Клас Е (240.0.0.0 — 255.0.0.0)
-
- Класова адресація витрчала багато IPv4-адрес.

Класова адресація була замінена більш новою і актуальною безкласовою системою адресації, яка не використовує правила класів (А, В, С).



Призначення IP-адрес

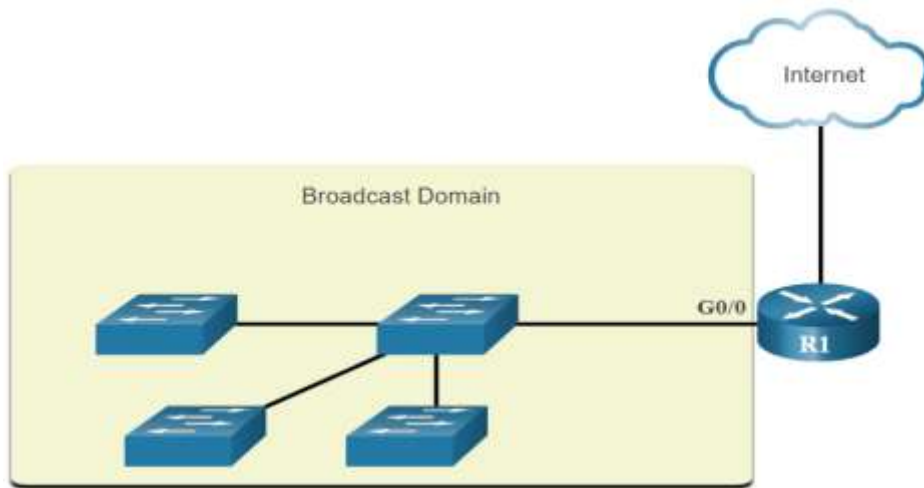
- Адміністрація адресного простору Інтернет (IANA, Internet Assigned Numbers Authority) керує та розподіляє блоки IP-адрес до п'яти регіональних інтернет-реєстраторів (RIR, Regional Internet Registries).
- Регіональні інтернет-реєстратори (RIR) відповідальні за розподіл IP-адрес між інтернет-провайдерами (ISP), які в свою чергу, надають блоки адрес IPv4 організаціям та меншим інтернет-провайдерам.



Сегментація мережі

Широкомовні домени та сегментація

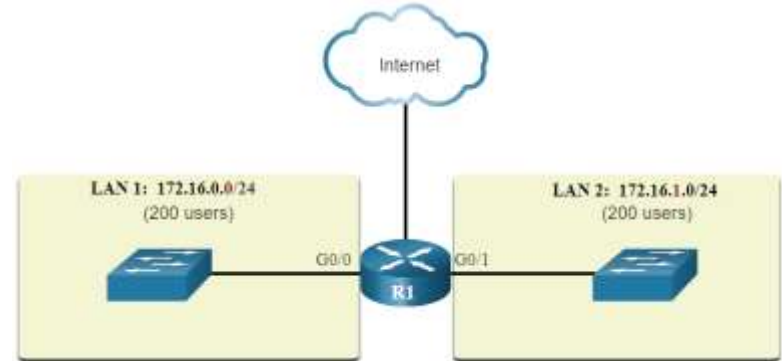
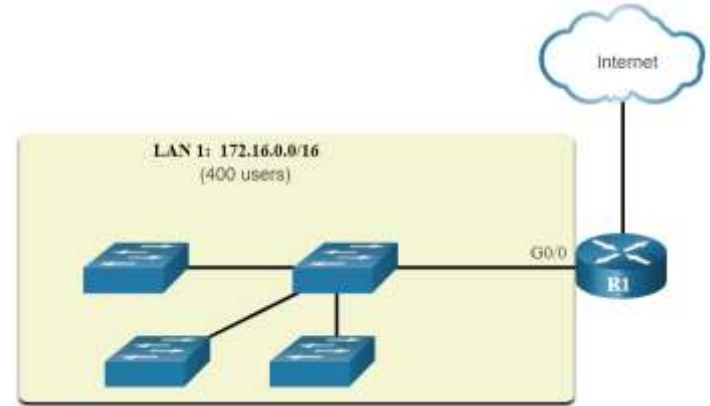
- Багато протоколів використовують широкомовні або групові розсилки (наприклад, ARP використовує широкомовну розсилку для пошуку інших пристроїв, вузли надсилають за допомогою DHCP широкомовні пакети для пошуку DHCP-сервера.)
- Комутатори розповсюджують широкомовні повідомлення з усіх інтерфейсів, за винятком того інтерфейсу, на якому вони були отримані.



- Єдиний пристрій, який призупиняє широкомовну розсилку - це маршрутизатор.
- Маршрутизатори не розповсюджують широкомовні повідомлення.
- Таким чином, кожен інтерфейс маршрутизатора під'єднується до широкомовного домену і широкомовні повідомлення розповсюджуються тільки в межах цього конкретного широкомовного домену.

Проблеми, які виникають з великими широкомовними доменами

- Проблема з великим широкомовним доменом полягає в тому, що вузли можуть розповсюджувати надмірну кількість широкомовних повідомлень, які негативно впливають на роботу мережі.
- Для вирішення цієї проблеми потрібно зменшити розмір мережі, створивши менші широкомовні домени, що можливо за допомогою процесу розподілу на підмережі (subnetting).
- Розподілити мережну адресу 172.16.0.0/16 на дві підмережі по 200 користувачів: 172.16.0.0/24 і 172.16.1.0 /24.
- Широкомовні пакети тепер розповсюджуються в межах лише цих менших широкомовних доменах.



Причини сегментації мереж

- Розподіл на підмережі зменшує загальний мережний трафік і покращує продуктивність мережі.
- Такий підхід можна використати для реалізації політики безпеки між підмережами.
- Підмережа зменшує кількість пристроїв, які впливають на надмірний об'єм широкомовного трафіку.
- Підмережі використовуються з різних причин, включаючи:

Місце розташування



Група або функція



Тип пристрою



Розподіл мережі IPv4 на підмережі

Створення підмережі на межі октету

- Мережі найпростіше розподіляти на підмережі на межі октетів /8, /16 та /24.
- Зверніть увагу, що збільшення довжини префікса зменшує кількість вузлів у кожній підмережі.

Довжина префікса	Маска підмережі	Маска підмережі у двійковому форматі (n = мережа, h = вузол)	Кількість вузлів
/8	255.0.0.0	nnnnnnnn . hhhhhhhh . hhhhhhhh . hhhhhhhh 11111111 . 00000000 . 00000000 . 00000000	16 777 214
/16	255.255.0.0	nnnnnnnn . nnnnnnnn . hhhhhhhh . hhhhhhhh 11111111 . 11111111 . 00000000 . 00000000	65 534
/24	255.255.255.0	nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh 11111111 . 11111111 . 11111111 . 00000000	254

Створення підмережі на межі октету (Продовж.)

- У першій таблиці наведено розподіл мережі 10.0.0.0/8 на підмережі за допомогою префікса /16, а в другій таблиці - /24.

Адреса підмережі (256 можливих підмереж)	Діапазон вузлів (65 534 можливих вузлів у підмережі)	Широкомовна адреса
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Адреса підмережі (65 536 можливих підмереж)	Діапазон вузлів (254 можливих вузлів у підмережі)	Широкомовна адреса
10.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

Створення підмережі на межі октету (Продовж.)

- Зверніться до таблиці, щоб розглянути шість способів розподілу на підмережі мережі з префіксом /24.

Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111100	64	2

Розподіл на підмережі з
префіксом /16 і /8

Розподіл на підмережі з префіксом /16 і /8

Створення підмереж з префіксом /16

- У таблиці висвітлюються всі можливі варіанти створення підмереж з префіксом /16.

Довжина префікса	Маска підмережі	Мережна адреса (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.100000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.110000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	16384	2

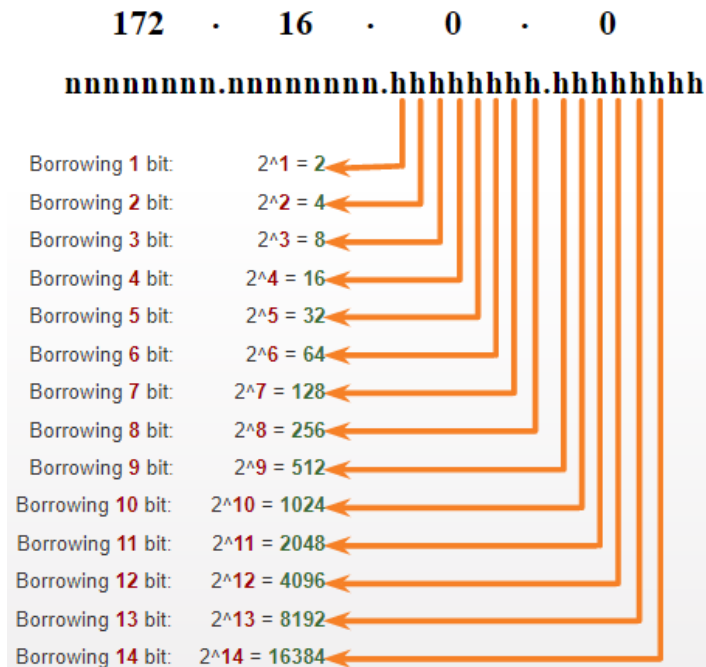
Розподіл на підмережі з префіксом /16 і /8

Створення 1000 підмереж з префіксом /8

Розглянемо велике підприємство, якому потрібно не менше 100 підмереж і яке обрало приватну адресу 172.16.0.0/16 як свою внутрішню адресу мережі.

- На рисунку показано кількість підмереж, які можна створити при запозиченні бітів з третього і четвертого октетів.
- Зверніть увагу, що тепер може бути запозичено до 14 бітів з вузлової частини (тобто останні два біти не можуть бути запозичені).

Щоб задовольнити вимогу 100 підмереж для підприємства, 7 бітів (тобто $2^7 = 128$ підмереж) потрібно було б запозичити (всього 128 підмереж).

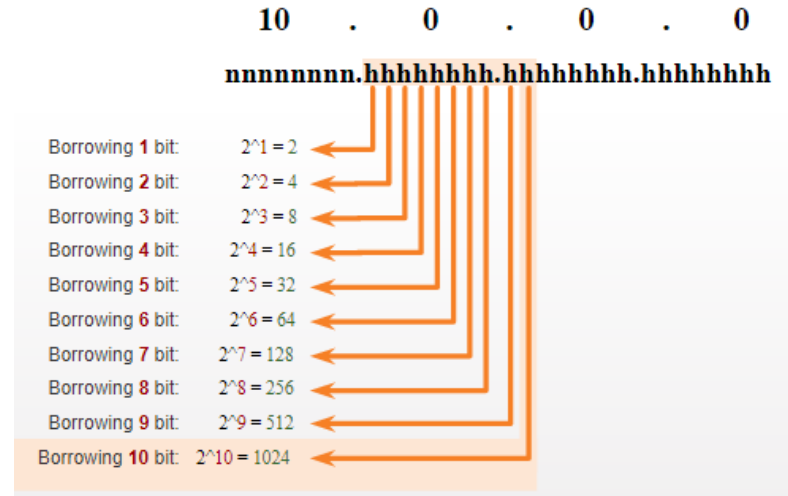


Створення 1000 підмереж з префіксом /8

Розглянемо невеликого інтернет-провайдера (ISP), який потребує 1000 підмереж для своїх клієнтів, використовуючи мережну адресу 10.0.0.0/8, що означає, що в мережній частині є 8 бітів і ще 24 біти для створення підмереж, які можна запозичити з позиції вузлових бітів.

- На рисунку показано кількість підмереж, які можна отримати при запозиченні бітів з другого і третього октетів.
- Зверніть увагу, що тепер може бути запозичено до 22 бітів з позиції вузлових бітів (тобто останні два біти не можуть бути запозичені).

Щоб задовольнити вимогу 1000 підмереж для підприємства, 10 бітів (тобто $2^{10}=1024$ підмережі) потрібно було б запозичити (всього 1024 підмережі).

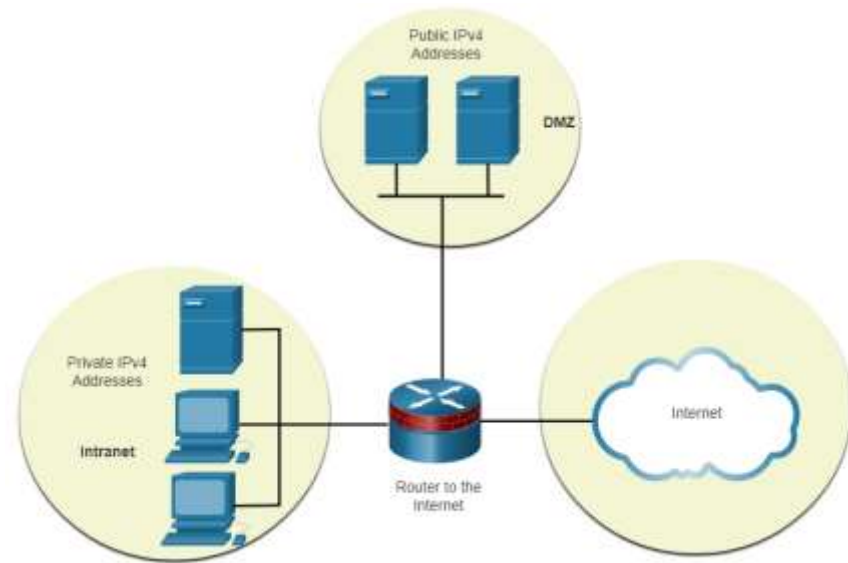


Розподіл на підмережі ВІДПОВІДНО ДО ВИМОГ

Приватна підмережа та публічний адресний простір IPv4

Корпоративні мережі мають:


- Інтранет (Intranet) – це внутрішня частина мережі компанії, зазвичай використовує приватні адреси IPv4.
- DMZ - це частина мережі компанії, що містить ресурси, доступні в Інтернеті, наприклад сервери. Пристрої в DMZ використовують публічні адреси IPv4.
- Компанія може використовувати адресу 10.0.0.0/8 і розподілити мережу на підмережі на межі /16 або /24.
- Пристрої DMZ повинні бути налаштовані за допомогою публічних IP-адрес.



Розподіл на підмережі відповідно до вимог Зменшення кількості невикористаних IPv4-адрес вузла та збільшення кількості підмереж

При плануванні підмереж необхідно врахувати два аспекти:

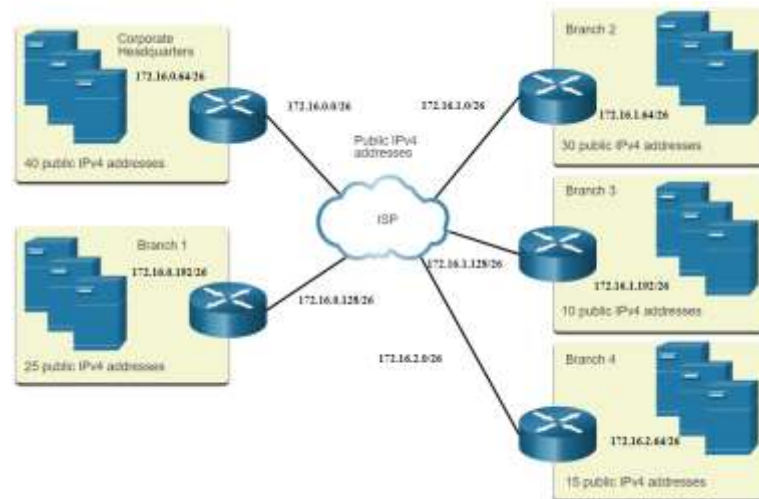
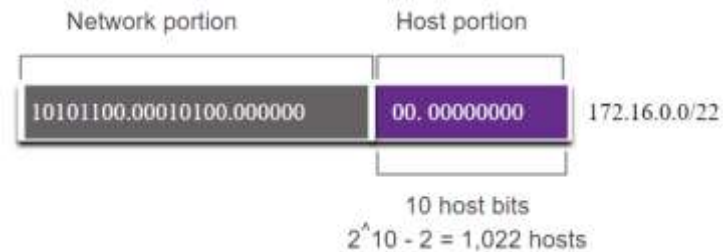
- Необхідну кількість адрес вузлів у кожній мережі
- Необхідну кількість окремих підмереж



Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/25	255.255.255.128	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nhhhhhhhh 11111111 . 11111111 . 11111111 . 10000000	2	126
/26	255.255.255.192	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnhhhhhhh 11111111 . 11111111 . 11111111 . 11000000	4	62
/27	255.255.255.224	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnhhhhhh 11111111 . 11111111 . 11111111 . 11100000	8	30
/28	255.255.255.240	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnhhhhh 11111111 . 11111111 . 11111111 . 11110000	16	14
/29	255.255.255.248	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnnhhhh 11111111 . 11111111 . 11111111 . 11111000	32	6
/30	255.255.255.252	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnnnhhh 11111111 . 11111111 . 11111111 . 11111100	64	2

Приклад: Ефективний розподіл на підмережі IPv4

- У цьому прикладі інтернет-провайдер (ISP) виділив корпоративному офісу для використання публічну адресу мережі 172.16.0.0/22 (10 вузлових бітів), яка забезпечує 1022 адреси вузлів.
- Існує п'ять відділів, а це означає, що потрібно п'ять під'єднань до Інтернету. Отже, організації потрібно 10 підмереж, а найбільшій підмережі необхідно 40 адрес.
- Виділено 10 підмереж з маскою підмережі /26 (тобто 255.255.255.192).

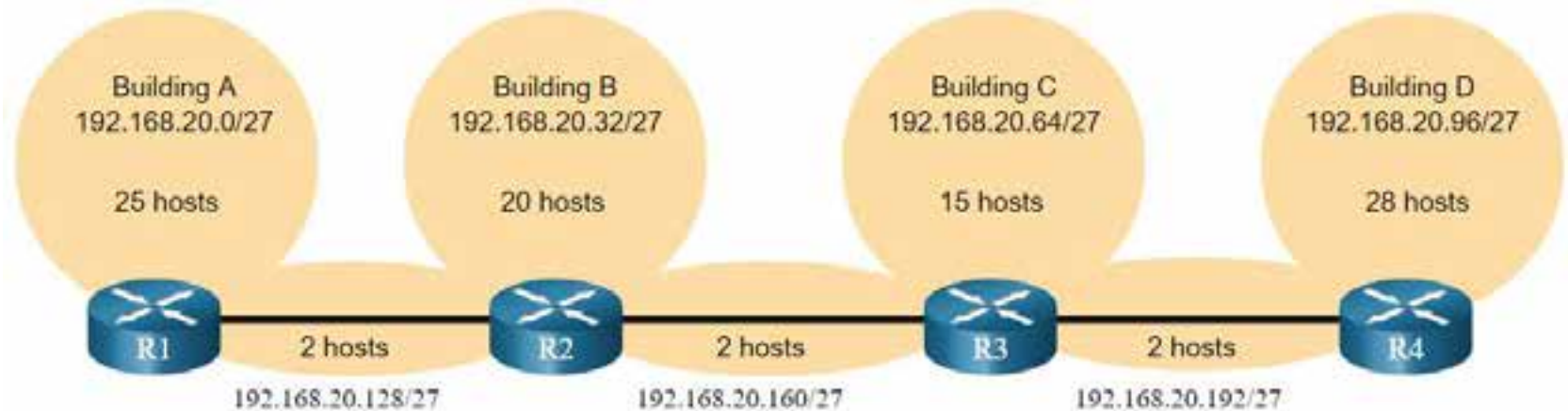


Маска підмережі змінної довжини (VLSM)

Збереження адрес IPv4

З огляду на топологію, потрібно 7 підмереж (тобто чотири локальні мережі (LAN) і три мережі (WAN)). Найбільша кількість вузлів знаходиться у Будівлі D - 28 вузлів.

- Маска /27 забезпечуватиме 8 підмереж з 30 IP-адресами вузлів і, отже, підтримуватиме цю топологію.



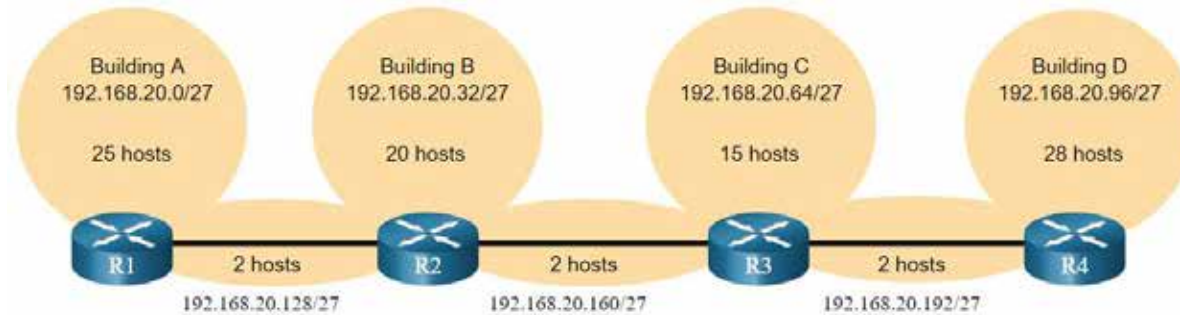
Збереження адрес IPv4 (Продовж.)

Однак, канали між мережами WAN «точка-точка» потребують тільки дві адреси, а отже, витрачається 28 адрес із загальної кількості 84 не використовуваних адрес.

Host portion
 $2^5 - 2 = 30$ host IP addresses per subnet

$30 - 2 = 28$
Each WAN subnet wastes 28 addresses

$28 \times 3 = 84$
84 addresses are unused



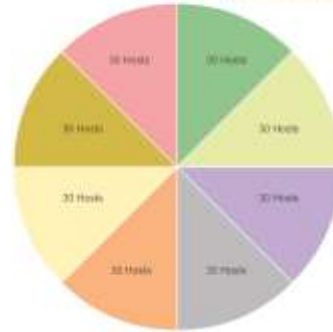
- Застосування традиційної схеми розподілу мережі на підмережі за таким сценарієм є неефективним і допускає недоцільне витрачання ресурсів.
- Маска підмережі змінної довжини (VLSM, Variable Length Subnet Mask) розроблена, щоб уникнути недоцільного витрачання адрес при розподілі мережі на підмережі.

Маска підмережі змінної довжини (VLSM)

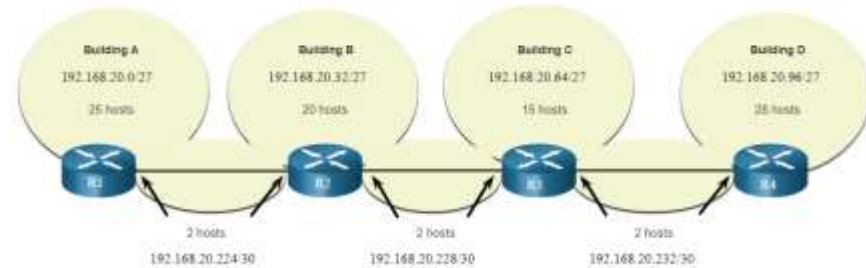
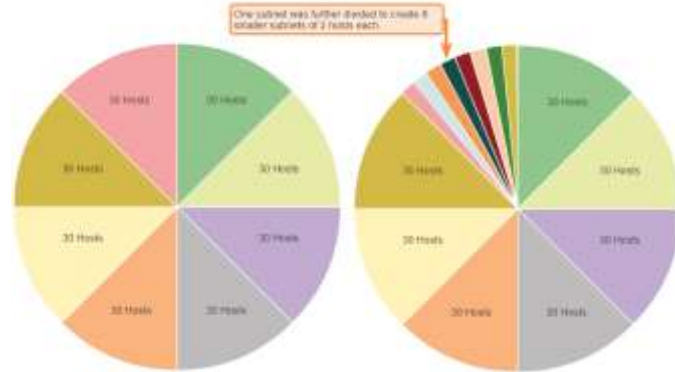
Маска підмережі змінної довжини (VLSM)

- Ліворуч показано традиційну схему підмережі (тобто, підмережі з однаковою маскою), а праворуч показано, як використовувати VLSM для розподілу мережі на підмережі та як розподілити останню підмережу на вісім підмереж з префіксом /30.
- Здійснюючи розподіл за допомогою VLSM завжди починайте із вимог щодо кількості вузлів у найбільшій підмережі та розподіляйте підмережу, доки не будуть виконані вимоги щодо кількості вузлів у найменшій підмережі.
- Отримана топологія за допомогою VLSM.

Traditional Subnetting Creates Equal Sized Subnets

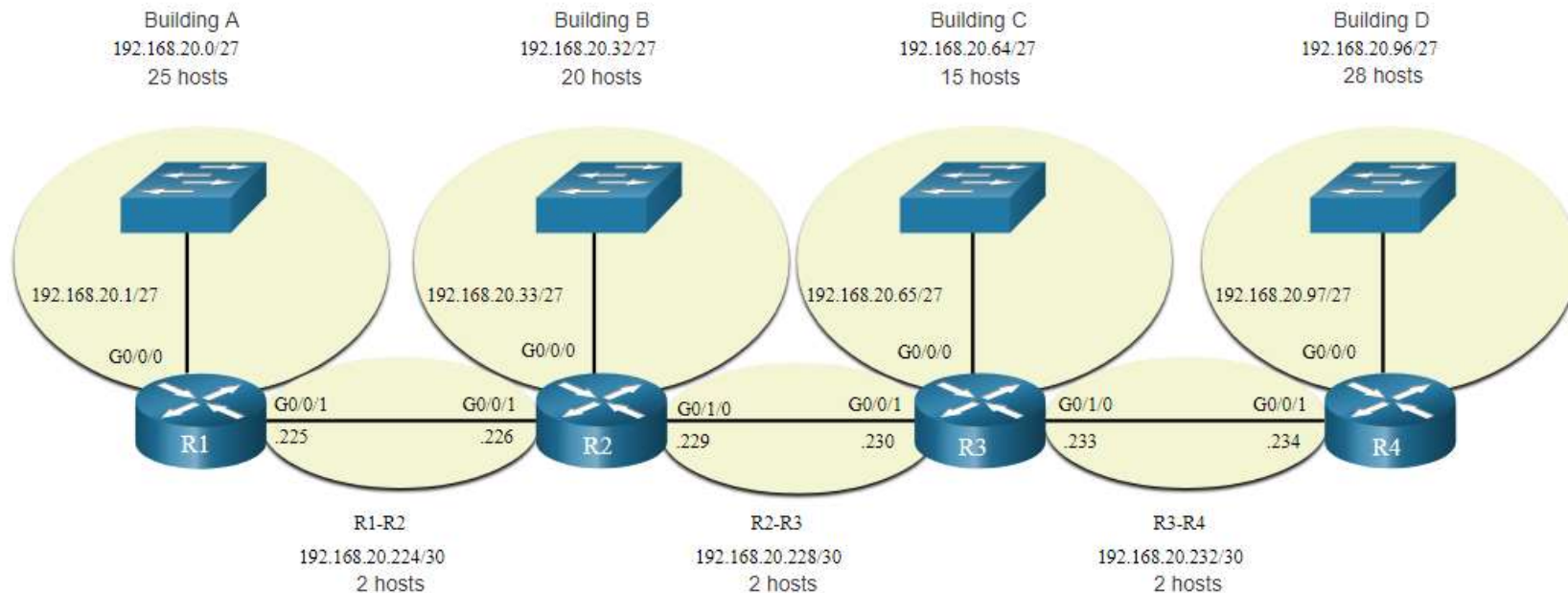


Subnets of Varying Sizes



Призначення адрес топології VLSM

- При використанні підмереж VLSM, локальним мережам (LAN) та мережам між маршрутизаторами (WAN) можна виділяти адреси без зайвих витрат, як показано на схемі логічної топології.



Структуроване проектування

Планування адресації мережі IPv4

Планування IP-мережі має вирішальне значення для розвитку та масштабування корпоративної мережі в майбутньому.

- Вам потрібно знати, скільки потрібно підмереж, скільки необхідно вузлів у кожній підмережі, які пристрої входять до складу підмереж, які частини мережі використовують приватні адреси, а які - публічні, і багато інших визначальних факторів.

При плануванні розподілу мережі IPv4 на підмережі необхідно дослідити вимоги, що висуваються організаціями щодо використання мережі та передбачити структуру підмереж.

- Здійсніть ґрунтовний аналіз вимог, що висуваються до мережі, зокрема розгляньте всю мережу та визначте, як сегментувати кожну область.
- Визначте, скільки необхідно підмереж і вузлів у кожній підмережі.
- Визначте діапазони адрес DHCP та діапазони VLAN Рівня 2.

Призначення адрес пристроям

В межах мережі існують різні типи пристроїв, яким потрібні такі адреси:

- **Клієнтські пристрої кінцевих користувачів** – Більшість використовують DHCP для зменшення помилок та навантаження на персонал служби підтримки мережі. Клієнти IPv6 можуть отримати інформацію про адресу за допомогою DHCPv6 або SLAAC.
- **Сервери та периферійні пристрої** – Вони повинні мати передбачувану статичну IP-адресу.
- **Сервери, які доступні з Інтернету** – Сервери, повинні мати публічну IPv4-адресу, доступ до якої здійснюється за допомогою NAT.
- **Проміжні пристрої** – Цим пристроям адреси присвоюються для керування мережею, моніторингу та безпеки.
- **Шлюз** – Маршрутизатори та пристрої брандмауера є шлюзом для вузлів у цій мережі.

При проектуванні схеми IP-адресації, як правило, рекомендується мати заданий шаблон призначення адрес для кожного типу пристроїв.

Що ми вивчили у цій підтемі?

- Структура IP-адреси являє собою 32-бітну ієрархічну мережну адресу, яка визначає мережну й вузлову частини. Для визначення мережної та вузлової частини, пристрої у мережі використовують, для IP-адреси та пов'язаної з нею маски підмережі, процес який називається логічною операцією І (AND).
- Призначення IPv4-пакетів може бути одноадресним, широкомовним і груповим.
- Існують глобально керовані IP-адреси, призначені IANA, і є три діапазони приватних мережних IP-адрес, які не можуть бути глобально маршрутизованими, але можуть бути використаними в усіх внутрішніх приватних мережах.
- Зменшуйте великі широкомовні домени шляхом розподілу підмереж на менші широкомовні домени, що в свою чергу зменшить загальний мережний трафік та підвищить продуктивність мережі.
- Підмережі IPv4 створюються за допомогою одного або декількох вузлових бітів, які використовуються у якості мережних бітів. Мережі найпростіше розподіляти на підмережі на межі октетів /8, /16 та /24.

Що ми вивчили у цій підтемі? (Продовж.)

- Великі мережі можуть бути розподілені на підмережі на межі /8 або /16.
- Щоб зменшити кількість не використовуваних адрес вузлів у підмережі, використовуйте VLSM-розподіл.
- VLSM дозволяє розподілити мережний простір на нерівні частини. При використанні VLSM завжди потрібно починати із вимог щодо кількості вузлів у найбільшій підмережі. Продовжуйте розподіл на підмережі, допоки не будуть задоволені вимоги щодо кількості вузлів у найменшій підмережі.
- При розробленні схеми адресації мережі враховуйте внутрішні, DMZ і зовнішні вимоги. При проектуванні схеми IP-адресації, зазвичай рекомендується використовувати готовий шаблон призначення адрес кожному типу пристроїв.

Нові терміни і команди

- | | |
|---|---|
| <ul style="list-style-type: none">• Довжина префікса• Логічна операція I• Адреса мережі• Широкомовна адреса• Перша доступна адреса вузла• Остання доступна адреса вузла• Одноадресна, ширококомовна та групова розсилки• Приватна адреса• Публічна адреса• Трансляція мережних адрес (NAT)• Адреса зворотнього зв'язку (Loopback)• Автоматична приватна IP-адресація (APIPA)• Класова адресація (класи A, B, C, D та E) | <ul style="list-style-type: none">• Адміністрація адресного простору Інтернет (IANA)• Регіональні інтернет-реєстратори (RIRs)• AfriNIC, APNIC, ARIN, LACNIC та RIPE NCC• Широкомовний домен• Підмережа• Межа октету• Маска підмережі змінної довжини (VLSM) |
|---|---|

Адресація IPv6



Завдання

Мета : Реалізувати схему адресації підмережі IPv6.

Назва теми	Мета вивчення теми
Проблеми з IPv4	Пояснити необхідність адресації IPv6.
Подання адрес IPv6	Пояснити який вигляд мають адреси IPv6.
Типи адрес IPv6	Порівняти типи мережних адрес IPv6.
Статичне налаштування глобальної індивідуальної адреси (GUA) та локальної адреси каналу (LLA)	Пояснити, як налаштовувати статичні глобальні індивідуальні адреси та локальні адреси каналу мережі IPv6.
Динамічна адресація для глобальних індивідуальних адрес (GUA) IPv6	Пояснити, як динамічно налаштовувати глобальні індивідуальні адреси.

Завдання (Продовж.)

Назва розділу: Адресація IPv6

Мета розділу: Реалізувати схему адресації IPv6.

Назва теми	Мета вивчення теми
Динамічна адресація для локальних адрес каналу (LLA) IPv6	Динамічно налаштовувати локальну адресу каналу (link-local).
Групові адреси IPv6	Визначити адреси IPv6.
Розподіл мережі IPv6 на підмережі	Реалізувати схему адресації розподілу мережі IPv6 на підмережі.

Проблеми з IPv4

Потреба в IPv6

- Адресний простір протоколу IPv4 вичерпується. Протокол IPv6 був розроблений як послідовник протоколу IPv4 та має набагато більший 128-бітний адресний простір.
- Розроблення IPv6 також включало виправлення обмежень IPv4 та внесення додаткових покращень.
- Зі збільшенням кількості активних інтернет-користувачів, виснаженням адресного простору IPv4, проблемами з NAT та розвитком IoT, прийшов час розпочати перехід на IPv6.



Сумісне використання протоколів IPv4 і IPv6

Як IPv4, так і IPv6 будуть співіснувати найближчим часом, і перехід триватиме декілька років.

Фахівці IETF створили різні протоколи та інструменти, які допомагають мережним адміністраторам поступово здійснити перехід своїх мереж на IPv6. Методи переходу можна розділити на три категорії:

- **Подвійний стек (Dual stack)** – пристрої подвійного стека одночасно працюють з протокольними стеками як IPv4, так і IPv6.
- **Тунелювання (Tunneling)** – це метод передачі пакета IPv6 через мережу IPv4. Пакет IPv6 інкапсульований всередині пакета IPv4, аналогічно іншим типам даних.
- **Перетворення (Translation)** – перетворення мережних адрес 64 (NAT64) дозволяє пристроям під керуванням IPv6 взаємодіяти з пристроями під керуванням IPv4 за допомогою методу перетворення, аналогічного методу перетворення NAT для IPv4.

Примітка: Тунелювання і перетворення призначені для переходу на рідну IPv6-адресу та повинні використовуватися тільки там, де це необхідно. Метою повинні бути рідні IPv6-комунікації від джерела до місця призначення.

Подання адрес IPv6

Формати адрес IPv6

- Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень.
- IPv6-адреси не чутливі до регістру і можуть бути записані як в нижньому регістрі, так і у верхньому.
- Основний формат для запису IPv6 адреси - x:x:x:x:x:x:x:x, при цьому кожен x складається з чотирьох шістнадцяткових значень.
- Для IPv6 гекстет (hextet) - неофіційний термін, який використовують для позначення сегмента з 16 бітів або чотирьох шістнадцяткових значень.
- Приклади запису адрес IPv6 в основному форматі.

```
2001:0db8:0000:1111:0000:0000:0000:0200
```

```
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

Правило 1 – Пропуск початкових нульових розрядів

Перше правило, яке допоможе скоротити запис адреси IPv6 - це пропуск усіх початкових нулів (0) у будь-якому гекстеті.

Приклади:

- 01ab можна подати як 1ab
- 09f0 можна подати як 9f0
- 0a00 можна подати як a00
- 00ab можна подати як ab

Примітка: Це правило застосовується лише до початкових 0, а НЕ до кінцевих 0, інакше адреса буде незрозумілою.

Тип	Формат
Основний	2001: 0db8: 0000:1111: 000 0:0000: 0000: 0000: 0200
Пропуск початкових нулів	2001 : db8 : 0: 1111 : 0 : 0 : 0 : 200

Правило 2 – Подвійні двокрапки

Подвійні двокрапки (::) можуть замінити будь-який єдиний, суміжний рядок одного або декількох 16-бітних гекстетів, що складаються з усіх нулів.

Наприклад:

- 2001:db8:cafe:1:0:0:0:1 (початкові 0 не вказано) можна подати як 2001:db8:cafe:1::1

Примітка: Подвійні двокрапки (::) можуть використовуватися лише один раз у межах адреси, інакше в результаті може виникнути декілька адрес.

Тип	Формат
Основний формат	2001: 0db8: 0000:1111: 0000 : 0000 : 0000 : 0200
Стиснутий	2001:db8:0:1111::200

Типи адрес IPv6

Індивідуальна, групова і альтернативна адреси

Існує три типи адрес IPv6:

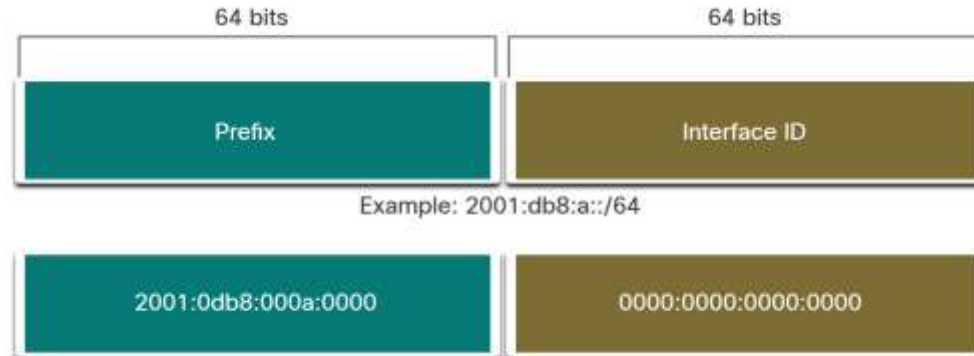
- **Індивідуальна (unicast)** – індивідуальна адреса IPv6 однозначно ідентифікує інтерфейс на пристрої з підтримкою IPv6.
- **Групова (multicast)** – групова адреса IPv6 використовується для надсилання одного пакета IPv6 на декілька адрес призначення.
- **Альтернативна (anycast)** – альтернативна адреса IPv6 - це будь-яка індивідуальна адреса IPv6, яку можна призначати декільком пристроям. Пакет, надісланий на альтернативну адресу, перенаправляється до найближчого пристрою, який має цю адресу.

Примітка: На відміну від IPv4, IPv6 не використовує широкомовної адреси. Однак, є групова адреса IPv6 для усіх вузлів, що дає аналогічний результат.

Довжина префікса IPv6

Довжина префікса представлена скісною рисою та використовується для позначення мережної частини адреси IPv6.

Довжина префікса може знаходитись у діапазоні від 0 до 128. Рекомендована довжина префікса IPv6 для локальних мереж та більшості інших типів мереж - /64, як показано на рисунку.

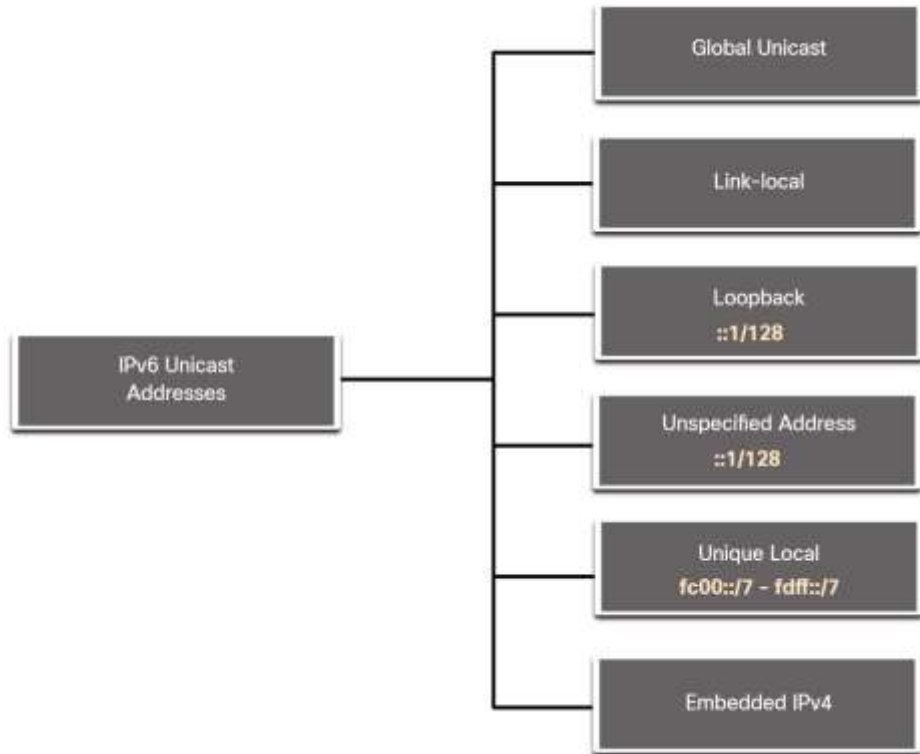


Примітка: Строго рекомендовано використовувати 64-бітний ідентифікатор інтерфейсу для більшості мереж. Це відбувається тому, що для автоналаштування адреси без збереження стану (SLAAC) використовується 64 біти для ідентифікатора інтерфейсу. Це також полегшує створення підмереж та їх керування.

Типи індивідуальних адрес IPv6

На відміну від пристроїв з підтримкою IPv4, які мають тільки одну адресу, IPv6-адреси зазвичай мають дві індивідуальні (unicast) адреси:

- **Глобальну індивідуальну адресу (GUA)** – аналогічну публічній адресі IPv4. Це глобально унікальні в усьому світі адреси, що маршрутизуються в Інтернеті.
- **Локальну адресу каналу (LLA)** – потрібну для кожного пристрою з підтримкою IPv6. Локальні адреси не є маршрутизованими і обмежуються одним каналом.



Примітка про унікальну локальну адресу (ULA)

Унікальні локальні адреси IPv6 (діапазон від fc00::/7 до fdff::/7) мають деяку схожість з приватними адресами RFC 1918 для IPv4, але при цьому між ними є істотні відмінності:

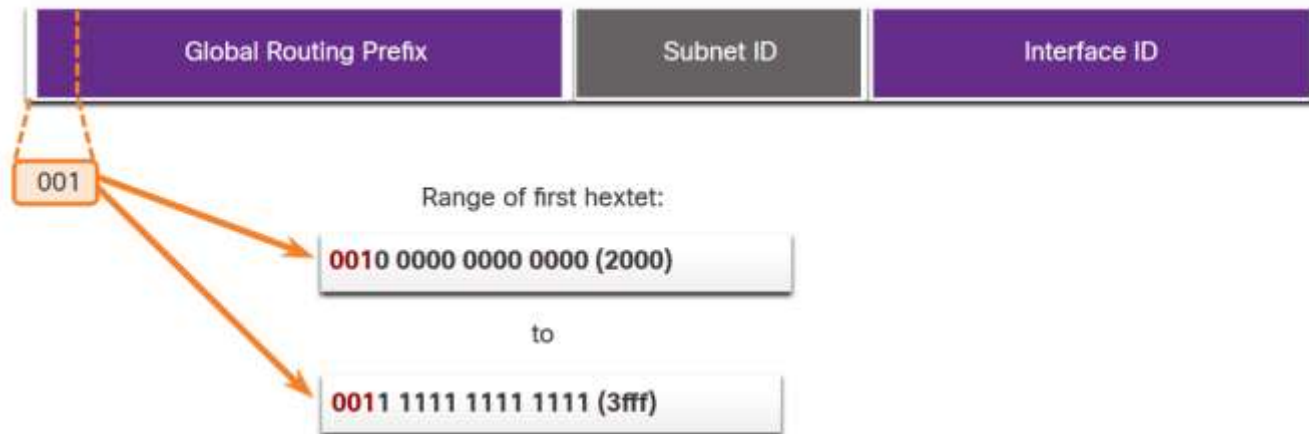
- Унікальні локальні адреси використовуються для локальної адресації в межах мережі або між окремим (обмеженим) колом мереж.
- Унікальні локальні адреси можна використовувати для пристроїв, яким ніколи не потрібно мати доступ до іншої мережі.
- Унікальні локальні адреси не маршрутизуються глобально і не перетворюються в глобальну адресу IPv6.

Примітка: Багато мереж також використовують приватні адреси RFC 1918, щоб спробувати захистити або приховати свою мережу від потенційних ризиків безпеки. Це ніколи не було цільовим використанням ULA.

Глобальні індивідуальні адреси IPv6

Глобальні індивідуальні адреси (GUA, Global Unicast Addresses) IPv6 глобально унікальні та доступні для маршрутизації в Інтернеті IPv6.

- В даний час призначаються тільки глобальні індивідуальні адреси (GUA) з першими трьома бітами 001 або 2000::



Структура глобальної індивідуальної адреси IPv6

Префікс глобальної маршрутизації:

- Префікс глобальної маршрутизації - це префіксна або мережна частина адреси, яка призначається постачальником, наприклад, інтернет-провайдером, клієнту чи мережі. Префікс глобальної маршрутизації залежить від політики постачальника послуг Інтернету (ISP).

Ідентифікатор підмережі

- Поле Ідентифікатор підмережі (Subnet ID) - це область між префіксом глобальної маршрутизації та ідентифікатором інтерфейсу (Interface ID). Ідентифікатор підмережі використовується організаціями для позначення підмереж в межах своєї мережі.

Ідентифікатор інтерфейсу

- Ідентифікатор інтерфейсу IPv6 еквівалентний вузловій частині адреси IPv4. Наполегливо рекомендується в більшості випадків використовувати префікс підмережі /64, що створює 64-бітний ідентифікатор інтерфейсу.

Примітка: IPv6 дозволяє пристрою призначати адресу вузла, що складається з усіх 0 або з усіх 1. Адреса всі-0 зарезервована як альтернативна (anycast) адреса підмережі маршрутизатора і повинна призначатися тільки маршрутизаторам.

Локальна IPv6-адреса каналу

Локальна IPv6-адреса каналу (LLA) дозволяє пристрою взаємодіяти з іншими пристроями з підтримкою IPv6, що знаходяться в одному і тому ж каналі (підмережі) і тільки в ньому.

- Пакети з локальною адресою каналу джерела або призначення не можуть бути перенаправлені поза межі каналу, в якому створюється пакет.
- Однак кожен IPv6-сумісний мережний інтерфейс повинен мати локальну адресу каналу (LLA).
- Якщо локальну адресу каналу не налаштовано статично на інтерфейсі, пристрій автоматично створює її самостійно.
- Локальні IPv6-адреси каналу знаходяться в діапазоні fe80::/10.



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

Статичне налаштування
глобальної індивідуальної
адреси (GUA) та локальної
адреси каналу (LLA)

Статичне налаштування глобальної індивідуальної адреси (GUA) та локальної адреси каналу (LLA)

Статичне налаштування GUA та LLA на маршрутизаторі

Більшість команд налаштування та перевірки мережі IPv6 в операційній системі Cisco IOS схожі на свої аналоги для мережі IPv4. У багатьох випадках єдиною відмінністю між ними є використання **ipv6** замість **ip** всередині команд.

- Для налаштування глобальної індивідуальної адреси IPv6 на інтерфейсі використовується команда: **ipv6 address ipv6-address/prefix-length**.
- У прикладі показано команди для налаштування глобальної індивідуальної адреси на інтерфейсі G0/0/0 маршрутизатора R1:

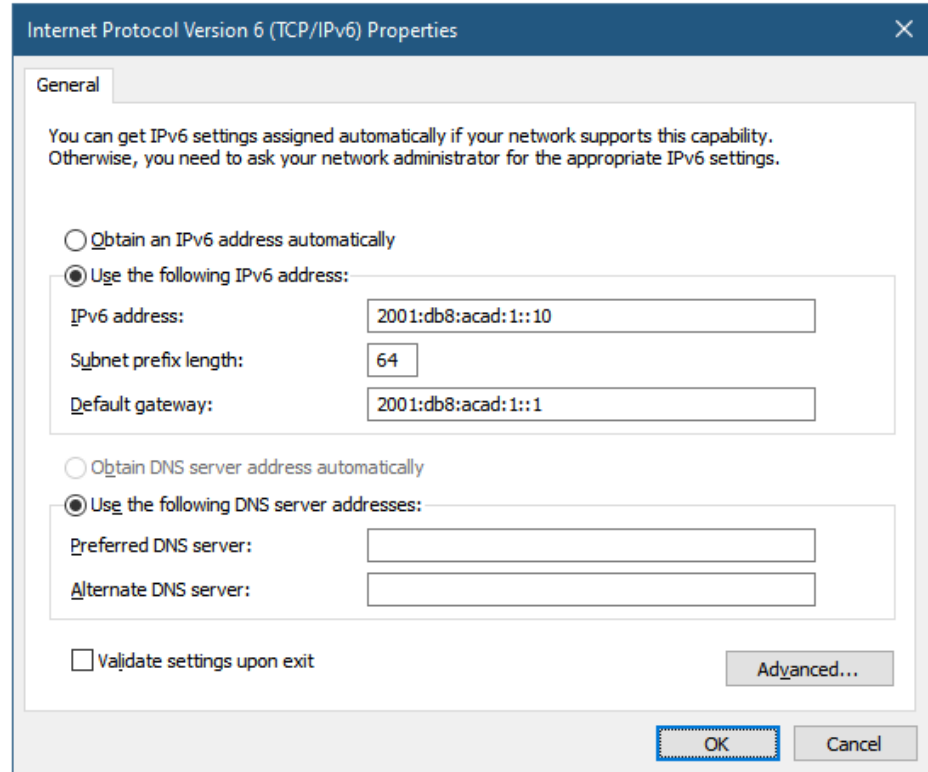
```
R1(config)# interface gigabitethernet 0/0/0  
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64  
R1(config-if)# no shutdown  
R1(config-if)# exit
```

Статичне налаштування глобальної індивідуальної адреси (GUA) та локальної адреси каналу (LLA)

Статична конфігурація GUA на вузлі Windows

- Статичне налаштування адреси IPv6 на вузлі аналогічне налаштуванню адреси IPv4.
- GUA або LLA інтерфейсу маршрутизатора можна використовувати як шлюз за замовчуванням. Найпрактичніше використовувати LLA.

Примітка: При використанні DHCPv6 або SLAAC, локальна адреса каналу маршрутизатора автоматично вказується як адреса шлюзу за замовчуванням.



Статичне налаштування глобальної індивідуальної адреси (GUA) та локальної адреси каналу (LLA)

Статичне налаштування індивідуальної локальної адреси каналу

Статичне налаштування локальної адреси каналу дозволяє створити адресу, яку легше розпізнати і запам'ятати.

- Для налаштування локальної адреси каналу використовується команда **ipv6 адреси ipv6-link-local-address link-local**.
- У прикладі показані команди для налаштування локальної адреси на інтерфейсі G0/0/0 маршрутизатора R1:

```
R1(config)# interface gigabitethernet 0/0/0
R1 (config-if) # адреса ipv6 fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

Примітка: Одна і та ж локальна адреса може бути налаштована на кожному каналі до тих пір, поки вона є унікальною для цього каналу. Поширеною практикою є створення іншої LLA на кожному інтерфейсі маршрутизатора, щоб полегшити ідентифікацію маршрутизатора та конкретного інтерфейсу.

