Лекція

з дисципліни: «Клієнт-серверне програмування»

на тему: «*Networks. IP-Addressing. IP-Networks*»

ПЛАН ЛЕКЦІЇ

1. Ком’ютерні мережі.
2. Мережева модель та рівні взаємодії.
3. IP-адресація.
4. IP-мережі.

1. Ком’ютерні мережі.

Комп’ютерна мережа - це сукупність комп’ютерів, оснащених спеціальним комунікаційним обладнанням і програмним забезпеченням, а також периферійних пристроїв, які з’єднані між собою каналами зв’язку.

Комп’ютерна мережа забезпечує :

- колективну роботу над даними і обмін даними між користувачами мережі;
- спільне використання програмного забезпечення;
- спільне використання периферійних пристроїв.

Комп’ютерні мережі умовно поділяються за територіальним принципом, типом, призначенням, типом комп’ютерів у мережі, розташуванням комп’ютерів.

За територіальним принципом мережі поділяються на:

- локальні мережі створюються, як правило, в межах однієї організації чи одного приміщення.
- регіональні мережі об’єднують користувачів міста, області чи невеликих країн.
- глобальні комп’ютерні мережі об’єднують користувачів, що розташовані в усьому світі і, як правило, складаються з декількох тисяч окремих регіональних мереж, які з’єднані між собою.

Мережі «клієнт-сервер» - це мережі, у якій мережні ресурси сконцентровані на одному комп’ютері, що називається виділеним. Виділеним називається сервер, інші комп’ютери оголошуються робочими станціями.

Робоча станція може й надалі виконувати функції автономного комп’ютера.

Сервер виконує управління мережею, підтримує її працездатність, зберігає загальну інформацію і поновлює її, швидко опрацьовує запити

клієнтів, керує захистом файлів і каталогів, виконує резервне копіювання даних і т.д.

У телекомунікаціях протокол зв'язку — це система цифрових правил для обміну даними всередині або між комп'ютерами.

Всі сучасні пристрої обмінюються між собою даними через мережі. Щоб один пристрій міг передати інформацію іншому пристрою, вони повинні діяти спільно. Два пристрої зобов'язані якимось чином розуміти, як встановлювати між собою сесію, які параметри передачі даних використовувати, як визначати і що робити у разі помилок, як завершувати передачу і т.д. Іншими словами, потрібен певний алгоритм, певний набір правил. Цей набір правил і називається протокол.

Мережеві протоколи визначають загальний формат і набір правил для обміну повідомленнями між пристроями. Прикладом використання набору протоколів в мережевому зв'язку є взаємодія між веб-сервером і веб-клієнтом. Ця взаємодія використовує ряд протоколів і стандартів у процесі обміну інформацією між ними. Різні протоколи взаємодіють один з одним, щоб гарантувати, що повідомлення будуть прийняті і зрозумілі обома сторонами.

Прикладами протоколів є наступні.

Протокол прикладного рівня – протокол передачі гіпертексту (HTTP, HyperText Transfer Protocol): визначає, яким чином взаємодіють веб-сервер і веб-клієнт. HTTP визначає зміст і формат запитів і відповідей, якими обмінюються клієнт і сервер. Для управління процесом передачі повідомлень між клієнтом і сервером HTTP звертається до інших протоколів.

Транспортний протокол – протокол управління передачею (TCP, Transmission Control Protocol): управляє окремими сеансами зв'язку між серверами і клієнтами в Інтернеті. TCP ділить повідомлення HTTP на дрібніші частини – сегменти. Ці сегменти передаються між веб-сервером і клієнтськими процесами, запущеними на вузлі призначення. TCP також відповідає за управління розміром і швидкістю, з якою відбувається обмін повідомленнями між сервером і клієнтом.

Інтернет-протокол – протокол IP: відповідає за прийом форматованих сегментів від TCP, інкапсуляцію їх в пакети, привласнення їм відповідних адрес і їх доставку по найкращому шляху до вузла призначення.

Протоколи мережевого доступу описують дві основні функції – зв'язок по каналу передачі даних і фізична передача даних по мережевому середовищу. Протоколи управління каналами передачі даних приймають пакети від протоколу IP і форматують їх для передачі в середовищі. Стандарти і протоколи фізичної передачі даних управляють тим, як сигнали посилаються і як вони інтерпретуються клієнтами при отриманні. Одним з прикладів протоколу мережевого доступу є Ethernet.

Протоколи IP, HTTP і DHCP (Dynamic Host Configuration Protocol) є частиною набору протоколів Інтернет, який називається протоколом управління передачею/протоколом IP (TCP/IP). Сімейство протоколів TCP/IP є відкритим стандартом, тобто ці протоколи знаходяться у вільному доступі

для користувачів, і будь-який постачальник може впроваджувати ці протоколи на апаратних засобах або в ПЗ.

2. *Мережева модель та рівні взаємодії.*

У далекому 1969 році в США підрозділ Міністерства оборони, який називався DARPA, розробила прототип сучасного інтернету – мережу під назвою Arpanet. Спочатку це були об'єднані чотири обчислювальні модулі, потім ще 11. Мережа поступово росла і розвивалася, включаючи вже термінали у Великій Британії, а також Норвегії. Так, якщо 1977 року Arpanet складалася з усього трохи більше сотні хостів, то вже 1983 року це число зросло до 4 тисяч. Починаючи з 1983 року, вона стала першою у світі мережею, в якій була реалізована маршрутизація пакетів даних. Протоколом маршрутизації для роботи цієї мережі став протокол IP – один із найважливіших протоколів передачі даних в Інтернеті сьогодні.

Оскільки варіантів комп'ютерних мереж може бути нескінченне число, щоб уникнути плутанини були розроблені мережеві моделі, основною з яких стала OSI (The Open Systems Interconnection model). Вона визначала основні правила та вимоги до мережевих протоколів. Більшість алгоритмів зв'язку, що застосовуються сьогодні, ґрунтуються на стандарті OSI, що визначає рівні взаємодії систем.

Модель передбачає сім варіантів таких взаємодій:

- Прикладний рівень
- Сеансовий рівень
- Рівень представлення
- Транспортний рівень
- Мережевий рівень
- Канальний рівень
- Фізичний рівень

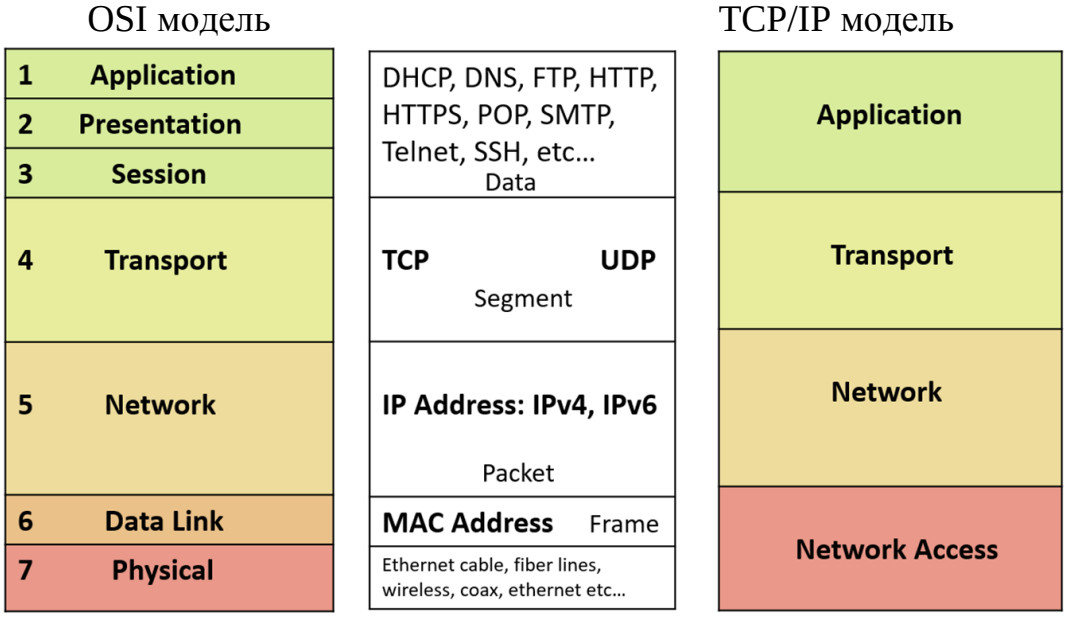


Рис. 1 Структура мережевих моделей

Група протоколів за певними рівнями називається стеком протоколів. Сучасний Інтернет побудований на стеку протоколів TCP/IP. Як очевидно з назви стека TCP/IP – він складається із двох частин, протоколу TCP і протоколу IP. Забігаючи наперед — IP-протокол вирішує питання з адресацією, тоді як TCP – реалізує трансфер даних і стежить, щоб клієнт точно отримав свої байти. Цей стек використовує чотири рівні з перерахованих вище:

- Прикладний рівень
- Транспортний рівень
- Мережевий рівень
- Канальний рівень

Прикладний рівень у TCP/IP

Прикладний рівень відповідає за працездатність усіляких мережевих додатків. Такі програми можуть використовувати свої персональні протоколи обміну даними. За ознаками взаємодії прикладних процесів виділяють два типи прикладного програмного забезпечення: програма-клієнт та програма-сервер. Протоколи прикладного рівня зорієнтовано на конкретні прикладні завдання. Це можуть бути браузери, що функціонують через HTTP, клієнти для завантаження по FTP, програми для роботи з електронною поштою SMTP, SSH (надійна комунікація з хостом), DNS (співвідношення IP-адрес і символьних імен) та ін.