Динамічна адресація для глобальних індивідуальних адрес (GUA) IPv6

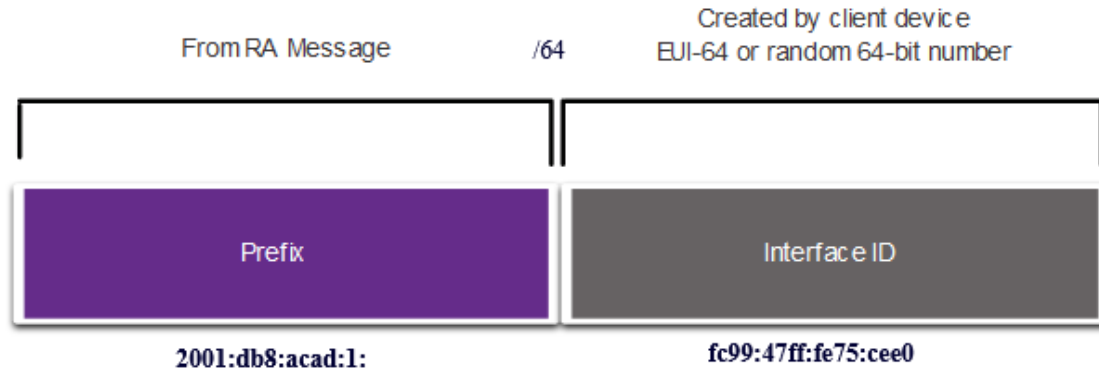
RS і RA повідомлення

Пристрої динамічно отримують глобальні індивідуальні адреси за допомогою протоколу IMAP і міжмережного протоколу керуючих повідомлень версії 6 (ICMPv6, Internet Control Message Protocol).

- Повідомлення Запит маршрутизатора (RS, Router Solicitation) надсилаються вузловими пристроями для виявлення маршрутизаторів IPv6
- Повідомлення Анонсування маршрутизатора (RA, Router Advertisement) надсилаються маршрутизаторами, щоб інформувати вузли як отримати GUA IPv6 і надати необхідну інформацію про мережу, зокрема:
 - Мережний префікс і довжину префікса
 - Адреса шлюзу за замовчуванням
 - Адреса DNS і доменне ім'я
- Повідомлення RA може надати три методи налаштування глобальної індивідуальної адреси IPv6:
 - Автоматичне налаштування адреси без відстеження стану (SLAAC, Stateless Address Autoconfiguration)
 - SLAAC і DHCPv6-сервер без відстеження стану адреси
 - DHCPv6 з відстеженням стану адреси (без SLAAC)

Метод 1: SLAAC

- SLAAC - це метод, який дозволяє пристрою створювати власну глобальну індивідуальну адресу без сервера DHCPv6.
- Пристрої отримують необхідну інформацію для налаштування глобальної індивідуальної адреси з повідомлень RA ICMPv6 локального маршрутизатора.
- Префікс надається в RA, і пристрій використовує процес EUI-64 або метод випадкової генерації для створення ідентифікатора інтерфейсу.

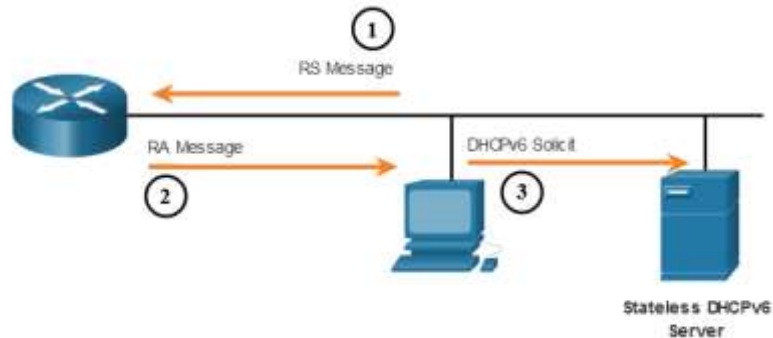


Метод 2: SLAAC і DHCPv6 без відстеження стану адреси

RA може інформувати пристрій використовуючи для цього як SLAAC, так і DHCPv6 без відстеження стану.

Повідомлення RA пропонує пристроям використовувати наступне:

- SLAAC для створення власної глобальної індивідуальної адреси IPv6.
- Локальну адресу каналу маршрутизатора, IPv6-адресу джерела RA як адресу шлюзу за замовчуванням.
- Сервер DHCPv6 без відстеження стану адрес, для отримання іншої інформації, такої як адреса DNS-сервера та доменне ім'я.



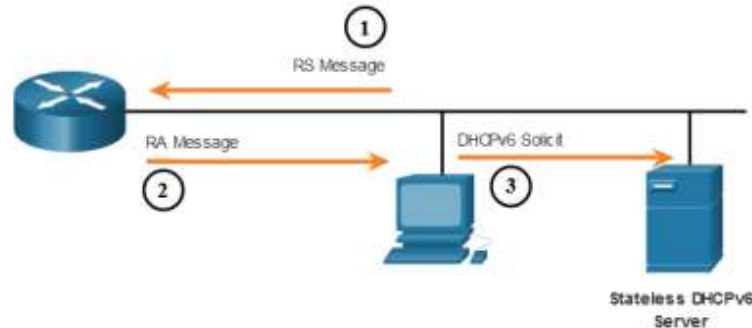
Метод 3: DHCPv6 з відстеженням стану адреси

Повідомлення RA може надати пристрою використовувати DHCPv6 з відстеженням стану.

DHCPv6 з відстеженням стану аналогічний DHCP для IPv4. Пристрій може автоматично отримувати глобальну індивідуальну адресу, довжину префікса та адреси DNS-серверів від DHCPv6-сервера з відстеженням стану.

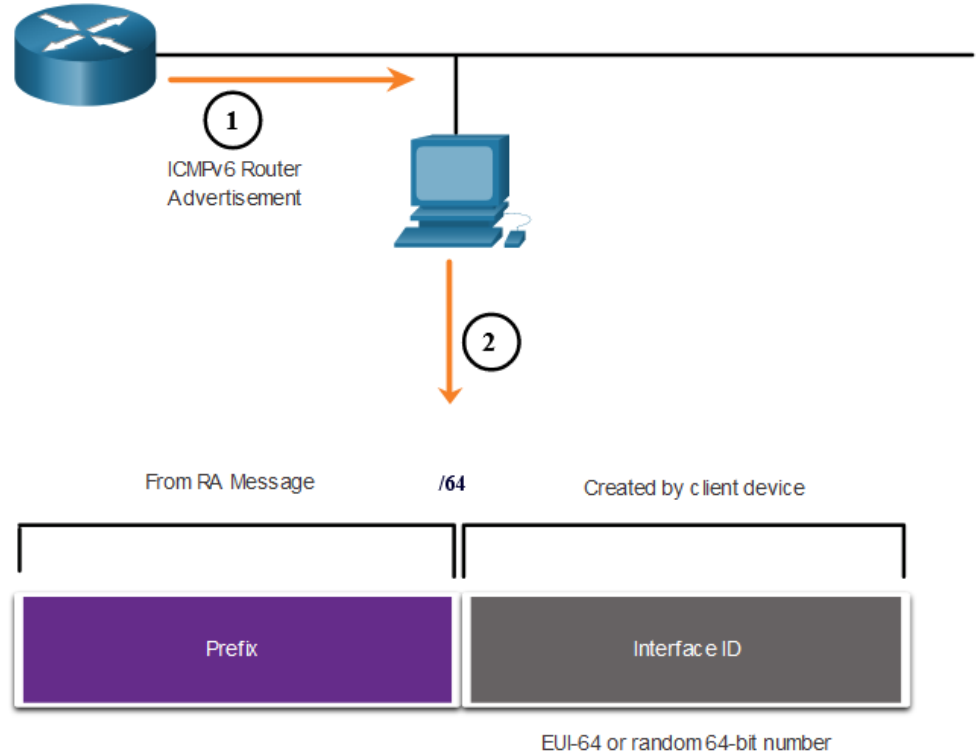
Повідомлення RA пропонує пристроям використовувати наступне:

- Локальну адресу маршрутизатора, IPv6-адресу джерела RA як адресу шлюзу за замовчуванням.
- DHCPv6-сервер без відстеження стану для отримання глобальної індивідуальної адреси, адреси DNS-сервера, доменного імені та іншої необхідної інформації.



Процес EUI-64 і випадково згенерований ідентифікатор інтерфейсу

- Коли повідомлення RA має тип SLAAC або SLAAC + DHCPv6 без відстеження стану, клієнт повинен згенерувати свій власний ідентифікатор інтерфейсу.
- Ідентифікатор інтерфейсу може бути створений за допомогою процесу EUI-64 або випадково згенерованого 64-бітного числа.



Процес EUI-64 і випадково згенерований ідентифікатор інтерфейсу

Організація IEEE визначила розширений унікальний ідентифікатор (EUI, Extended Unique Identifier) або модифікований процес EUI-64, який виконує такі дії:

- 16-бітне значення fffe (у шістнадцятковому форматі) вставляється в середину 48-бітної Ethernet MAC-адреси клієнта.
- 7-й біт клієнта MAC-адреси інвертується з 0 на 1.
- Наприклад:

48-бітна MAC-адреса	fc:99:47:75:ce:e0
Ідентифікатор інтерфейсу EUI-64	fe:99:47:ff:fe:75:ce:e0

Випадково згенеровані ідентифікатори інтерфейсу

Залежно від операційної системи пристрій може використовувати випадково згенерований ідентифікатор інтерфейсу замість того, щоб використовувати MAC-адресу та процес EUI-64.

Починаючи з Windows Vista, в операційних системах Windows використовується випадково згенерований ідентифікатор інтерфейсу замість створеного за допомогою EUI-64.

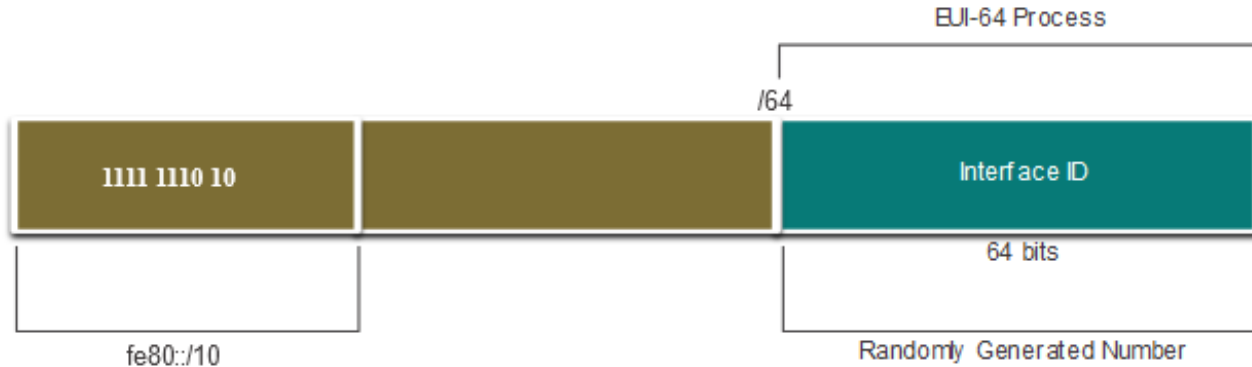
```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . :
IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\>
```

Примітка: Для забезпечення унікальності будь-якої індивідуальної IPv6-адреси (unicast), клієнт може використовувати процес виявлення дублювання адрес (DAD, Duplicate Address Detection). Це схоже на ARP-запит для власної адреси. Якщо відповіді немає, то адреса унікальна.

Динамічна адресація для локальних адрес каналу (LLA) IPv6

Динамічні локальні адреси каналу (LLA)

- Всі інтерфейси IPv6 повинні мати локальну IPv6-адресу каналу.
- Як і глобальні, індивідуальні адреси IPv6, локальні адреси каналу також можуть бути налаштовані динамічно.
- На рисунку показано, що локальна адреса каналу (LLA) динамічно створюється при використанні префікса fe80/10 та ідентифікатора інтерфейсу за допомогою процесу EUI-64 або випадково згенерованого 64-бітного числа.



Динамічна адресація для локальних адрес каналу (LLA) IPv6

Динамічні LLA у Windows

Операційні системи, такі як Windows, зазвичай використовують один і той же метод як для створеної SLAAC GUA, так і для динамічно призначеної LLA.

Випадково згенерований ідентифікатор інтерфейсу за допомогою EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . . :
IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Шлюз за замовчуванням. . . . . : fe80::1
C:\ >
```

Випадково згенерований 64-бітний ідентифікатор інтерфейсу:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . . :
IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\ >
```

Динамічні локальні адреси каналу на маршрутизаторах Cisco

Маршрутизатори Cisco автоматично створюють локальну IPv6-адресу каналу щоразу, коли інтерфейсу призначено GUA. За замовчуванням маршрутизатори Cisco IOS використовують EUI-64 для створення ідентифікатора інтерфейсу для всіх LLA на інтерфейсах IPv6.

Приклад динамічно налаштованої локальної адреси каналу (LLA) на інтерфейсі G0/0/0 маршрутизатора R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Перевірка налаштувань адреси IPv6

Маршрутизатори Cisco автоматично створюють локальну IPv6-адресу каналу щоразу, коли інтерфейсу призначено GUA. За замовчуванням маршрутизатори Cisco IOS використовують EUI-64 для створення ідентифікатора інтерфейсу для всіх LLA на інтерфейсах IPv6.

Приклад динамічно налаштованої локальної адреси каналу (LLA) на інтерфейсі G0/0/0 маршрутизатора R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Обладнання ISR4221-2x1GE, адреса 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Групові адреси IPv6

Призначення групових адрес IPv6

Групові адреси IPv6 мають префікс `ff00::/8`. Групові адреси IPv6 поділяються на два типи:

- Відомі групові адреси
- Групові адреси запитуваного вузла

Примітка: Групові адреси можуть бути тільки адресами призначення, а не адресами джерела.

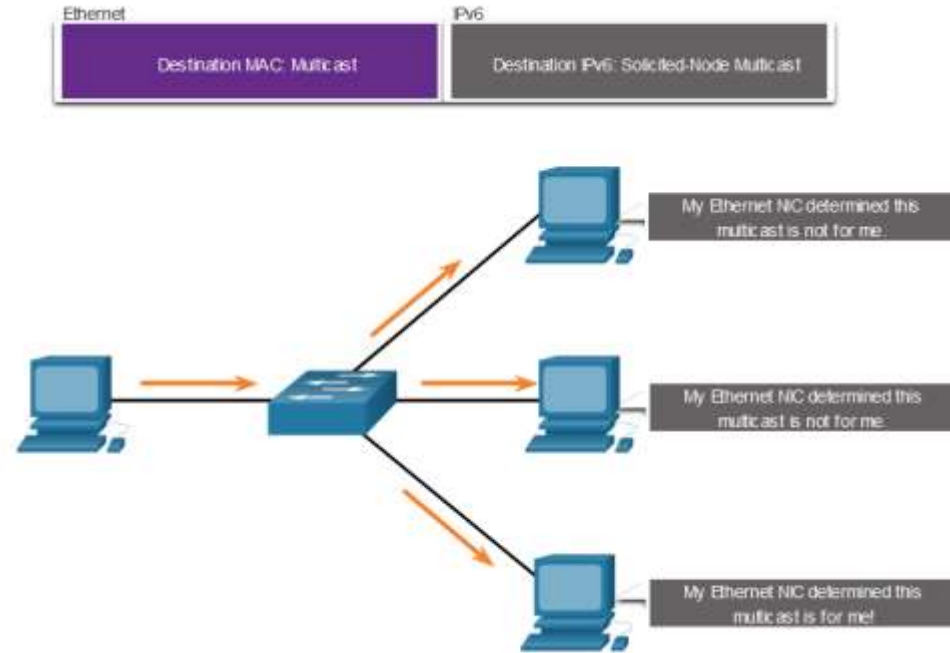
Призначення групових адрес IPv6

Призначені групові адреси - це зарезервовані групові адреси для попередньо визначеної групи пристроїв. Є дві поширені групи призначених групових адрес IPv6:

- **Групова розсилка для усіх вузлів ff02::1** - це групова розсилка, до якої під'єднуються усі пристрої з підтримкою IPv6. Пакет, який надійшов у цю групу, приймається і обробляється усіма інтерфейсами IPv6 в каналі або мережі.
- **Групова розсилка для усіх маршрутизаторів ff02::2** - це групова розсилка, до якої під'єднано усі маршрутизатори IPv6. Маршрутизатор стає учасником цієї групи, коли переходить під керування протоколу IPv6 за допомогою команди `ipv6 unicast-routing` глобального режиму конфігурації.

Групова IPv6-адреса запитуваного вузла

- Групова адреса запитуваного вузла подібна до адреси групової розсилки для усіх вузлів.
- Перевага групової адреса запитуваного вузла полягає в тому, що вона зіставляється з особливою груповою адресою Ethernet.
- Це дозволяє мережній платі Ethernet фільтрувати кадр, аналізуючи MAC-адресу призначення, не надсилаючи його до процесу IPv6, щоб переконатися, що пристрій дійсно є вузлом призначення пакету IPv6.

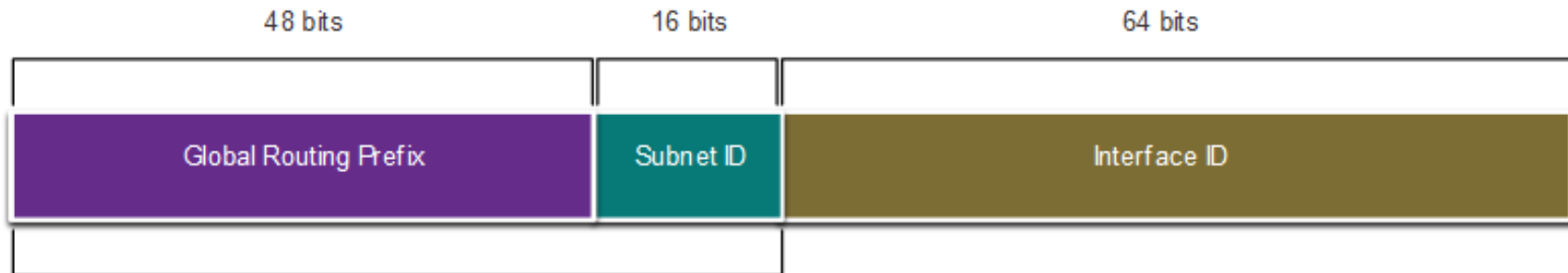


Розподіл мережі IPv6 на підмережі

Розподіл на підмережі з використанням ідентифікатора підмережі

Протокол IPv6 був розроблений з урахуванням підмереж.

- Окреме поле Ідентифікатор підмережі глобальної індивідуальної адреси IPv6 використовується для створення підмереж.
- Поле Ідентифікатор підмережі (Subnet ID) - це область між префіксом глобальної маршрутизації (Global Routing Prefix) та ідентифікатором інтерфейсу (Interface ID).



A /48 routing prefix + 16 bit Subnet ID = /64 prefix

Приклад створення підмереж IPv6

Організації призначено префікс глобальної маршрутизації 2001:db8:acad::/48 з 16-бітним ідентифікатором підмережі:

- Дозволяє створити 65 536 /64 підмереж, як показано на рисунку.
- Префікс глобальної маршрутизації однаковий для всіх підмереж.
- Для кожної підмережі збільшується лише шістнадцятковий ідентифікатор підмережі.

Increment subnet ID to create 65,536 subnets

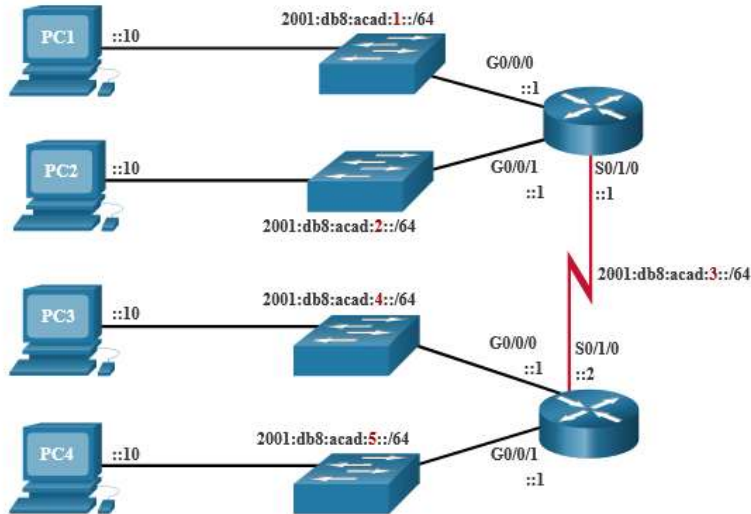
```
2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64
2001:db8:acad:0009::/64
2001:db8:acad:000a::/64
2001:db8:acad:000b::/64
2001:db8:acad:000c::/64
Subnets 13 – 65,534 not shown
2001:db8:acad:fff::/64
```

Розподіл мережі IPv6 на підмережі

Розподіл підмережі IPv6

На прикладі топологія вимагає п'ять підмереж, по одній для кожної локальної мережі (LAN), а також для послідовного зв'язку між маршрутизаторами R1 та R2.

П'ять підмереж IPv6 було виділено з полям ідентифікаторів підмережі 0001 - 0005. Кожна підмережа /64 надаватиме більше адрес, ніж коли-небудь знадобиться.



Address Block 2001:0db8:acad::/48

5 subnets allocated from 65,536 available subnets

```
2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64

2001:db8:acad:ffff::/64
```

Налаштування маршрутизатора з підмережами IPv6

У прикладі показано, що кожен з інтерфейсів на маршрутизаторі R1 налаштований на іншу підмережу IPv6.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

Що ми вивчили у цій темі?

- Теоретично максимальна кількість IPv4 адрес 4,3 мільярда.
- Фахівці IETF створили різні протоколи та інструменти, які допомагають мережним адміністраторам поступово здійснити перехід своїх мереж на IPv6.
- Технології переходу можна розділити на три категорії: подвійний стек, тунелювання та перетворення адрес.
- Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень.
- Основний формат для запису IPv6 адреси - x:x:x:x:x:x:x:x, де кожен x складається з чотирьох шістнадцяткових значень.
- Існує три типи IPv6-адрес: індивідуальна, групова, альтернативна адреси.
- Індивідуальна адреса IPv6 однозначно ідентифікує інтерфейс на пристрої з підтримкою IPv6.
- Глобальна індивідуальна адреса (GUA) IPv6 глобально унікальна та доступна для маршрутизації в Інтернеті IPv6.
- Локальна IPv6-адреса каналу (LLA) дозволяє пристрою взаємодіяти з іншими пристроями під керуванням IPv6, що знаходяться в одному і тому ж каналі (підмережі) і тільки в ньому.
- Для налаштування глобальної індивідуальної адреси IPv6 на інтерфейсі використовується команда: **ipv6 address** *ipv6-address/prefix-length*.
- Пристрій динамічно отримує глобальну індивідуальну IPv6-адресу через повідомлення ICMPv6. Маршрутизатори IPv6 періодично розсилають повідомлення RA ICMPv6 кожні 200 секунд для усіх пристроїв під керуванням IPv6.

Що ми вивчили у цій темі? (Продовж.)

- Повідомлення RA мають три методи: SLAAC, SLAAC і DHCPv6-сервер без відстеження стану та DHCPv6 з відстеженням стану (без SLAAC).
- Ідентифікатор інтерфейсу може бути створений за допомогою процесу EUI-64 або випадково згенерованого 64-бітного числа.
- Цей процес використовує 48-бітну MAC-адресу Ethernet клієнта і в середину цієї адреси вставляє ще 16 бітів для створення 64-бітного ідентифікатора інтерфейсу.
- Залежно від операційної системи, пристрій може використовувати випадково згенерований ідентифікатор інтерфейсу.
- Всі IPv6 повинні мати локальну IPv6-адресу каналу. LLA можна налаштувати статично або створити динамічно.
- Маршрутизатори Cisco автоматично створюють локальну IPv6-адресу каналу щоразу, коли інтерфейсу призначено глобальну індивідуальну адресу.
- Існує два типи групових IPv6-адрес: відома групова адреса і групова адреса запитуваного вузла.
- Дві загальноприйняті групи IPv6-адрес для групової розсилки: групова розсилка для усіх вузлів ff02::1 та групова розсилка для усіх маршрутизаторів ff02::2.
- Групова адреса запитуваного вузла аналогічна адресі групової розсилки для усіх вузлів. Перевага групової адреса запитуваного вузла полягає в тому, що вона відповідає спеціальній адресі групової розсилки Ethernet.
- Протокол IPv6 був розроблений з урахуванням підмереж. Окреме поле Ідентифікатор підмережі глобальної індивідуальної адреси IPv6 використовується для створення підмереж.

Нові терміни та команди

- Гекстет
- Локальна адреса каналу (LLA)
- Адреса ipv6
- show ipv6 interface brief
- Автоматичне налаштування адреси без відстеження стану (SLAAC, Stateless Address Autoconfiguration)
- Анонсування маршрутизатора (RA, Router Advertisement)
- Запит маршрутизатора (RS, Router Solicitation)
- Процес EUI-64
- Групова адреса запитуваного вузла

Протокол ICMP v4/v6



Завдання

Мета : Використання різних засобів для перевірки мережного з'єднання.

Назва теми	Мета вивчення теми
Повідомлення ICMP	Пояснити як протокол ICMP використовується для перевірки мережного з'єднання.
Тестування за допомогою ping і traceroute	Використовувати утиліти ping і traceroute для тестування мережного з'єднання.

Повідомлення ІСМР

Повідомлення ICMPv4 і ICMPv6

- Міжмережний протокол керуючих повідомлень (ICMP, Internet Control Message Protocol) забезпечує зворотній зв'язок щодо питань, пов'язаних з обробкою IP-пакетів за певних умов.
- ICMPv4 - це протокол обміну повідомленнями для IPv4. ICMPv6 - це протокол обміну повідомленнями для IPv6 і включає додаткову функціональність.
- ICMP-повідомлення, спільні для ICMPv4 і ICMPv6:
 - Досяжність вузла.
 - Пункт призначення або служби недоступні.
 - Перевищено час очікування.

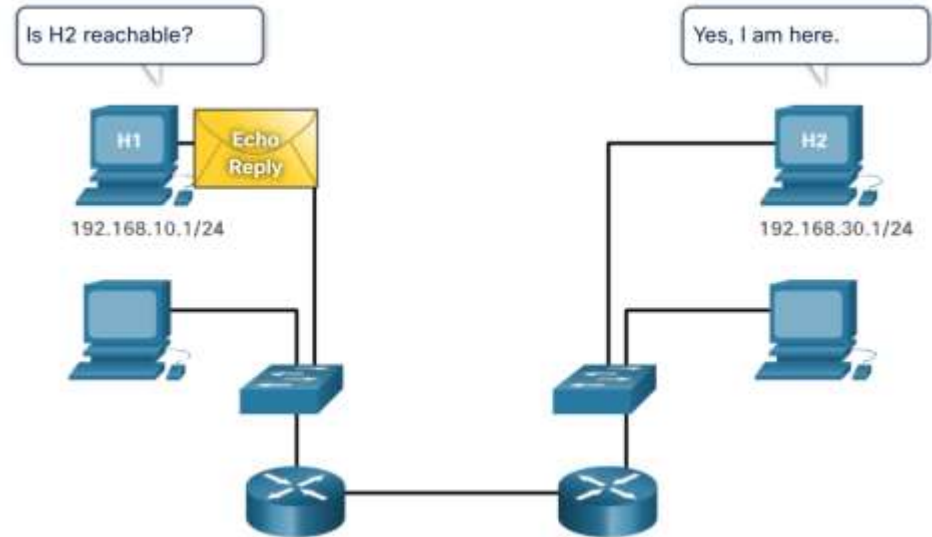
Повідомлення ICMP є необов'язковими та часто заборонені в межах мережі з міркувань безпеки.

Досяжність вузла

Ехо-повідомлення ICMP можна використовувати для перевірки досяжності вузла в IP-мережі.

Як наведено у прикладі:

- Локальний вузол надсилає ICMP ехо-запит іншому вузлу.
- Якщо вузол доступний, то вузол призначення відповідає, надсилаючи ехо-відповідь.



Пункт призначення або служби недоступні

- ICMP-повідомлення Пункт призначення недосяжний (Destination Unreachable) використовується для сповіщення джерела, що вузол призначення або служби для цього пакета недоступні.
- Повідомлення буде містити код, який вказує на те, чому пакет не може бути доставлено.

Приклади деяких кодів повідомлень про недоступність вузла призначення для ICMPv4:

- 0 - Мережа недоступна.
- 1 - Вузол недоступний.
- 2 - Протокол недоступний.
- 3 - Порт недоступний.

Приклади деяких кодів повідомлень про недоступність вузла призначення для ICMPv6:

- 0 - Немає маршруту до пункту призначення.
- 1 - Зв'язок з пунктом призначення адміністративно заборонений (наприклад, брандмауер).
- 2 - Поза межами адреси джерела.
- 3 - Адреса недоступна.
- 4 - Порт недоступний.

Примітка. Протокол ICMPv6 має схожі, але дещо відмінні коди повідомлень Пункт призначення недосяжний (Destination Unreachable).

Перевищено час очікування

- Коли поле Час життя (TTL, Time to Live) у пакеті зменшиться до 0, то вузлу джерела буде надіслано повідомлення ICMPv4 Перевищено час очікування.
- ICMPv6 також надсилає повідомлення Перевищено час очікування у такій ситуації. Замість поля TTL в IPv4, протокол ICMPv6 використовує поле Обмеження переходів (Hop Limit) в IPv6, щоб визначити, чи закінчився термін дії пакету.

```
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Примітка.: Повідомлення Перевищено час очікування (Time Exceeded) використовуються інструментом traceroute.

Повідомлення ICMPv6

У ICMPv6 має нові можливості та вдосконалену функціональність, які не знайти в ICMPv4, включаючи чотири нові протоколи як частину протоколу виявлення сусідів (NDP або ND, Neighbor Discovery Protocol).

Обмін повідомленнями між маршрутизатором IPv6 і пристроєм IPv6, включає динамічний розподіл адрес, який є таким:

- Запит маршрутизатора (RS, Router Solicitation).
- Анонсування маршрутизатора (RA, Router Advertisement).

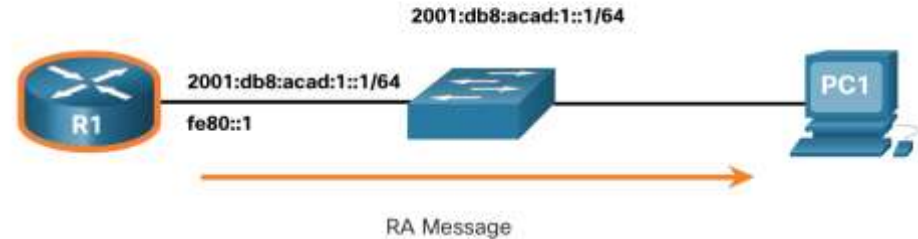
Обмін повідомленнями між пристроями IPv6, включаючи виявлення дублікатів адреси та визначення адреси, є такими:

- Запит сусіда (NS, Neighbor Solicitation,).
- Анонсування сусіда (NA, Neighbor Advertisement).

Примітка. ICMPv6 ND також включає в себе переспрямування повідомлення, яке має функцію, схожу на подібну функцію переспрямування повідомлення, що використовується в ICMPv4.

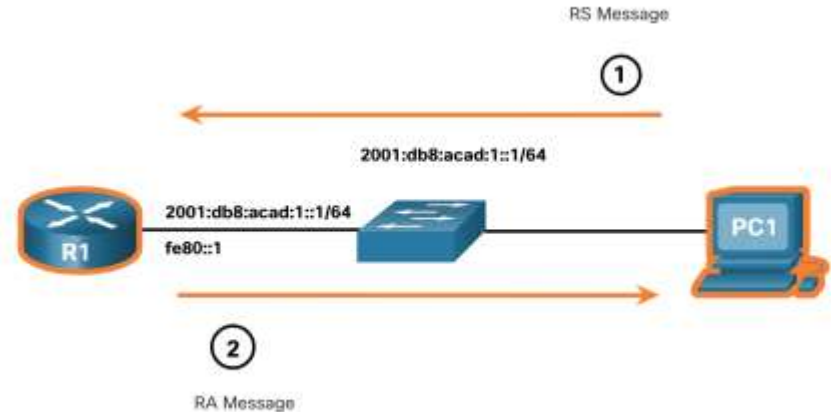
Повідомлення ICMPv6 (Продовж.)

- Повідомлення RA надсилаються маршрутизаторами з підтримкою IPv6 кожні 200 секунд для надання інформації про адресацію вузлам з підтримкою IPv6.
- Повідомлення RA може включати таку інформацію про адресацію вузла, як префікс, довжина префікса, DNS-адреса та доменне ім'я.
- Вузол, який використовує SLAAC, встановить як шлюз за замовчуванням локальну адресу каналу маршрутизатора, який надіслав повідомлення RA.



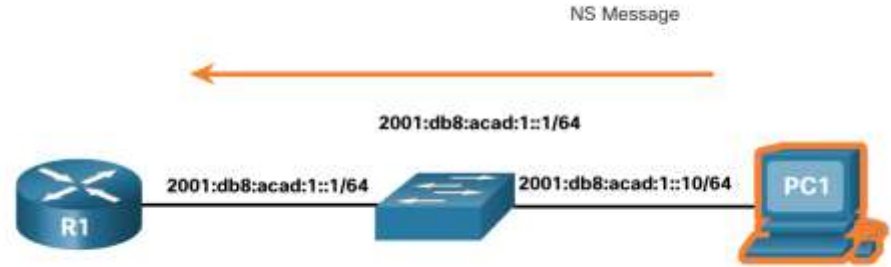
Повідомлення ICMPv6 (Продовж.)

- Маршрутизатор з підтримкою IPv6 також надсилатиме повідомлення RA у відповідь на повідомлення RS.
- На рисунку PC1 надсилає повідомлення RS, щоб визначити, як динамічно отримувати інформацію про свою адресу IPv6.
 - R1 відповідає на повідомлення RS повідомленням RA.
 - PC1 надсилає повідомлення RS: «Привіт, я щойно завантажився. Чи є в мережі маршрутизатор IPv6? Мені потрібно знати, як динамічно отримувати інформацію про свою адресу IPv6».
 - Маршрутизатор R1 відповідає повідомленням RA. «Привіт усім пристроям із підтримкою IPv6. Я R1, і ви можете використовувати SLAAC для створення глобальної індивідуальної адреси IPv6. Префікс - 2001:db8:acad:1::/64. До речі, використовуйте мою локальну адресу fe80::1 як шлюз за замовчуванням».



Повідомлення ICMPv6 (Продовж.)

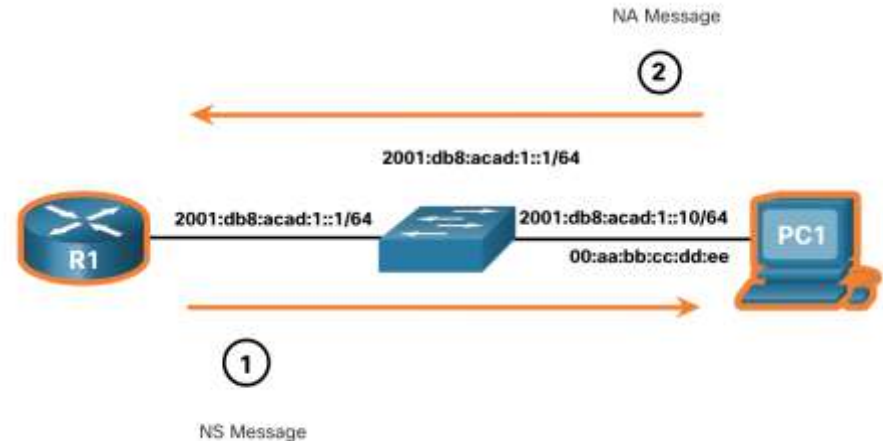
- Пристрій, якому призначено глобальну адресу IPv6 або локальну адресу, може здійснювати виявлення дублікатів адрес (DAD), щоб гарантувати унікальність адреси IPv6.
- Щоб перевірити унікальність адреси, пристрій надсилає NS повідомлення зі своєю власною адресою IPv6 як адресою призначення.
- Якщо інший пристрій в мережі має цю адресу, він відповідає повідомленням NA.



Примітка: Процес DAD не є обов'язковим, але RFC 4861 рекомендує його виконувати для визначення індивідуальної адреси.

Повідомлення ICMPv6 (Продовж.)

- Щоб визначити MAC-адресу призначення, пристрій надсилатиме повідомлення NS на адресу запитуваного вузла.
- Повідомлення має містити відому (цільову) IPv6 адресу. Пристрій, який має цільову IPv6 адресу, відповідь повідомленням NA, що буде містити його Ethernet MAC-адресу.
- На рисунку, маршрутизатор R1 надсилає повідомлення NS на адресу 2001:db8:acad:1::10 з проханням вказати його MAC-адресу.



Тестування за допомогою ping і traceroute

Тестування за допомогою ping та traceroute

Утиліта ping - Перевірка зв'язку

- Утиліта **ping** - це інструмент для тестування IPv4 і IPv6, який використовує ICMP ехо-запит та ехо-відповідь для перевірки зв'язку між вузлами та надає підсумок, що включає показник успішності та середній час в обидва кінці до пункту призначення.
- Якщо протягом цього інтервалу відповіді не отримано, команда ping видає повідомлення про те, що відповідь не була отримана.
- Зазвичай для першого ехо-запиту потрібно виконати визначення адреси (ARP або ND) перед відправкою ехо-запиту ICMP.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2

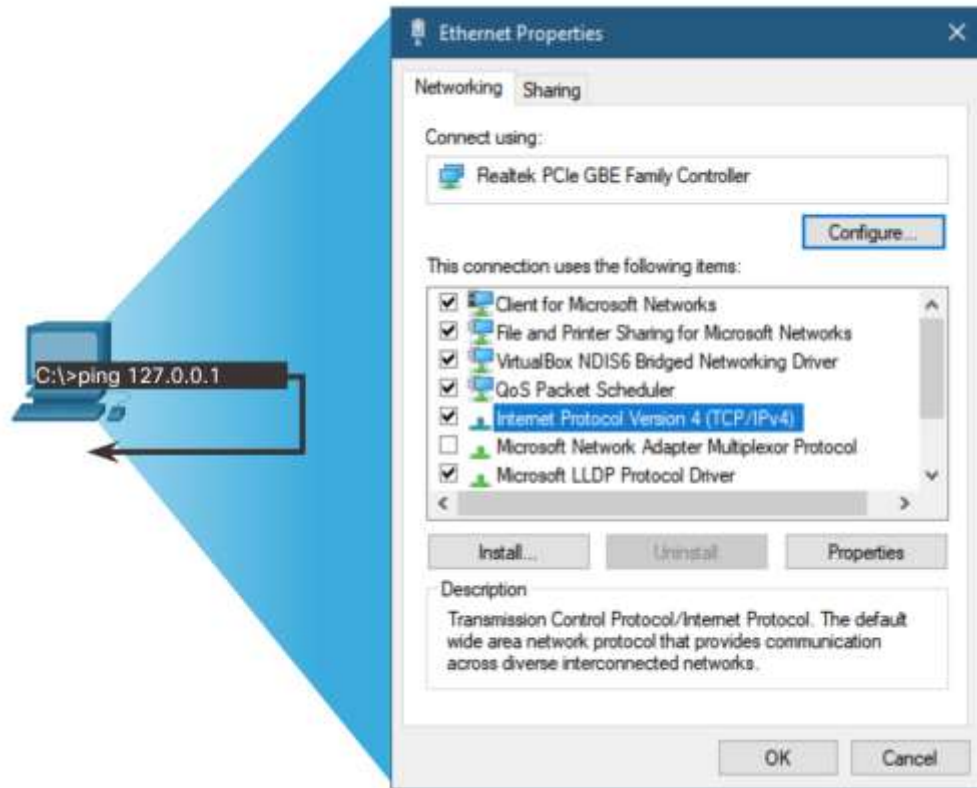
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Тестування інтерфейсу loopback за допомогою команди ping

Утиліту ping можна використовувати для тестування внутрішньої конфігурації IPv4 або IPv6 на локальному вузлі. Для виконання цього тесту, потрібно відправити команду на локальну адресу loopback 127.0.0.1 для IPv4 (::1 для IPv6).

Відповідь від 127.0.0.1 для IPv4 або від ::1 для IPv6 означає, що IP-протокол правильно налаштовано на вузлі.

- Повідомлення про помилку вказує на те, що стек протоколів TCP/IP не працює на вузлі.

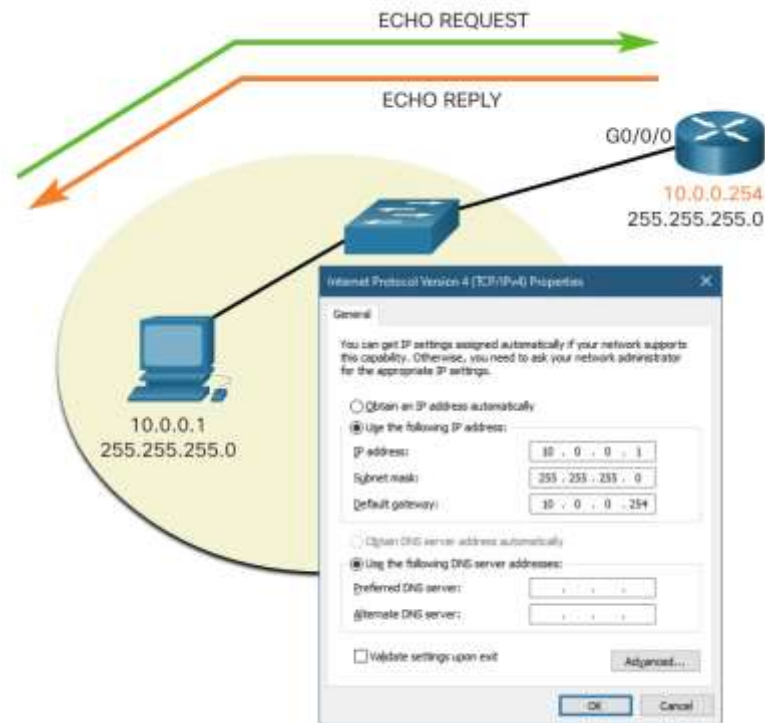


Перевірка зв'язку зі шлюзом за замовчуванням за допомогою команди ping

Ви також можете використовувати команду **ping**, щоб перевірити чи може вузол обмінюватися даними в локальній мережі.

Для цієї перевірки найчастіше використовується адреса шлюзу за замовчуванням, оскільки маршрутизатор практично завжди знаходиться в робочому стані.

- Успішне відправлення команди на шлюз за замовчуванням вказує на те, що вузол та інтерфейс маршрутизатора, що виступає як шлюз за замовчуванням, правильно функціонують в локальній мережі.
- Якщо адреса шлюзу за замовчування не відповідає, команда може бути відправлена на IP-адресу іншого вузла в локальній мережі, який, як відомо, працює.



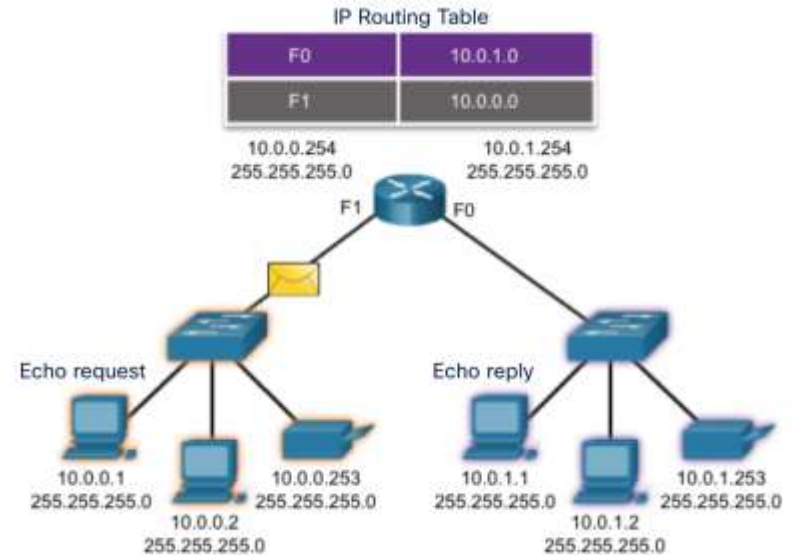
Тестування за допомогою ping та traceroute

Встановлення зв'язку з віддаленим вузлом за допомогою команди ping

Утиліта ping також може використовуватися для перевірки здатності локального вузла взаємодіяти в локальній мережі.

Локальний вузол може пропінгувати вузол у віддаленій мережі. Якщо відправлений ping виявився успішним, то може бути перевірено функціонування великої частини локальної мережі.

Примітка: Багато адміністраторів мережі обмежують або забороняють введення ICMP-повідомлень, тому відсутність відповіді на запити **ping**, може бути наслідком обмежень безпеки.



Утиліта Traceroute – Тестування шляху

- Traceroute (**tracert**) - це утиліта, яка використовується для перевірки шляху між двома вузлами та виводить перелік хопів (hop), які були успішно досягнуті на шляху до вузла призначення.
- Утиліта traceroute визначає сумарний час проходження сигналу в прямому і зворотному напрямках (RTT) повідомляє про можливу відсутність відповіді на одному з переходів. Символ зірочка (*) використовується для позначення втраченого пакета або відсутності відповіді на пакет.
- Ця інформація може бути використана для пошуку проблемного маршрутизатора на шляху або може вказати, що маршрутизатор налаштований так, щоб не відповідати.

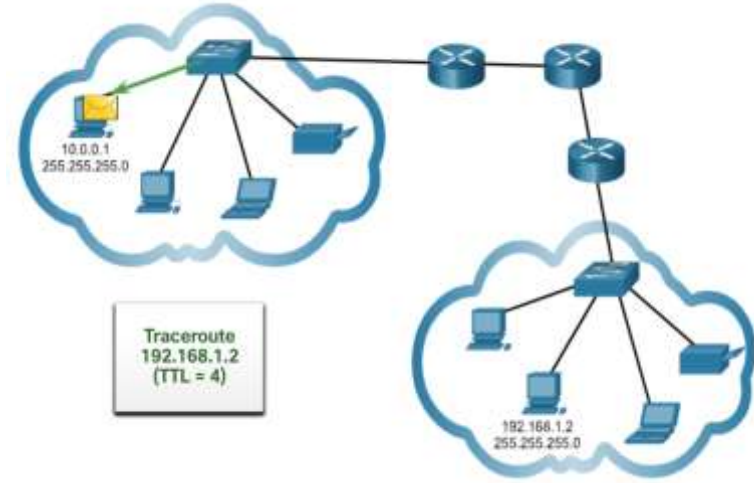
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

 0  192.168.10.2    0 msec  0 msec  0 msec
 1  192.168.10.2    1 msec  0 msec  0 msec
 2  192.168.20.2    2 msec  1 msec  0 msec
 3  192.168.30.2    1 msec  0 msec  0 msec
 4  192.168.40.2    0 msec  0 msec  0 msec
```

Примітка: Утиліта traceroute використовує функцію поля Час життя (TTL) в IPv4 та поля Обмеження переходів (Hop Limit) в IPv6 в заголовках Рівня 3 (разом з ICMP-повідомленням Перевищено час очікування (Time exceeded)).