Як відбувається передача інформації

Трансфер пакетів від одного мережного вузла іншому забезпечує протокол IP – протокол мережного рівня. Щоб дані перейшли від хоста-відправника до хоста-отримувача, необхідно повідомити IP-адресу одержувача та відправника, а також вказати номер порту. Поєднання IP-адреси та номера порту за яким здійснюється передача даних називають сокетом. Для спрощення стандартів прийнято використовувати певні порти в залежності від функціонального призначення програми. Приміром, поштовий SMTP-сервер слухає 25 порт, POP3-сервер налаштований на 110 порт тощо. Більшість додатків на ПК є клієнтами та номери портів для них виділяються динамічно операційною системою. Серверні порти мають номер до 1024, клієнтські порти йдуть із більш великим значенням. Скажімо, сокет при зверненні до сервера порт HTTP може бути представлений як: 194.106.118.30:80. Відповідь у цьому випадку надходитиме на сокет виду aaa.bbb.ccc.ddd:xxxxx.

Щоб мати можливість звертатися до того чи іншого мережного інтерфейсу, протоколом застосовуються IP-адреси, що відповідають одній із двох версій протоколу: IPv4 та IPv6. Для версії IPv4 використовуються 32-бітові адреси по 4 октети (вісім позицій під нуль або одиницю). Завдяки IP-адресам, що закріплені за пакетами даних, мережа визначає, з якого вузла той чи інший пакет надійшов і до якого хосту його слід відправити. Застосовувати довгі адресні записи з тридцяти двох нулів та одиниць не дуже зручно, тому IP-адресу вирішили вказувати у десятковій системі. Оскільки адресний простір протоколу IPv4 обмежено 4 294 967 296 адресами, було

розроблено оновлений варіант протоколу – IPv6, у якому використовується довжина адреси 128 біт.

Для зручності адресації замість числових значень використовується символьно-цифрове ім’я хоста. Щоб перетворити IP-адресу на доменне ім’я застосовується сервіс доменних імен DNS (Domain Name Server). DNS моніторить 53-й порт UDP (рідше – TCP).

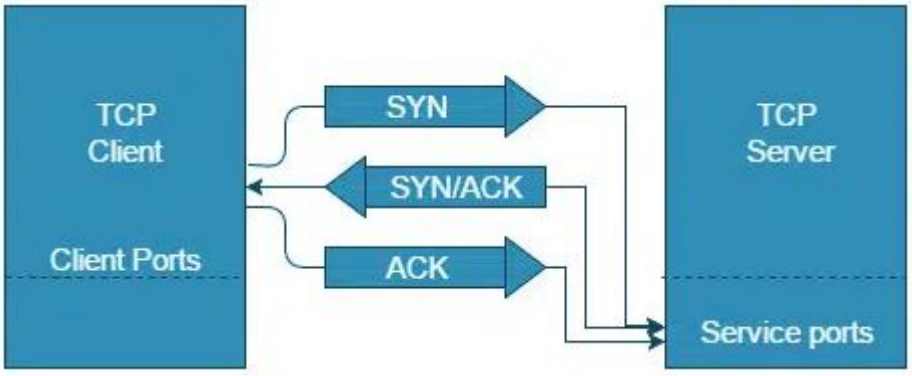
Глобальна мережа складається з багатьох з’єднаних локальних мереж. Ця особливість вплинула на запис IP-адреси: вона включає як дані про адресу мережі, так і інформацію про адресу хоста в цій мережі. Щоб можна було визначити, де закінчується адреса мережі та починається адреса комп’ютера в цій мережі, вигадали маску підмережі. Це свого роду інструкція, яка говорить про те, як слід читати IP-адресу, де межа між адресою мережі та адресою хоста.

Работа транспортного рівня у TCP/IP

Центральним протоколом транспортного рівня TCP/IP є TCP (Transmission Control Protocol), крім нього ще використовуються два допоміжні протоколи – UDP (User Datagram Protocol) і SCTP. На відміну від UDP, в якому передача датаграм відбувається без встановлення з’єднання, механізм передачі даних через TCP гарантує точне пересилання даних. З цієї причини, на практиці частіше використовується TCP – він перевіряє передані пакети з даними та при виявленні помилок, перезапитує пакети знову. Крім того, протокол TCP стежить за правильною послідовністю переданих пакетів. Передача даних за допомогою TCP починається з так званого “рукостискання” – процедури встановлення з’єднання, яке виконується за три кроки.

Клієнт надсилає одержувачу фрагмент даних з номером послідовності та прапором SYN. Сервер виділяє пам’ять для обробки завдання та повертає відправнику фрагмент з номером послідовності та прапорами SYN та ACK, після чого перемикається в режим SYN-RECEIVED. У разі збою в роботі сервер сигналізує клієнту про проблему, посилаючи сегмент із прапором RST (отримавши відмову, хост-відправник припиняє спроби встановити з’єднання). Отримавши прапор SYN, клієнт передає сегмент із прапором

ACK, і якщо цей прапор вузол вже отримав, включається режим ESTABLISHED. Якщо за десять секунд сервер не відповідає, клієнт повторює свій запит. Коли сервер із режимом SYN-RECEIVED отримує пакет із прапором ACK, він включає режим ESTABLISHED. Не дочекавшись відповіді, після деякого часу він вимикає сокет, включаючи режим CLOSED.



Завершується сесія між двома хостами за три кроки:

- Клієнт шле хосту прапор FIN
- Вузол повертає прапори відповіді ACK, FIN, що свідчить про закінчення зв’язку.
- Клієнт зупиняє з’єднання, після чого надсилає хосту сигнал про завершення сесії у вигляді прапора ACK.