Утиліта Traceroute – Тестування шляху (Продовж.)

- Перша послідовність повідомлень, відправлених командою traceroute, матиме значення поля TTL, яке рівне 1. Дане значення TTL викликає перевищення часу очікування відповіді на пакет IPv4 на першому маршрутизаторі. Потім цей маршрутизатор відповідає ICMPv4-повідомленням Перевищено час очікування.
- Потім traceroute поступово збільшує поле TTL (2, 3, 4...) для кожної наступної послідовності повідомлень. Таким чином трасуються адреси кожного переходу, у міру того як перевищення часу очікування відповіді відбувається далі на маршруті.
- Значення в полі TTL продовжує збільшуватися до тих пір, поки не буде досягнуто вузол призначення, або до певного заздалегідь встановленого максимального рівня.



Що ми вивчили?

- Міжмережний протокол керуючих повідомлень (ICMP, Internet Control Message Protocol) надає зворотній зв'язок щодо питань, пов'язаних з обробкою IP-пакетів за певних умов.
- Повідомлення ICMP, загальні для ICMPv4 і ICMPv6, є: досяжність вузла, пункт призначення або служби недоступні та перевищено час очікування.
- Обмін повідомленнями між маршрутизатором IPv6 і пристроєм IPv6 разом із динамічним розподілом адрес, включають RS і RA. Повідомлення між пристроями IPv6 включають перенаправлення (аналогічно IPv4), NS і NA.
- Ping (як в IPv4, так і в IPv6) використовує повідомлення ехо-запит та ехо-відповідь ICMP для перевірки зв'язку між вузлами.
- Утиліту ping можна використовувати для тестування внутрішньої конфігурації IPv4 або IPv6 на локальному вузлі.
- Traceroute (tracert) - це утиліта, яка виводить перелік переходів (хопів), через які проходить шлях пакета.

Нові терміни і команди

- Протокол ICMP
- Протокол ICMPv4
- Протокол ICMPv6
- Команда ping
- Команда traceroute
- Команда tracert
- Протокол виявлення сусідів (NDP або ND, Neighbor Discovery Protocol)
- Запит маршрутизатора (RS, Router Solicitation)
- Анонсування маршрутизатора (RA, Router Advertisement)
- Запит сусіда (NS, Neighbor Solicitation)
- Анонсування сусіда (NA, Neighbor Advertisement)
- Час життя (TTL, Time to Live)

Транспортний рівень



Завдання

Мета : Порівняти операцій протоколів транспортного рівня з точки зору підтримки наскрізного з'єднання.

Назва теми	Мета вивчення теми
Транспортування даних	Пояснити призначення транспортного рівня при керуванні наскрізним з'єднанням.
Огляд TCP	Пояснити характеристики TCP.
Огляд UDP	Пояснити характеристики UDP.
Номери портів	Пояснити, як TCP і UDP використовують номери портів.
Процес TCP-з'єднання	Пояснити як процеси створення і завершення сеансів TCP сприяють надійному передаванню даних.
Надійність і керування потоком	Пояснити, як відбувається передавання блоків даних протоколу TCP і забезпечується їх гарантована доставка.
Передавання даних UDP	Порівняти операцій протоколів транспортного рівня з точки зору підтримки наскрізного з'єднання..

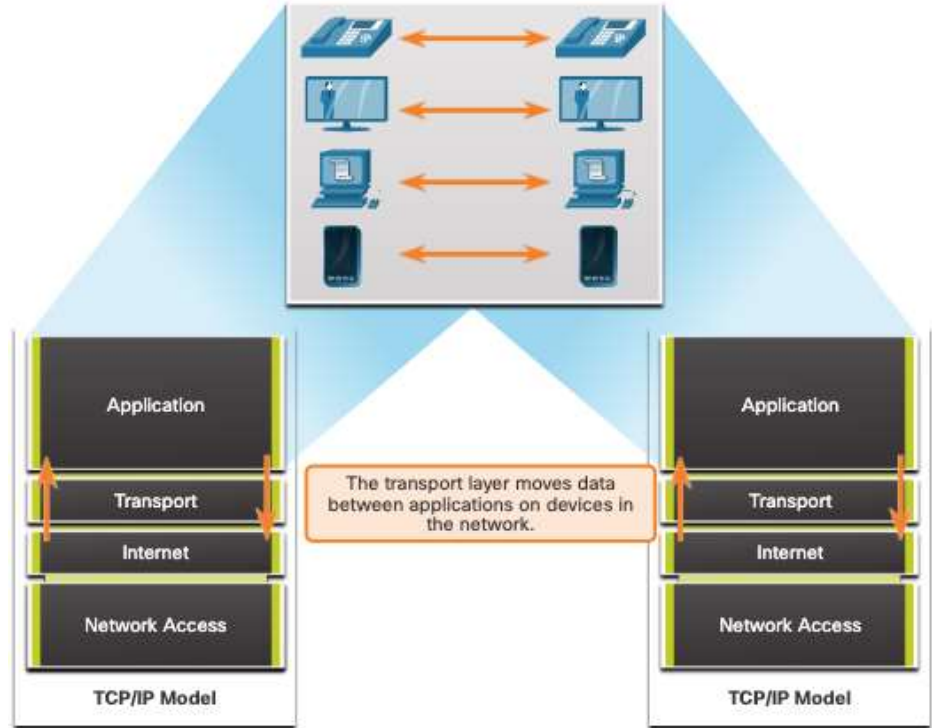
Транспортування даних

Транспортування даних

Роль транспортного рівня

Транспортний рівень:

- відповідає за логічні зв'язки між застосунками, запущеними на різних вузлах.
- з'єднує рівень застосунків і нижчі рівні, які відповідають за передавання даних мережею.

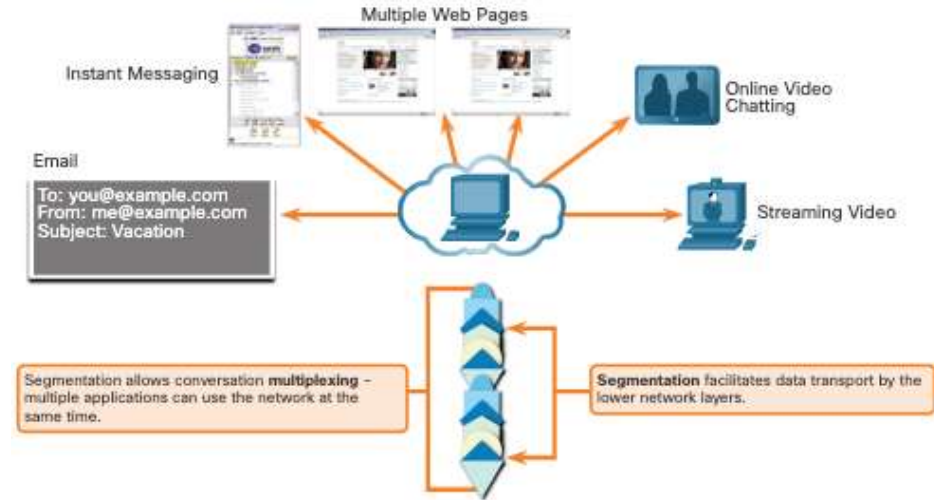


Транспортування даних

Обов'язки транспортного рівня

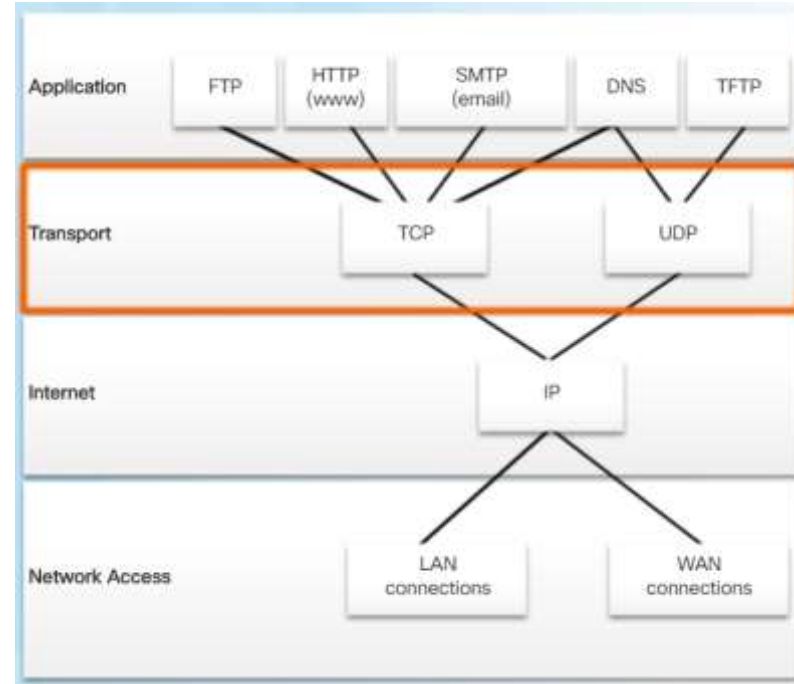
Транспортний рівень має кілька зон відповідальності:

- Відстеження окремих сеансів зв'язку.
- Сегментація даних і впорядкування сегментів.
- Додавання інформації заголовку.
- Визначення, розмежування та керування кількома розмовами.
- Використання сегментації та мультиплексування для поєднання різних комунікаційних діалогів у одному каналі зв'язку.



Протоколи транспортного рівня

- IP не впливає на спосіб доставки або транспортування пакетів.
- Протоколи транспортного рівня визначають спосіб передавання повідомлень між вузлами, і відповідають за керування вимогами надійності діалогу.
- Транспортний рівень включає протоколи TCP і UDP.

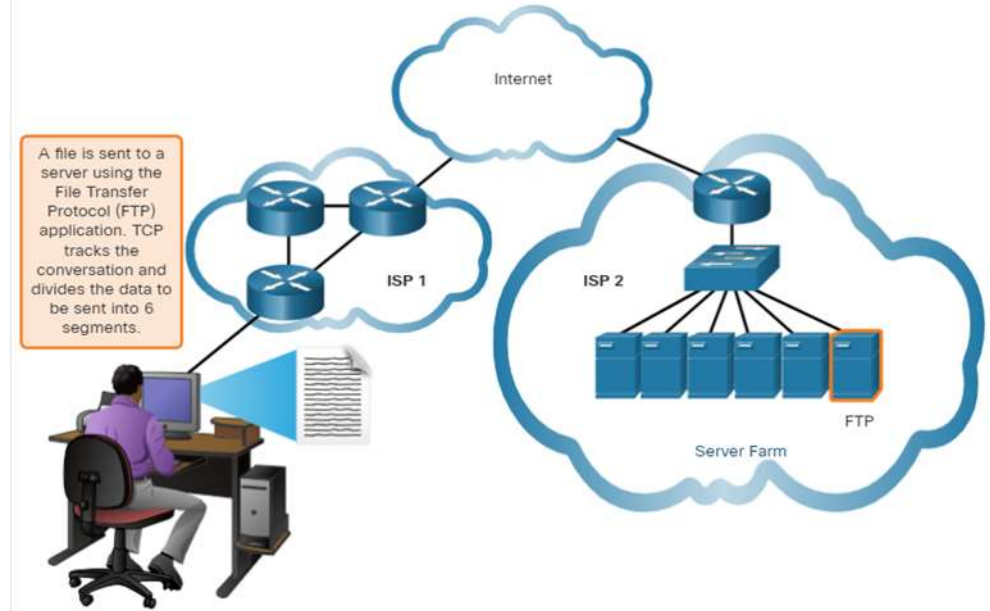


Транспортування даних

Протокол TCP

TCP забезпечує надійність і контроль за потоком даних. Основні функції TCP:

- Нумерація і відстеження сегментів даних, переданих конкретному вузлу від визначеного застосунку.
- Підтвердження отримання даних.
- Повторне надсилання будь-яких непідтверджених даних через певний проміжок часу.
- Відновлення послідовності даних, які могли надійти в неправильному порядку.
- Надсилання даних з ефективною швидкістю, прийнятною для одержувача

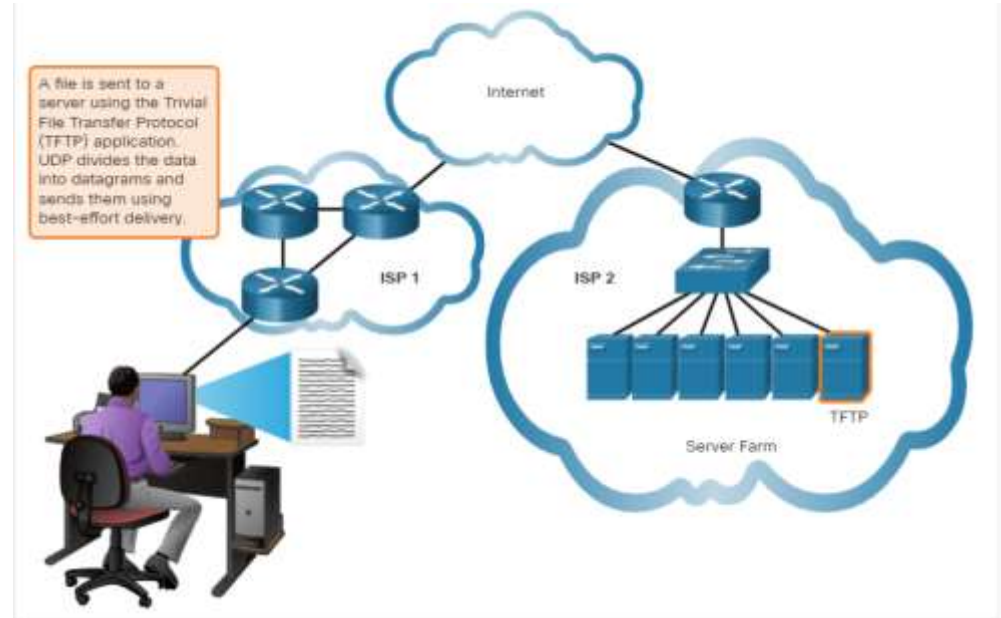


Транспортування даних

Протокол UDP

UDP забезпечує основні функції для доставки дейтаграм між відповідними застосунками, з незначними накладними витратами та перевіркою даних.

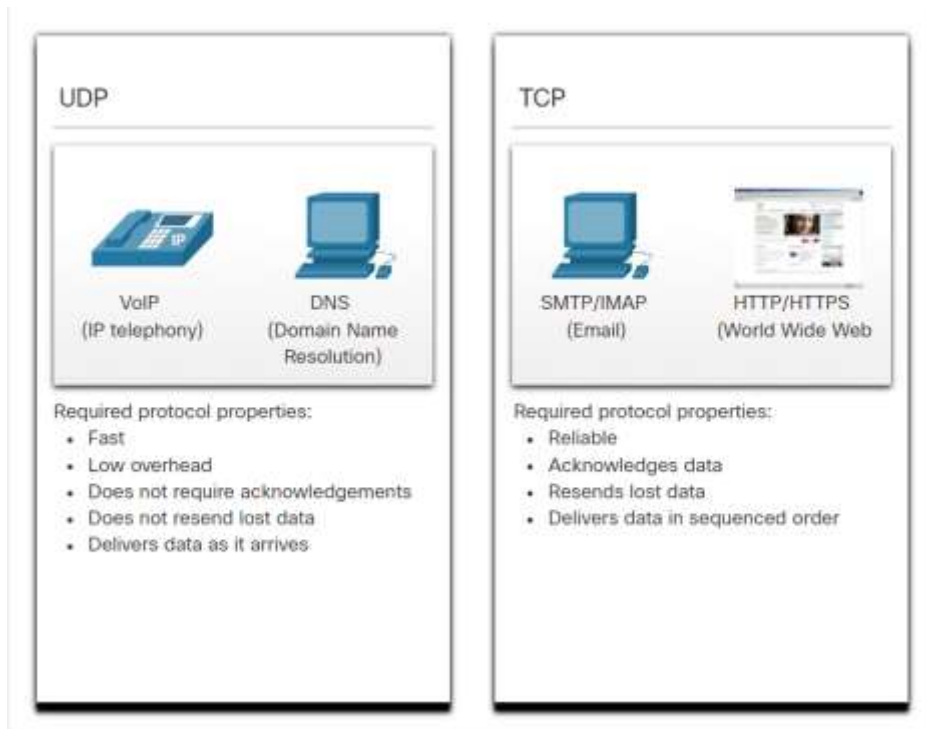
- UDP - це протокол без встановлення з'єднання.
- UDP не гарантує доставки, проте робить все можливе, оскільки немає підтвердження того, що дані отримані за місцем призначення.



Відповідний протокол транспортного рівня для відповідного застосунку

Окрім цього, UDP використовується застосунками, які працюють у режимі запит-відповідь, де дані подаються невеликими порціями, а повторне надсилання виконується досить швидко.

Якщо важливо, щоб усі дані надходили і оброблялися у належній послідовності, як транспортний протокол слід використовувати TCP.



Огляд ТСР

Функції TCP

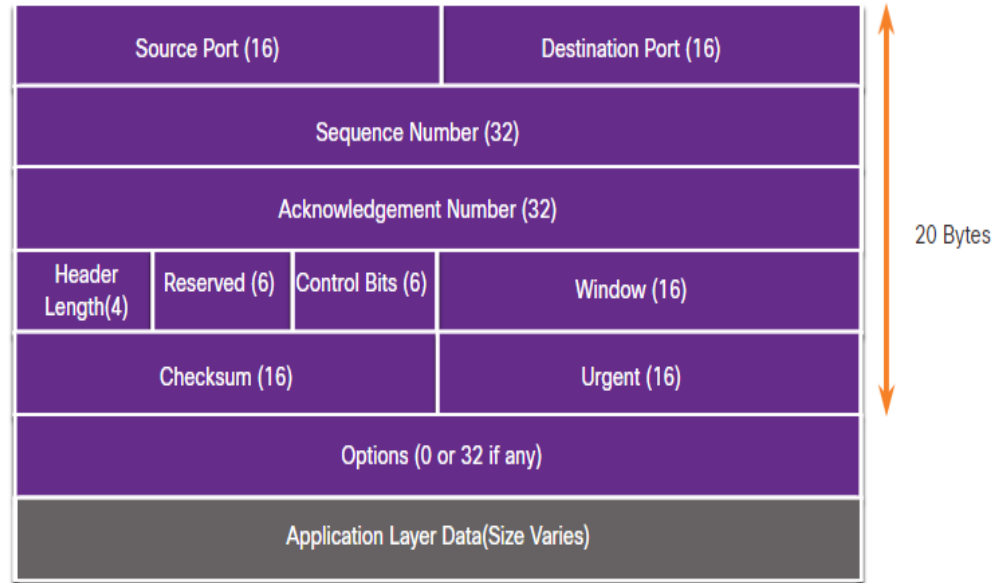
- **Встановлення сеансу** - TCP - це орієнтований на з'єднання протокол, який перш ніж розпочати пересилання будь-якого трафіку узгоджує деталі та налаштовує постійне з'єднання (або сеанс) між пристроями джерела і призначення.
- **Забезпечення надійної доставки** - У процесі передавання мережею з багатьох причин може трапитися пошкодження або повна втрата сегментів. TCP гарантує, що кожен сегмент, який надсилається джерелом, надходить до пункту призначення.
- **Забезпечення впорядкованої доставки** - Оскільки у мережі може існувати декілька шляхів з різною пропускну здатністю, дані можуть надходити в неправильному порядку.
- **Підтримка керування потоком** - Мережні вузли мають обмежені ресурси (зокрема, пам'ять і обчислювальну потужність). Коли TCP виявляє, що ці ресурси перевантажені, він може надіслати запит до застосунку відправника з проханням зменшити швидкість потоку даних.

Огляд TCP

Заголовок TCP

TCP - це протокол із контролем стану (stateful), який відстежує стан сеансів зв'язку.

Для цього, TCP фіксує надіслану інформацію, а також підтвердження про її отримання.



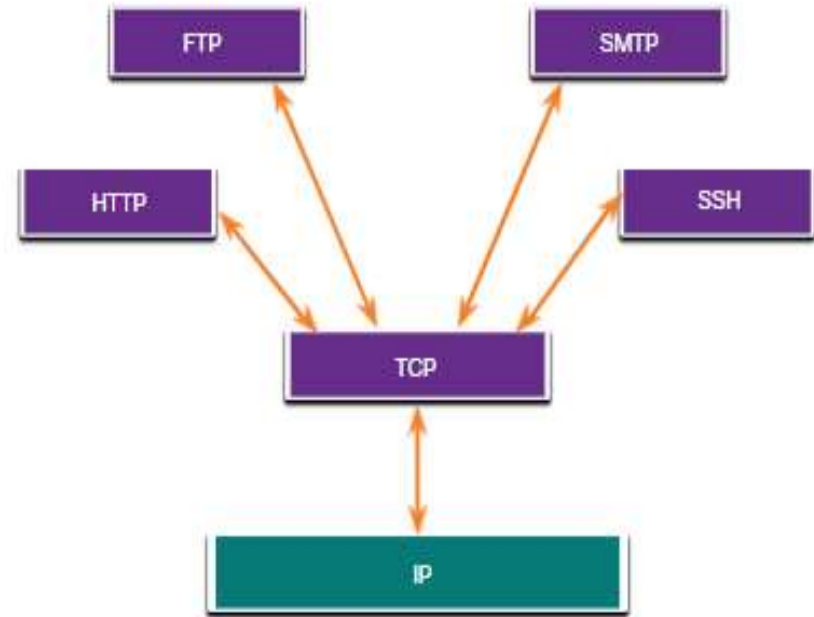
Огляд TCP

Поля TCP-заголовка

Поля заголовка TCP	Опис
Порт джерела	16-бітне поле, яке використовується для ідентифікації застосунку відправника за номером порту.
Порт призначення	16-бітне поле, яке використовується для ідентифікації застосунку призначення за номером порту.
Порядковий номер	32-бітне поле, яке використовується для відновлення послідовності надходження даних.
Номер підтвердження	32-бітне поле, яке використовується для позначення того, що дані були отримані, а також номеру наступного байта, який очікується від джерела.
Довжина заголовку	4-бітне поле, відоме як зміщення даних, що вказує на довжину заголовка сегмента TCP.
Зарезервовано	Поле довжиною 6 бітів, яке зарезервоване для майбутнього використання.
Контрольні біти	Поле з 6 бітів, яке містить двійкові коди або прапорці, що позначають призначення або функцію TCP-сегмента.
Розмір вікна	16-бітне поле, яке використовується для позначення кількості байтів, які можуть бути прийняті за один раз.
Контрольна сума	Поле розміром 16 бітів, яке використовується для перевірки помилок у даних та у заголовку сегмента.
Показчик терміновості	16-бітне поле, яке використовується як ознака того, що сегмент містить термінові дані.

Застосунки, які використовують TCP

TCP виконує усі завдання, пов'язані з розбиттям потоку даних на сегменти, забезпеченням надійності, керуванням потоком даних і перегрупуванням сегментів.



Огляд UDP

Огляд UDP

Функції UDP

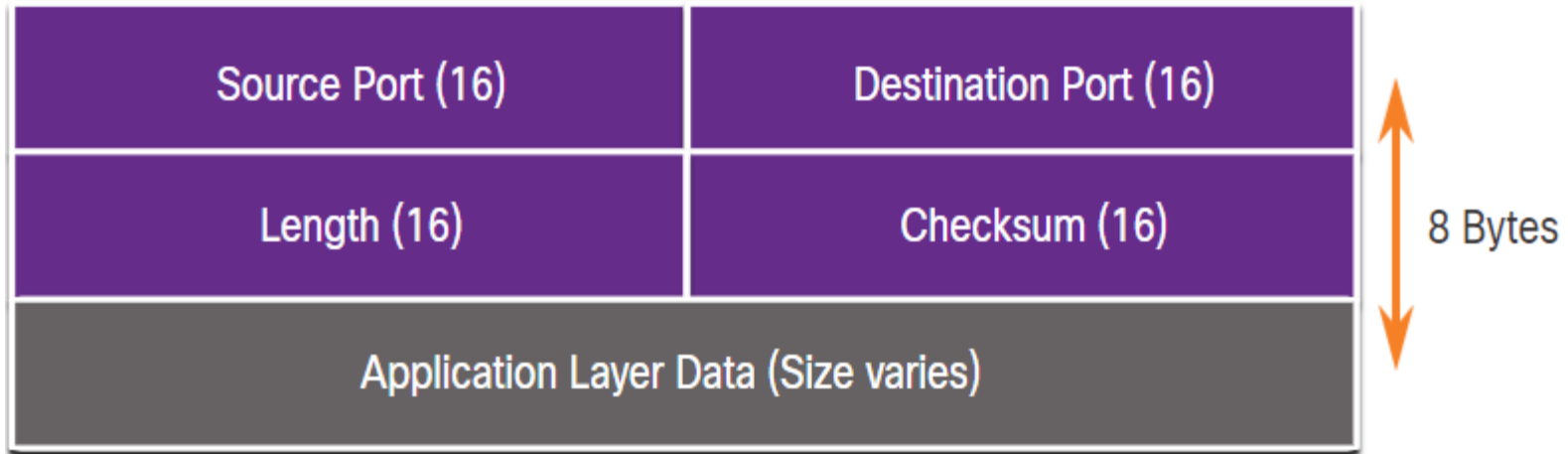
Основні характеристики UDP:

- Дані обробляються у порядку їх надходження.
- Будь-які втрачені сегменти повторно не надсилаються.
- Немає попереднього налаштування сеансу з'єднання.
- Відправник не інформується про доступність ресурсів з боку одержувача.

Огляд UDP

Заголовок UDP

У порівнянні з TCP, заголовок UDP набагато простіший, оскільки містить лише чотири поля і потребує 8 байтів (тобто 64 біти).



Огляд UDP

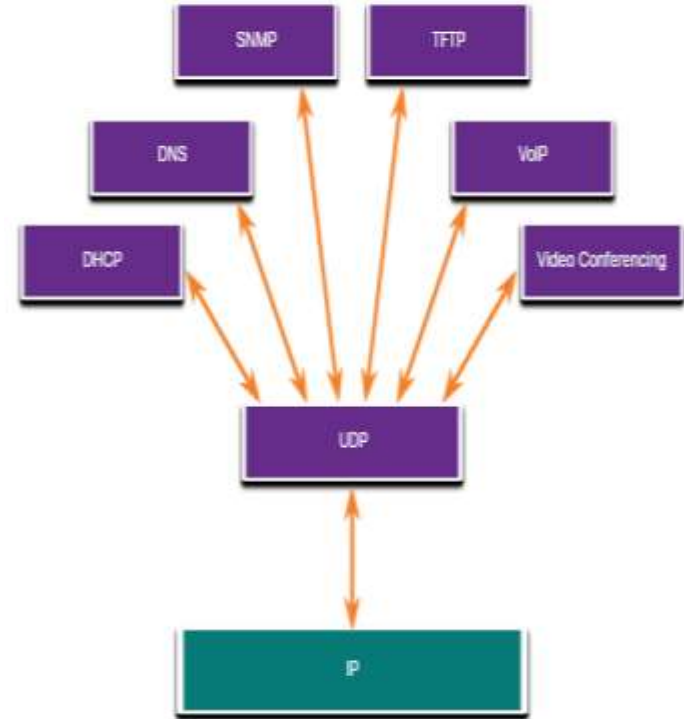
Поля UDP-заголовка

У таблиці визначено та описано чотири поля заголовка UDP.

Поля заголовка UDP	Опис
Порт джерела	16-бітне поле, яке використовується для ідентифікації застосунку відправника за номером порту.
Порт призначення	16-бітне поле, яке використовується для ідентифікації застосунку призначення за номером порту.
Довжина	16-бітне поле, яке вказує довжину заголовка UDP-дейтаграми.
Контрольна сума	16-бітне поле, яке використовується для перевірки наявності помилок у даних і в заголовку дейтаграм.

Застосунки, які використовують UDP

- Мультимедійні і відео застосунки, що працюють наживо - Такі програми допускають деякі втрати даних, при цьому вимагають дуже малих затримок або повної їх відсутності. Прикладами можуть бути VoIP і потокове відео.
- Прості застосунки типу "запит-відгук"- Застосунки, що працюють у режимі простих транзакцій, при якому вузол, що надсилає запит, може не отримати відповіді. До них належать DNS і DHCP.
- Програми, які самі забезпечують надійність - Однонаправлені з'єднання, які не потребують керування потоком, виявлення помилок, підтвердження про доставку та виправлення помилок, або ці функції може забезпечити сам застосунок. Прикладами є SNMP і TFTP.




Номери портів

Декілька окремих комунікацій

Протоколи транспортного рівня TCP і UDP використовують номери портів для керування кількома одночасними діалогами.

Номер порту джерела пов'язаний з вихідною програмою на локальному вузлі, тоді як номер порту отримувача пов'язаний з програмою призначення з боку отримувача.



The diagram consists of two adjacent purple rectangular boxes. The left box is labeled 'Source Port (16)' and the right box is labeled 'Destination Port (16)'. A thin vertical line is positioned to the right of the rightmost box.

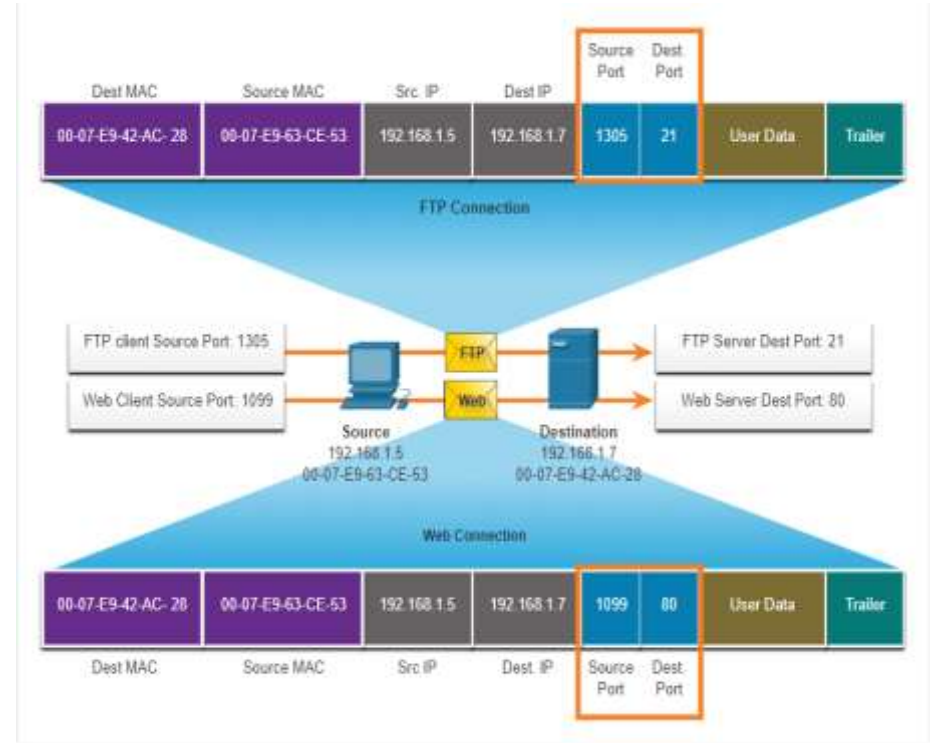
Source Port (16)

Destination Port (16)

Номери портів

Пари сокетів

- Номери портів джерела та призначення прописані в сегменті.
- Далі ці сегменти інкапсулюються в IP-пакети.
- Комбінацію вихідної IP-адреси та номера порту джерела, або IP-адреси отримувача та відповідного номера порту призначення, називають сокетом.
- Сокети дозволяють розрізнити декілька процесів, запущених на клієнтському комп'ютері, а також розмежовувати кілька звернень до серверного процесу.



Номери портів

Групи номерів портів

Група портів	Діапазон номерів	Опис
Відомі порти	від 0 до 1023	<ul style="list-style-type: none">•Ці номери портів зарезервовані для традиційних або популярних служб і програм, таких як веб-браузери, поштові клієнти та клієнти віддаленого доступу.•Визначені добре відомі порти для серверних застосунків загального призначення дозволяють клієнтам легко ідентифікувати пов'язані з ними служби.
Зареєстровані порти	від 1024 до 49151	<ul style="list-style-type: none">•Ці номери портів призначаються IANA за запитом суб'єкта для використання конкретними процесами або програмами.•Цими процесами, насамперед, є окремі застосунки, які користувач обрав для установки, а не традиційні програми, які використовують відомі номери портів.•Наприклад, компанія Cisco зареєструвала порт 1812 для процесу автентифікації RADIUS-сервера.
Приватні та/або динамічні порти	від 49152 до 65535	<ul style="list-style-type: none">•Ці порти також відомі як <i>одноденні порти</i>.•ОС клієнта зазвичай призначає номери портів динамічно, коли ініціюється з'єднання зі службою.•Після цього динамічний порт використовується для ідентифікації клієнтського застосунку протягом усього з'єднання.

Номери портів

Групи номерів портів (Продовж.)

Відомі номери портів

Номер порту	Протокол	Прикладний рівень
20	TCP	File Transfer Protocol (FTP) - Дані
21	TCP	File Transfer Protocol (FTP) - Контроль
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Сервер
68	UDP	Dynamic Host Configuration Protocol - Клієнт
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

Номери портів

Команда netstat

TCP-з'єднання невідомого походження можуть становити серйозну загрозу безпеці. Netstat є важливим інструментом для перевірки з'єднань.

```
C:\> netstat
Active Connections
Proto Local Address Foreign Address State
TCP 192.168.1.124:3126 192.168.0.2:netbios-ssn ESTABLISHED
TCP 192.168.1.124:3158 207.138.126.152:http ESTABLISHED
TCP 192.168.1.124:3159 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3160 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3161 sc.msn.com:HTTP ESTABLISHED
TCP 192.168.1.124:3166 www.cisco.com:http ESTABLISHED
```

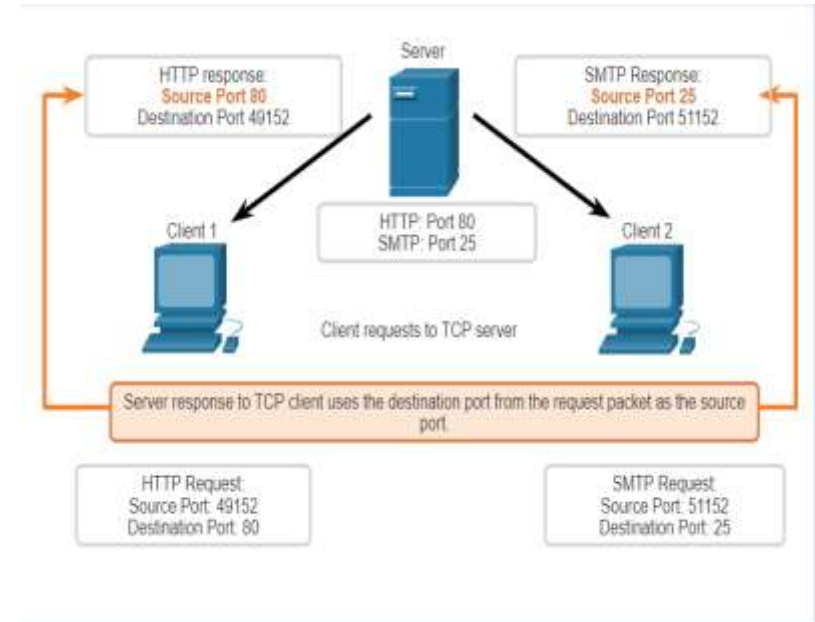
Процес ТСР-з'єднання

Процес TCP-з'єднання

Процеси сервера TCP

Кожен прикладний процес, запущений на сервері, налаштований на використання певного номера порту.

- Сервер не може мати дві служби, які працюють на одному і тому ж порті в межах одного сеансу транспортного рівня.
- Активна серверна програма, пов'язана з визначеним портом, вважається відкритою. Це означає, що транспортний рівень приймає і обробляє сегменти, адресовані цьому порту.
- Будь-який вхідний запит клієнта, адресований правильному сокету, приймається, а дані передаються серверному застосунку.



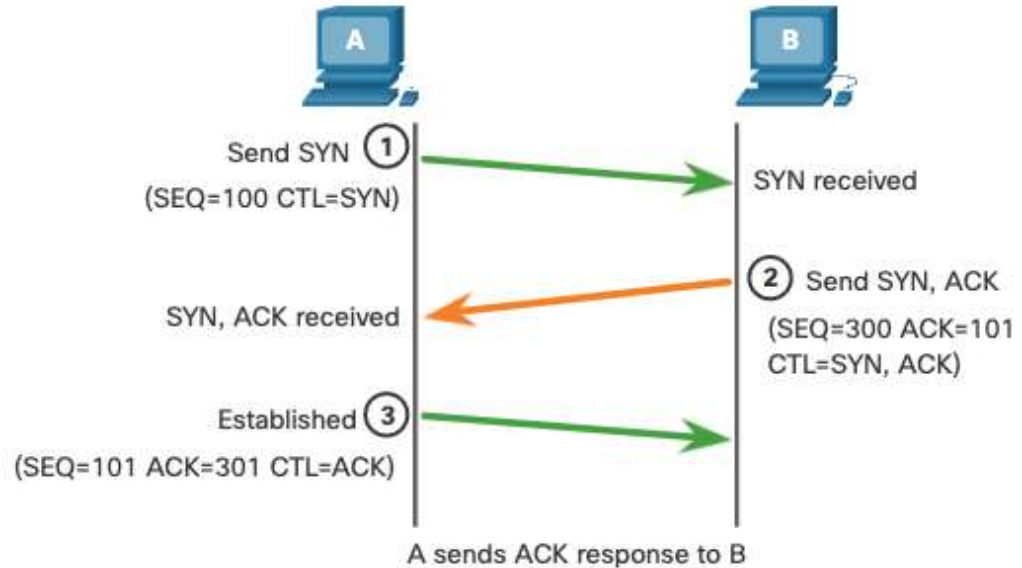
Процес TCP-з'єднання

Встановлення TCP-з'єднання

Крок 1: Клієнт ініціює з'єднання типу "клієнт-сервер", надсилаючи запит до сервера.

Крок 2: Сервер підтверджує сеанс обміну даними за принципом "клієнт-сервер" і робить запит на відкриття з'єднання типу "сервер-клієнт".

Крок 3: Клієнт, що розпочинав з'єднання, зі свого боку підтверджує відкриття сеансу зв'язку між сервером і клієнтом.



Процес TCP-з'єднання

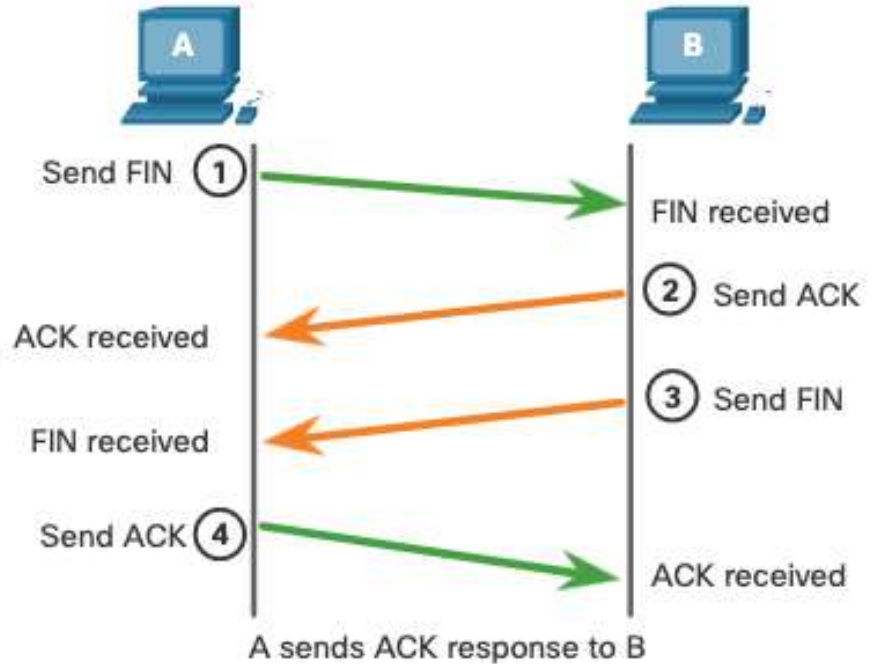
Закриття сеансу

Крок 1: Коли у клієнта немає більше даних для розміщення у потік, він надсилає сегмент зі встановленим прапорцем FIN.

Крок 2: Сервер надсилає ACK аби підтвердити отримання FIN для закриття сеансу зв'язку між клієнтом і сервером.

Крок 3: Сервер надсилає клієнту прапорець FIN для завершення сеансу зі свого боку.

Крок 4: Клієнт у відповідь надсилає сегмент ACK, щоб підтвердити отримання FIN від сервера.



Аналіз тристороннього рукостискання TCP

Функції тристороннього рукостискання:

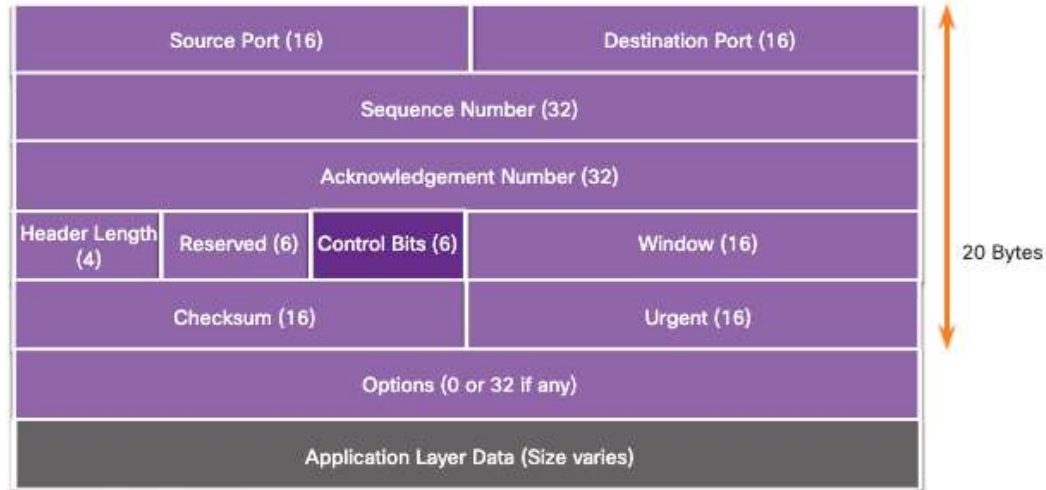
- Встановлює присутність цільового пристрою у мережі.
- Підтверджує, що на пристрої призначення активовано відповідну службу і він приймає запити на номер порту, який клієнт-ініціатор має намір використовувати.
- Повідомляє пристрій призначення, що клієнт збирається налаштувати з'єднання за цим номером порту.

Після завершення обміну інформацією, сеанси закриваються і з'єднання розривається. Механізми передавання даних і встановлення з'єднання забезпечують функцію надійності TCP.

Аналіз тристороннього рукостикування TCP (Продовж.)

Вирізняють шість прапорців контрольних бітів:

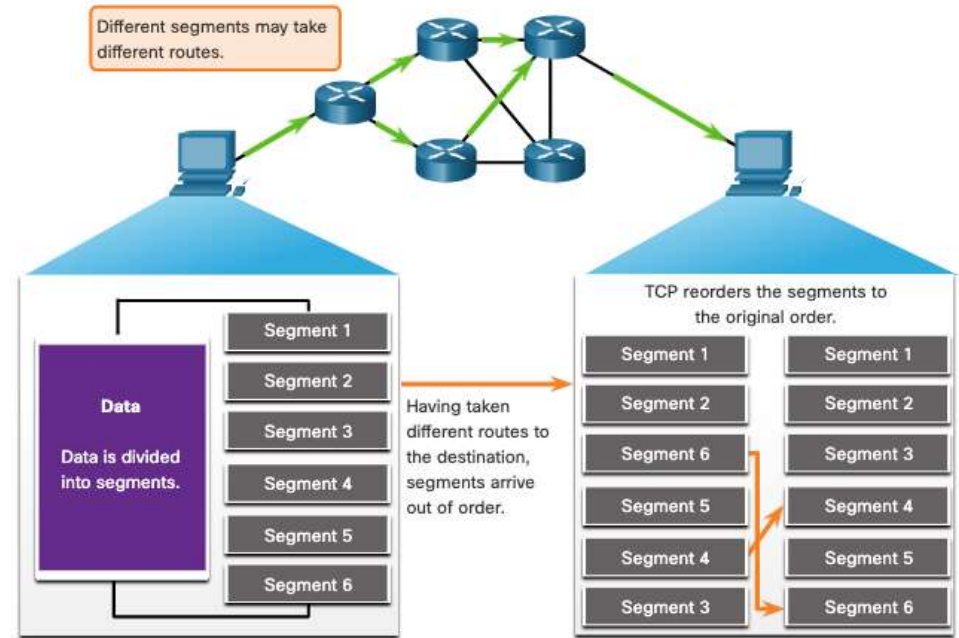
- **URG** - Urgent - показник терміновості.
- **ACK** - Acknowledgment – прапорець підтвердження, який використовується при встановленні або припиненні з'єднання.
- **PSH** - Push - функція проштовхування.
- **RST** - Reset - перемикає з'єднання, коли стається помилка або затримка у часі.
- **SYN** - Synchronize - синхронізація порядкових номерів, які використовуються при встановленні з'єднання.
- **FIN** - Немає більше даних від відправника, використовуються для припинення сеансу.



Надійність і керування ПОТОКОМ

Надійність TCP - Гарантована і впорядкована доставка

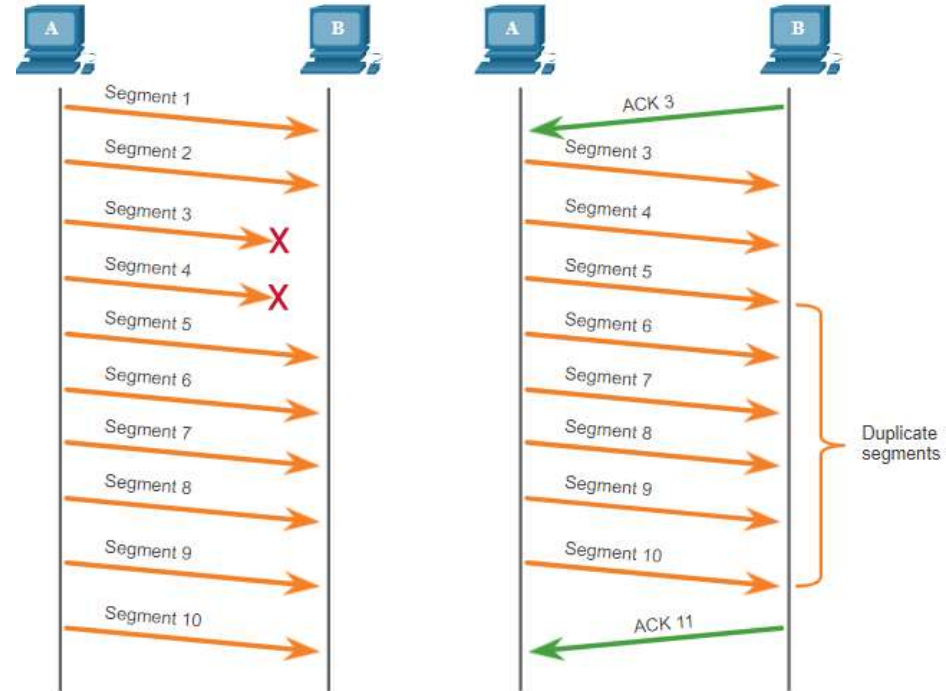
- TCP також допомагає підтримувати потік пакетів, щоб уникнути перевантаженості пристроїв.
- Часто трапляється, що TCP-сегменти не прибувають до місця призначення.
- Необхідно отримати усі сегменти і відновити з них вихідну послідовність даних.
- Для цього у заголовку кожного пакета зазначаються порядкові номери.



TCP Надійність — Втрата даних і ретрансляція

Незалежно від того, наскільки добре спроектована мережа, час від часу має місце втрата даних.

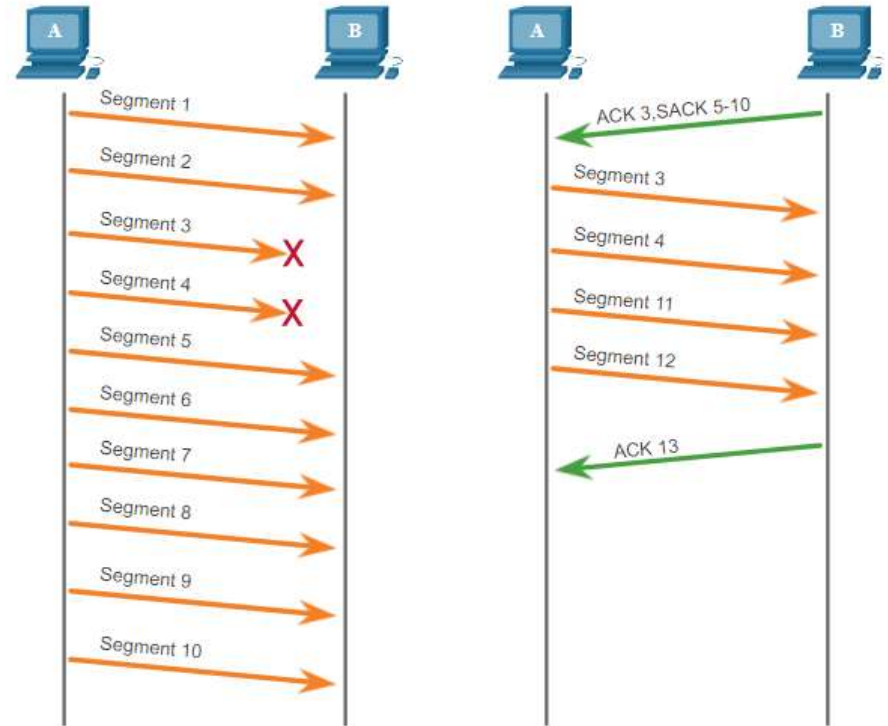
TCP забезпечує методи керування цими втратами сегментів. Серед цих методів - механізм повторного передавання сегментів для непідтверджених даних.



Надійність TCP — Втрата даних і ретрансляція (Продовж.)

Сучасні операційні системи вузлів зазвичай використовують додаткові функції TCP під назвою вибірконе підтвердження (SACK), яке узгоджується під час тристороннього рукостискання.

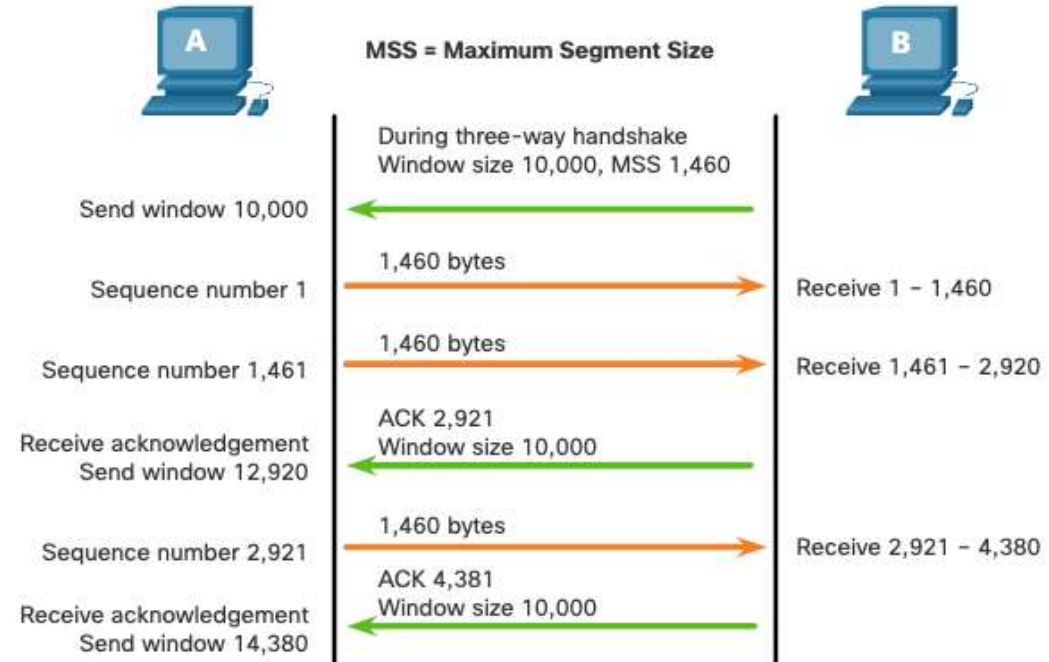
Якщо обидва вузли підтримують SACK, одержувач може явно підтвердити, які сегменти (байти) були отримані, навіть якщо послідовність надсилання була порушена.



Керування потоком TCP — Розмір вікна та підтвердження

TCP також забезпечує механізми керування потоками даних.

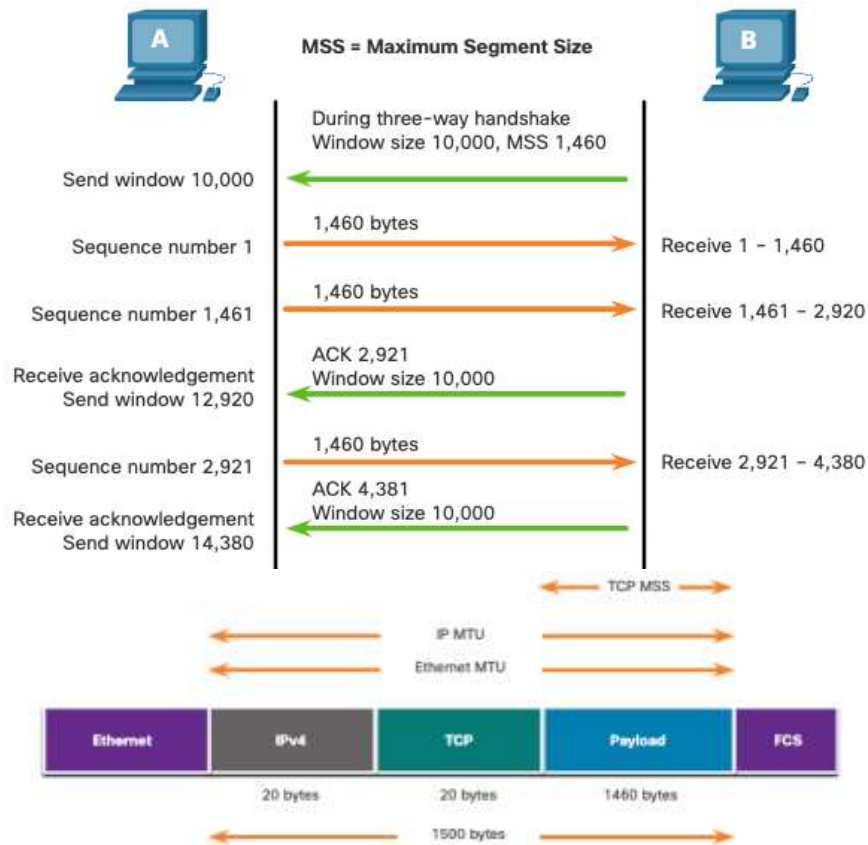
- Керування потоком - це кількість даних, які сторона призначення може надійно отримати і обробити.
- Керування потоком даних допомагає підтримувати надійність передавання за протоколом TCP за рахунок регулювання швидкості потоку даних між вузлами джерела та призначення впродовж усього сеансу.



Керування потоком TCP – Максимальний розмір сегмента (MSS)

Максимальний розмір сегмента (MSS) — це максимальний обсяг даних, які може отримати пристрій призначення.

- Зазвичай MSS становить 1460 байтів при використанні IPv4.
- Вузол визначає величину свого поля MSS, вилучаючи заголовки IP і TCP з максимальної одиниці передавання даних (MTU) Ethernet, що за замовчуванням складає 1500 байтів.
- 1500 мінус 60 (20 байтів для заголовка IPv4 і 20 байтів для заголовка TCP) залишає 1460 байтів.

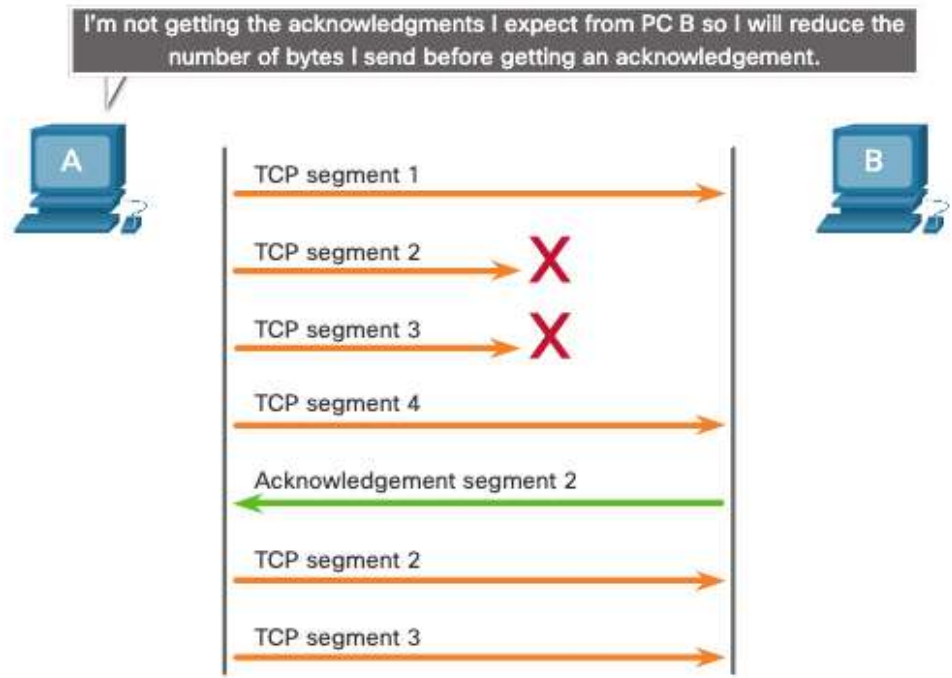


Надійність і керування потоком TCP

Керування потоком TCP - Уникнення перевантаженості

При виникненні тисняви у мережі, перевантажений маршрутизатор змушений відкидати пакети.

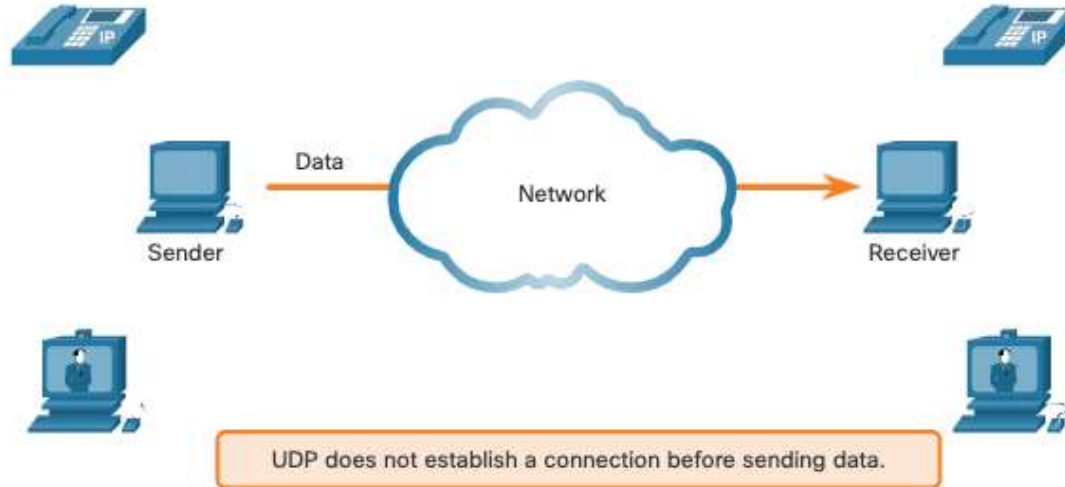
Для уникнення тисняви та керування нею, TCP використовує різноманітні механізми оброблення перевантаженості, таймери та алгоритми.



Передавання даних UDP

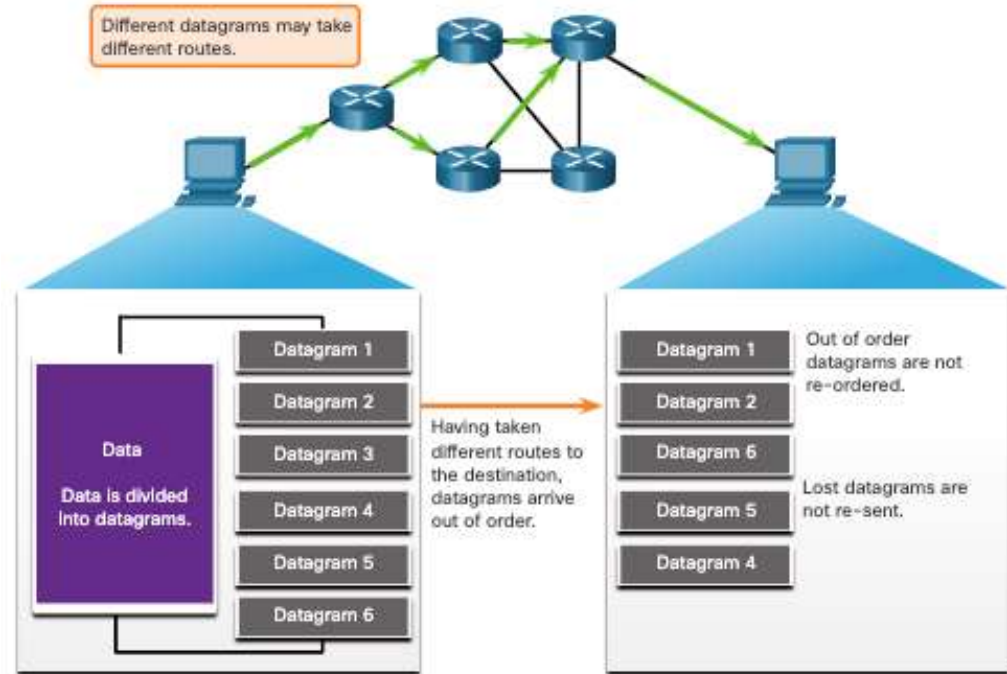
Низькі накладні витрати UDP проти надійності

UDP не встановлює з'єднання. UDP забезпечує низькі накладні витрати транспортування, оскільки для цього протоколу характерний невеликий заголовок дейтаграм і відсутність контролю мережного трафіку .



Відтворення послідовності дейтаграм UDP

- На відміну від TCP, UDP не відстежує порядкові номери.
- UDP не має можливості відновити порядок надсилання дейтаграм.
- UDP просто збирає дані у тій послідовності, у якій вони були отримані, і передає їх прикладній програмі.

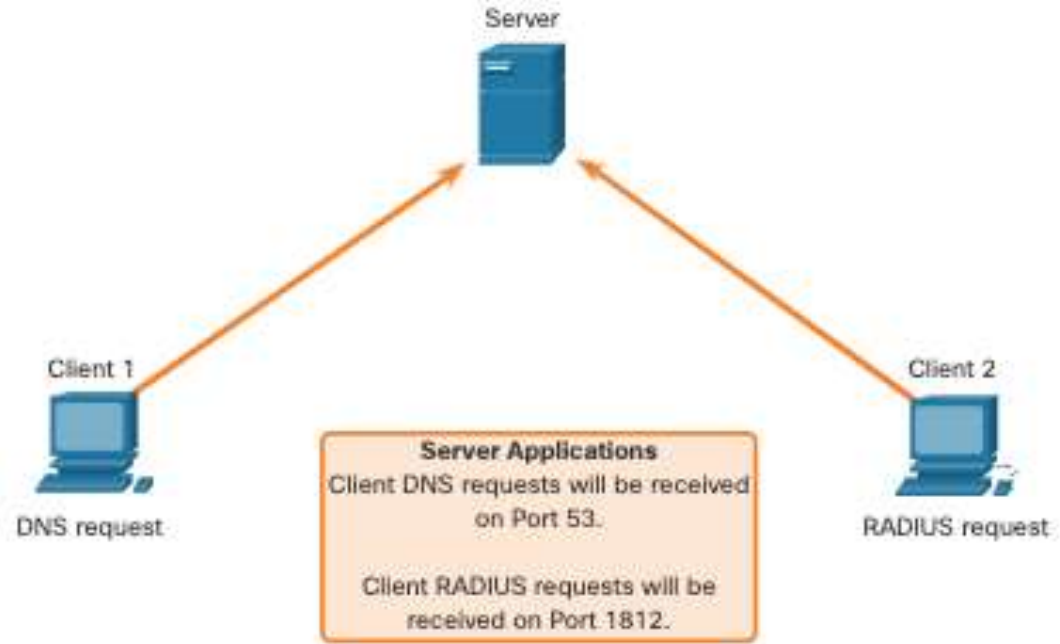


Передавання даних UDP

Процеси і запити UDP-сервера

Серверним застосункам на основі UDP також призначені відомі або зареєстровані номери портів.

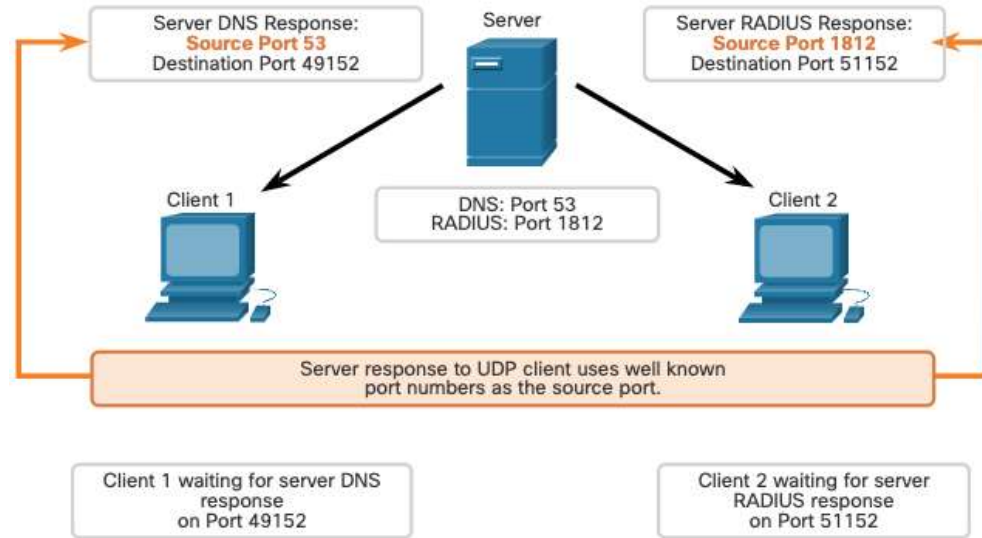
Коли протокол UDP отримує дейтаграму, призначену для одного з цих портів, він перенаправляє дані до відповідного застосунку на основі його номера порту.



Передавання даних UDP

Клієнтські процеси UDP

- Процес UDP-клієнта динамічно вибирає номер порту із визначеного діапазону і використовує його як порт джерела під час обміну даними.
- Порт призначення, як правило, це добре відомий або зареєстрований номер порту, призначений серверному процесу.
- Після того, як клієнт обрав порти джерела і отримувача, ця пара портів використовується у заголовку всіх дейтаграм у процесі передавання.



Що ми вивчили?

- Транспортний рівень виконує роль зв'язкового між прикладним рівнем і нижніми рівнями, які забезпечують передавання даних мережею.
- Транспортний рівень включає протоколи TCP і UDP.
- TCP налаштовує сеанси з'єднання, забезпечує надійність, підтримує доставку даних у порядку їх надсилання та виконує керування потоком.
- UDP - це простий протокол, який забезпечує основні функції транспортного рівня.
- UDP відтворює повідомлення у порядку надходження даних, втрачені сегменти повторно не надсилаються, немає попереднього налаштування сеансу зв'язку, UDP не інформує відправника про доступність ресурсів.
- Протоколи транспортного рівня TCP і UDP використовують номери портів для керування декількома одночасними діалогами.
- Кожен прикладний процес, запущений на сервері, налаштований на використання певного номера порту.
- Номер порту призначається автоматично або налаштовується вручну системним адміністратором.
- Щоб одержувач міг відтворити оригінальне повідомлення, необхідно отримати усі дані та відновити із сегментів їх початкову послідовність.

Що ми вивчили? (Продовж.)

- У заголовку кожного пакету використовуються порядкові номери.
- Керування потоком допомагає підтримувати надійність передавання TCP за рахунок регулювання швидкості надсилання даних між вузлами джерела й отримувача.
- У кожному TCP-сегменті джерело може передати 1460 байтів даних. Це типовий MSS, який може отримати пристрій призначення.
- Процес надсилання підтверджень вузлом призначення при обробці отриманих байтів і постійне регулювання вікна надсилання джерела відомі як "розсувне вікно".
- Для контролю та уникнення тисняви TCP використовує кілька механізмів обробки перевантаженості.

Нові терміни і команди

- Мультиплексування діалогів
- Сегменти
- Дейтаграми
- Протокол, орієнтований на з'єднання
- Протокол без встановлення з'єднання.
- Протокол без відстеження стану
- Керування потоками
- Впорядкована доставка
- Пари сокетів
- netstat

- Тристороннє рукостискання
- SYN
- ACK
- FIN
- URG
- PSH
- RST
- Початковий порядковий номер (ISN)
- Вибіркове підтвердження (SACK)
- Розсувне вікно
- Максимальний розмір сегмента (MSS)
- Максимальний блок передавання даних (MTU)
- Уникнення перевантаженості

Протоколи прикладного рівня



Завдання

- **Мета** : Пояснити роботу протоколів прикладного рівня при наданні підтримки застосункам кінцевого користувача.

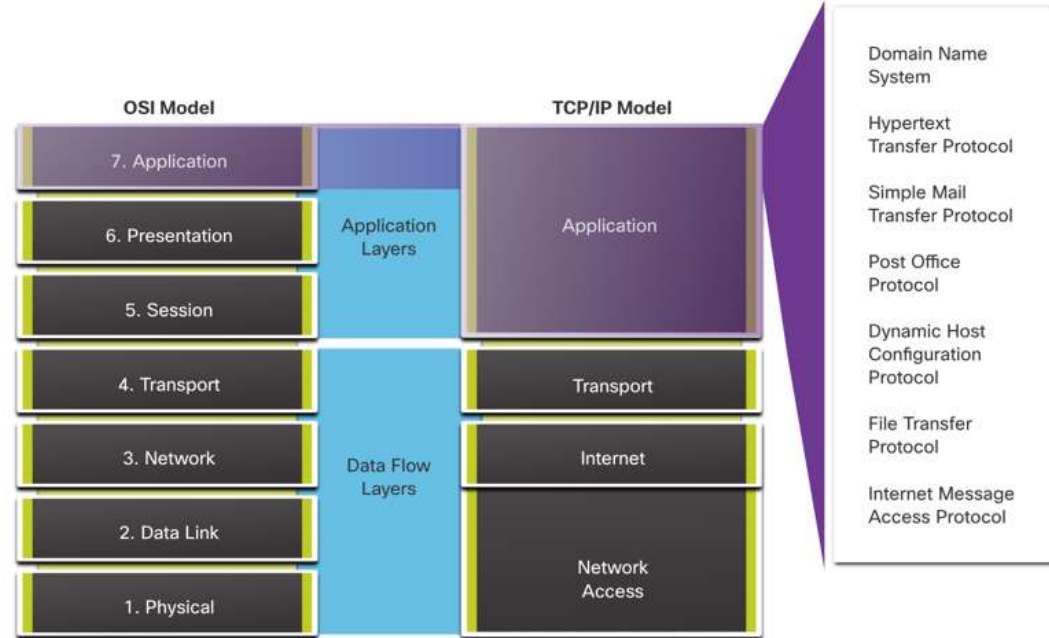
Назва теми	Мета вивчення теми
Прикладний, подання даних і сеансовий	Пояснити, як рівні прикладних програм, подання даних і сеансів спільно працюють для забезпечення мережних сервісів застосункам кінцевого користувача.
Однорангове з'єднання	Пояснити функціонування застосунків кінцевих користувачів у одноранговій мережі.
Протоколи веб та електронної пошти	Пояснити роботу протоколів Інтернету й електронної пошти.
Послуги IP-адресації	Пояснити принципи роботи протоколів DNS і DHCP.
Файлові сервіси	Пояснити, як працюють протоколи обміну файлами.

Прикладний, подання даних і
сеансовий

Прикладний, подання даних і сеансовий

Прикладний рівень

- Верхні три рівні моделі OSI (прикладний, подання даних і сеансовий) визначають функції прикладного рівня TCP/IP.
- Прикладний рівень забезпечує інтерфейс між застосунками, які використовуються для з'єднання, і базовою мережею, по якій передаються повідомлення.
- До найбільш відомих протоколів прикладного рівня належать HTTP, FTP, TFTP, IMAP і DNS.



Прикладний, подання даних і сеансовий

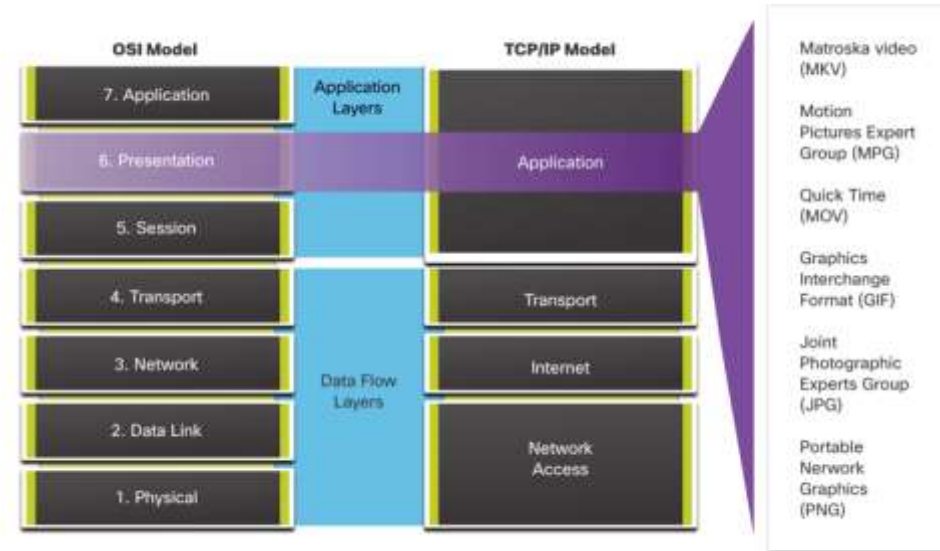
Подання даних і сеансовий рівень

Рівень подання даних виконує три основні функції:

- Форматування або перетворення даних на боці джерела у формат, сумісний для сприйняття пристроєм призначення.
- Ущільнення даних у спосіб, придатний для розпакування пристроєм призначення.
- Шифрування даних для передавання і розшифрування даних при отриманні.

Функції сеансового рівня:

- створення і підтримка діалогів між прикладними програмами джерела і одержувача.
- обмін інформацією для ініціювання діалогів, підтримки їх активного стану та перезапуску сеансів, які перериваються або простоють протягом тривалого періоду часу.



Протоколи прикладного рівня TCP/IP

- Прикладні протоколи TCP/IP визначають формат і контрольну інформацію, необхідну для багатьох поширених функцій інтернет-зв'язку.
- Протоколи прикладного рівня використовуються пристроями як джерела, так і призначення протягом сеансу обміну даними.
- Для успішного з'єднання протоколи прикладного рівня, реалізовані з боку відправника і одержувача, повинні бути сумісні між собою.

Система імен DNS - Domain Name System (або Service) (Система/ служба доменних імен)

- TCP, UDP клієнт 53
- перетворює доменні імена, такі як cisco.com, на IP-адреси.

Налаштування хоста DHCP - Dynamic Host Configuration Protocol (Протокол динамічного налаштування вузла)

- UDP клієнт 68, сервер 67
- Динамічно призначає IP-адреси для повторного використання.

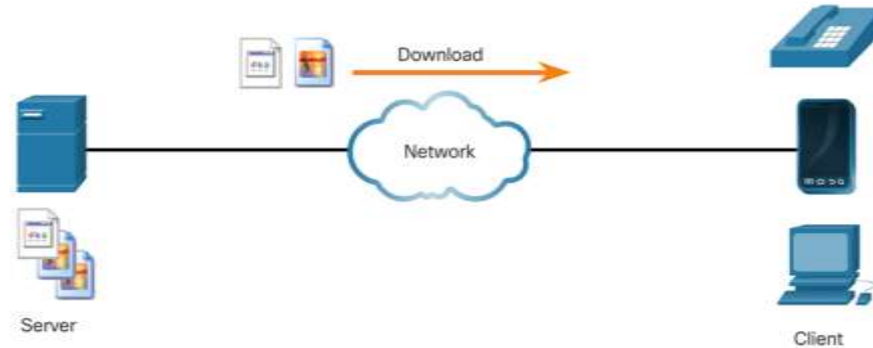
Web HTTP - Hypertext Transfer Protocol (Протокол передавання гіпертексту)

- TCP 80, 8080
- Набір правил для обміну текстом, графічними зображеннями, аудіо, відео та іншими мультимедійними файлами у всесвітній павутині.

Однорангове з'єднання

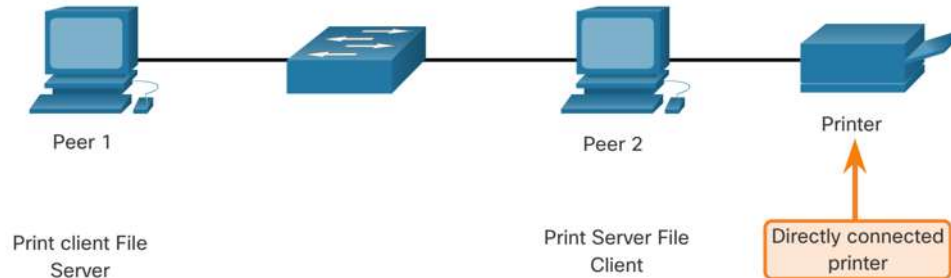
Модель клієнт-сервер

- Клієнтські та серверні процеси розглядаються на прикладному рівні.
- У моделі клієнт-сервера пристрій, що запитує інформацію, називається клієнтом, а пристрій, що відповідає на запит, - сервером.
- Протоколи прикладного рівня описують формат запитів і відповідей між клієнтами і серверами.



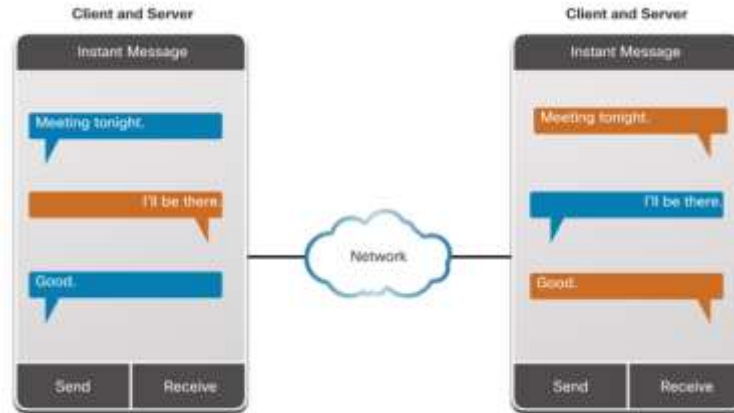
Однорангові мережі

- В одноранговій моделі (P2P) два або більше комп'ютерів, з'єднаних по мережі, можуть спільно використовувати ресурси (наприклад, принтери і файли), без виділеного сервера.
- Кожен під'єднаний кінцевий пристрій (відомий як вузол) може функціонувати і як сервер, і як клієнт.
- Один комп'ютер може взяти на себе роль сервера для однієї транзакції, і водночас бути клієнтом для іншої. Ролі клієнта і сервера встановлюються за запитом.



Однорангові застосунки

- Використання P2P дозволяє пристрою бути як клієнтом, так і сервером в рамках одного з'єднання.
- Деякі однорангові програми використовують гібридну систему, де кожен вузол звертається до сервера індексів, щоб з'ясувати розташування ресурсу, розміщеного на іншому вузлі.



Протоколи веб та електронної пошти

Протокол передавання гіпертексту (HTTP) і мова розмітки гіпертексту (HTML)

Коли у веб-браузері вводиться веб-адреса або уніфікований покажчик ресурсів (URL, Uniform Resource Locator), браузер встановлює з'єднання з веб-службою. Веб-служба запущена на сервері, який використовує протокол HTTP.

Щоб краще зрозуміти, як взаємодіють веб-браузер і веб-сервер, розглянемо процес відкриття веб-сторінки у браузері.

Крок 1

Браузер інтерпретує три частини URL-адреси:

- http (протокол або схема)
- www.cisco.com (ім'я сервера)
- index.html (назва файлу, що запитується)



Протокол передавання гіпертексту (HTTP) і мова розмітки гіпертексту (HTML)

Крок 2

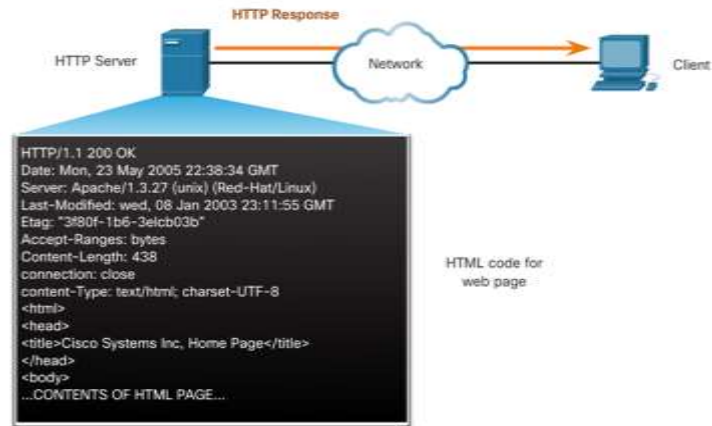
Далі, браузер за назвою сервера перетворює `www.cisco.com` на числову IP-адресу, яка використовується для під'єднання до сервера.

Клієнт ініціює HTTP-запит до сервера, надіславши до нього GET із запитом на файл `index.html`.



Крок 3

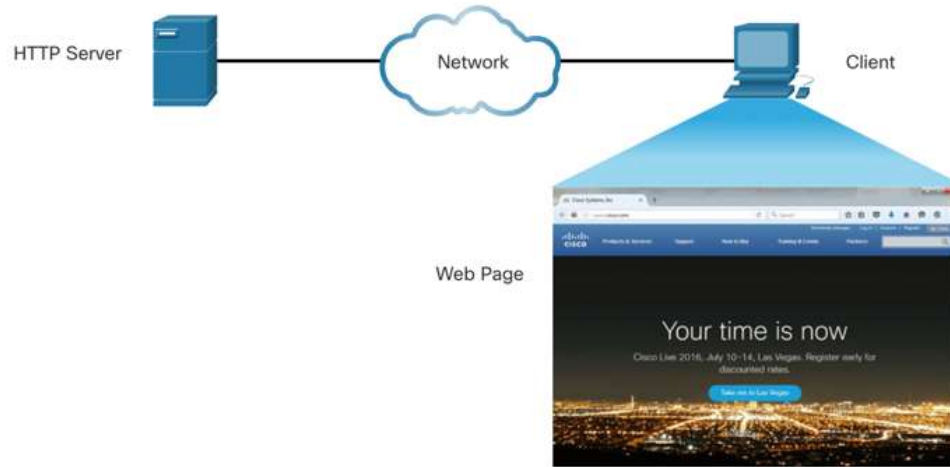
У відповідь на цей запит сервер спрямовує до браузера HTML-код цієї веб-сторінки.



Протокол передавання гіпертексту (HTTP) і мова розмітки гіпертексту (HTML)

Крок 4

Браузер перетворює цей HTML-код і форматує сторінку для вікна браузера.

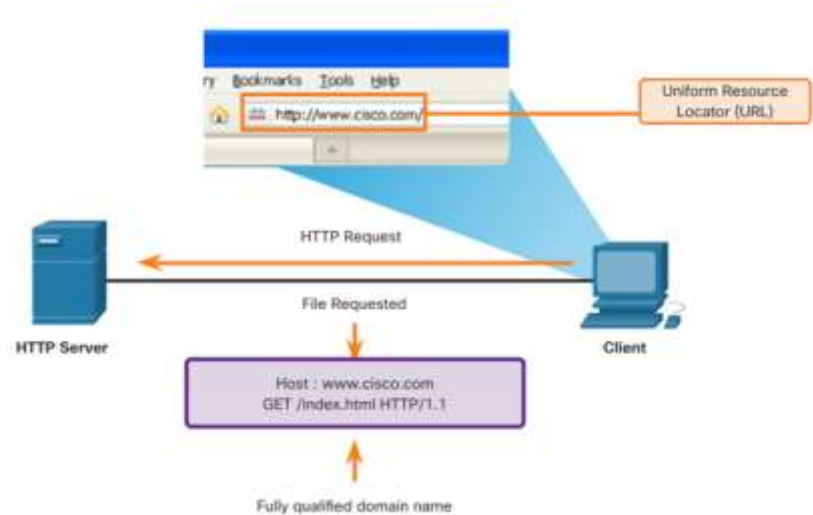


HTTP і HTTPS

HTTP - це протокол типу «запит-відповідь», який зазначає типи повідомлень, що використовуються у ході з'єднання.

Найпоширеніші типи повідомлень:

- **GET** - Для запиту даних клієнтом. Клієнт (веб-браузер) надсилає повідомлення GET веб-серверу для запиту HTML сторінок.
- **POST** - Для завантаження файлів даних на веб-сервер, наприклад дані форми.
- **PUT** - З його допомогою ресурси або контент, такі як зображення, заливаються на веб-сервер.



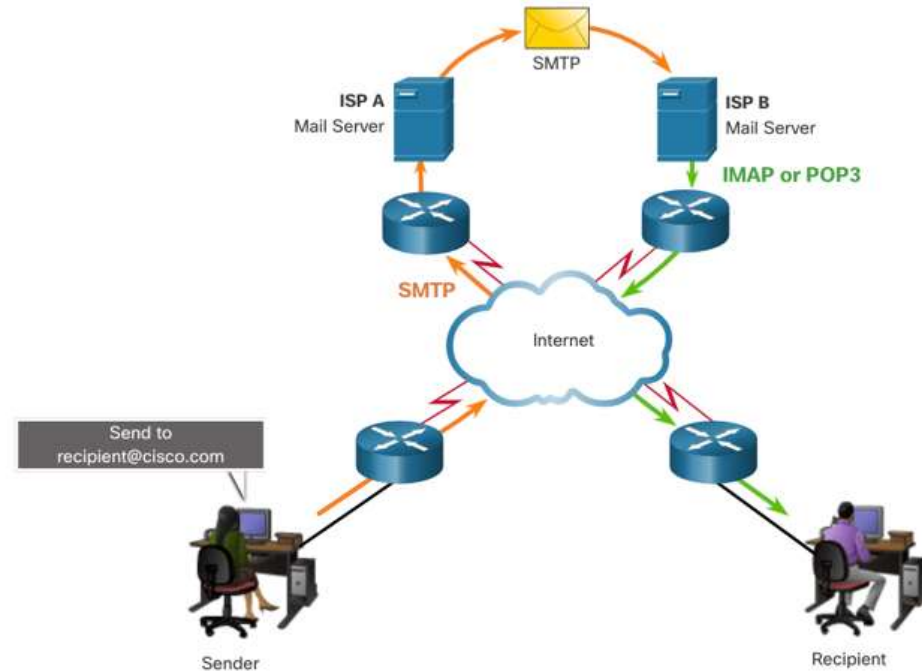
Примітка.: Протокол HTTP не гарантує безпеки. Для безпечного передавання даних через Інтернет, слід використовувати HTTPS.