Сфера застосування UDP обмежується програмами з потоковими даними – IPTV, Voice over IP, онлайн-іграх і т.д.

Міжмережевий рівень

Протоколи мережевого рівня TCP/IP забезпечують взаємодію мереж різної архітектури тощо. Основним протоколом мережного рівня технології TCP/IP є міжмережевий протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів тощо.

Головне завдання міжмережевого протоколу IP — це маршрутизація пакетів даних між різнотипними комп'ютерними мережами. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує, за необхідності, фрагментацію та дефрагментацію цих пакетів.

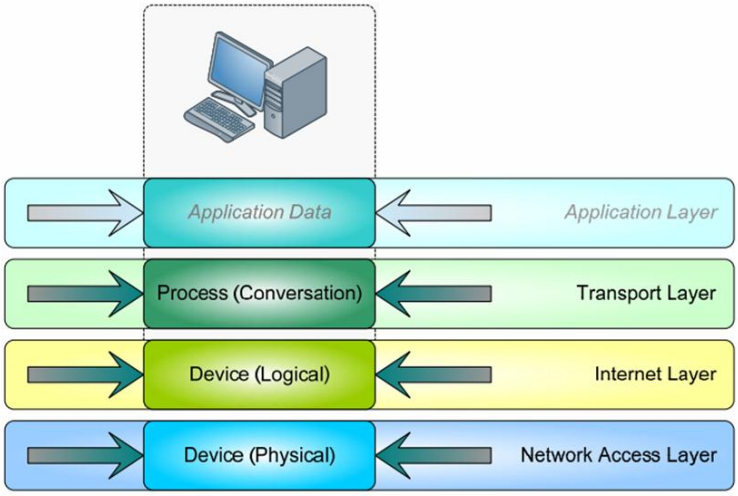
Рівень доступу до середовища передачі (Network Access Layer)

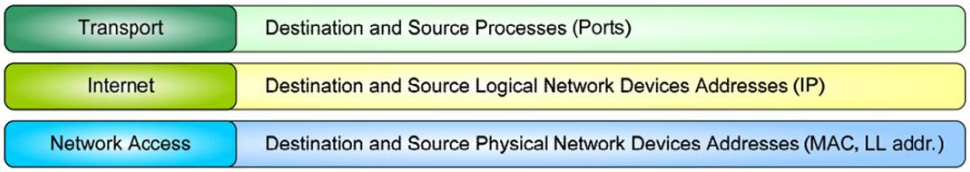
Функції:

відображення IP-адреси в фізичні адреси мережі (MAC-адреси);

інкапсуляція IP-дейтаграм в кадри для передачі по фізичному каналу і передачі кадрів.

На цьому рівні працює протокол ARP, який здійснює відображення адреси IP > MAC.





Адреса керування доступом до пристрою (MAC-адреса) — це унікальний ідентифікатор, призначений контролеру мережевого інтерфейсу (NIC) для зв’язку на канальному рівні сегмента мережі.

MAC-адреси використовуються як мережеві адреси для більшості мережевих технологій IEEE 802, включаючи Ethernet, Wi-Fi і Bluetooth.

Порт — це спеціальна програмна конструкція програмного забезпечення або конкретного процесу, яка служить кінцевою точкою зв’язку, що використовується протоколами транспортного рівня набору Інтернет-протоколів, такими як TCP і UDP.

Порт — це уявне місце, куди можуть надходити вхідні пакети інформації.

Для кожного з протоколів TCP і UDP стандарт визначає можливість одночасного виділення на хості до 65536 унікальних портів, ідентифікуються номерами від 0 до 65535. При передачі по мережі номер порту в заголовку пакета використовується (разом з IP-адресою хоста) для адресації конкретного додатка (і конкретного, належного йому, мережевого з'єднання).

У звичайній клієнт-серверної моделі додаток або чекає вхідні дані (або запиту на з'єднання; «слухає порт»; роль сервера), або посилає дані (або запит на з'єднання) на відомий порт, відкритий додатком-сервером (роль клієнта).

Типово додатком видається порт з довільним (наприклад, найближчим вільним, великим 1023) номером. При необхідності додаток може запитати конкретний (зумовлений) номер порту. Так, веб-сервери зазвичай відкривають для очікування з'єднання визначений 80 порт протоколу TCP.