Протоколи електронної пошти

Електронна пошта (email) - це спосіб передавання, зберігання і отримання електронних повідомлень у мережі. Email-повідомлення зберігаються у базах даних на поштових серверах. Email-клієнти зв'язуються з ними для надсилання і отримання електронних повідомлень.

Для роботи електронної пошти використовуються такі протоколи:

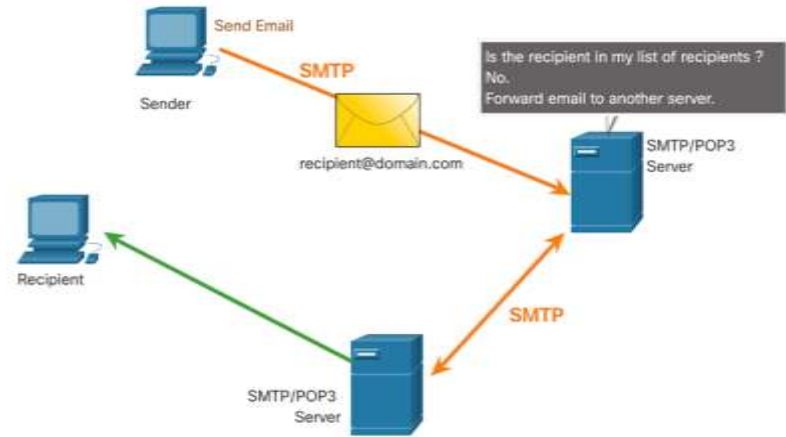
- Simple Mail Transfer Protocol (SMTP) – для надсилання пошти.
- Post Office Protocol (POP) & IMAP — для отримання пошти клієнтами.



Протоколи веб та електронної пошти

SMTP, POP та IMAP

- Коли клієнт надсилає повідомлення електронної пошти, SMTP-процес клієнта з'єднується з SMTP-процесом сервера через відомий порт 25.
- Після встановлення з'єднання, клієнт намагається передати email-повідомлення серверу.
- Коли сервер отримує повідомлення, він розміщує його у локальній поштовій скриньці, якщо одержувач є користувачем цього сервера, або пересилає повідомлення на інший поштовий сервер для доставки.
- При надсиланні електронного повідомлення, email-сервер призначення може бути зайнятий або не на зв'язку. У такому випадку SMTP ставить повідомлення у чергу очікування для подальшого надсилання.



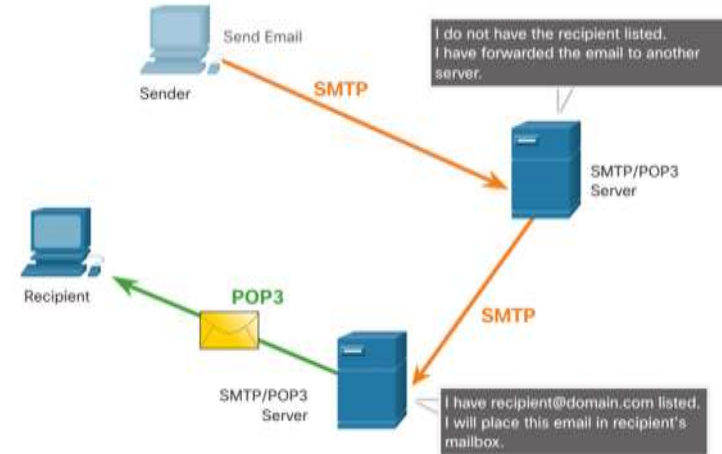
Примітка: Згідно SMTP повідомлення повинно містити заголовок з email-адресами одержувача та відправника, а також тіло повідомлення.

Протоколи веб та електронної пошти

SMTP, POP та IMAP

POP використовується застосунком для отримання email-повідомлень з поштового сервера. За допомогою POP пошта завантажується на бік клієнта, після чого видаляється із сервера.

- Сервер запускає сервіс POP, пасивно прослуховуючи TCP-порт 110 щодо надходження запитів від клієнта.
- Коли клієнт хоче скористатися цим сервісом, він надсилає запит на встановлення TCP-з'єднання із сервером.
- Коли з'єднання встановлене, сервер POP надсилає привітання.
- Далі клієнт і POP-сервер обмінюються командами і відповідями, до закриття або переривання з'єднання.



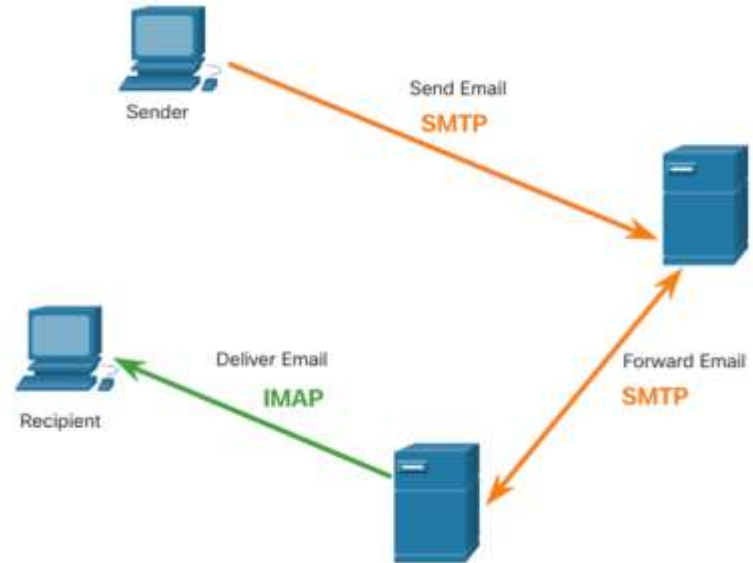
Примітка: Оскільки POP не зберігає повідомлення, його використання небажане для малих підприємств, які потребують централізованого рішення для резервного копіювання.

Протоколи веб та електронної пошти

SMTP, POP та IMAP

IMAP - це ще один протокол, який описує спосіб отримання повідомлень електронної пошти.

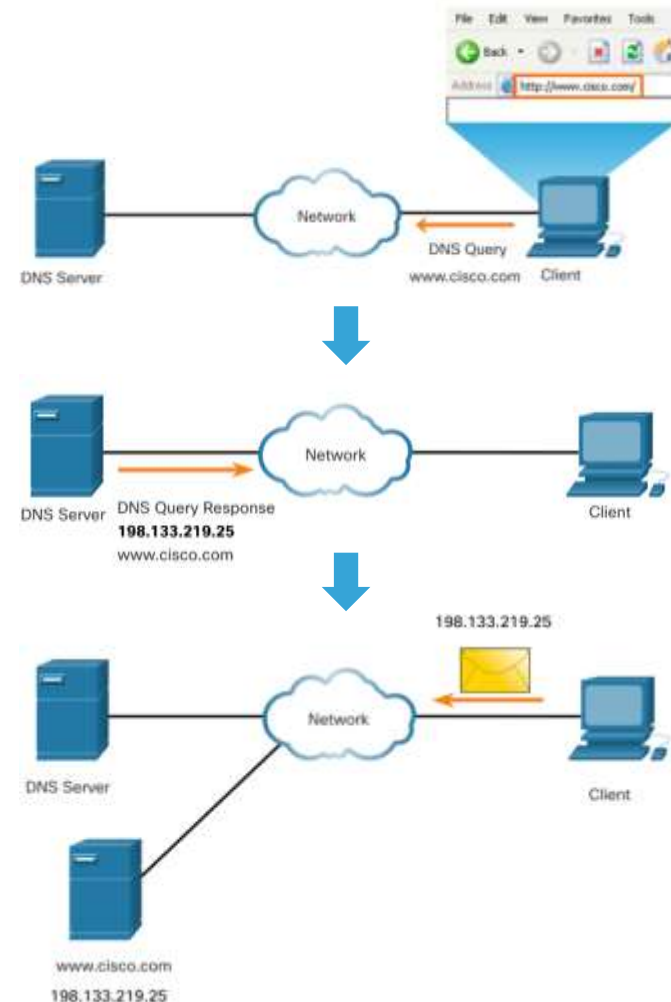
- На відміну від POP, коли користувач під'єднується до сервера з підтримкою IMAP, до клієнтського застосунку завантажуються копії повідомлень. Оригінальні повідомлення зберігаються на сервері, поки не будуть видалені вручну.
- Коли користувач вирішує видалити повідомлення, сервер синхронізує цю дію і видаляє повідомлення у себе.



Послуги IP-адресації

Служба доменних імен

- Доменні імена були визначені для перетворення числової IP-адреси на просте, впізнаване ім'я.
- Людям набагато легше запам'ятати повнокваліфіковані доменні імена (FQDNS), такі як `http://www.cisco.com`, аніж `198.133.219.25`.
- Протокол DNS визначає автоматизований сервіс, який зіставляє імена ресурсів з відповідними числовими мережними адресами. Повідомлення містить формат запитів, відповідей і дані.



Формат DNS-повідомлень

На DNS-серверах зберігаються різні типи ресурсних записів, які використовуються для перетворення імен. Ці записи містять ім'я, адресу і тип запису.

До таких типів записів належать:

- **A** - Адреса IPv4 кінцевого пристрою
- **NS** - Авторитетний сервер імен
- **AAAA** - Адреса IPv6 кінцевого пристрою. (вимовляється як "куад Ей")
- **MX** - Запис для поштового сервера домену.

При зверненні клієнта процес DNS-сервера спочатку переглядає власні записи у спробі перетворити ім'я. Якщо розпізнати ім'я, використовуючи збережені записи не вдається, сервер звертається до інших серверів для перетворення імені.

Після того, як відповідність знайдено і числова адреса повертається серверу, який надсилав запит, він тимчасово зберігає цю адресу на випадок, якщо запит на те саме ім'я надійде повторно.

Формат DNS-повідомлень (Продовж.)

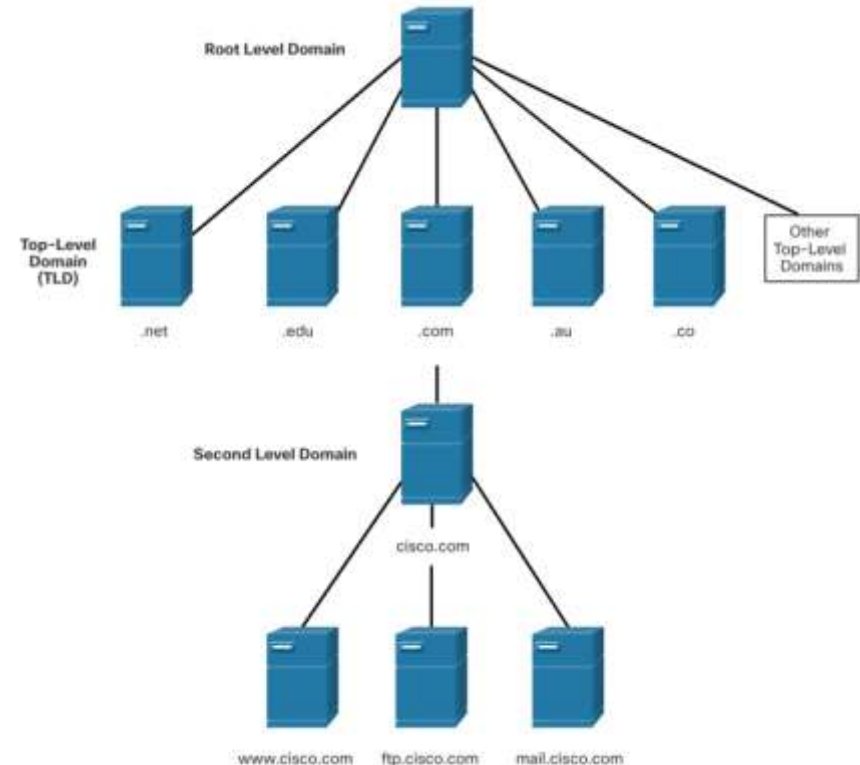
DNS використовує однаковий формат повідомлень, який складається із запитання, відповіді, авторитетного джерела і додаткової інформації, для усіх типів клієнтських запитів і відгуків серверів. а також передавання ресурсних записів між серверами.

Розділ DNS-повідомлень	Опис
Запитання	Запитання до сервера імен
Відповідь	Ресурсні записи, які відповідають на запитання
Авторитет	Ресурсні записи, які вказують на авторитетне джерело
Додатковий	Ресурсні записи, що містять додаткову інформацію

Послуги IP-адресації

Ієрархія DNS

- Як видно з рисунку, протокол DNS використовує ієрархічну систему для створення бази даних, що забезпечує перетворення імен.
- Кожен DNS-сервер підтримує певний файл бази даних і відповідає лише за зіставлення імен з IP для цієї невеликої частини всієї структури DNS.
- Коли DNS-сервер отримує запит на переклад імені, яке не належить до його DNS-зони, він перенаправляє запит для перетворення на інший DNS-сервер у межах відповідної зони.
- Приклади доменів верхнього рівня:
 - **.com** - бізнес або промисловість
 - **.org** - некомерційна організація
 - **.au** - Австралія



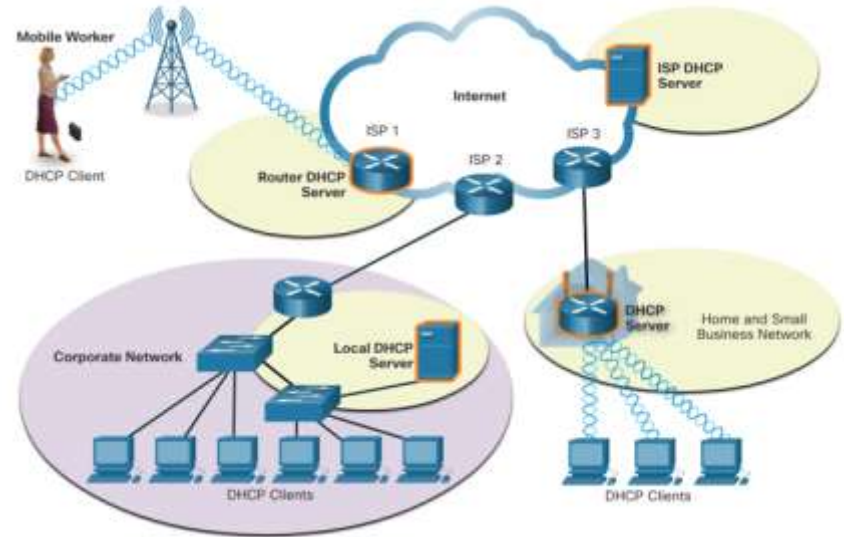
Команда nslookup

- Nslookup - це утиліта операційної системи комп'ютера, яка дозволяє користувачу вручну сформулювати запит до DNS-сервера для розпізнавання заданого імені хоста.
- Ця утиліта також може використовуватися для усунення проблем із перетворенням і перевірки поточного стану серверів імен.
- Запуск команди **nslookup** відображає DNS-сервер за замовчуванням, налаштований на вашому пристрої.
- Ім'я вузла або домену можна ввести в режимі **nslookup**.

```
C:\Users> nslookup
Default Server: dns-sj.cisco.com
Address: 171.70.168.183
> www.cisco.com
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: origin-www.cisco.com
Addresses: 2001:420:1101:1::a
          173.37.145.84
Aliases: www.cisco.com
> cisco.netacad.net
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: cisco.netacad.net
Address: 72.163.6.223
>
```

Протокол динамічного налаштування вузла (DHCP)

- Протокол динамічного налаштування вузла (DHCP) для IPv4 автоматизує призначення IPv4-адрес, маски підмережі, адреси шлюзу та інших параметрів IPv4.
- DHCP забезпечує динамічну адресацію у порівнянні зі статичною. Статична адресація передбачає введення інформації про IP-адресу вручну.
- При під'єднанні до мережі, вузол звертається до DHCP-сервера і запитує адресу. DHCP-сервер обирає адресу із налаштованого діапазону адрес, який називають пулом, і призначає її (передає в оренду) вузлу.
- У більшості мереж використовують як DHCP, так і статичну адресацію. DHCP використовується для вузлів загального призначення, зокрема для кінцевих пристроїв користувача. Статична адресація традиційно застосовується для таких мережних пристроїв, як маршрутизатори-шлюзи, комутатори, сервери та принтери.

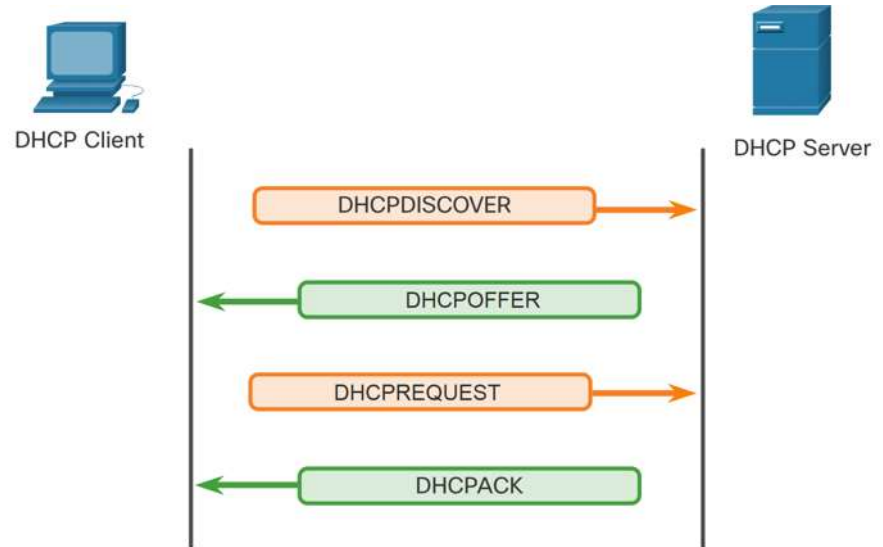


Примітка: DHCP для IPv6 (DHCPv6) надає аналогічні сервіси для клієнтів IPv6, окрім адреси шлюзу за замовчуванням. Її можна отримати тільки динамічно зі спеціальних повідомлень анонсування маршрутизатора (Router Advertisement, RA).

Принципи роботи протоколу DHCP

Процес DHCP:

- Коли IPv4-пристрій із налаштованим DHCP вмикається або під'єднується до мережі, клієнт передає широкомовне повідомлення DHCP (DHCPDISCOVER) з метою виявити у мережі будь-які доступні DHCP-сервери.
- DHCP-сервер відповідає повідомленням DHCPOFFER, у якому пропонує клієнту орендувати деяку адресу. (Якщо клієнт отримує більше однієї пропозиції від кількох DHCP-серверів у мережі, він повинен обрати одну.)
- Клієнт надсилає DHCP-запит (DHCPREQUEST) аби ідентифікувати конкретний сервер та пропозицію, яку він приймає.
- Далі сервер відповідає підтвердженням (DHCPACK), яке остаточно засвідчує надання параметрів клієнтові у тимчасове користування.
- Якщо пропозиція більше недійсна, обраний сервер відповідає повідомленням про негативне підтвердження DHCP (DHCPNAK), після чого процес повинен розпочатися з нового повідомлення DHCPDISCOVER.



Примітка: DHCPv6 має набір повідомлень, аналогічних до DHCPv4. Повідомлення DHCPv6: SOLICIT, ADVERTISE, INFORMATION REQUEST, та REPLY.

Файлові сервіси

Протокол передавання файлів (FTP)

File Transfer Protocol (FTP) розроблений для обміну даними між клієнтом і сервером. FTP клієнт - це застосунок, який працює на комп'ютері для завантаження даних з FTP-сервера і передавання даних на нього.



1. Control Connection:

Client opens first connection to the server for control traffic.



2. Data Connection:

Client opens second connection for data traffic.



Крок 1 - Клієнт встановлює перше з'єднання із сервером для керування трафіком, використовуючи порт TCP 21. Трафік складається з клієнтських команд і відповідей сервера.

Крок 2 - Клієнт встановлює друге з'єднання із сервером для фактичного передавання даних через порт 20 TCP. Це з'єднання створюється щоразу, коли з'являються дані для передавання.

Крок 3 - Обмін даними відбувається в обох напрямках. Клієнт може завантажувати (pull) дані з сервера, або записувати (push) дані на сервер.

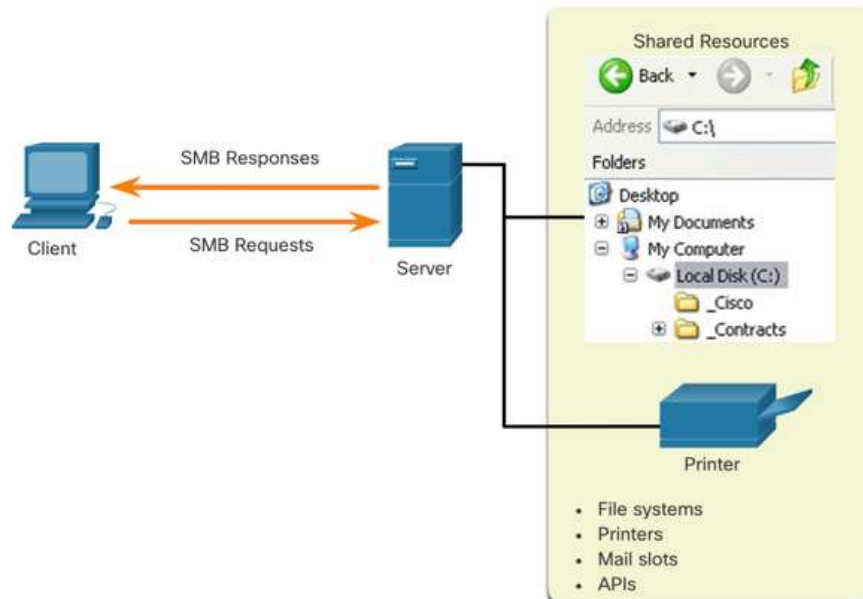
Протокол SMB

Протокол блоку серверних повідомлень (Server Message Block, SMB) — це клієнт-серверний протокол спільного доступу до файлів на основі запитів та відгуків. Сервери можуть надавати доступ до своїх ресурсів клієнтам у мережі.

Три функції SMB-повідомлень:

- Запуск, автентифікація і завершення сеансів
- Контроль доступу до файлів і принтерів
- Надання дозволу програмі надсилати повідомлення на іншій пристрій або отримувати повідомлення від нього.

На відміну від файлообмінників, підтримуваних FTP, клієнти встановлюють із серверами довготривале з'єднання. Після встановлення зв'язку користувач клієнтської програми може отримати доступ до ресурсів на сервері так, наче цей ресурс локальний.



Що ми вивчили у цій підтемі?

- Протоколи прикладного рівня використовуються для обміну даними між програмами, запущеними на пристроях відправника й отримувача. Рівень подання даних забезпечує три основні функції: форматування або подання даних, стиснення і шифрування даних для передавання та їх розшифрування при отриманні. Сеансовий рівень створює та підтримує діалоги між прикладними програмами джерела і одержувача.
- У моделі клієнт-сервера пристрій, що запитує інформацію, називається клієнтом, а пристрій, що відповідає на запит, - сервером.
- В одноранговій мережі типу P2P два або більше комп'ютерів, з'єднаних по мережі, можуть спільно використовувати ресурси, без будь-якого виділеного сервера.
- Найпоширеніші типи HTTP-повідомлень - це GET, POST і PUT.
- Функціонування електронної пошти підтримують три окремі протоколи: SMTP, POP та IMAP.
- Протокол DNS зіставляє імена ресурсів з відповідними числовими мережними адресами.
- Сервіс DHCP для IPv4 автоматизує призначення вузлам IPv4-адрес, масок підмереж, параметрів шлюзу за замовчуванням, а також інших мережних параметрів IPv4. DHCPv6 використовує повідомлення SOLICIT, ADVERTISE, INFORMATION REQUEST і REPLY.
- FTP-клієнт - це застосунок, який працює на комп'ютері для завантаження даних з FTP-сервера і передавання даних на нього.
- Повідомлення SMB виконують такі три функції: запуск, автентифікація та припинення сеансу; контроль доступу до файлів і принтерів; а також надання дозволу програмам надсилати повідомлення на інший пристрій або отримувати повідомлення від нього.

Нові терміни та команди

- | | |
|--|--|
| <ul style="list-style-type: none">• Прикладний рівень• Рівень подання даних• Сеансовий рівень• Модель клієнт-сервер• Однорангове з'єднання• Уніфікований покажчик ресурсу (URL)• Уніфікований ідентифікатор ресурсів (URI)• HTTP/HTTPS• GET• POST• PUT• SMTP• POP• IMAP | <ul style="list-style-type: none">• Служба доменних імен (Domain Name System, DNS)• Fully-Qualified Domain Names (FQDNs)• nslookup• Протокол динамічного налаштування вузла (Dynamic Host Configuration Protocol, DHCP)• DHCPDISCOVER• DHCPOFFER• DHCPREQUEST• DHCPACK• Протокол передавання файлів (File Transfer Protocol, FTP)• Блок серверних повідомлень (Server Message Block, SMB) |
|--|--|

Створення невеликої мережі



Завдання

Мета : Реалізуйте схему для невеликої мережі, що включає маршрутизатор, комутатор і кінцеві пристрої.

Назва теми	Мета вивчення теми
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 вихідних даних команд ping і tracert для перевірки з'єднання та встановлення відповідної працездатності мережі.
Команди вузла та IOS	Використання команд вузла та IOS для одержання інформації про пристрої у 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.

Пристрої у невеликій мережі

Пристрої у невеликій мережі

Топології невеликої мережі

- Більшість підприємств невеликі, тому не дивно, що й більшість корпоративних мереж також невеликі.
- Архітектура невеликої мережі зазвичай проста.
- 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 даних організації. Невеликими мережами керує місцевий IT-фахівець або позаштатний фахівець (за контрактом).

Вибір пристроїв для невеликої мережі

Як і великі мережі, невеликі мережі вимагають планування та проектування, щоб відповідати вимогам користувачів. Планування забезпечує належне врахування всіх вимог, факторів витрат та варіантів розгортання. Одним з перших архітектурних рішень є використання проміжних пристроїв для підтримки мережі

До факторів, які слід враховувати при виборі мережних пристроїв, належать:

- вартість
- швидкість і типи портів/інтерфейсів
- масштабованість
- можливості та сервіси операційної системи

IP-адресація для невеликої мережі

При реалізації мережі створіть і використовуйте схему IP-адресації. Усі вузли та пристрої в мережі Інтернет повинні мати унікальну адресу. До пристроїв, які будуть враховувати схему IP-адресації, відносять такі:

- Пристрої кінцевого користувача - кількість та тип з'єднань (тобто, дротовий, бездротовий, віддалений доступ)
- Сервери та периферійні пристрої (наприклад, принтери та камери безпеки)
- Проміжні пристрої, включаючи комутатори та точки доступу

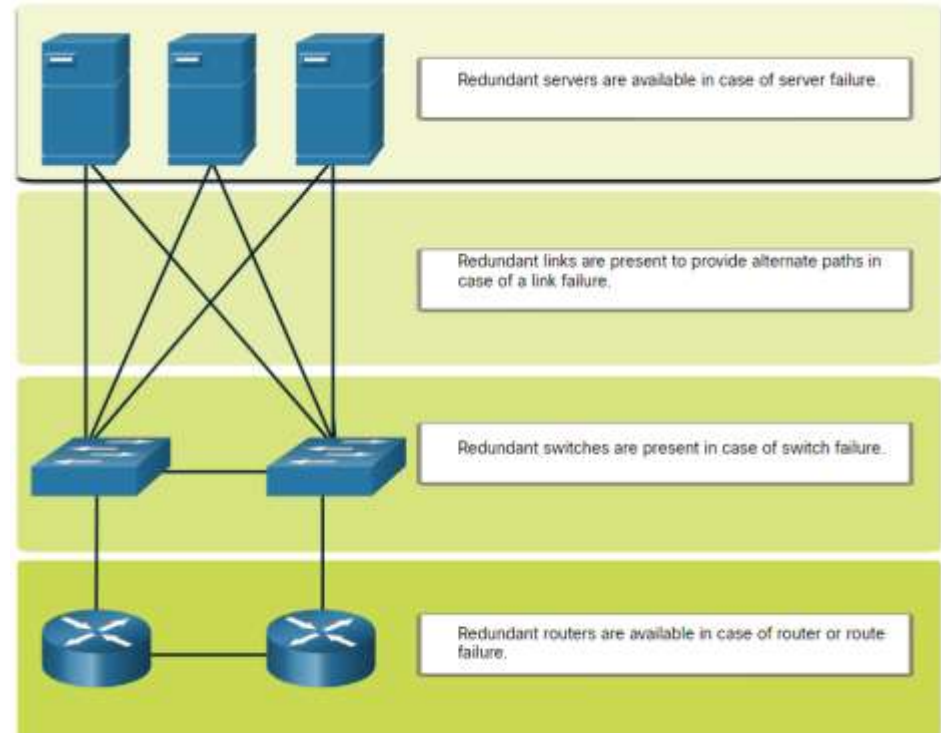
Рекомендується планувати, документувати та підтримувати схему IP-адресації залежно від типу пристрою. Використання запланованої схеми IP-адресації полегшує визначення типу пристрою та усунення несправностей.

Пристрої у невеликій мережі

Резервування у невеликій мережі

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

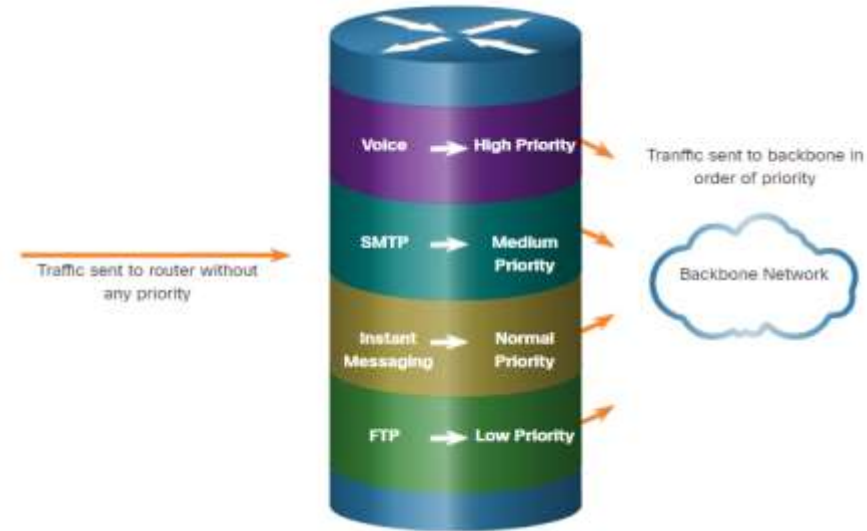
Резервування забезпечується шляхом встановлення дублювального обладнання. Цього також можна досягти, поставивши дублювальні мережні посилання для критичних областей.



Пристрої у невеликій мережі

Керування трафіком

- Метою проектування мережі є підвищення продуктивності працівників та мінімізація простоїв 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. Вдале проектування мережі дозволить забезпечити якість обслуговування (QoS).
- Пріоритетна черга включає в себе чотири види. Черга з високим пріоритетом завжди порожніє першою.



Застосунки та протоколи невеликої мережі

Застосунки та протоколи невеликої мережі

Загальні застосунки

Після налаштування мережа все ще потребує певних типів застосунків і протоколів для роботи. Мережа корисна настільки, наскільки корисні застосунки, що у ній використовуються.

Існує дві форми програмного забезпечення (ПЗ) або процесів, які забезпечують доступ до мережі:

- **Мережні застосунки:** програми, які реалізують протоколи прикладного рівня і здатні безпосередньо встановлювати зв'язок з нижніми рівнями стеку протоколів.
- **Сервіси прикладного рівня:** для програм, які не знають мережі, існують програми, які взаємодіють з мережею та готують дані для передавання.

Застосунки та протоколи невеликої мережі

Загальні протоколи

Мережні протоколи підтримують застосунки і служби, що використовуються співробітниками в невеликій мережі.

- Адміністраторам мережі зазвичай потрібен доступ до мережних пристроїв і серверів. Два найпоширеніших рішення віддаленого доступу - Telnet та Secure Shell (SSH).
- Протокол передачі гіпертексту (HTTP) і захищений протокол передачі гіпертексту (HTTPS) використовуються між веб-клієнтами та веб-серверами.
- Простий протокол передачі пошти (SMTP) використовується для надсилання електронної пошти, протокол поштового зв'язку (POP3) або протокол доступу до Інтернет-пошти (IMAP) використовуються клієнтами для отримання електронної пошти.
- Протокол передачі файлів (FTP) та безпечний протокол передачі файлів (SFTP) використовуються для завантаження файлів між клієнтом та сервером FTP.
- Протокол динамічної конфігурації вузла (DHCP) використовується клієнтами для отримання конфігурації IP від сервера DHCP.
- Служба доменних імен (DNS) перетворює доменні імена на IP-адреси.

Примітка: Сервер може надавати кілька мережних сервісів. Наприклад, сервер може мати електронну пошту, FTP і SSH сервер.

Застосунки та протоколи невеликої мережі

Загальні протоколи (Продовж.)

Ці мережні протоколи містять основний набір інструментів мережі, що визначає:

- Процеси на обох кінцях сеансу зв'язку
- Типи повідомлень
- Синтаксис повідомлень
- Значення інформаційних полів
- Як надсилаються повідомлення та очікувану відповідь
- Взаємодію з наступним рівнем нижче

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

Застосунки для передавання голосу та відео

- Сьогодні компанії все частіше використовують IP-телефонію та потокові медіа для спілкування з клієнтами та діловими партнерами, а також дозволяють своїм працівникам віддалено працювати.
- Адміністратор мережі повинен переконатися, що в мережі встановлено належне обладнання, і що мережні пристрої налаштовані для забезпечення пріоритетної доставки.
- Фактори, які адміністратор невеликої мережі повинен враховувати при підтримці застосунків у режимі реального часу:
 - **Інфраструктура** - чи спроможна вона підтримувати застосунки в режимі реального часу?
 - **VoIP** - VoIP, як правило, дешевше, ніж IP-телефонія, але за рахунок якості та можливостей.
 - **IP-телефонія** - для цього використовуються спеціалізовані сервери для керування викликами та сигналізацією.
 - **Застосунки в режимі реального часу** - мережа повинна підтримувати механізми якості обслуговування (QoS), щоб мінімізувати проблеми із затримкою. Транспортний протокол у режимі реального часу (RTP) та протокол керування передачею у реальному часі (RTCP) - два протоколи, що підтримують застосунки в реальному часі.

Масштабування до більших мереж

Масштабування до більших мереж

Розширення невеликої мережі

Зростання є природним процесом для багатьох малих підприємств, і їх мережі повинні розширюватись 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 та логічна топологія
- **Інвентаризація пристроїв** - Список пристроїв, які складають мережу або використовуються у ній
- **Бюджет** - Деталізований IT-бюджет, включаючи бюджет на закупівлю обладнання на фінансовий рік
- **Аналіз трафіку** - Протоколи, застосунки і сервіси та відповідні вимоги до трафіку повинні бути задокументовані

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

Масштабування до більших мереж

Аналіз протоколів

Важливо розуміти тип трафіку, який проходить через мережу, а також поточний трафік. Існує кілька інструментів керування мережею, які можна використовувати з цією метою.

Щоб визначити закономірності руху трафіку, важливо зробити наступне:

- Захопити трафіку під час пікового використання, щоб отримати чітке уявлення про різні типи трафіку.
- Виконати захоплення на різних сегментах мережі та пристроях, оскільки деякий трафік буде локальним для певного сегмента.
- Інформацію, яка зібрана аналізатором протоколу, оцінити 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.

Масштабування до більших мереж

Використання службової мережі

Багато операційних систем надають вбудовані засоби для відображення такої інформації щодо використання мережі. Ці інструменти можна використовувати для захоплення «знімка» інформації, наприклад:

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

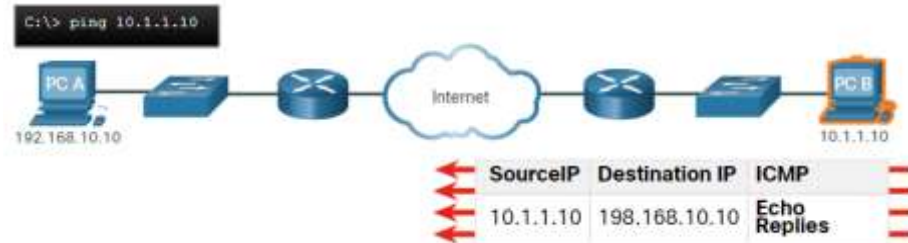
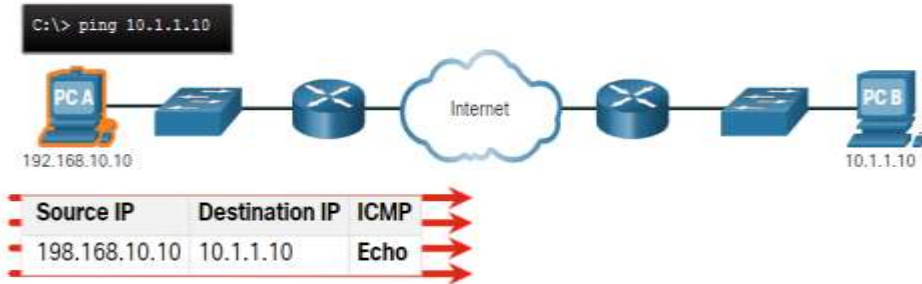
Документування знімків для співробітників у невеликій мережі протягом певного періоду часу дуже корисно для визначення вимог до протоколів і пов'язаних з ними потоків трафіку.

Перевірка з'єднання

Перевірка з'єднання за допомогою команди Ping

Незалежно від того, чи ваша мережа невелика та нова, чи ви масштабуєте існуючу мережу, ви завжди захочете переконаватися у тому, що компоненти належним чином під'єднані один до одного та до Інтернету.

- Команда ping, яка доступна в більшості операційних систем, є найефективнішим способом швидкої перевірки зв'язку з рівня між IP-адресою джерела та призначення.
- Команда ping використовує у протоколі Internet Control Message (ICMP) ехо-повідомлення (ICMP Type 8) та ехо-відповіді (ICMP Type 0).



Перевірка з'єднання

Перевірка з'єднання за допомогою команди Ping (Продовж.)

На вузлі з ОС Windows 10 команда ping надсилає чотири послідовні ICMP ехо-повідомлення і очікує чотири послідовні ICMP ехо-відповіді від вузла призначення. Команда ping в IOS надсилає п'ять ехо-повідомлень ICMP та відображає індикатор для кожної отриманої ехо-відповіді ICMP.

Елемент	Опис
!	<ul style="list-style-type: none">•Знак оклику вказує на успішне отримання ехо-відповіді.•Він перевіряє зв'язок рівня 3 між джерелом та отримувачем.
.	<ul style="list-style-type: none">•Період означає, що минув час очікування ехо-відповіді.•Це вказує на те, що проблема з під'єднанням сталася десь уздовж шляху
U	<ul style="list-style-type: none">•У верхньому регістрі U вказує на те, що маршрутизатор на шляху відповів повідомленням про помилку ICMP типу 3 «пункт призначення недоступний».•До можливих причин можна віднести те, що маршрутизатор не знає напрямку до цільової мережі або не зміг знайти вузол в цільовій мережі.

Примітка: Інші можливі відповіді на команду ping включають Q, M, ? або &. Однак, їх значення в даному розділі не розглядається.

Перевірка з'єднання

Розширена команда Ping

Cisco IOS пропонує розширений режим для команди **ping** .

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**.

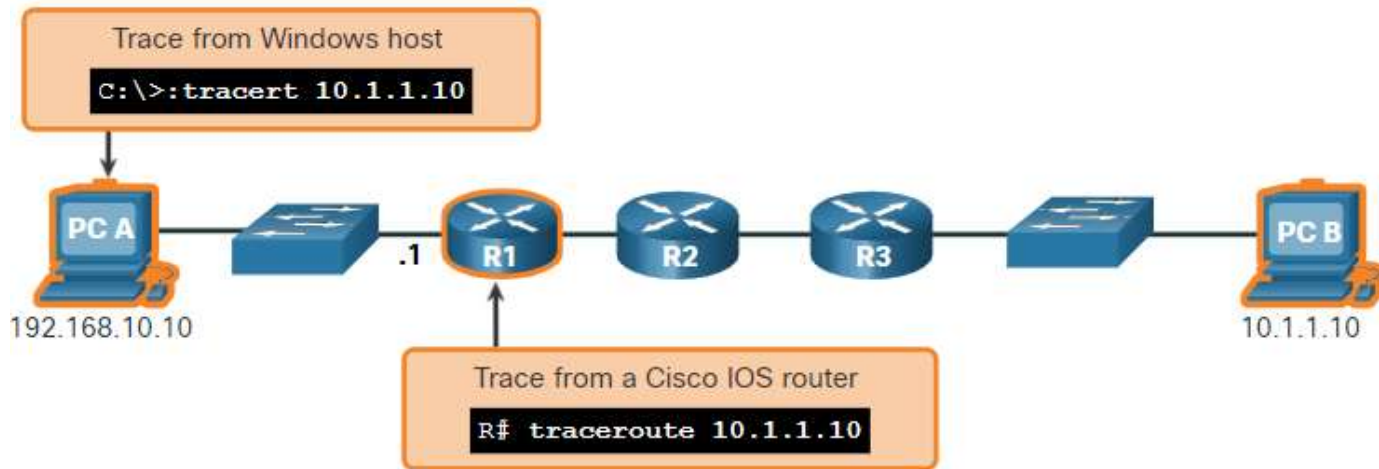
Примітка: Натискання **Enter** приймає вказані значення за замовчуванням. Команда **ping ipv6** використовується для розширеної команди ping для IPv6.

```
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#
```


Перевірка з'єднання за допомогою команди Traceroute

Команда ping корисна для швидкого визначення наявності проблеми зі з'єднанням рівня 3. Однак вона не визначає, де знаходиться проблема.

- Traceroute може допомогти знайти проблемні зони рівня 3 в мережі. Трасування повертає список переходів, коли пакет направляється через мережу.
- Синтаксис команди трасування залежить від операційної системи.



Перевірка з'єднання за допомогою команди Traceroute (Продовж.)

- Нижче наведено приклад результату виконання команди **tracert** на вузлі з ОС Windows 10.

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

- Єдина успішна відповідь була від шлюзу на R1. Запити трасування до наступного переходу вичерпано, як зазначено зірочкою (*), а це означає, що маршрутизатор наступного переходу не відповів або є помилка в мережному шляху. У цьому прикладі виникає проблема між R1 і R2.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.10.1
  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>
```

Перевірка з'єднання за допомогою команди Traceroute (Продовж.)

Нижче наведено зразки результатів виконання 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#
```

```
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 *
```

- Ліворуч трасування підтверджено: успішно досягнуто PC B.
- Праворуч вузол 10.1.1.10 був недоступний, а у вихідних даних показано зірочки, де відповіді вичерпано. Таймаути вказують на потенційну проблему в мережі.
- Використовуйте **Ctrl-Shift-6** для переривання **traceroute** у Cisco IOS.

Примітка: Реалізація Windows traceroute (tracert) надсилає echo-запити ICMP. Cisco IOS і Linux використовують UDP з неприпустимим номером порту. Кінцевий вузол призначення поверне ICMP-порту недоступне повідомлення.

Розширена команда Traceroute

Як і розширена команда **ping**, існує також розширена команда **traceroute**. Вона дозволяє адміністратору налаштовувати параметри, пов'язані з командною операцією.

Команда Windows **tracert** дозволяє вводити декілька параметрів через опції в командному рядку. Однак, в ній необхідно керувати інакше, ніж у розширеній команді IOS **traceroute**. Нижче наведено 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>
```

Розширена команда Traceroute (продовж.)

- Опції розширеної команди Cisco IOS **traceroute** дозволяє користувачеві створити особливий тип трасування, налаштовуючи параметри, пов'язані з роботою команди.
- Розширена команда `traceroute` вводиться в привілейованому режимі EXEC шляхом введення **traceroute** без IP-адреси призначення. IOS супроводжуватиме вас через параметри команд, представивши ряд підказок, пов'язаних із встановленням різних параметрів.
- **Примітка:** Натискання **Enter** приймає вказані значення за замовчуванням.

```
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#
```

Базовий рівень мережі

- Одним з найбільш ефективних інструментів для моніторингу та усунення несправностей продуктивності мережі є створення базового рівня мережі.
- Одним із способів запуску базового рівня є копіювання та вставлення результатів виконання команди `ping`, трасування 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.
- Корпоративні мережі повинні мати великі базові рівні; більш широкі, ніж ми можемо описати в цьому курсі. Професійні програмні засоби доступні для зберігання та підтримки базової інформації.

Команди вузла та IOS

Налаштування IP-конфігурації на вузлі з ОС Windows

У Windows 10 ви можете отримати доступ до деталей IP-адреси з **Network and Sharing Center** для швидкого перегляду чотирьох важливих налаштувань: адреси, маски, маршрутизатора та DNS. Або ви можете запустити команду **ipconfig** з командного рядка комп'ютера з ОС Windows.

- Використовуйте команду **ipconfig /all** для перегляду MAC-адреси, а також інших деталей щодо адресації 3 рівня пристрою
- Якщо вузол налаштований як клієнт DHCP, конфігурацію IP-адреси можна оновити за допомогою команд **ipconfig /release** та **ipconfig /renew** .
- Служба DNS-клієнта на комп'ютерах з ОС Windows також оптимізує продуктивність вирішення імен DNS, зберігаючи раніше перетворені імена в пам'яті. Команда **ipconfig /displaydns** відображає всі кешовані DNS-записи на комп'ютері з ОС Windows.

```
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)
```


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.
- У командному рядку використовуйте команду **ifconfig** для відображення стану поточних активних інтерфейсів та їх IP-конфігурації.
- Команда **ip address** на Linux використовується для відображення адрес і їх властивостей. Її також можна використовувати для додавання або видалення IP-адрес.

```
[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
```

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

Налаштування IP-конфігурації на вузлі з macOS

- У графічному інтерфейсі вузла Mac відкрийте **Network Preferences > Advanced** для отримання інформації про IP-адресацію.
- Команда **ifconfig** також може бути використана у командному рядку для перевірки IP -конфігурації інтерфейсу .
- Інші корисні команди macOS для перевірки IP-налаштувань вузла включають в себе **networksetup -listallnetworkservices** та **networksetup -getinfo <network service>**.