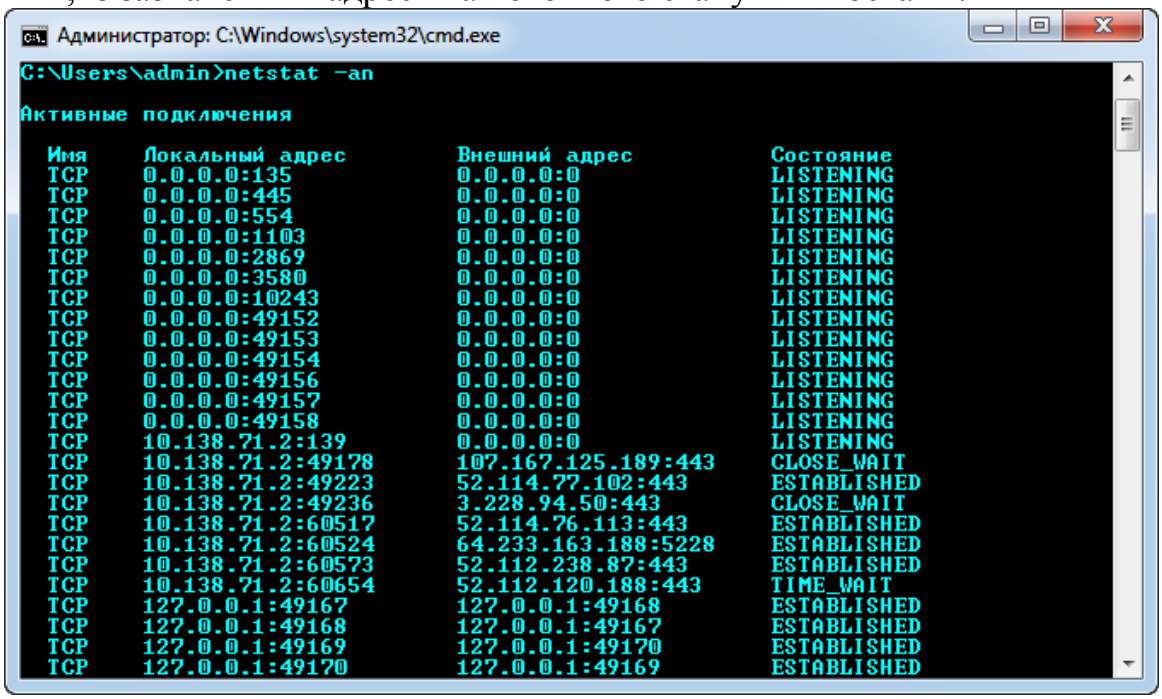
Порти TCP не перетинаються з портами UDP. Тобто, порт 1234 протоколу TCP не заважатиме обміну за UDP через порт 1234.

Ряд номерів портів стандартизований.

Port number	Protocol
20	FTP [data transfer]
21	FTP [Control command]
22	SSH
23	Telnet
53	DNS
80	HTTP
443	HTTPS

Для контролю мережевих з'єднань можна використовувати набір команд, введених у терміналі. Наприклад, за допомогою команди iptrace (UNIX) виконується трасування (аналіз, відстеження) пакетів на рівні мережного інтерфейсу. Виклик даних про трасування даних у шістнадцятковому та текстовому форматах здійснюється за допомогою команди ipreport, а команда trpt виконає трасування пакетів TCP на транспортному рівні, показавши їх порядок прямування, час і стан з'єднання TCP.

Щоб переглянути на комп'ютері під керуванням Windows всі встановлені з'єднання, необхідно відкрити термінал (cmd) та ввести команду netstat -an. У вікні командного рядка буде виведено список TCP та UDP коннектів, із зазначенням адреси та поточного стану між хостами.



3. *IP-адресація.*

IP-адреса є ієрархічною адресою, яка складається з двох частин: мережевої і вузлової. У 32-бітовому потоці одна частина бітів складає мережу, а інша – вузол. Біти в мережевій частині адреси мають бути

однаковими для усіх пристроїв, які знаходяться в одній і тій же мережі. Біти у вузловій частині адреси мають бути унікальними, щоб можна було визначити конкретний вузол в мережі. Незалежно від того, чи співпадають десяткові числа в двох IPv4-адресах, якщо два вузли мають одну бітову комбінацію в певній мережевій частині 32-бітового потоку, то ці два вузли знаходяться в одній і тій же мережі.

Format	IPv4 Address presentation	Size
Binary	11000000101010000001100101100100	32 bits
Binary	11000000 . 10101000 . 00011001 . 01100100	4x8 bits
Decimal Dotted	192 . 168 . 25 . 100	4x8 bits

Рис. 2 Структура IP-адреси

У діапазоні адрес кожної мережі IPv4 існують три типи адрес:

- вузлові адреси;
- мережева адреса;
- широкомовна адреса.