```
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$
```

Команди вузла та IOS

Команда arp

Команда **arp** виконується з командного рядка Windows, Linux або Mac. Команда надає перелік всіх пристроїв, які зараз знаходяться в ARP-кеші вузла.

- Команда **arp -a** відображає відому IP-адресу та прив'язку MAC-адреси. 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.
- Кеш можна очистити, використовуючи команду **netsh interface ip delete arpcache** у тому випадку, якщо адміністратор мережі хоче заповнити кеш оновленою інформацією.

Примітка: Можливо, вам знадобиться доступ адміністратора на вузлі, щоб мати можливість використовувати команду **netsh interface ip delete arpcache** .

Повторний огляд команди show

Команда	Опис
show running-config	Перевіряє поточні налаштування та параметри
show interfaces	Перевіряє стан інтерфейсу і відображає будь-які повідомлення про помилки
show ip interface	Перевіряє інформацію 3 рівня на інтерфейсі
show arp	Перевіряє список відомих вузлів у локальних мережах Ethernet
show ip route	Перевіряє відомості про маршрутизацію 3 рівня
show protocols	Перевіряє, які протоколи працюють
show version	Перевіряє пам'ять, інтерфейси та ліцензії пристрою

Команда show cdp neighbors

CDP надає такі відомості про кожний пристрій CDP-сусіда:

- **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** - чи є конкретний пристрій комутатором Рівня 2 або комутатором Рівня 3
- **Платформа** - апаратна платформа пристрою.

Команда **show cdp neighbors detail** показує IP-адресу сусіднього пристрою.

```
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#
```

Команда show ip interface brief

Однією з найбільш часто використовуваних команд є команда **show ip interface brief** . Ця команда надає більш скорочені вихідні дані, ніж команда **show ip interface** . Вона надає зведення ключової інформації для всіх мережних інтерфейсів на маршрутизаторі.

```
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#
```

```
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
```

Методи пошуку та усунення несправностей

Основні етапи пошуку та усунення несправностей

Крок	Опис
Крок 1. Визначення проблеми	<ul style="list-style-type: none">•Це перший крок у процесі усунення несправностей.•Хоча на цьому кроці можна використовувати інструменти, найчастіше розмова з користувачем є більш кориснішою.
Крок 2. Формування припущень щодо можливої причини несправності.	<ul style="list-style-type: none">•Після того, як проблема виявлена, спробуйте сформулювати припущення щодо ймовірних причин.•Цей крок часто призводить до більшої кількості можливих причин проблеми.
Крок 3. Перевірка припущень щодо визначення причини несправності.	<ul style="list-style-type: none">•Виходячи з ймовірних причин, протестуйте свої теорії, щоб визначити, яка з них є причиною проблеми.•Технік може застосувати швидке виправлення, щоб перевірити чи вирішує воно проблему.•Якщо швидке виправлення проблеми не усуне, можливо, вам доведеться вивчити проблему, щоб встановити точну причину.
Крок 4. Розроблення плану дій та реалізація рішення	Визначивши точну причину проблеми, розробіть план дій для її усунення та реалізуйте його.
Крок 5. Перевірка рішення та впровадження превентивних заходів	<ul style="list-style-type: none">•Після того, як ви виправили проблему, перевірте повну функціональність.•За необхідності застосуйте профілактичні заходи.
Крок 6. Документування отриманих даних, вжитих заходів та результатів	<ul style="list-style-type: none">•Завершальним етапом процесу пошуку й усунення несправностей є документування отриманих даних, вжитих заходів і результатів.•Це дуже важливо для подальшого використання.

Вирішення проблеми або її ескалація?

- У деяких ситуаціях неможливо негайно вирішити проблему. Проблема слід загострити, коли вона потребує рішення менеджера, певного досвіду або рівня доступу до мережі, недоступного фахівцю з усунення несправностей.
- Політика компанії повинна чітко вказати, коли і як фахівець повинен загострювати проблему.

Методи пошуку та усунення несправностей

Команда debug

- Команда IOS **debug** дозволяє адміністратору відображати повідомлення про процес, протокол, механізм та повідомлення про події в режимі реального часу для аналізу.
- Всі команди **debug** вводяться в привілейованому режимі EXEC. Cisco IOS дозволяє звужувати вихідні дані **debug** , включаючи лише відповідну функцію або підфункцію. Використовуйте команди **debug** тільки для усунення специфічних проблем.
- Щоб переглянути короткий опис всіх параметрів команди debug, використовуйте команду **debug ?** в привілейованому режимі EXEC у командному рядку.
- Щоб вимкнути певну функцію налагодження, додайте ключове слово **no** перед командою **debug**
- Крім того, ви можете ввести форму команди **undebug** в привілейованому режимі EXEC.
- Щоб відключити відразу всі активні команди debug, використовуйте команду **undebug all** .
- Будьте обережні, використовуючи деякі команди **debug**, оскільки вони можуть згенерувати значний обсяг вихідних даних і можуть використовувати велику частину системних ресурсів. Маршрутизатор може настільки зайнятися відображенням повідомлень **debug**, що у нього не буде достатньої потужності для виконання своїх мережних функцій або навіть прослуховування команд, щоб вимкнути налагодження.

Методи пошуку та усунення несправностей

Команда terminal monitor

- **debug** та деякі інші вихідні повідомлення IOS не відображаються автоматично на віддалених з'єднаннях. Це пояснюється тим, що повідомлення журналу не можуть відобразитися на вту-лініях.
- 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** .

```
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#
```

```
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#
```

Сценарії пошуку та усунення несправностей

Сценарії пошуку та усунення несправностей

Проблеми з дуплексною експлуатацією та невідповідністю налаштувань

- 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 Autonegotiation Ethernet полегшує конфігурацію, мінімізує проблеми та максимально збільшує продуктивність зв'язку між двома з'єднаними мережами Ethernet. Під'єднані пристрої спочатку оголошують підтримувані можливості, а потім обирають режим найвищої продуктивності, підтримуваний обома сторонами.
- 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 умов дуплексної невідповідності, продуктивність зв'язку буде дуже низькою.
- Дуплексні невідповідності зазвичай викликані неправильно налаштованим інтерфейсом або, в рідкісних випадках, невдалим автоматичним налаштуванням. Невідповідність дуплексу може бути складно усунути, оскільки зв'язок між пристроями все ще відбувається.

Проблеми з IP-адресацією на пристроях IOS

- Двома поширеними причинами неправильного призначення IPv4 є помилки призначення вручну або пов'язані з DHCP проблеми.
- 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** чи **show ip interface brief**, щоб перевірити, чи призначені IPv4-адреси для мережних інтерфейсів. Наприклад, виконання команди **show ip interface brief** як показано, перевірить стан інтерфейсів 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#
```

Проблеми з IP-адресацією на кінцевих пристроях

- На комп'ютерах під керуванням 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).
- 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.
 - **Примітка:** Інші операційні системи, такі як Linux та OS X, не використовують APIPA.
- 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 Windows, використовуйте команду **ipconfig** .

Несправності, пов'язані зі шлюзом за замовчуванням

- Шлюз за замовчуванням для кінцевого пристрою - це найближчий мережний пристрій, що належить до тієї ж мережі, що і кінцевий пристрій, який може пересилати трафік в інші мережі. Якщо пристрій має неправильну або неіснуючу адресу шлюзу за замовчуванням, він не зможе встановлювати зв'язок з пристроями у віддалених мережах.
- 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 перевірити шлюз за замовчуванням на комп'ютерах під керуванням Windows, використовуйте команду **ipconfig**.
- 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.

Пошук та усунення несправностей, пов'язаних з DNS

- Користувачі часто помилково пов'язують роботу інтернет-посилання з доступністю DNS.
- Адреси DNS-серверів можуть бути призначені вручну або автоматично.
- Хоча для компаній і організацій це звичайне керування власними DNS-серверами, для розпізнавання імен можна використовувати будь-який доступний DNS-сервер.
- Cisco пропонує OpenDNS, який забезпечує захищену службу DNS, фільтруючи фішингові та деякі сайти шкідливих програм. Адреса OpenDNS - 208.67.222.222 та 208.67.220.220. Для домашнього та корпоративного використання доступні розширені функції, такі як фільтрування веб-вмісту та безпека.
- Використовуйте **ipconfig /all** як показано, щоб перевірити, який DNS-сервер використовується на комп'ютері Windows.
- Команда **nslookup** є ще одним корисним інструментом усунення несправностей DNS для ПК. За допомогою **nslookup** користувач може вручну розміщувати DNS-запити і аналізувати DNS-відповідь.

Обладнання та приклади налаштування



ЗМІСТ

АНАЛІЗ ІНФОРМАЦІЙНИХ СТРУКТУР НАВЧАЛЬНИХ ЗАКЛАДІВ ..2

1.1. Особливості сучасної освіти.....2

1.2 Типові структури навчальних комп'ютерних лабораторій4

НАВЧАЛЬНІ КОМП'ЮТЕРНІ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ 11

2.1 Загальні підходи створення системи з віддаленим доступом 11

2.2 Апаратне забезпечення для системи з віддаленим доступом 13

WI-FI роутер Tp_link TL-WR840N 14

WI-FI роутер Mercusys AC12g 15

AX1500 Wi-Fi 6 Router.....20

Роутер MikroTik RB750Gr324

2.3 Розгортання систем з віддаленим доступом до НКЛ.....28

Варіант 1. Всі ресурси розташовані на одному вузлу локальної мережі НКЛ 28

Варіант 2. Ресурси різного типу розташовані на різних вузлах НКЛ34

Варіант 3. Отримання віддаленого доступу до робочого столу всіх комп'ютерів НКЛ 43

Варіант 4. Отримання повного доступу до всіх ресурсів НКЛ.....58

Додатки68

Додаток А Перелік команд загального налаштування роутеру MikroTik68

Додаток Б Перелік команд налаштування роутеру MikroTik для налаштування Firewall 70

Додаток В Перелік команд налаштування роутеру MikroTik для налаштування PPTP 72

АНАЛІЗ ІНФОРМАЦІЙНИХ СТРУКТУР НАВЧАЛЬНИХ ЗАКЛАДІВ

1.1. Особливості сучасної освіти

Одним із пріоритетних напрямів розвитку сучасної освіти є інформатизація всіх складових навчального процесу. Сучасний етап розвитку інформатизації системи освіти спрямований на подальше підвищення якості освіти, забезпечення конкурентоспроможності національної системи освіти на світовому ринку освітніх послуг, її інтеграцію у світовий освітній простір. Він передбачає реалізацію принципів відкритої освіти, підпорядкований сучасним освітнім парадигмам людиноцентризму та рівного доступу до якісної освіти [4].

Останнім часом в умовах COVID-19, та після 24 лютого 2022р, коли наша держава була підвернута ворожій агресії зі сторони Російської Федерації та значна кількість навчальних закладів переведена на дистанційний режим роботи особливого значення набули різноманітні засоби інформаційних комп'ютерних технологій та різноманітні методики їх впровадження у навчальний процес [2].

Безумовно, така складна ситуація, та соціально-економічні виклики суспільства сприяли підвищенню значимості дистанційної освіти в Україні.

Про стан та перспективи організації дистанційного навчання в закладах загальної середньої освіти України пишуть Ю. Бигич, Ю. Богачков, А. Букач, В. Буренко, В. Кухаренко, Т. Літвінова, Т. Свистунова, В. Харківець. Проблему використання елементів дистанційної освіти у вищій школі розглядають у своїх розвідках (І. Адамова, Ю. Василенко, А. Гуржій, О. Дмитрієнко, М. Жалдак, Л. Карташова, А. Кожевникова, Ю. Кравченко, О. Кузьмінська, Н. Лотошникова,

А. Самусенко, П. Стефаненко). Різним питанням організації дистанційного та цифрового навчання присвячено багато наукових праць, зокрема роботи В. Бикова, Н. Морзе, В. Кухаренка, О.Щербини [3; 5; 6; 7]. Але робіт щодо використання віддалених віртуальних лабораторій в українському сегменті наукових досліджень майже немає. Серед світового досвіду заслуговує на увагу досвід університету DEUSTO [1] (м. Більбао, Іспанія).

Однак, в такій складній ситуації, в той час коли багато закладів освіти працюють у дистанційних умовах, ефективне використання сучасних інформаційних технологій та прогресивних педагогічних засобів навчання неможливе без створення спеціалізованих умов у навчальних комп'ютерних лабораторіях (НКЛ) .

За таких умов, питання організації комп'ютерного середовища у навчальних лабораторіях та комп'ютерних класах ставить нові завдання до організації комп'ютерної мережі та програмно-технічного оснащення [5]. Основною метою цього процесу повинно бути розробка нових підходів до організації виконання лабораторних завдань для студентів та учнів, які знаходяться дома, за межами НКЛ (навчального закладу) шляхом створення умов аналогічних стаціонарній системи навчання.

Аналіз літератури та різноманітних методичних розробок показав, що в цьому напрямку слабо наведені організаційно-методичні засади використання та модернізації існуючого програмно-апаратного забезпечення НКЛ. Більшість авторів запроваджують різноманітні педагогічні підходи та моделі освітнього процесу і всебічно розглядають можливості використання додаткового програмного забезпечення спрямованого на підвищення ефективності взаємодії між учасниками освітнього процесу [3; 7]. Таким чином, передбачається, що всі учасники освітнього процесу використовують засоби особистої (домашньої) обчислювальної техніки.

Однак питання роботи існуючих НКЛ в таких умовах не достатньо розглянуті. В цей час, комп'ютерні класи (лабораторії) практично не готові до нових вимог освітнього процесу та в більшості випадків знаходяться у режимі простою або часткового використання. Безумовно, розробка засобів використання існуючих локальних інформаційних ресурсів НКЛ в умовах дистанційної освіти значно підвищить ефективність всього навчального процесу.

1.2 Типові структури навчальних комп'ютерних лабораторій

У закладах освіти існує багата кількість НКЛ, які відрізняються як рівнем оснащення обчислювальною технікою так і різноманітним програмним забезпеченням в залежності від спеціалізації та особливостей навчального процесу. Однак, з точки зору організаційної інформаційної та мережевої структури можна виділити найбільш поширені типові структури НКЛ, які використовуються у багатьох закладах середньої освіти та більшості вишів і, в багатьох випадках зовсім не пристосовано до завдань вирішення проблеми надання віддаленого доступу тим хто навчається дистанційно.

Під інформаційною структурою НКЛ будемо розуміти — комплекс програмно-технічних засобів, організаційних систем та нормативних документів, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток програмно-технічних засобів інформаційної взаємодії в межах комп'ютерної навчальної лабораторії. В межах цієї роботи основний аналіз будемо проводити з урахуванням тільки програмно-технічних засобів існуючих у НКЛ та її мережевої структури.

На засадах попереднього аналізу та досвіду можна виділити найбільш поширену найпростішу типову структуру НКЛ, яка використовується у багатьох закладах середньої освіти та більшості вишів (рис. 1.1).

Така типова структура ефективно працює при умовах її безпосереднього використання в аудиторії та може включати: мережеве обладнання, робочі станції (персональні комп'ютери), мультимедійне обладнання, які зазвичай об'єднані на засадах однорангової мережі Microsoft. Така структура НКЛ дозволяє ефективно використовувати мережу Інтернет, локальні прилади та локальне програмне забезпечення, але зовсім не пристосована для використання учасниками освітнього процесу в дистанційних умовах. Таким чином, основна спрямованість інформаційних потоків – це однонаправлений обмін інформацією «ізнутри – назовні». Тільки, за умови розгалуженої кабельної мережі, викладачі зможуть проводити онлайн лекції з лабораторії зі студентами та учнями, які працюють дистанційно (дома). Жодних можливостей використати наявну комп'ютерну техніку та програмне забезпечення із дому не передбачено.

При такому підході більшість інформаційних ресурсів є слабо керованими та потребують постійної присутності співробітників навчально-допоміжного персоналу.

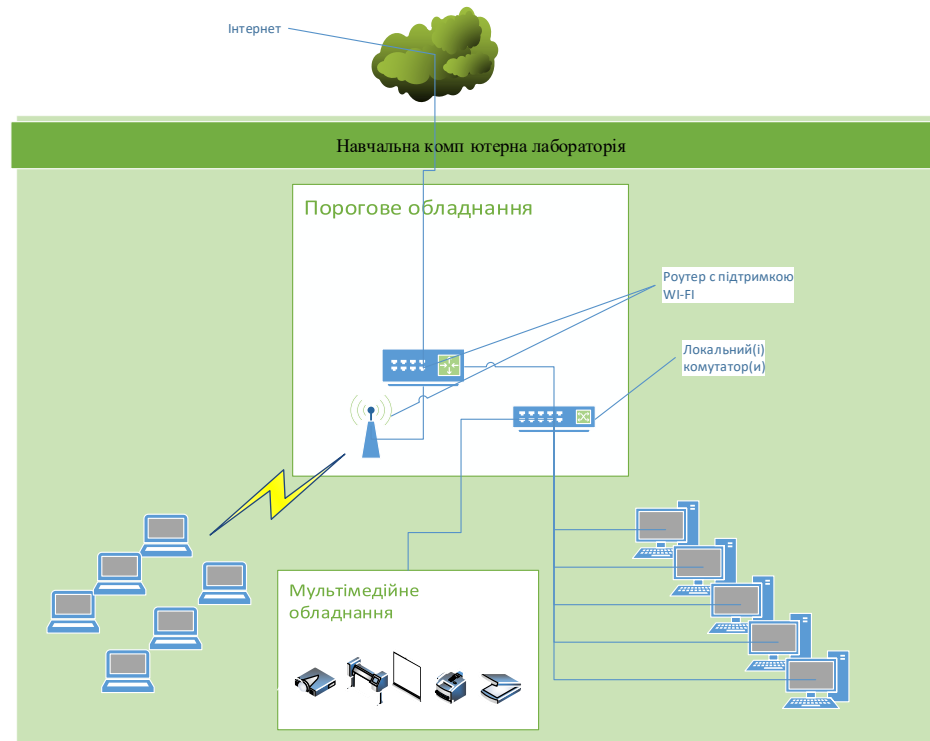


Рис.1.1 Найпростіша інформаційна структура НКЛ

Тим не менш, значною перевагою цієї інформаційної системи є:

- мала вартість,
- незначні вимоги до кваліфікації обслуговуючого персоналу,
- мінімальна програмно-технічна підтримка та можливість забезпечити виконання основних завдань навчального процесу при роботі у стаціонарному (денному, очному) режимі.

Основним недоліком її є відсутність можливостей використати наявну обчислювальну техніку в дистанційних умовах, коли всі учасники освітнього процесу знаходяться поза межами НКЛ.

У деяких навчальних закладах для підвищення ефективності інформаційної системи додатково використовують файловий сервер та друксервер. Більшість таких серверів створено на засадах використання розподіленого файлового доступу мережі Ms Windows (рис. 1.2).

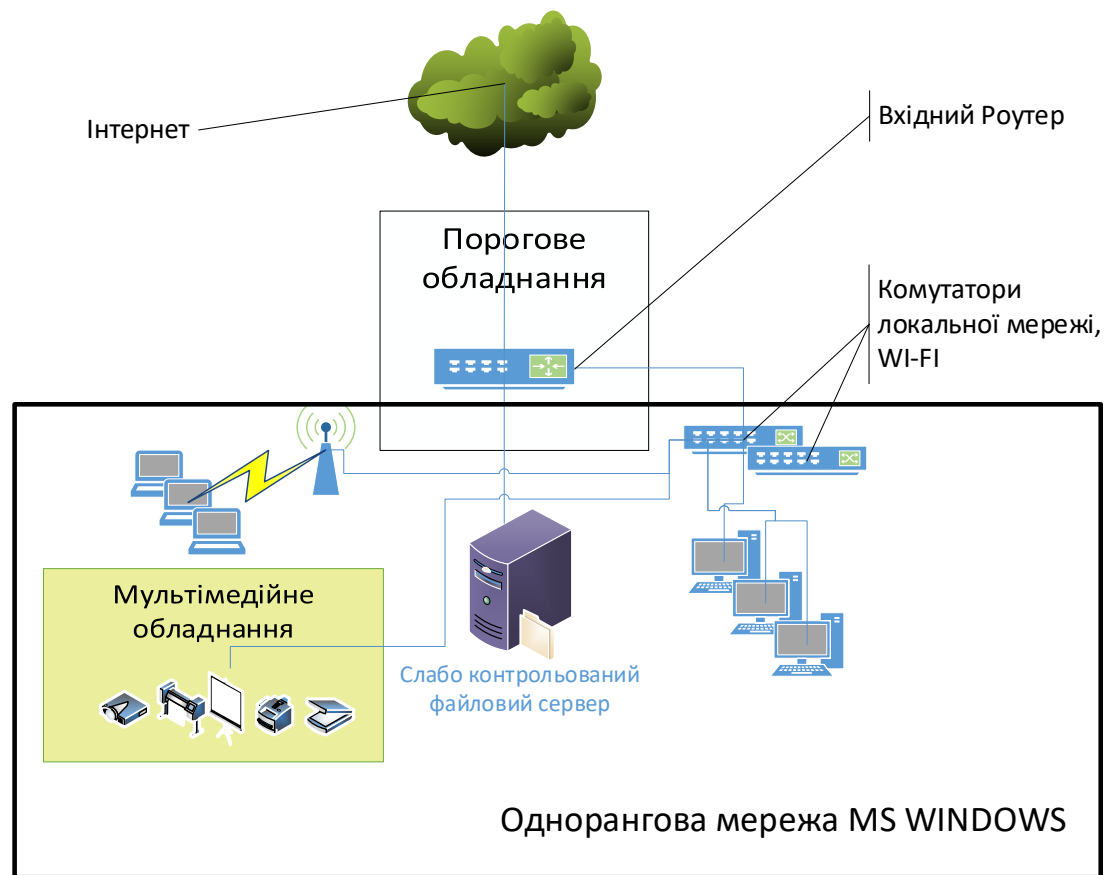


Рис.1.2. Типова схема найбільш поширеної інформаційної системи з підтримкою обміну файлами

При такому підході існують наступні недоліки:

- більшість файлових ресурсів буде слабо керуватись та працювати у режимі «тільки читання для ВСІХ» або обмеженого доступу «на запис» – для деяких користувачів;
- навчальні заклади зіштовхуються з багатьма питаннями безпеки, а в деяких випадках йдуть на організацію «неконтрольованої файлової кучі» – будь хто може «покласти» файл та будь хто може його видалити.

На рисунку 1.3 показано спрощену схему НКЛ більш складної інформаційної –технічної структури, яка характерна для вищих навчальних закладів і дуже рідко використовується у закладах середньої освіти. Основною особливістю її є наявність розгалуженої мережі та окремо виділених обчислювальних машин великої продуктивності з серверними операційними системи (Microsoft Windows Server, linux server). Така структура дозволяє:

- створити умови для централізованого керування обчислювальними ресурсами за рахунок використання Microsoft Active Directory (Ms AD) або LDAP;
- забезпечити умови для подальшого розвитку інформаційної системи;
- використати програмного забезпечення віддалено доступу на засадах RDP до окремих серверів, принтерів, окремих робочих станцій;
- більш швидко запровадити перехід до дистанційних засобів навчання;
- створити умови для повної інтеграції усіх інформаційних ресурсів.

Однак, не багата кількість навчальних закладів перейшла на створення єдиного домену для всіх структурних підрозділів.

До недоліків системи створення єдиного домену Ms AD можна віднести наступне:

- потрібен навчально-допоміжний персонал більш високої кваліфікації;
- необхідне виділення окремих потужних обчислювальних машин для додаткових сервісів та служб;
- сервера Ms Windows є ядром такої системи, від якого залежить функціонування всієї інформаційної системи, тому необхідно створювати додатково систему резервного копіювання та підтримки;
- значна вартість ліцензійного програмного забезпечення для серверів;
- необхідність придбання додаткових ліцензій на користувачів (приладів);
- велика розгалуженість локальної мережі та структурних підрозділів та приладів, як правило, не дозволяє повністю використовувати переваги домену, наприклад, особисті комп'ютери викладачів та студентів, спеціалізовані структурні підрозділи і таке інше.

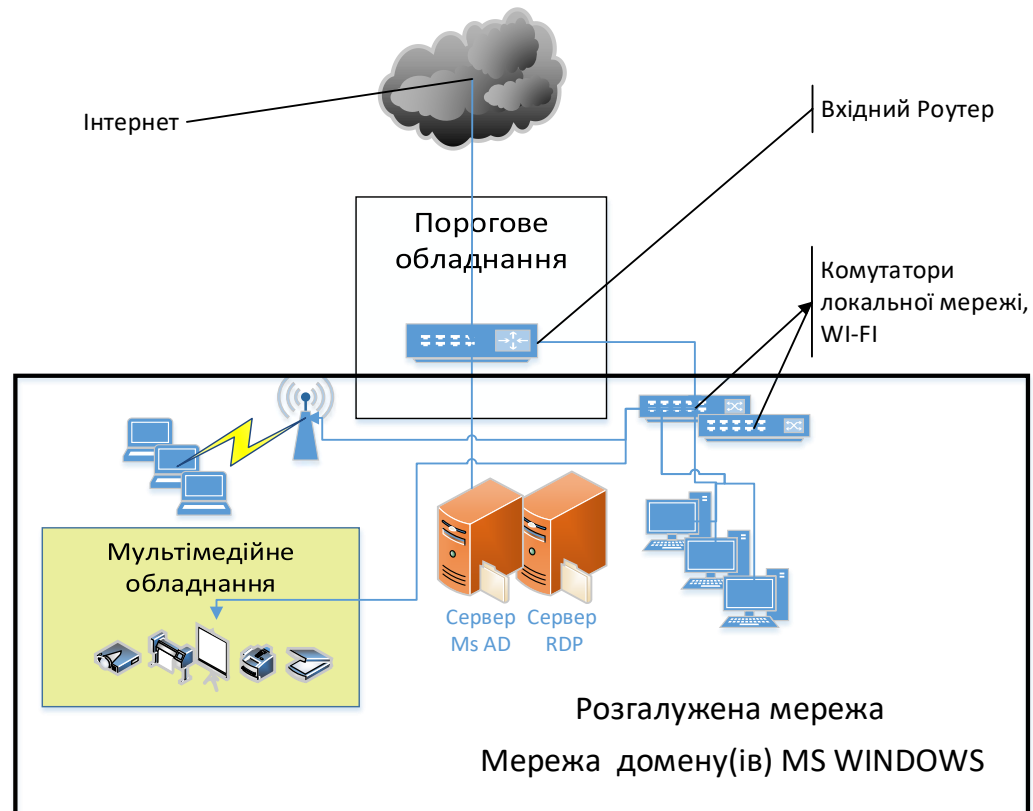


Рис.1.3. Типова схема керуємої інформаційної системи з підтримкою домену Ms AD

ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ

2.1 Загальні підходи створення системи з віддаленим доступом

Важливим кроком у створенні системи з віддаленим доступом є етапи аналізу та планування переходу всієї інформаційної системи на використання віддаленого доступу. У загальному випадку необхідно вирішити низьку завдань та обов'язково врахувати наступне:

1. Можливість отримання реальної IP адреси (пула адресів).
2. Кількість, типи та різноманітність інформаційних ресурсів, які повинні бути надані у віддаленому доступі. При цьому, потрібно врахувати необхідні умови основних завдань навчального процесу з метою забезпечення достатньої якості виконання лекційних занять та завдань до лабораторних робіт.
3. Реальний стан наявних інформаційних ресурсів, їх спроможність працювати у віддаленому та безперервному (або необхідному) режимі, можливість їх переналагодження та модернізації .
4. Фінансові можливості придбання додаткового програмного та апаратного забезпечення (комп'ютери, складові комп'ютерів, комплектуючі, програмне забезпечення, роутери, тип мережевої кабельної системи та інше).
5. Наявність та кваліфікація навчально-допоміжного персоналу, спроможного виконати монтаж, налаштування та обслуговування додаткового програмно-апаратного забезпечення.
6. Приблизний термін впровадження запланованих рішень.

У лабораторії ДІСЕНП кафедри ІТС Луганського національного університету відповідно до завдань проекту EASMUS+ MoPED було проведено дослідження та впровадження різноманітних варіантів НКЛ з віддаленим доступом. Досвід їх впровадження засвідчив той факт, що завдання аналізу та планування всієї інформаційної системи є складним, багатоітераційним процесом та потребує повного комплексного підходу. Для цього необхідно окреслити основні показники ефективності системи НКЛ з віддаленим доступом. Серед мінімального набору таких показників є: відсоток реалізації елементів навчального плану за допомогою НКЛ, стабільність та наявність підключення, швидкість доступу до інформаційних ресурсів, наявність фінансування та кваліфікація навчально-допоміжного персоналу.

В окремих випадках необхідно приймати рішення спрямовані на першочергове виконання завдань, які можливо виконати та впровадити в існуючих умовах в стислий термін. Після їх виконання знову проводити комплексний аналіз. Таким чином вдається поступово досягнути значних результатів у досягненні проміжної мети. Цей процес не повинен зупинятися з метою постійного вдосконалення існуючих рішень інформатизації навчального процесу та підвищення якості дистанційної освіти. Це дозволяє створити передумови створення освітньої екосистеми (яка включає не лише НКЛ) та забезпечить її сталий розвиток.

Однак, з багатьох можливих рішень по створенню інформаційної системи з віддаленим доступом в межах цієї роботи окреслимо тільки декілька швидких та поширених випадків. При цьому будемо вважати, що в нас є реальна ІР адреса, в наявності необхідний допоміжний персонал, достатньо фінансових коштів та термін впровадження нас влаштовує.

- **Випадок 1.** Всі ресурси розташовані на одному вузлу локальної мережі НКЛ.

- **Випадок 2.** Ресурси різного типу (в кількості одного кожного типу) розташовані на різних вузлах НКЛ, які використовують різні порти TCP/IP. Іншими словами – один ВЕБ сервер, один принтер, один сервер RDP (віддаленого робочого стола) і так далі.
- **Випадок 3.** Ресурс одного типу, що використовує один порт але розташовані на різних вузлах НКЛ та за рахунок організаційних заходів може бути змінено.
- **Випадок 4.** Повний доступ до всіх ресурсів НКЛ.

Слід зауважити, що перших два випадка можуть бути створені на багатьох типах порогових приладів. У третьому випадку треба проводити ґрунтовний попередній аналіз щодо можливостей наявного програмно-технічного забезпечення.

2.2 Апаратне забезпечення для системи з віддаленим доступом

Одним з важливіших етапів створення НКЛ з віддаленим доступом є вибір засобу приєднання локальної мережі до мережі Інтернет. Існує декілька методів, однак всі вони поєднуються у два поширених підходи:

1. Створення порогового приладу на засадах виділеної обчислювальної машини з декількома мережевими адаптерами та налаштування системи доступу за рахунок можливостей певної операційної системи
2. Використання в якості порогового приладу окремого роутера та налаштування його.

В межах цієї роботи розглянемо другий варіант. Безумовно, існує велика кількість роутерів, які можуть бути використані в якості порогового обладнання НКЛ. В межах цієї роботи розглянемо тільки деякі приклади:

- WI-FI роутер Tp_link TL-WR840N [11];
- WI-FI роутер Mercusys AC12g[12];
- WI-FI роутер Tp_link AX1500 Wi-Fi 6[13];
- Роутер MikroTik RB750Gr3 без підтримки WI-FI[14]

WI-FI роутер Tp_link TL-WR840N

Це недорогий роутер швидкістю до 300 МБ/с, який має 4 LAN порти зі швидкістю 100МБ/с та 1 WAN порт та відносно не дорогий – 700 грн, кількість антен – 2.

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис 2.4 адреса вже налаштована на 192.168.112.1).

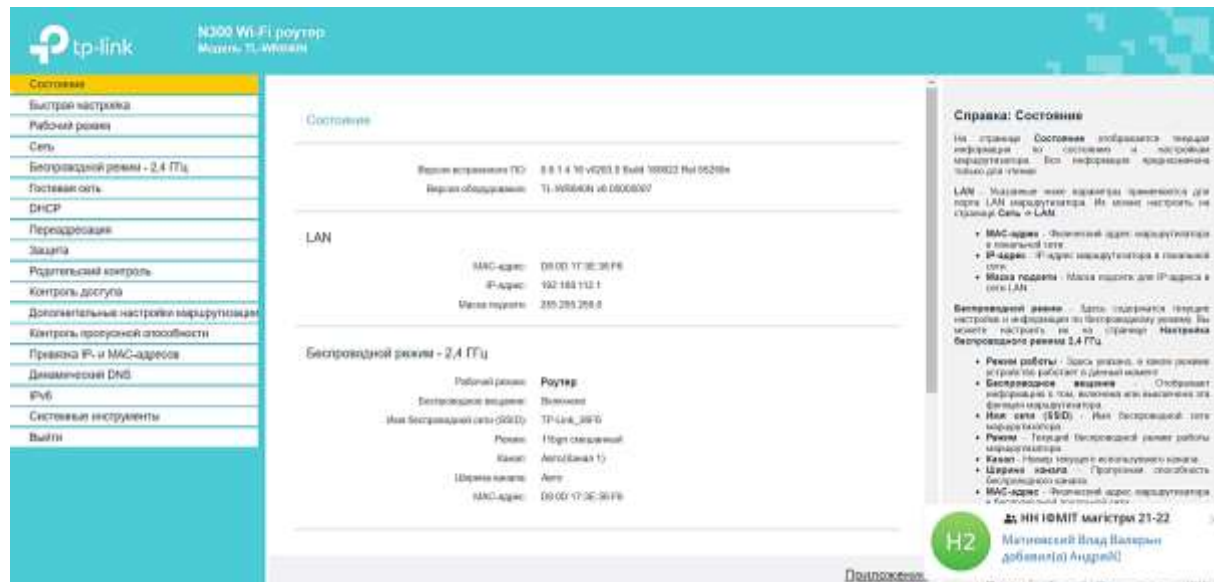


Рис 2.4 Стан Tr_link TL-WR840N

Для його попереднього налаштування слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу (рис.2.5).

WI-FI роутер Mercusys AC12g

Це більш сучасний роутер має загальну швидкість до 1200 Мбіт/с у двох діапазонах, який має 3 LAN порти зі швидкістю 1ГБ/с та 1 WAN порт та відносно не дорогий – 1500грн.



Рис. 2.5 Налаштування та підготовка до роботи

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис 2.6 адреса вже налаштована на 192.168.113.1).



Рис.2.6 Стан роутеру Mercusys AC12g

Для його попереднього налаштування слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу (рис.2.7-2.9).

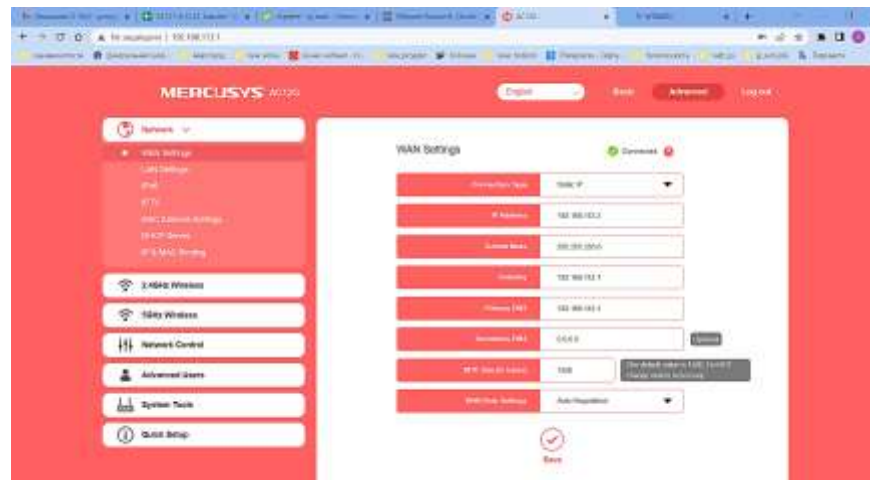


Рис. 2.7 Зовнішня адреса



Рис. 2.7 Локальна адреса



Рис.2.9 Налаштування DHCP WI-FI роутер Mercusys AC12g

AX1500 Wi-Fi 6 Router

Це сучасний роутер має загальну швидкість до 1500 Мбіт/с у двох діапазонах, який має 4 LAN порти зі швидкістю 1ГБ/с та 1 WAN порт та відносно не дорогий – 2500грн.

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис 2.10).

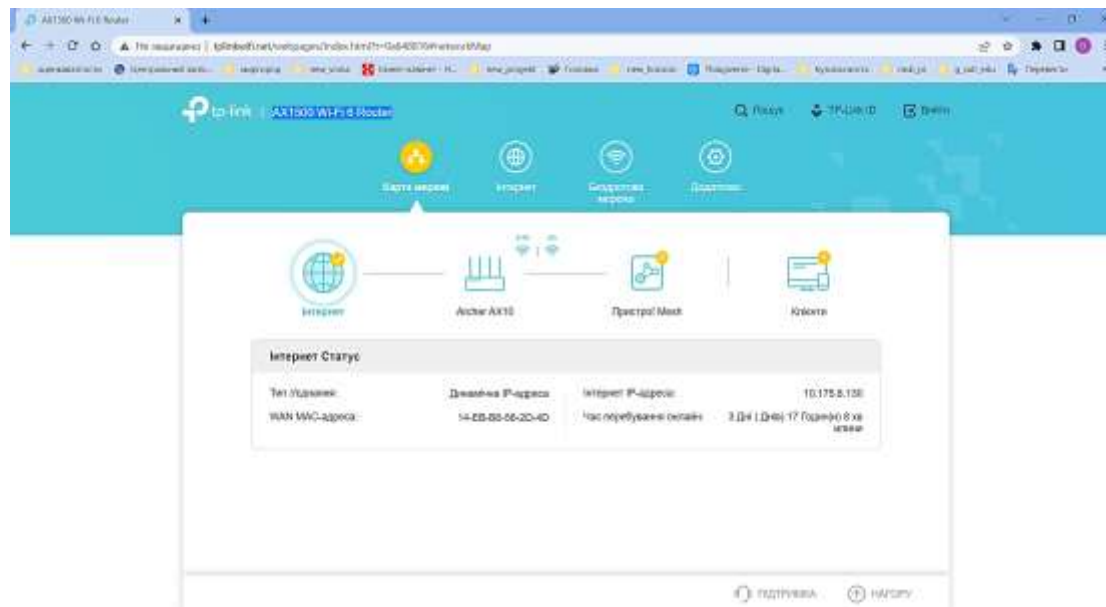


Рис. 2.10 Стан роутеру

Всі налаштування робляться аналогічно попереднім роутерам. Слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу

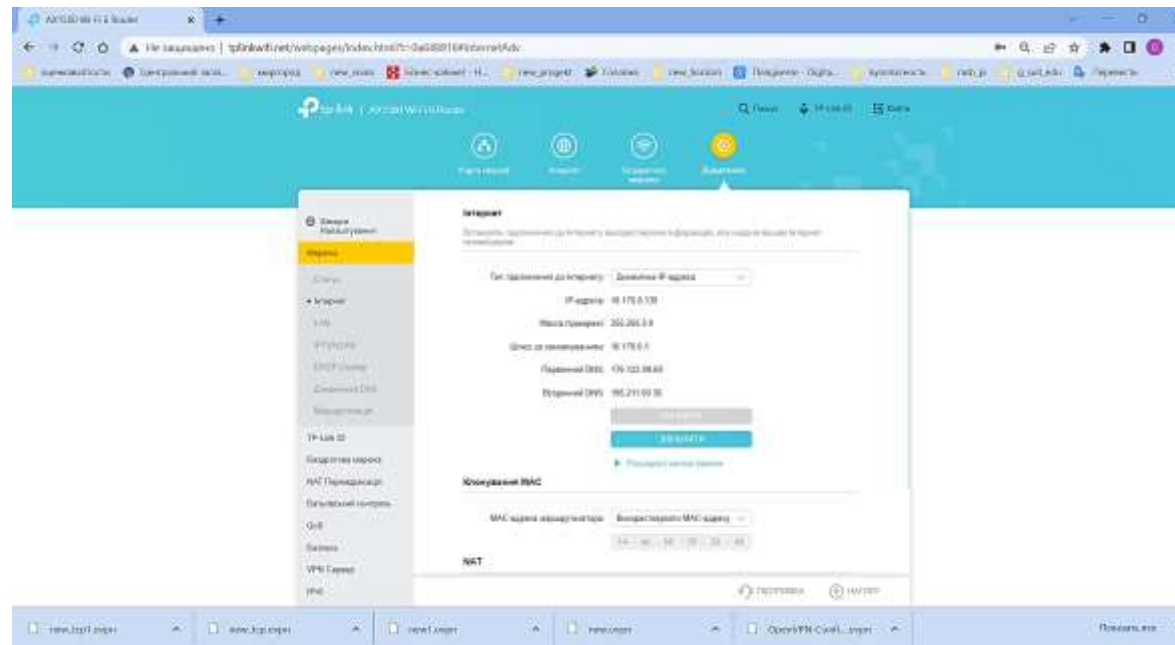


Рис 2.11 Налаштування зовнішньої адреси

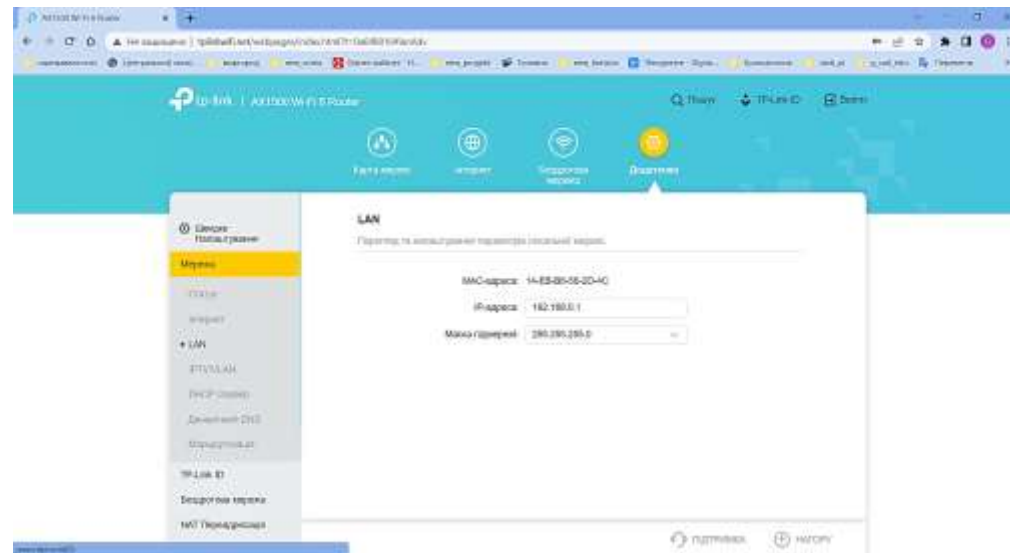


Рис 2.12 Налаштування зовнішньої адреси

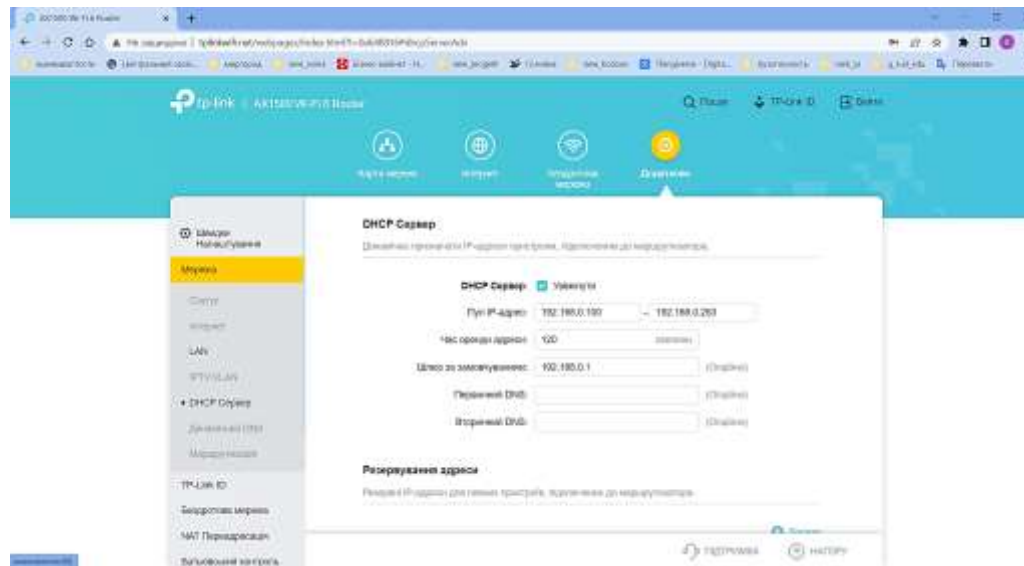


Рис 2.12 Налаштування DHCP

Роутер MikroTik RB750Gr3

Налаштування цього роутеру суттєво відрізняється від попередніх. Роутер не має попередньо призначених інтернет портів та локальних портів.

Роутер має 5 рівноцінних портів зі швидкістю 1ГБ/с та ціну 2400грн.

Для налаштування використовується браузер або спеціалізована програма WINBOX. Після очищення конфігурації (або за замовчанням) вважається, що 1 порт (ether1) – Інтернет з'єднання, а з 2 по 5 – локальна мережа. [15]

Слід відзначити, що роутери бренду MikroTik мають уніфікований принцип налаштування (внутрішня операційна система RouterOS) та відрізняються тільки характеристиками суцього технічного характеру: кількість портів, типи портів,

швидкість маршрутизації пакетів, обсяг таблиці MAC адрес та інше. У межах цієї роботи, в якості порогового приладу розглянемо роутер **MikroTik RB750Gr3** з операційною системою **RouterOS v6.49.6 (stable)**.

Попередньо, для достовірності даних, скинемо конфігурацію MikroTik (рис. 2.13, а) та налаштуємо її знову (так як показано на рис. 2.13, б).

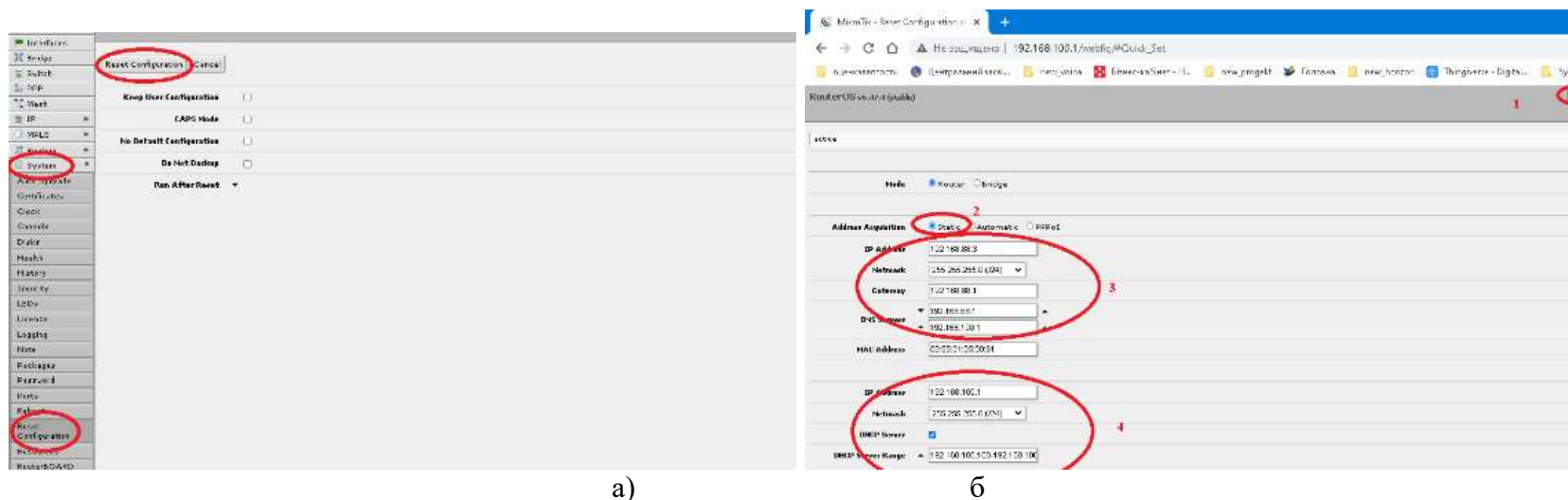


Рис. 2.13. Скидання конфігурації та попереднє налаштування

Таким чином, будемо вважати, що внутрішня локальна мережа має адресу 192.168.100.0 mask 255.255.255.0, внутрішня адреса порогового приладу (роутеру MikroTik) – 192.168.100.1, зовнішній інтерфейс (підключено Інтернет) – у першому порту – ether1 та має реальну IP адресу, наприклад 91.222.42.145, що надано провайдером за допомогою NAT на адресу 192.168.88.3 (рис. 2.14).

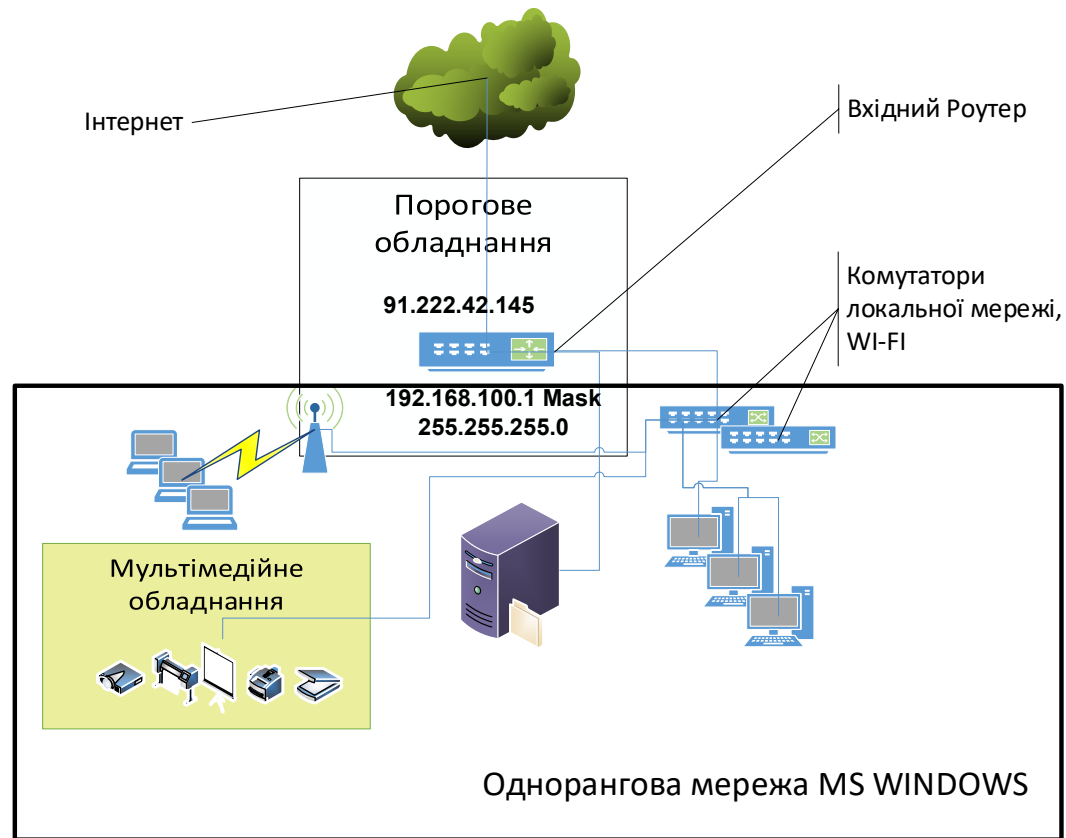
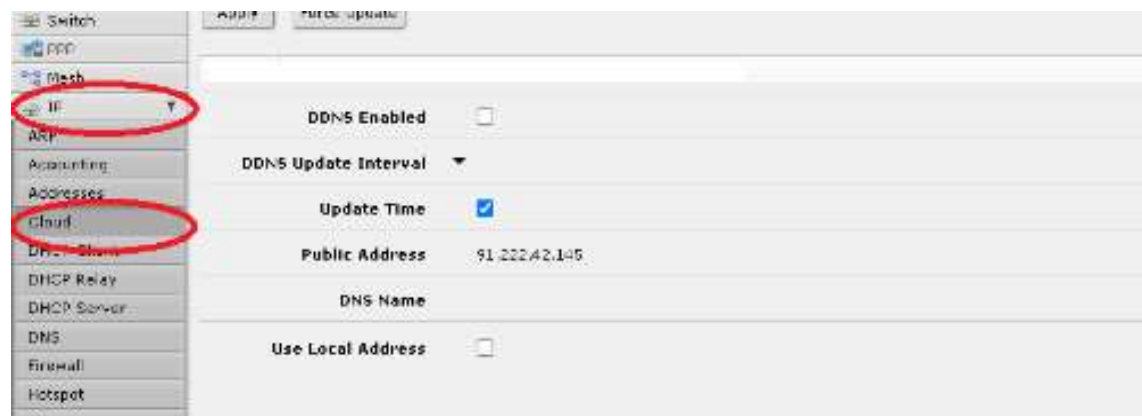
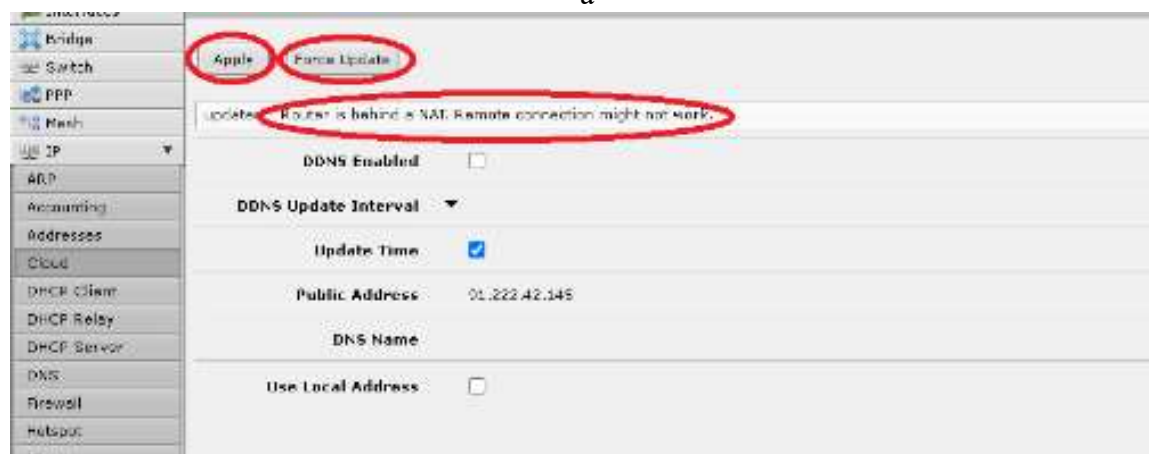


Рис. 2.14. Приклад адресації мережі НКЛ

Один із засобів перевірити зовнішні налаштування роутера MikroTik це перейти із локальної мережі за адресом порогового роутеру, в даному випадку, це: `hrpt://192.168.100.1` та обрати меню «IP» —«Cloud» потім кнопку “Force Update”. Після чого потрібно почекати поки відбудеться оновлення (рис. 2.15, а) та переглянути отримане повідомлення у верхній частині вікна додатку (рис. 2.15,б).



а



б

Рис. 2.15. Перевірка порогового роутеру

Якщо у Вас є повідомлення, як на рис 2.15б: «Router is behind a NAT. Remote connection might not work.» або «...service might not work», то треба звернутись до провайдера – у вас не має реальної IP адреси. У процесі практичного

впровадження з'ясовано, що оновлення працює не стабільно та з великими затримками, а в деяких випадках – не видає помилки навіть в умовах повної відсутності реальної IP адреси.

2.3 Розгортання систем з віддаленим доступом до НКЛ

Варіант 1. Всі ресурси розташовані на одному вузлу локальної мережі НКЛ

Розглянемо деякі можливі ситуації. Всі ресурси розташовані на одному вузлу локальної мережі НКЛ – наприклад, на внутрішній адресі – 192.168.100.2 . Це самий простий засіб організації віддаленого доступу до НКЛ та не потребує суттєвої переробки інформаційної структури.

В цьому випадку на багатьох роутерах є можливість скористатися параметром DMZ. Слід зауважити, що адреса локального інформаційного ресурсу повинна бути статичного, тобто без використання DHCP.

DMZ (від англ. demilitarized zone) – це сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних [8]. Як загальнодоступний може виступати, наприклад, вебсервіс: сервер, що його забезпечує, який фізично розміщений у локальній мережі (Інтранет), повинен відповідати на будь-які запити із зовнішньої мережі (Інтернет), при цьому інші локальні ресурси (наприклад, файлові сервери, робочі станції) необхідно ізолювати від зовнішнього доступу. Мета DMZ — надати додатковий рівень безпеки в локальній мережі, який дозволяє мінімізувати збитки в разі атаки на один із загальнодоступних сервісів: зовнішній зловмисник має прямий доступ тільки до обладнання в DMZ [9].

На рисунках 2.16-2.18 показано як це зробити на роутерах:

- Tp_link TL-WR840N – адреса ще не вказано – треба замінити 0.0.0.0 на необхідну адресу вузла локальної мережі, перекинути «стан» в положення «включити» та натиснути кнопку «зберегти» (рис. 2.16);
- Mercusys AC12g – показано для вузла локальної мережі з адресом 192.168.113.100 та потім перекинути «DMZ Server» в положення «ON» (рис. 2.17);
- Tp_link AX1500 – показано для вузла локальної мережі з адресом 192.168.0.100 та потім встановити «DMZ» в положення «увімкнути» (рис. 2.18).

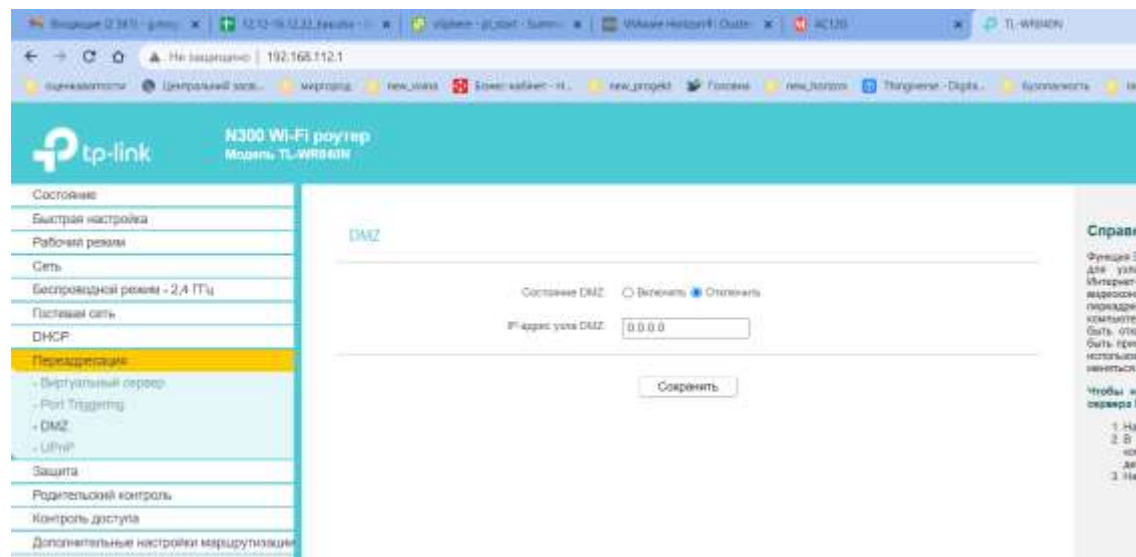


Рис. 2.16 Налаштування DMZ для Tp_link TL-WR840N



Рис. 2.17 Налаштування DMZ для Mercusys AC12g

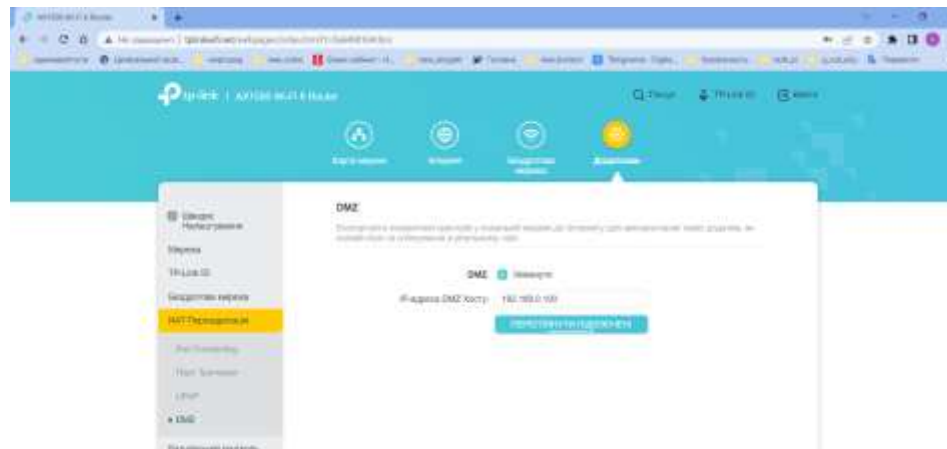


Рис. 2.18 Налаштування DMZ для Tr_link AX1500

Найбільш складні налаштування для роутеру Mikrotik. Для цього необхідно: вибираємо «IP» – «FireWall», закладка «Nat» (рис. 2.19) та тиснемо кнопку “Add New” – відобразиться сторінка параметрів (рис 2.20), на якій вводимо:

- Поле **Chain** – Dstnat (обов'язково) спрямованість пакету. У нашому випадку перенаправлення із зовнішньої мережі на внутрішню.
- Поле **Dst. Address**– 91.222.42.145 (зовнішній IP адрес роутеру), адреса призначення у пакеті. В деяких випадка, провайдер може надавати реальну IP адресу за допомогою свого NAT. В умовах експерименту це 192.168.88.3 – наш роутер використовує протокол NAT провайдера.
- Поле **In. Interface** – ether1 – зовнішній інтерфейс роутеру.
- Поле **Action** – Dst-nat – переадресувати із зовнішньої мережі у внутрішню.
- Поле **To Addresses**– 192.168.100.2 – внутрішня адреса вашого вузла з ресурсами (обов'язково).
- Крім того, коли не задавати поля **Dst. Address** та **In. Interface**, то це правило буде працювати на всьому зовнішньому трафіку.

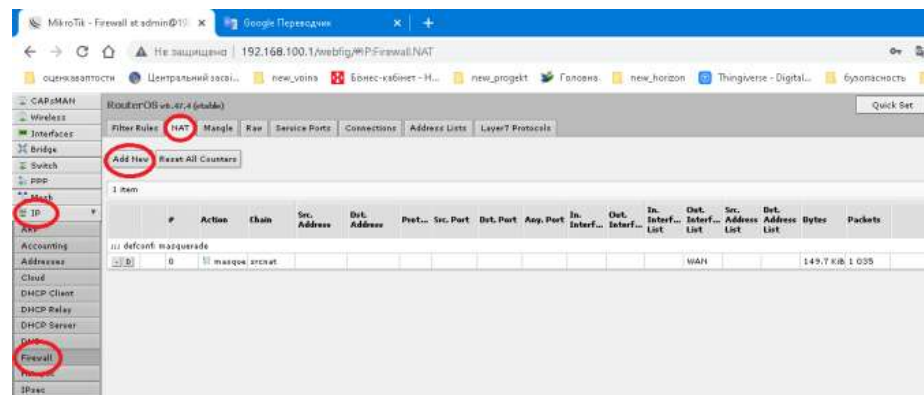


Рис. 2.19. Перехід до налаштування NAT

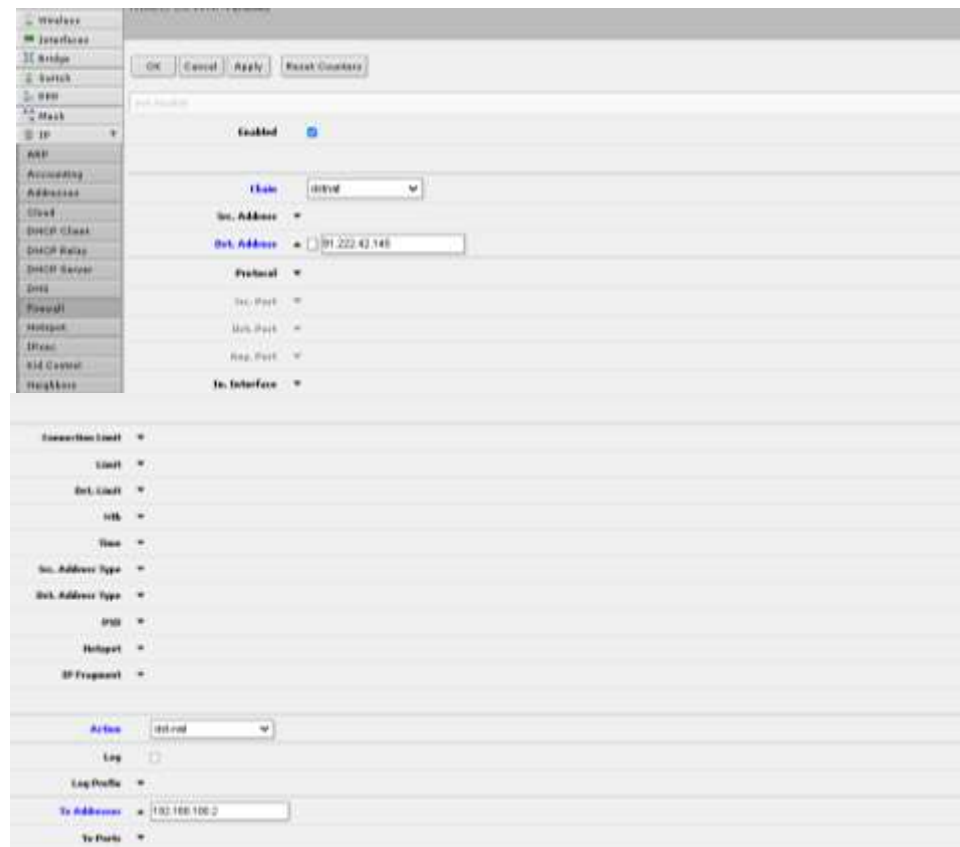


Рис. 2.20. Налаштування NAT для одного ресурсу

В результаті буде два правила Nat (рис. 2.21).



Рис. 2.21. Правила Nat для одного ресурсу

Якщо, налаштуєте роутер у новому стані, без спеціалізованих налаштувань, то все повинно працювати. В іншому випадку треба переглянути та налаштувати правила «Firewall». В загальному випадку повинно бути 11 правил «Firewall». Перелік команд наведено у Додатку А. (у меню «IP» – «FireWall», закладка «Filter Rules» (рис. 2.22).

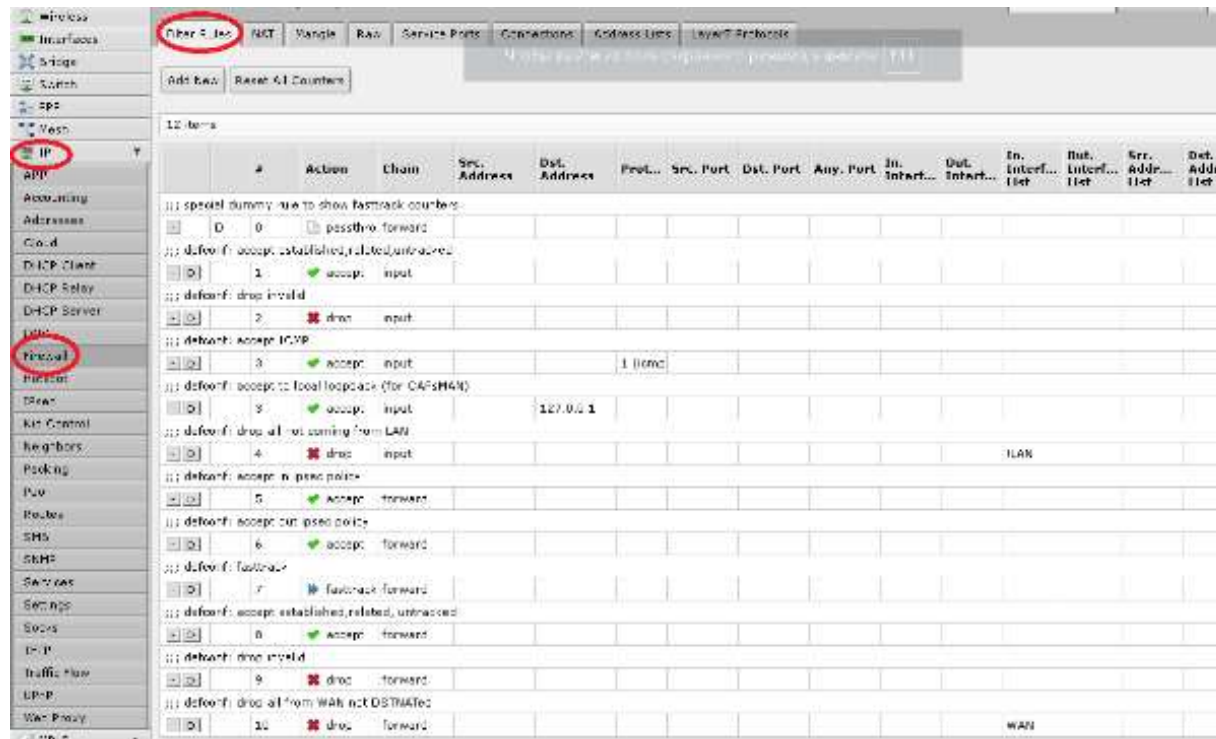


Рис. 2.22. Правила Filter Rules при першому налаштуванні

Варіант 2. Ресурси різного типу розташовані на різних вузлах НКЛ

Коли ресурси різного типу розташовані на різних вузлах НКЛ для задачі організації віддалено доступу треба ґрунтовно врахувати особливості протоколів (портів), що використовує кожний ресурс.

Треба врахувати три особливості:

1. З технічної документації встановити номери портів, що використовує кожна служба (ресурс), яка розташована на окремому вузлу локальної мережі.

- Порти служб (ресурсів), що розташовані на різних вузлах локальної мережі не мають однакових номерів. Не може бути задіяно однакові порти на різних вузлах локальної мережі.
- За рахунок організаційних заходів є можливість перевизначення співпадаючих портів на інші номери. Однак потрібно провести аналіз можливостей клієнтського програмного забезпечення для цих служб.

Наприклад, є ВЕБ сервер – 192.168.0.7 (порти 80 та 443), поштовий сервер – 192.168.0.8 (порти 25 та 110), FTP сервер – 192.168.0.9 (21,20 та 1024-1240).

Слід відзначити, що для багатьох роутерів ця задача вирішується приблизно однаково – за рахунок використання переадресування портів (меню – «віртуальний сервер» або «port forwarding»).

На рисунках 2.23-2.25 наведено меню роутерів Tp_link TL-WR840N, Mercusys AC12g та AX1500 Wi-Fi 6. Детальне вирішення наведеного прикладу дано тільки для роутеру AX1500 Wi-Fi 6 на рисунках 2.26-2.27.

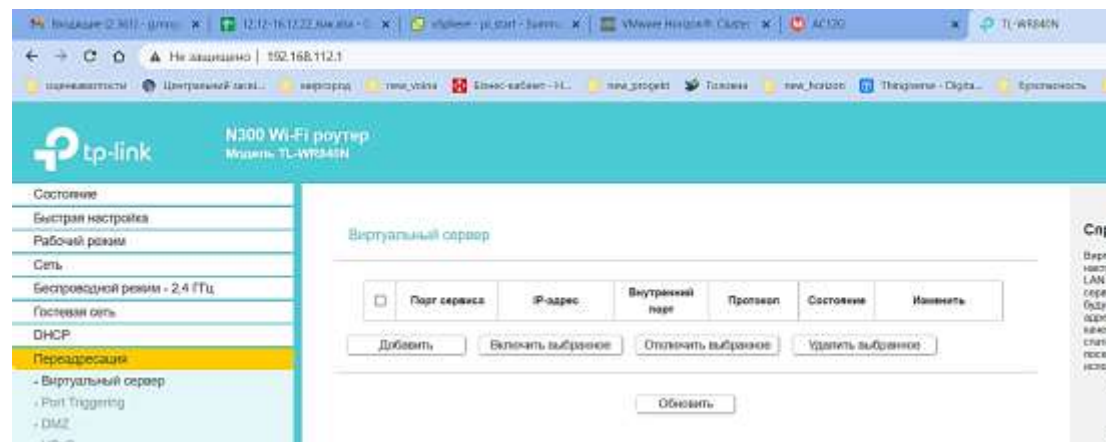


Рис. 2.23. Переадресування у роутері Tp_link TL-WR840N



Рис. 2.24. Переадресування у роутері Mercusys AC12g

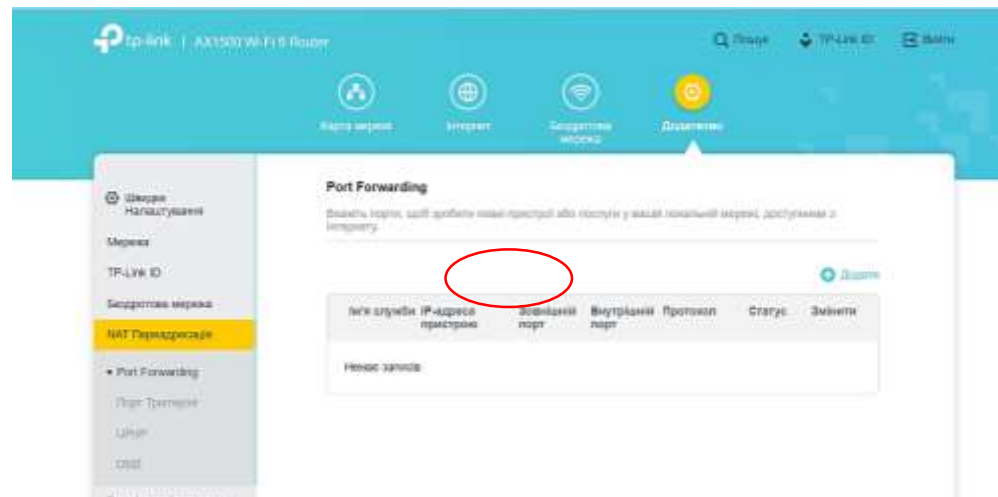


Рис. 2.25 Переадресація у сервері AX1500 Wi-Fi 6

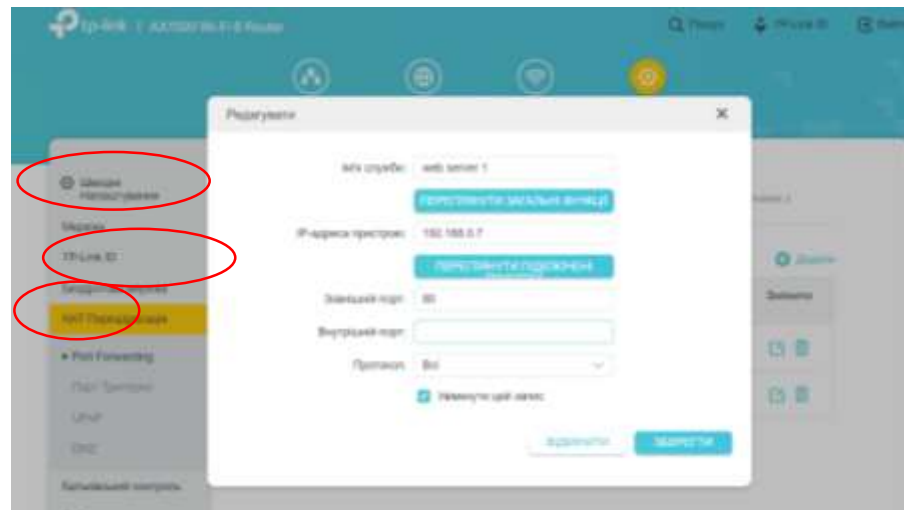


Рис. 2.26 Додавання ВЕБ – порт 80

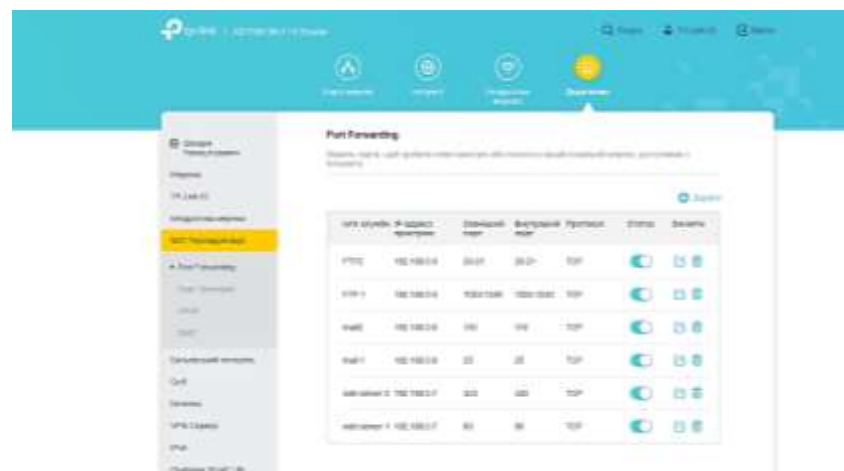


Рис. 2.27 Загальна таблиця налаштувань переадресування

Для роутеру Mikrotik [16] задача переадресування портів вирішується в інший метод. Для прикладу, є файловий ресурс мережі Microsoft на вузлу за адресом 192.168.100.2 та ВЕБ сервер – 192.168.100.7.

Файловий ресурс використовує багато портів, а ВЕБ сервер – порт 80. У такому випадку слід спочатку розташувати правило для ВЕБ серверу, а потім для файлового ресурсу. Слід враховувати, що порядок правил дуже важливий. Рекомендується більш «прости» ресурси розташовувати перед складними (менший номер правила). У будь-якому випадку є можливість змінити послідовність правил, перетягнув їх мишкою. Таким чином можна надати віддалений доступ багатьом ресурсам, якщо номери портів не співпадають.

Для виконання цього процесу треба перейти до правил NAT (рис. 2.19) та додати правило для ВЕБ серверу (рис. 2.28) з наступними параметрами:

- Поле **Chain** – Dstnat (обов'язково).
- Поле **Dst. Address**– 192.168.88.3 (зовнішній IP адрес роутеру).
- Поле **Protocol** – 6(tcp) – протокол ВЕБ серверу (обов'язково).
- Поле **Dst. Port** – 80 – порт ВЕБ серверу (обов'язково).
- Поле **In. Interface** – ether1 – зовнішній інтерфейс роутеру.
- Поле **Action** – Dst-nat.
- Поле **To Addresses**– 192.168.100.7 – внутрішня адреса ВЕБ серверу (обов'язково).

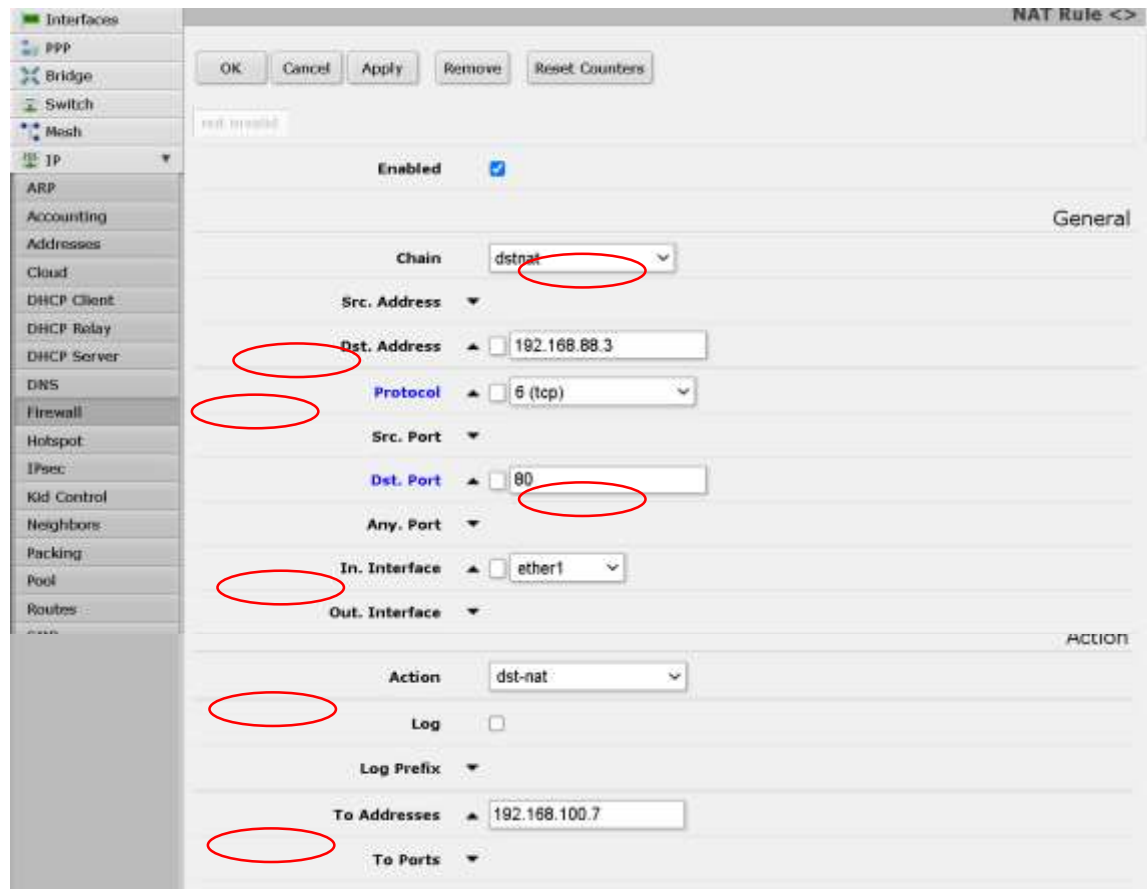


Рис. 2.28. Налаштування доступу до ВЕБ серверу

Потім , для другого вузлу, додаємо правило таке як у Варіанті 1. Таким чином призначаємо – всі інші порти – на адресу 192.168.100.2 .

У результаті повинно бути три правила (одно за замовчанням –masquerade) – дивись рис. 2.29.

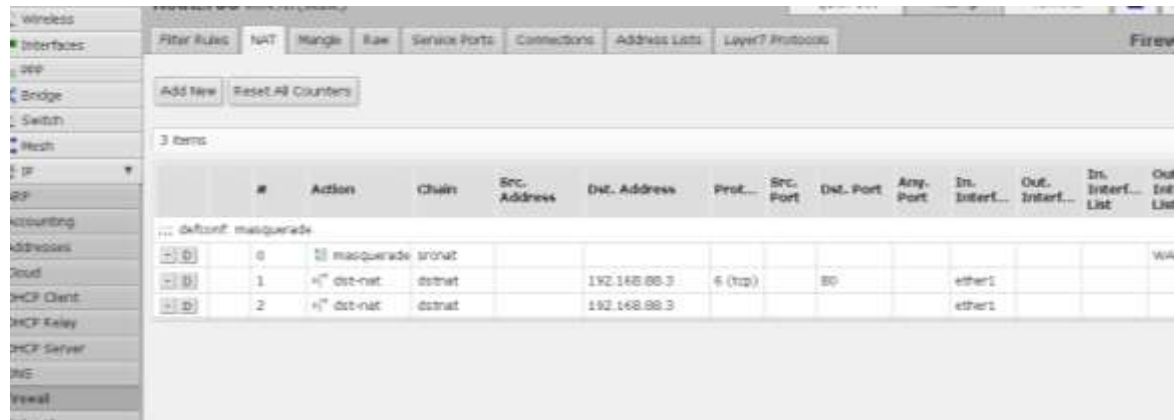


Рис. 2.29. Набір правил NAT для двох ресурсів

Слід відзначити, що є можливість для додавання другого ВЕБ серверу з адресом 192.168.100.9, якому теж потрібен порт 80 можна скористатися зміною порту на вхідному інтерфейсі, наприклад, 8081. Для цього створюємо правило за такою схемою:

- Поле **Chain** – Dstnat (обов'язково).
- Поле **Dst. Address**– 192.168.88.3 (зовнішній IP адрес роутеру).
- Поле **Protocol** – 6(tcp) – протокол ВЕБ серверу(обов'язково).
- Поле **Dst. Port** – 8081 – порт ВЕБ серверу (обов'язково).
- Поле **In. Interface** – ether1.
- Поле **Action** – Dst-nat.

- Поле **To Addresses**– 192.168.100.7 – внутрішня адреса ВЕБ серверу (обов'язково).
- Поле **To Port**– 80 – внутрішня адреса ВЕБ серверу (обов'язково).

У такому випадку у строчці адреса браузера користувачі повинні набрати – <http://192.168.88.3:8081/>

Це правило буде мати номер 3, то перенесемо мишкою його вище на номер 2 (рис. 2.30) та отримаємо чотири правила.



Рис. 2.30. Налаштування Nat з двома ВЕБ серверами та файловим ресурсом

Так необхідно створювати правила для багатьох ресурсів. Наприклад, для служби віддаленого робочого столу (192.168.100.13) за такими параметрами:

- Поле **Chain** – Dstnat (обов'язково).
- Поле **Dst. Address**– 192.168.88.3 (зовнішній IP адрес роутеру).
- Поле **Protocol** – 6(tcp) – протокол RDP серверу(обов'язково).
- Поле **Dst. Port** – 13389 – порт RDP серверу (обов'язково).

- Поле **In. Interface** – ether1.
- Поле **Action** – Dst-nat.
- Поле **To Addresses**– 192.168.100.13 – внутрішня адреса RDP серверу (обов'язково).
- Поле **To Port**– 3389 – внутрішня адреса RDP серверу (обов'язково).

У такому випадку у програмі «Підключення до віддалено робочого столу треба вказати адресу як показано на малюнку (рис. 2.31).

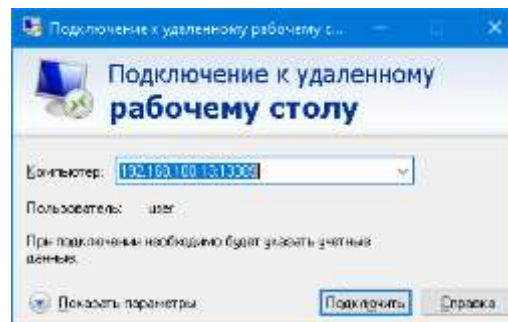


Рис. 2.31. Варіант підключення до віддалено робочого столу

Таким чином можна продовжувати створювати правила для всіх ресурсів НКЛ та слідкувати за всіма використаними портами. Такий варіант можливий для простих ресурсів НКЛ, у яких відомо перелік портів та їх можна перенаправити.

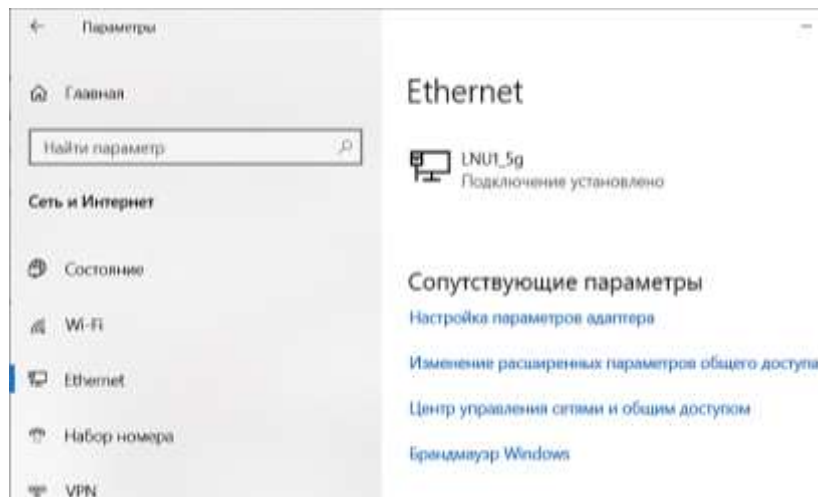
Таким чином, в результаті подібних дій, за рахунок організаційних заходів та принципу перепризначення портів є можливість створити віддалений доступ до всіх комп'ютерів НКЛ.

Варіант 3. Отримання віддаленого доступу до робочого столу всіх комп'ютерів НКЛ

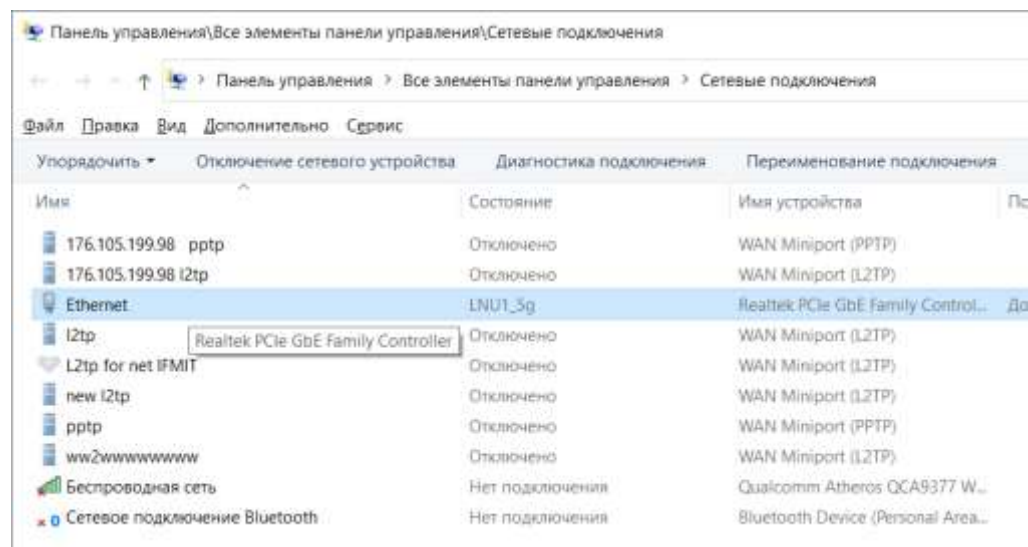
В попередньому розділі розглянуто питання організації віддаленого доступу до НКЛ у випадку коли всі порти служб мають різноманітні номери. Однак більш ґрунтовний аналіз цього процесу дозволяє стверджувати, що за рахунок впровадження додаткових організаційних заходів є можливість надати доступ до віддалених робочих столів всіх комп'ютерів НКЛ.