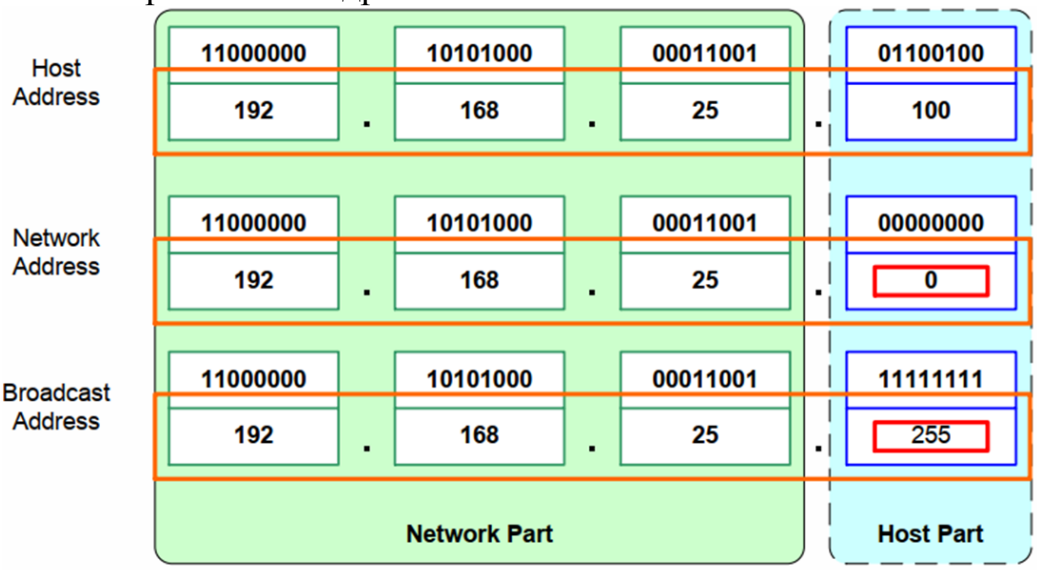


Рис. 3 Типи IP-адрес

Host Address - однозначно ідентифікує один мережевий пристрій (192.168.25.[1-254])

Network Address - Визначає всі підмережі. Усі біти вузла дорівнюють нулю. Використовується для маршрутизації (192.168.25.0)

Broadcast Address - Специфікує усі пристрої в під мережі. Використовується для трансляції на всі пристрої в одній мережі (192.168.25.255)

У IPv4-мережі вузли можуть взаємодіяти одним з трьох наступних способів.

Одноадресна розсилка (Unicast) - процес відправки пакету з одного вузла на індивідуальний.

Широкомовна розсилка (Broadcast) - процес відправки пакету з одного вузла на усі вузли в мережі.

Багатоадресна розсилка (Multicast) - процес відправки пакету з одного вузла вибраній групі вузлів, можливо, в різних мережах.

Ці три типи зв'язку використовуються в мережах передачі даних для різних цілей. У усіх трьох типах IPv4 адреса початкового вузла розміщена в заголовку пакету в якості адреси джерела.

Одноадресна передача використовується для звичайного обміну даними між вузлами як в мережі типу «клієнт/сервер», так і в одноранговій мережі. Для одноадресної розсилки пакетів в якості адреси призначення використовуються адреси цільового пристрою. Пакети можуть бути спрямовані через об'єднану мережу.

Трафік широкомовної розсилки використовується для відправки пакетів по усіх вузлах в мережі за допомогою групової адреси мережі. У пакеті широкомовної розсилки міститься IP-адреса призначення, у вузловій частині якої присутні тільки одиниці (1). Це означає, що пакети отримають і оброблять усі вузли в локальній мережі (домені широкомовної розсилки). Широкомовні розсилки передбачені в багатьох мережевих протоколах, наприклад в протоколі DHCP. Коли вузол отримує пакет, відправлений на мережеву широкомовну адресу, вузол обробляє цей пакет так само, як обробляє пакет, відправлений по одноадресній розсилці.

Використання широкомовної розсилки включає:

- проведення маршруту від адрес верхнього рівня до адрес нижнього рівня;
- запит адреси;
- на відміну від одноадресної розсилки, у разі якої пакети можуть бути відправлені по об'єднаній мережі, широкомовним пакетам заборонено проходити по локальній мережі. Це обмеження залежить від конфігурації маршрутизатора шлюзу і типу широкомовної розсилки.

Багатоадресна передача призначена для збереження пропускної спроможності IPv4-мережі. Така передача скорочує трафік, дозволяючи вузлу відправляти один пакет вибраній групі вузлів, які є частиною групи мультисповіщення. Щоб досягти цільових вузлів за допомогою одноадресного зв'язку, вузол-джерело повиннен відправляти окремий пакет на кожну адресу. У випадку з багатоадресною розсилкою вузол-джерело може відправляти один пакет, який досягає декількох тисяч вузлів призначення. Мережева взаємодія дублює багатоадресні потоки, щоб вони досягали тільки вказаних одержувачів.

Багатоадресна передача включає:

- широкомовну передачу відео і аудіо;
- обмін даними маршрутизації протоколами маршрутизації;
- поширення ПЗ;
- гру віддаленим способом.

Історично склалося так, що призначені адреси згрупували одноадресні діапазони в адреси з особливими розмірами, які називаються адресами класу A, класу B і класу C. Крім того, були визначені адреси класу D (групові) і класу E (експериментальні).