Наприклад, у НКЛ використовується мережа 192.168.0.0/24, шлюз – 192.168.0.1, DNS – 192.168.0.1. Загальна методика впровадження цього процесу зводиться до наступних кроків:

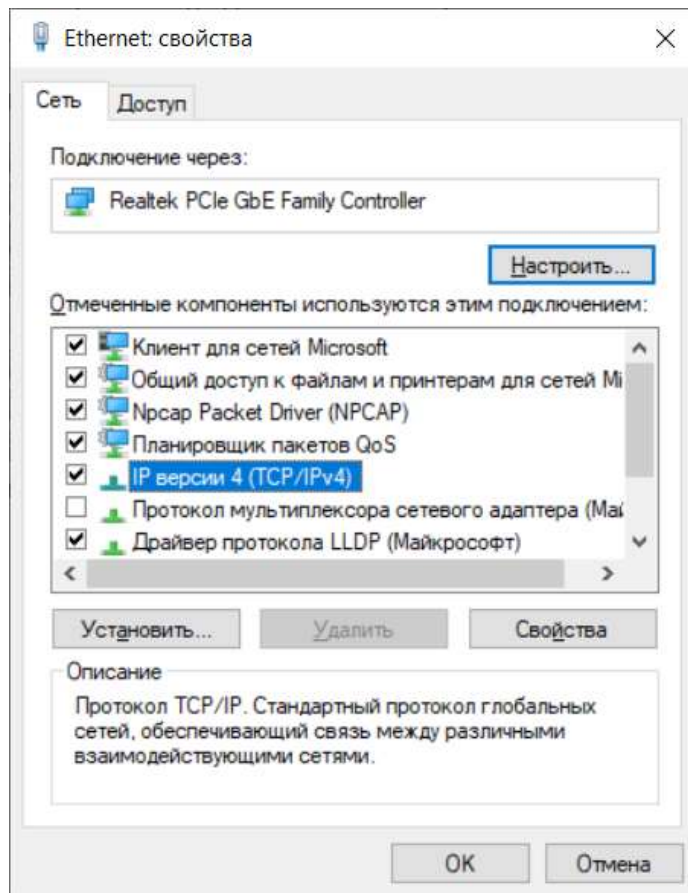
1. Переглянути систему адресації локальної мережі та відмовитись від використання DHCP.
 - а. Призначити статичні адреси всім комп'ютерам. Бажано ввести номери комп'ютерам та призначити подібні адреса (наприклад починаючи з 21). Комп'ютеру № 1 – 192.168.0.21, № 2 – 192.168.0.22 і так далі № 3 – 192.168.0.23 № 1 – 192.168.0.21. (Програма «Налаштування» – «мережа та Інтернет»)



Обрати «Ethernet» «Налаштування параметрів адаптеру»



права кнопка на адаптері – «властивості»



Обрати «IP версії 4 (TCP/IPv4) та натиснути «Властивості»

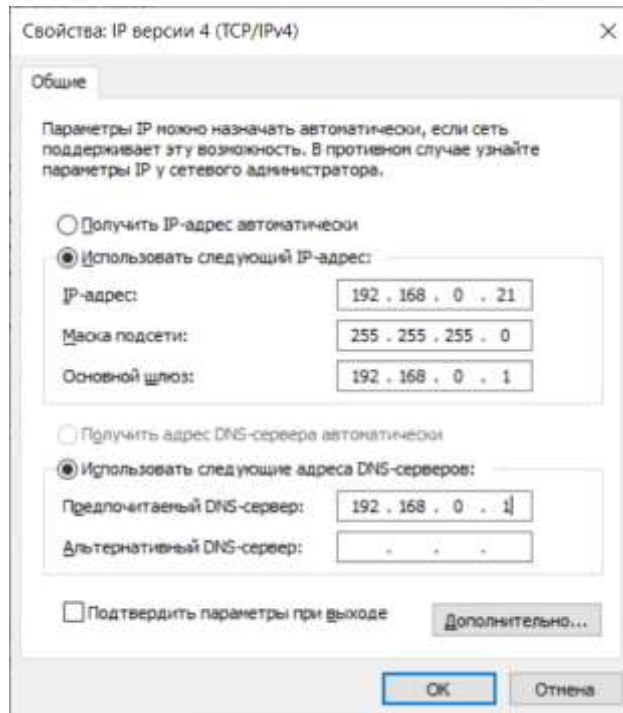


Рис. 2.32 Призначення статичної адреси

- в. Перевірити (або призначити) імена всіх комп'ютерів НКЛ. Наприклад, комп'ютеру № 1 з адресом 192.168.0.21 надати ім'я – comp1 комп'ютеру № 7 – 192.168.0.27 – comp7 і так далі

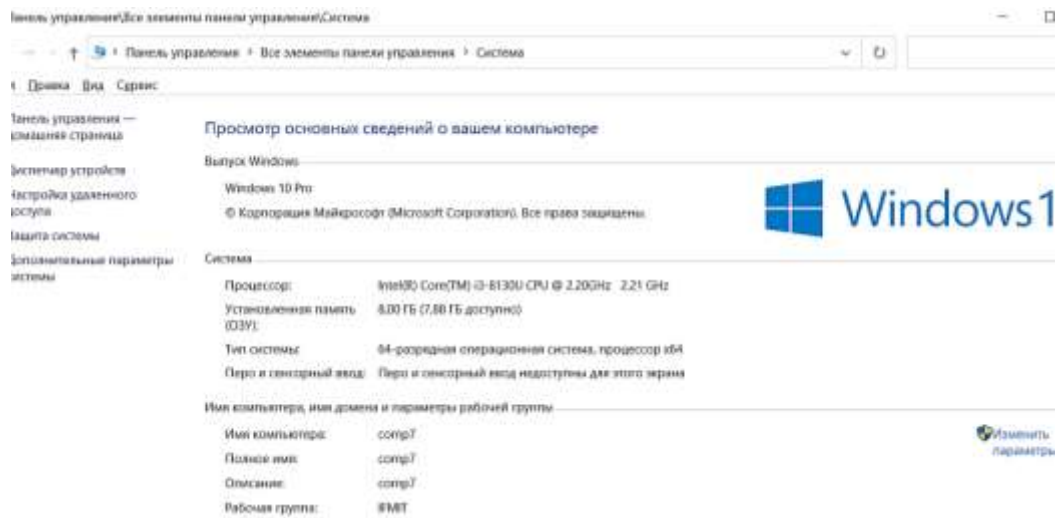
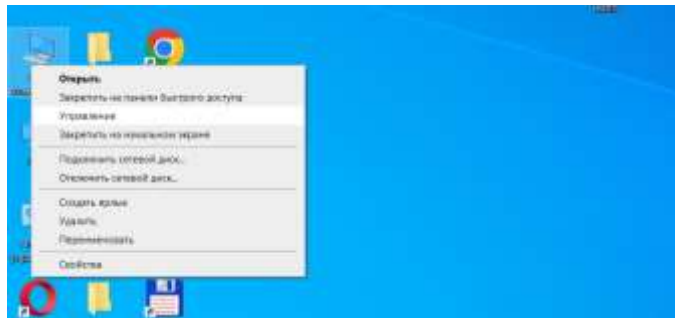
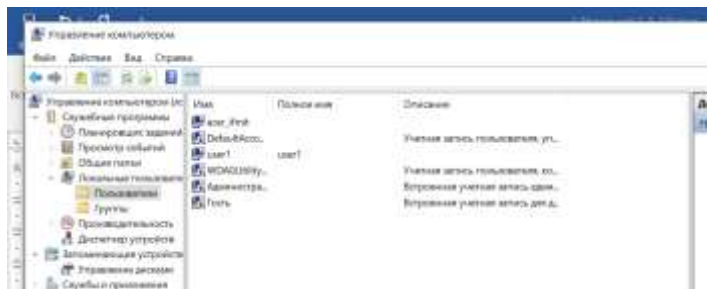


Рис. 2.33. Имя комп'ютера

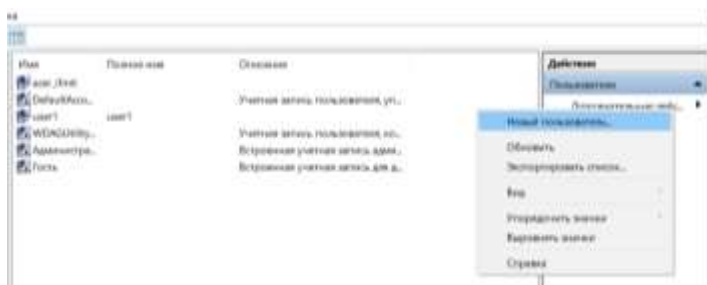
2. Створити необхідну користувачів на кожному комп'ютері та додати до користувачів віддаленого робочого столу
 - а. Створення користувача (Права кнопка миші на програмі «Мій комп'ютер»)



Обрати меню «Керування»



Клацнути на пустому місці «Новий користувач»



Задати параметри користувача

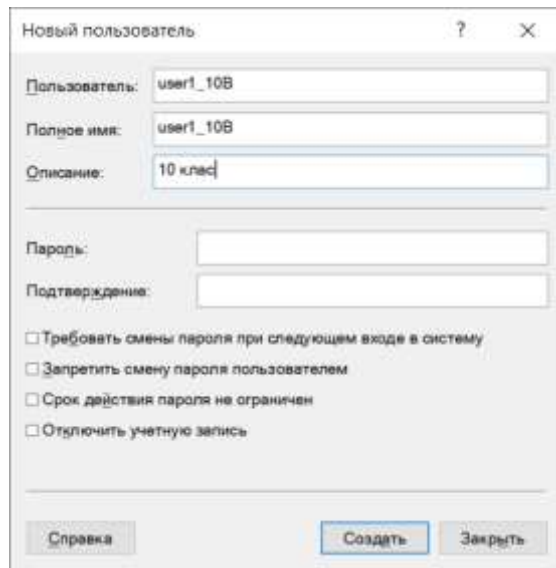
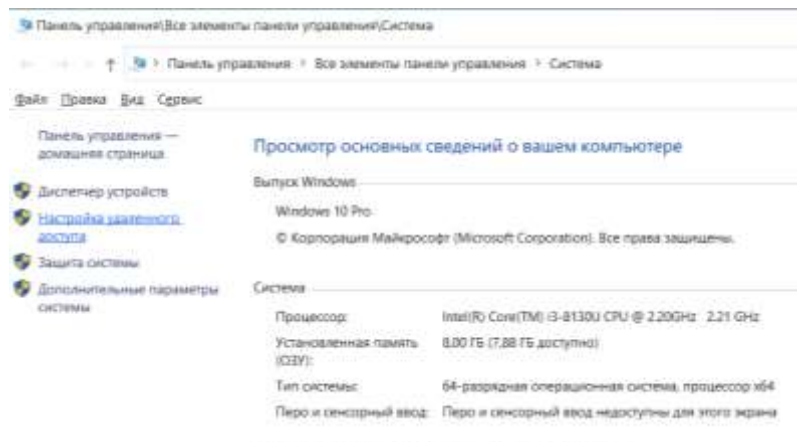
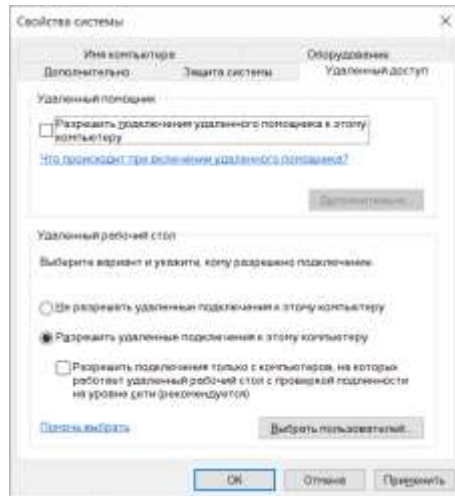


Рис. 2.34 Створення користувача

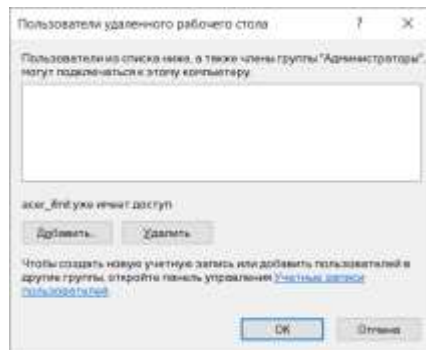
- в. Призначити необхідних користувача – користувачем віддаленого робочого столу (Програма «Мій комп'ютер» – права кнопка миші на пустому місці)



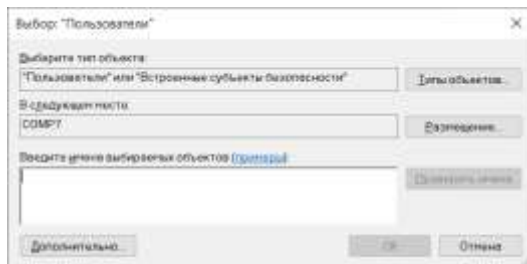
Обрати «Налаштування віддаленого доступу»



Вибрати «Вибрати користувачів»



Вибрати «Додати»



Вибрати «Додатково» та потім «Пошук»

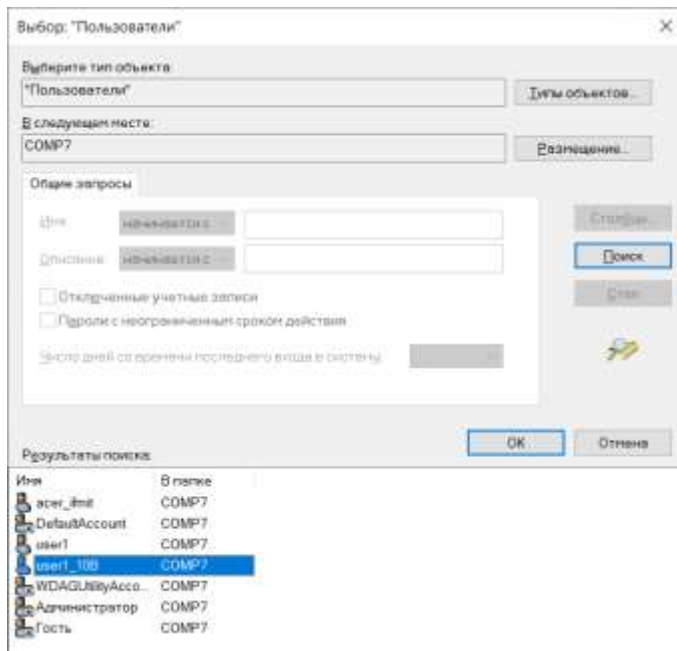


Рис. 2.35 Додавання користувача віддаленого

робочого столу

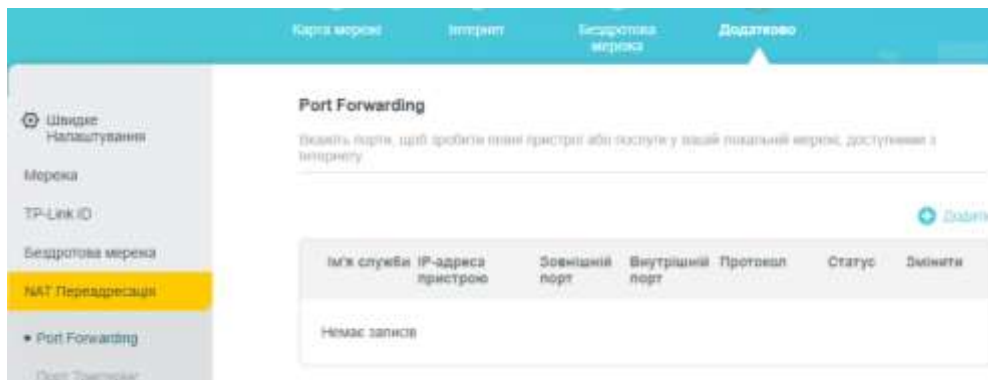
3. Обрати зовнішні порти та створити необхідні налаштування роутеру

а. Вибрати схему призначення зовнішніх портів. Наприклад:

- i. для комп'ютеру № 1 - $192.168.0.21 + 3389 = 3727$ приймаємо 3401,
- ii. для комп'ютеру № 2 – 3402,
- iii. Для комп'ютеру № 3 – 3403
- iv. і так далі

4. Створюємо необхідні відповідні записи на роутері.

а. Для більшості офісних роутерів це завдання вирішується приблизно однаково. Розглянемо для роутеру AX1500 Wi-Fi, переходимо на сторінку налаштувань (<http://192.168.0.1>) – «Додатково» – «NAT переадресація» – «Port Forwarding»



Обираємо «Додати» та заповнюємо відповідні поля згідно прийнятої схеми пере направлення портів

Додати запис Port Forwarding

Ім'я служби: ком 1
ПЕРЕВІРИТИ ЗАГАЛЬНІ ВНУТРІШНІ

IP-адреса пристрою: 192.168.0.21
ПЕРЕВІРИТИ ПІДКОНЕЧЕННЯ

Зовнішній порт: 3401

Внутрішній порт: 3389

Протокол: TCP

Увімкнути цей запис

ВІДМІНИТИ ЗБЕРЕЖИТИ

в результаті отримуємо

Port Forwarding

Вкажіть порти, які працюють на вашій пристрої або мережі у вашій локальній мережі, доступні з Інтернету

Ім'я служби	IP-адреса пристрою	Зовнішній порт	Внутрішній порт	Протокол	Статус	Змінити
ком 1	192.168.0.21	3401	3389	TCP	<input checked="" type="checkbox"/>	

Створюємо інші записи та додаємо всі наявні комп'ютери

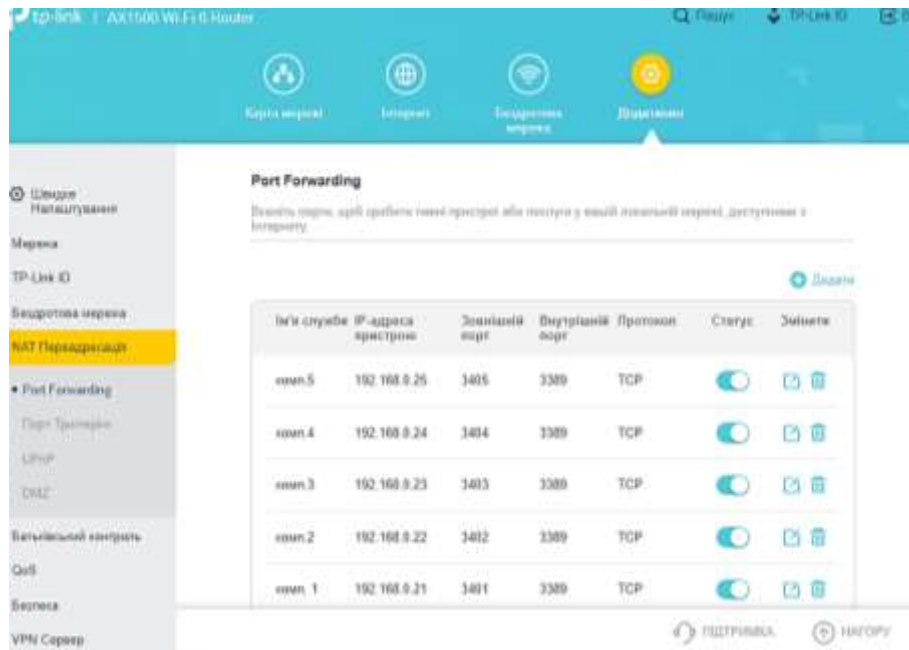


Рис. 2.36 Налаштування доступу до віддалених робочих столів у роутері AX1500 Wi-Fi

- б. Особливий випадок – роутер Mikrotik. Розглянемо той же випадок та послідовність дій у налаштуванні за допомогою програми winbox. При налаштуванні цього роутеру необхідно враховувати зовнішню адресу, наприклад 176.105.190.38.

Обираємо меню «IP» – «Firewall» (рис. 2.37)

Поле **In. Interface** – ether1 (ім'я зовнішнього інтерфейсу, до якого підключено Інтернет з'єднання (рис. 2.38)).

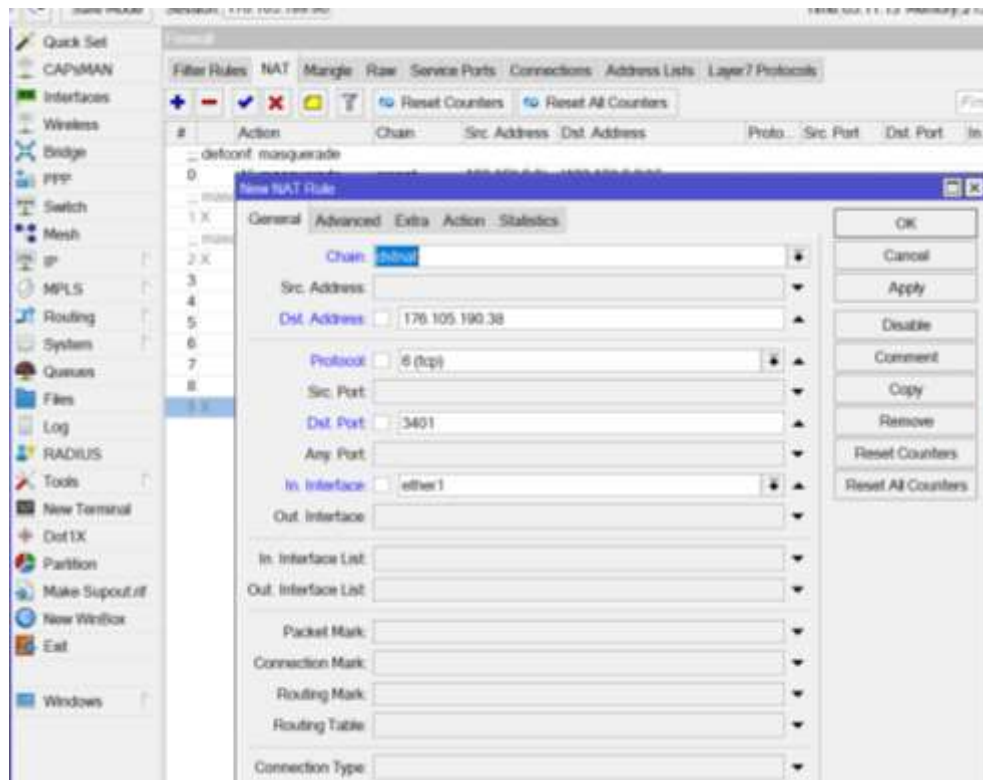


Рис. 2.38 Налаштування роутеру Mikrotik у програмі Winbox

Переходимо в закладку «Action» (рис.2.39)

Поле **Action** – Dst-nat.

Поле **To Addresses**– 192.168.0.21 – внутрішня адреса комп'ютеру № 1 (обов'язково).

Поле **To Port**– 3389 – внутрішня адреса ввіддаленого робочого столу комп'ютеру № 1(обов'язково).

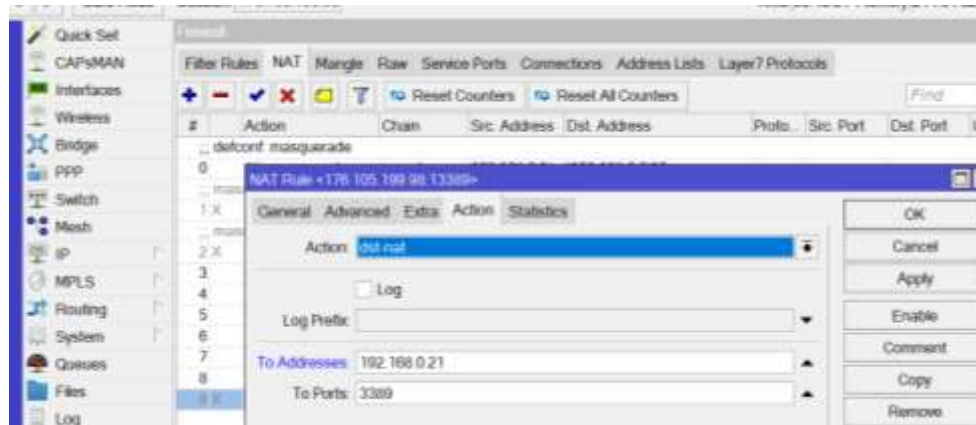


Рис. 2.39 Налаштування роутеру Mikrotik у програмі Winbox

Таким чином заповнюємо для всіх комп'ютерів з віддаленим робочим столом у НКЛ (рис. 2.40)

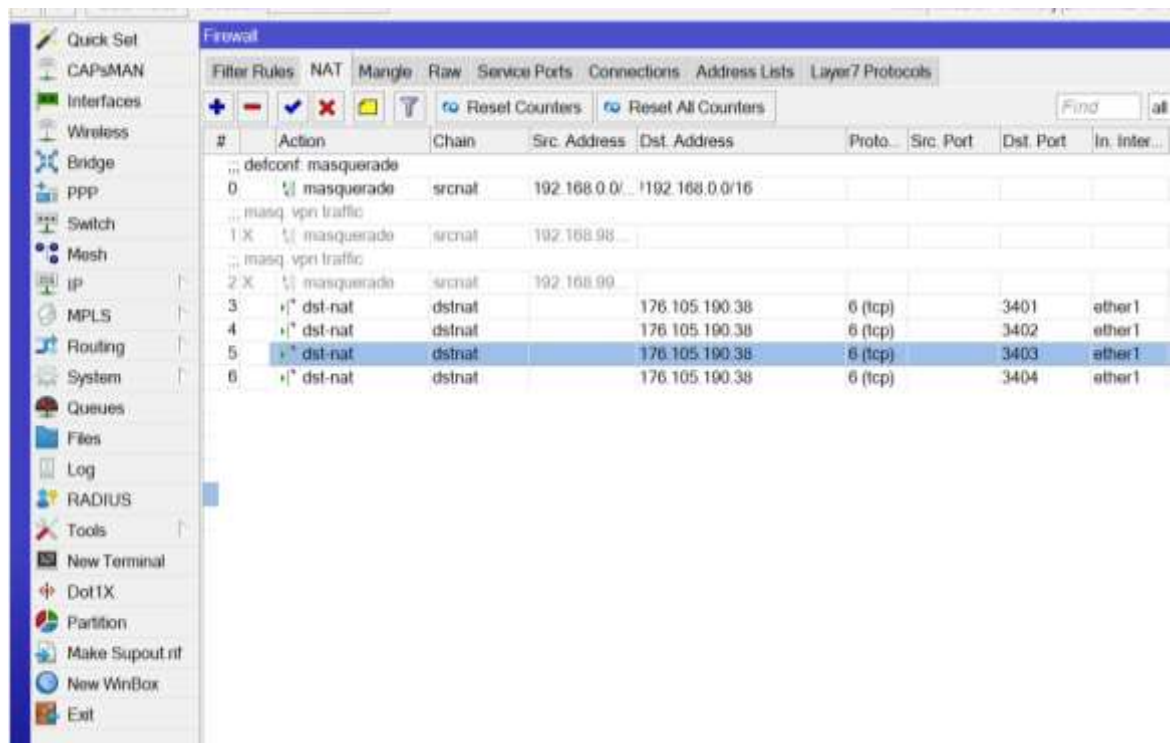


Рис. 2.40 Приклад створення доступу для комп'ютерів № 1-4

Варіант 4. Отримання повного доступу до всіх ресурсів НКЛ

Для отримання повного доступу до всіх мережевих ресурсів НКЛ найпростіше скористуватись VPN сервісом.

VPN буває декілька типів PPTP, L2TP, SSTP, OpenVPN та декілька типів тунелів. Це окреме питання, але в межах роботи розглянемо, як організувати найпростішу VPN типу PPTP. Ця VPN має безліч недоліків з питань безпеки, але її налаштування дуже швидке.

За рахунок використання цього сервісу вдається організувати доступ до всіх ресурсів НКЛ та досягти практично повної імітації присутності користувачів у НКЛ. Єдина різниця – здобувачі освіти не мають можливості використовувати консоль (клавіатура та миша) наявних комп'ютерів. Тому цей сервіс надає можливість використати саму мережу НКЛ (принтери, доступ до файлів та мережевих приладів) та надати доступ до всього програмного забезпечення, однак потребує переналаштування всіх комп'ютерів.

Отже, всіх перерахованих варіантів віддаленого підключення до НКЛ це найбільш ефективний.

Слід врахувати, що цей сервіс інтегровано у обжену кількість роутерів та їх вартість значно більша. Серед приладів-роутерів, які розглянуто в межах цієї роботи тільки два підтримують цю можливість:

- WI-FI роутер Tp_link TL-WR840N – не підтримує;
- WI-FI роутер Mercusys AC12g – не підтримує;
- **WI-FI роутер Tp_link AX1500 Wi-Fi 6 – підтримує;**
- **Роутер MikroTik RB750Gr3 – підтримує**

Безумовно, існують і інші засоби створення VPN, наприклад, на сервері Microsoft Windows. Для цього бажано мати сервер з двома мережевими платами та додатково інсталиювати роль «Сервер політики мережі» (NPAS).

Для створення VPN PPTP на роутері Tp_link AX1500 необхідно перейти на веб сторінку керування приладом та обрати меню «Додатково» – «VPN Сервер» – «PPTP» (рис. 2.41). Включити «PPTP», налаштувати параметри підключення та призначити діапазон IPадрес користувачів

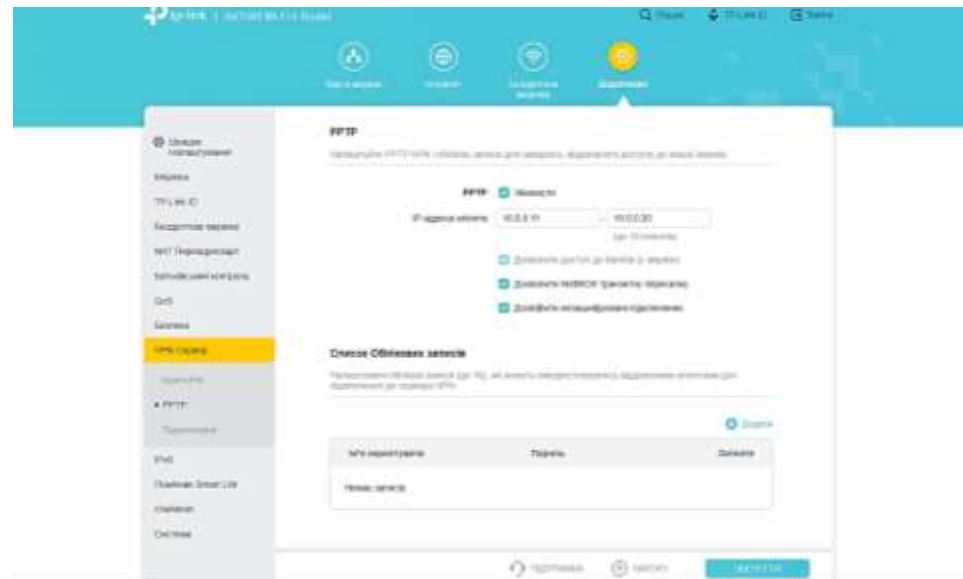


Рис. 2.41 Налаштування RADIUS на роутері Tr_link AX1500

Після цього необхідно створити користувачів. Для цього натиснути кнопку «+»Додати та вказати ім'я користувача та пароль (рис.2.42)

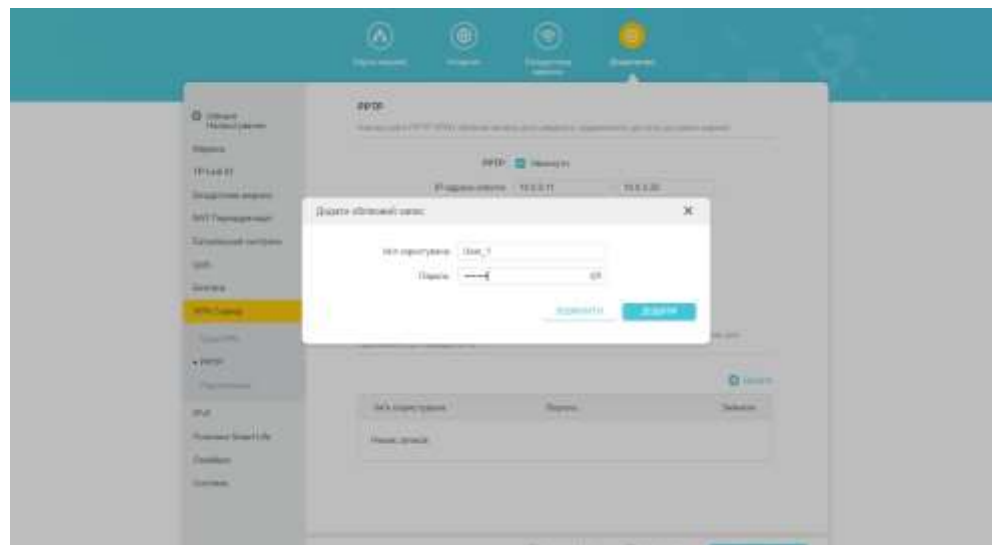


Рис. 2 .42 Додавання користувача VPN PPTP

Слід відзначити, що для цього роутеру є можливість створити до 16 користувачів, но одночасно можуть працювати тільки 10

Сервіс VPN PPTP є у системі роутеру MikroTik [17] та у випадку якщо роутер не приймав участі у багатьох налаштуваннях та переналаштування та ніколи не активізувався VPN практично все зробить система Mikrotik RouterOS. Особливістю цього роутеру є те що кількість користувачів обмежена тільки продуктивністю роутеру.

Для початкового налаштування правил FireWale натисніть кнопку «Quick Set» в правому верхньому куті (рис.2.43), увімкніть «VPN Access» введіть пароль та натисніть кнопку «Apply Configuration», а потім «WebFig» – у правому верхньому куті.

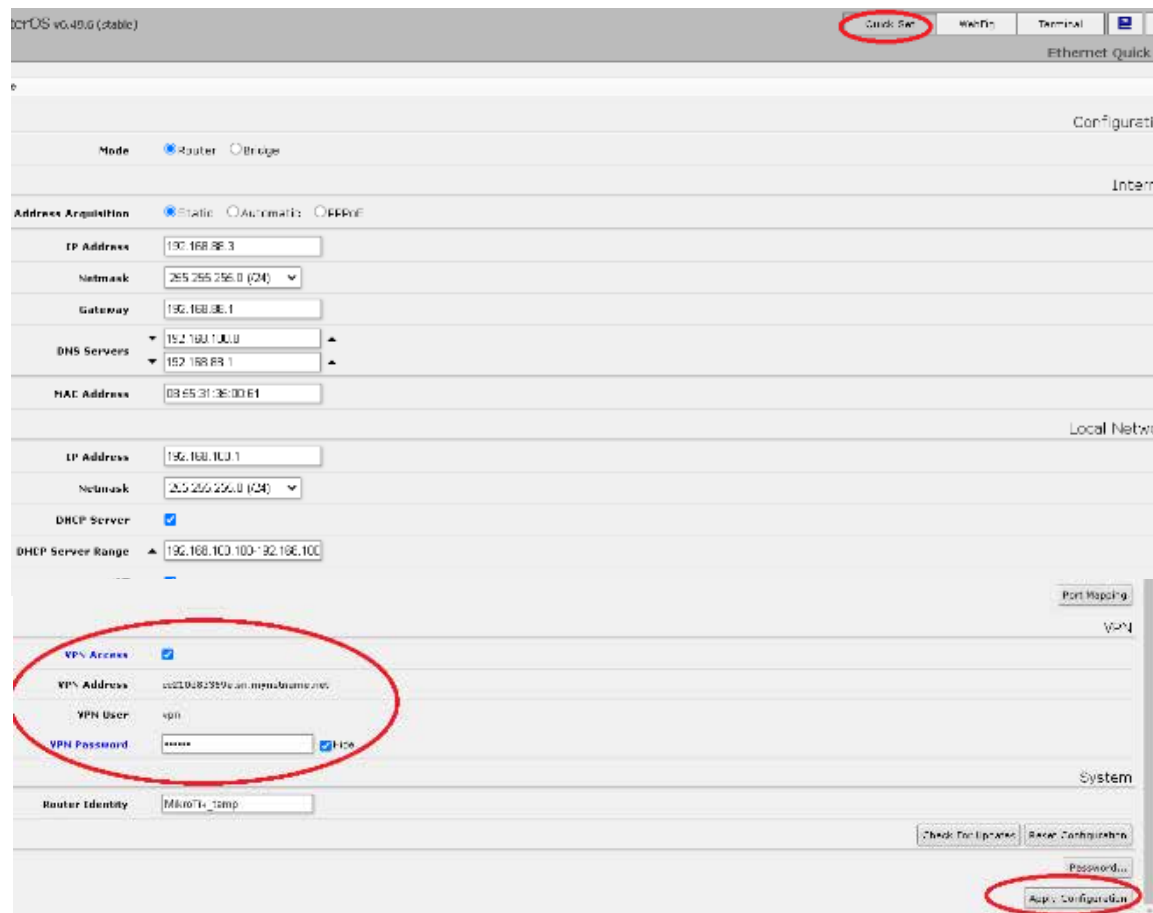


Рис. 2.43. Перехід до початкових налаштувань VPN

У меню «IP» – «FireWall», закладка «Filter Rules» повинно додатися декілька правил із загальною кількістю – не менш 17. А у меню «IP» – «FireWall», закладка «Nat» – на одно правило більше. Переходимо у меню «PPP» закладка

«PPTP Server» та перевіряємо параметр «Enable» – повинен бути включений (рис.2.44), звертаємо увагу на поле «Default Profile» – “default encryption”, тиснемо «ОК».

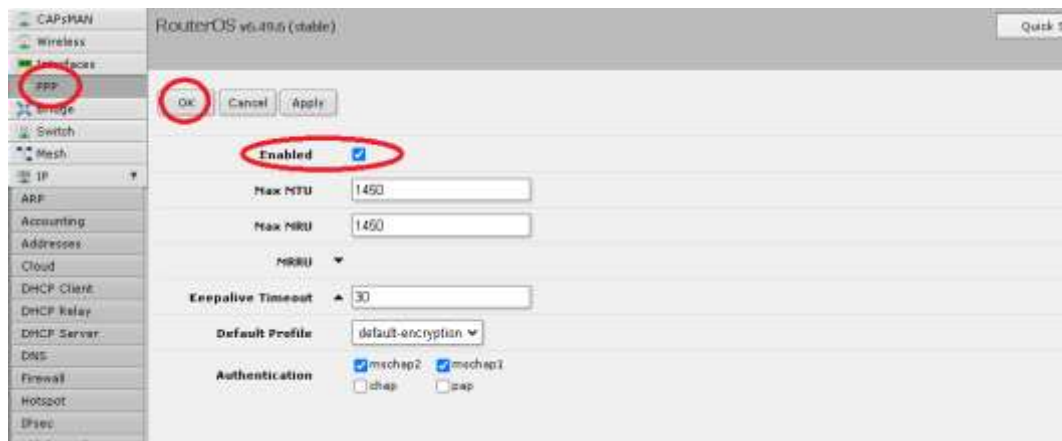
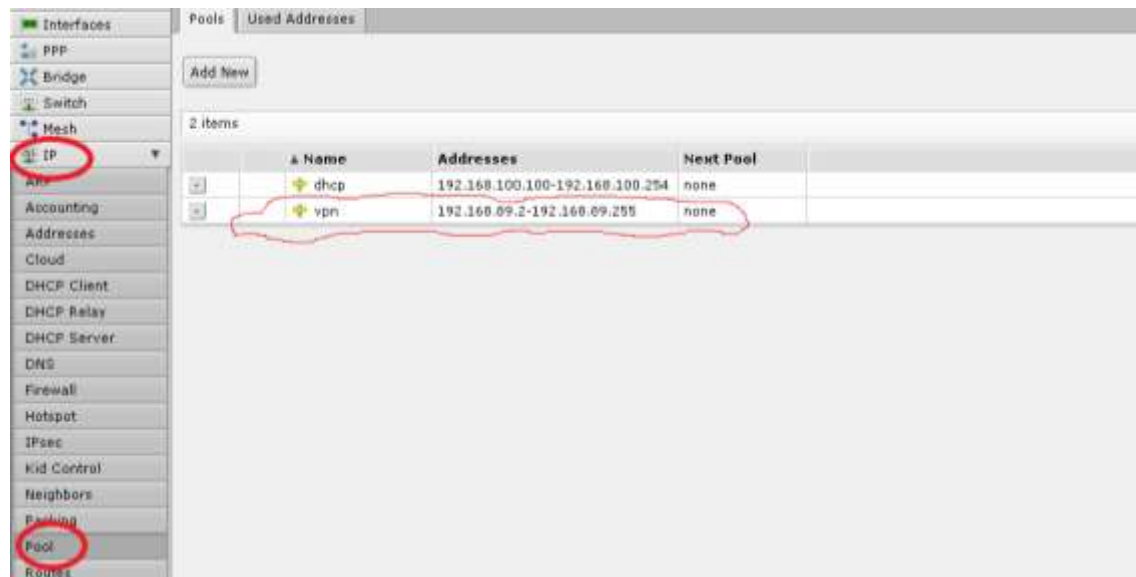


Рис. 2.44. Включити VPN Server

Потім, у цьому меню переходимо до «L2TP», «SSTP» та «OVPN Server» та їх статус «Enable» тимчасово відключаємо . Перевіряємо меню «IP» – «Pool», «IP» – «Routes» та «PPP» – закладка «Profiles» (рис. 2.45). Система Mikrotik RouterOS створить пул адрес 192.168.89.2 – 192.168.89.255. Важливо врахувати, що пул адрес з назвою VPN, не включає адресу «Profiles» “default-encryption” – 192.168.89.1.



а



б

Рис. 2.45. Перевірка налаштувань

Для остаточного налаштування переходимо у «PPP»– «Secrets» та за аналогією з користувачем VPN створюємо інших користувачів, а користувача VPN змінюємо ім'я з міркувань безпеки, а бо зовсім необхідно видалити (рис. 2.46).

Будьте уважні, з'ясовано, що ім'я користувачів слід використовувати з урахуванням регістру.



Рис. 2.46. Створення користувачів VPN у меню
«PPP»– «Secrets»

Це ще не остаточне налаштування, але все повинно працювати. На цьому попереднє налаштування буде завершено. Поступово створюємо інших користувачів (рис. 2.47)

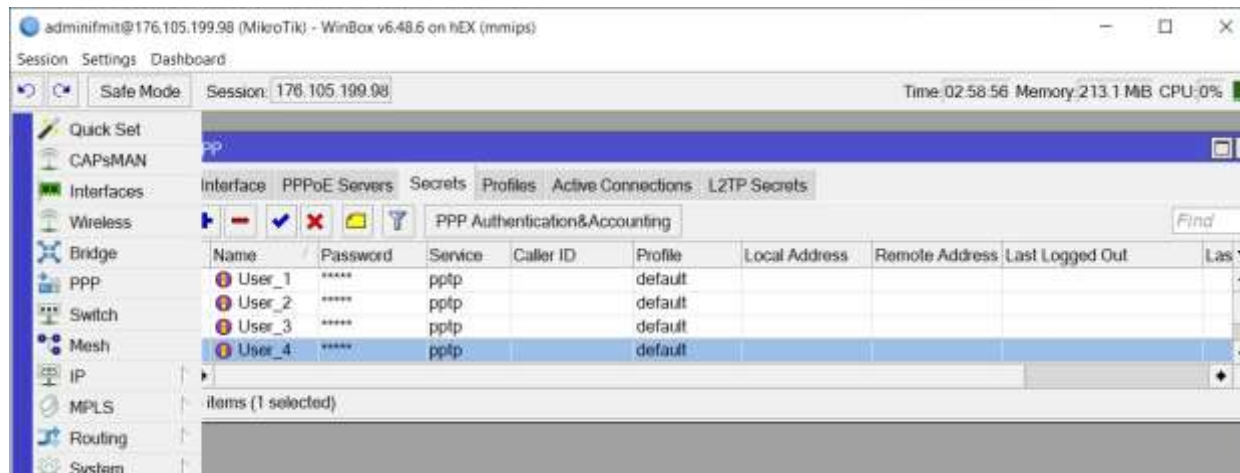


Рис. 2.47 Користувачі PPTP у роутері Mikrotik

Всі створені користувачі у меню «PPP» – «Secrets» будуть в змозі використовувати VPN клієнта на своїх персональних комп’ютерах після відповідного їх налаштування у додатку «Параметри» – «Мережа та Інтернет» – VPN – «+ Додати VPN підключення» (рис. 2.48, а) з параметрами, що вказані на рис. 2.48, б.



а

Добавить VPN-подключение

Поставщик услуг VPN
Windows (встроенный)

Имя подключения
Комп. название лаборатории

Имя или адрес сервера
91.222.42.140

Тип VPN
Протокол PPTP

Тип данных для входа
Имя пользователя и пароль

Имя пользователя (необязательно)
User_1

Пароль (необязательно)

Сохранить Отмена

б

Рис. 2.48. Налаштування користувача

У процесі впровадження цього рішення з'ясувалось ще одна особливість. При використанні VPN з'єднання у даному випадку шлюз за замовчанням буде налаштовано на адресу VPN – 192.168.89.1. Таким чином, в незалежності використаються зараз користувачем ресурси НКЛі або ні – увесь трафік Інтернет буде спрямовано на ваш канал та запити на інші ресурси Інтернет будуть проходити через ваше з'єднання. З'ясувалось, що вирішити цей недолік можливого за рахунок використання спеціального додаткового пакету СМАК – пакет адміністратору.

Додатки

Додаток А Перелік команд загального налаштування роутеру MikroTik

```
# створення bridge
/interface bridge
add admin-mac=DC:2C:6E:5D:1D:50 arp=proxy-arp auto-mac=no comment=defconf \
  name=bridge

# призначення IP адрес для локальної мережі (192.168.100.0/24)
/ip address
add address=192.168.100.1/24 interface=bridge network=\
  192.168.100.0

# додаткове налаштування інтерфейсів
/interface ethernet
set [ find default-name=ether1 ] arp=proxy-arp
set [ find default-name=ether2 ] arp=proxy-arp
set [ find default-name=ether3 ] arp=proxy-arp
set [ find default-name=ether4 ] arp=proxy-arp
set [ find default-name=ether5 ] arp=proxy-arp
# необов'язкове створення переліку інтерфейсів: LAN - локальний та WAN - до
# Інтернет
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
# призначення членів до переліків інтерфейсів до WAN - один до LAN bridge
/interface list member
add interface=bridge list=LAN
add interface=ether1 list=WAN
# створення пулів адрес для зручності конфігурування
/ip pool
add name=dhcp ranges=192.168.100.100-192.168.100.254
```

```
add name=vpn ranges=192.168.98.2-192.168.98.254
```

```
# налаштування двох DHCP серверів
```

```
/ip dhcp-server
```

```
add address-pool=dhcp disabled=no interface=bridge lease-time=24m name=dhcp
```

```
# налаштування мережі DHCP серверу
```

```
/ip dhcp-server network
```

```
add address=192.168.100.0/24 dns-server=\  
192.168.100.8,176.105.220.22,209.244.0.3 gateway=192.168.100.1
```

Додаток Б Перелік команд налаштування роутеру MikroTik для налаштування Firewall

```
# " дозволити masquerade"
/ip firewall nat add chain=srcnat out-interface-list=WAN \
ipsec-policy=out,none action=masquerade

# налаштування фільтрів
/ip firewall
# далі йде набір фільтрів, які мінімально необхідні
# " приймати established,related,untracked"
filter add chain=input action=accept \
    connection-state=established,related,untracked
# " блокувати invalid"
filter add chain=input action=drop connection-state=invalid

# " приймати ICMP"
filter add chain=input action=accept protocol=icmp

# " приймати to local loopback (for CAPsMAN)"
filter add chain=input action=accept dst-address=127.0.0.1

# " блокувати all not coming from LAN"
filter add chain=input action=drop in-interface-list=!LAN
# " приймати in ipsec policy"
filter add chain=forward action=accept ipsec-policy=in,ipsec
# " приймати out ipsec policy"
filter add chain=forward action=accept ipsec-policy=out,ipsec
# використовувати fasttrack"
filter add chain=forward action=fasttrack-connection \
connection-state=established,related
# " приймати established,related, untracke>
filter add chain=forward action=accept connection-state=established,related,untracked
# " блокувати invalid"
filter add chain=forward action=drop connection-state=invalid
# " блокувати all from крім dstnat
filter add chain=forward action=drop \
```



```
connection-state=new connection-nat-state=!dstnat in-interface-list=WAN
```

```
# блокувати непотрібні сервіси
```

```
/ip service
```

```
set telnet disabled=yes
```

```
set ftp disabled=yes
```

```
set www disabled=yes
```

```
set ssh disabled=yes
```

Додаток В Перелік команд налаштування роутеру MikroTik для налаштування PPTP

```
# дозволити masquerade всіх мереж але блокувати їх з'єднання з WAN
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" \
dst-address=!192.168.0.0/16 ipsec-policy=out,none out-interface-list=WAN \
src-address=192.168.0.0/16
# дозволити використовувати порт 1723
/ip firewall filter
add action=accept chain=input comment="allow pptp" dst-port=1723 \
in-interface-list=WAN protocol=tcp
```