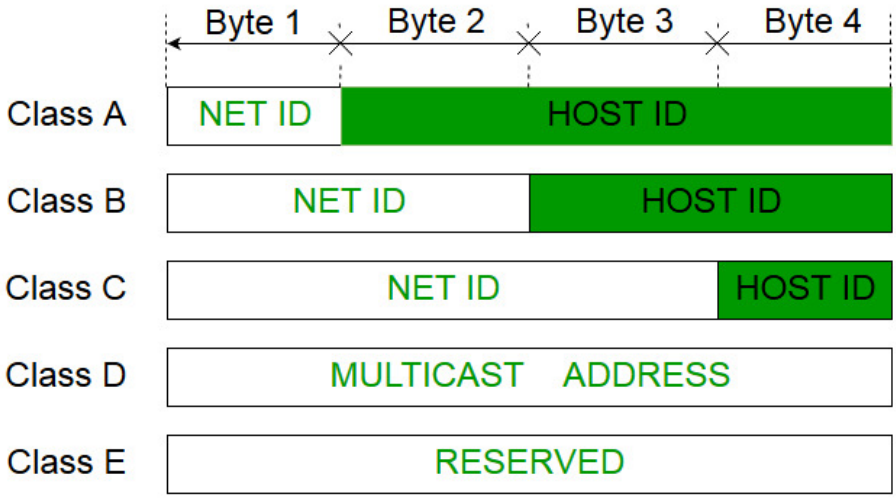


Рис. 4 Класи мереж

Блоки класу A

Блок адрес класу A розроблений для підтримки дуже великих мереж, що містять більш ніж 16 мільйонів адрес вузлів. Для позначення мережевої адреси IPv4-адреси класу A використовували фіксований префікс /8 з першим октетом. Інші три октети використовувалися для адрес вузлів. Усі адреси класу A вимагають, щоб найбільший розряд старшого октету дорівнював нулю. Це означає, що існувало тільки 128 можливих мереж класу A, від 0.0.0.0/8 до 127.0.0.0 /8. Навіть якщо адреси класу A зарезервували половину адресного простору, у зв'язку з їх обмеженням до 128 мереж вони можуть бути призначені тільки приблизно 120 компаніям або організаціям.

Блоки класу B

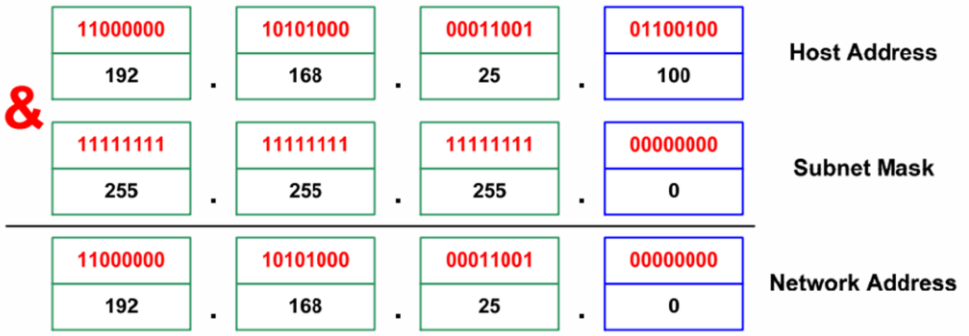
Адресний простір класу B розроблений для підтримки потреб невеликих і великих мереж, що містять приблизно 65 000 вузлів. IP -адреса класу B використовувала два старші октети для позначення мережевої адреси. Два октети, що залишилися, визначали адреси вузлів. Як і у випадку з класом A, адресний простір для класів адрес, що залишилися, має бути зарезервованим. Для адрес класу B два найстарші розряди старшого октету дорівнюють 10. Це обмежує блок адрес для класу B від 128.0.0.0/16 до 191.255.0.0/16. Призначення адрес класу B більш ефективне в порівнянні з класом A, оскільки 25% його загального простору IPv4-адрес було розділене серед приблизно 16 000 мереж.

Блоки класу C

Адресний простір класу C був доступний частіше за усі інші класи адрес. Це адресний простір призначений для надання адрес невеликим мережам з максимальною кількістю вузлів не більше 254. Блоки адрес класу C використовували префікс /24. Це означає, що мережа класу C використовувала тільки останній октет як адреси вузлів з трьома старшими

октетами для позначення мережевих адрес. Блоки адрес класу С відділяли адресний простір за допомогою фіксованого значення 110 найстарших розрядів старшого октету. Це обмежило блок адрес класу С від 192.0.0.0/24 до 223.255.255.0/24. Хоча цей блок зайняв тільки 12,5 % від загального об'єму адресного IPv4-простору, він надав адреси 2 мільйонам мереж.

При налаштуванні IP -вузла йому привласнюється не лише IP-адреса, але і маска підмережі. Як і IP-адреса, маска складається з 32 біт. Вона визначає, яка частина IP-адреси відноситься до мережі, а яка – до вузла. Маска порівнюється з IP-адресою побітно, зліва направо. У масці підмережі одиниці відповідають мережевій частині, а нулі – адресі вузла.



IPv6

Довжина IPv6-адреса складає 128 біт, написаних у вигляді рядка шістнадцяткових значень. Кожні 4 біта представлені однією шістнадцятковою цифрою, причому загальна кількість шістнадцяткових значень дорівнює 32. IPv6-адреси не чутливі до регістра, їх можна записувати як рядковими, так і прописними буквами.

Переважний формат для запису IPv6-адреси: x:x:x:x:x:x:x:x, де кожен «x» складається з чотирьох шістнадцяткових значень. Октети – це термін, який використовується для позначення 8 біт IPv4-адреси. У IPv6 шістнадцяткове число – це термін, використовуваний для позначення сегменту з 16 біт або чотирьох шістнадцяткових значень. Кожен «x» - це одне шістнадцяткове число, 16 біт або 4 шістнадцяткових цифр. У переважному форматі IPv6-адреса записана за допомогою 32 шістнадцяткових цифр. Проте, це не найоптимальніший спосіб представлення IPv6-адреси. Роглянемо два правила, які допоможуть скоротити кількість цифр, необхідних для представлення IPv6 - адреси.

Правило 1: пропуск початкових нулів

Перше правило для скорочення запису IPv6–адрес – пропуск усіх ведучих 0 (нулів) в шістнадцятковому записі. Наприклад:

001AB можна представити як 1AB;

09F0 можна представити як 9F0;

0A00 можна представити як A00;

00AB можна представити як AB.

Правило 2: пропуск усіх нульових блоків

Друге правило для скорочення запису адрес IPv6 полягає в тому, що подвійна двокрапка (::) може замінити будь-який єдиний, суміжний рядок

одного або декількох 16-бітових сегментів (хекстетів), що складаються з нулів.

Подвійна двокрапка (::) може використовуватися в адресі тільки один раз, інакше в результаті може виникнути декілька адрес. Поєднання цього правила з методом пропуску нулів допомагає значно скоротити запис IPv6 - адреса. Це називається стислим форматом.

4. *IP-мережі.*

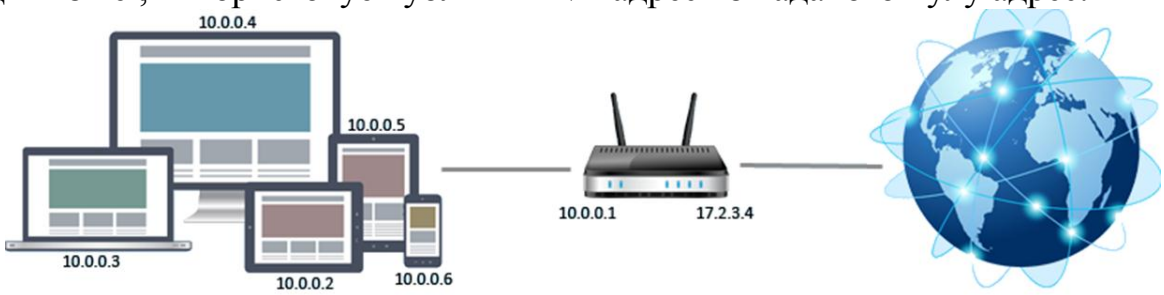
З поширенням персональних комп'ютерів і настанням ери Всесвітньої мережі стало очевидно, що 4,3 мільярда IPv4 -адрес буде недостатньо. Поява протоколу IPv6 стала довгостроковим рішенням, проте разом з цим знадобилися швидші способи усунення проблеми вичерпання адресного простору. IETF розробила ряд короткострокових рішень, у тому числі перетворення мережевих адрес (NAT, Network Address Translation) у приватні IPv4-адреси відповідно до RFC 1918.

Кількості публічних IPv4-адрес недостатньо, щоб призначити унікальні адреси усім пристроям, підключеним до Інтернету. В більшості випадків, мережі реалізуються з використанням приватних IPv4-адрес відповідно до RFC 1918. Ці приватні адреси використовуються у рамках організації або об'єкту з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію або організацію, приватні IPv4-адреси не можна використовувати для маршрутизації через інтернет. Для того, щоб дозволити пристрою з приватною IPv4-адресою доступ до пристроїв і ресурсів поза локальною мережею, приватну адресу спочатку необхідно перетворити в публічну адресу. NAT забезпечує перетворення приватних адрес в публічні адреси. Це дозволяє пристрою з приватною IPv4-адресою діставати доступ до ресурсів поза своєю приватною мережею, включаючи ресурси, знайдені в Інтернеті. У поєднанні з приватними IPv4-адресами, NAT продемонстрував свою доцільність відносно економії публічних IPv4-адрес. Одна публічна IPv4-адреса може спільно використовуватися сотнями, навіть тисячами пристроїв, для кожного з яких налагоджена унікальна приватна IPv4-адреса.

Без використання NAT адресний простір IPv4 був би вичерпаний задовго до настання 2000 року. Незважаючи на свої переваги, NAT має ряд обмежень. Вирішенням проблеми вичерпання простору IPv4-адрес і обмежень NAT є остаточний перехід на IPv6.

Перетворення мережевих адрес NAT використовується в різних цілях, проте основним завданням цього механізму є збереження публічних IPv4-адрес. Це досягається шляхом дозволу мережам використовувати приватні IPv4-адреси для внутрішньої взаємодії і перетворення їх в публічні адреси тільки у разі потреби. Додаткова перевага NAT – підвищення міри конфіденційності і безпеки мережі пояснюється тим, що цей механізм приховує внутрішні IPv4-адреси від зовнішніх мереж. Для маршрутизатора з підтримкою NAT можна налаштувати одну або декілька діючих публічних IPv4-адрес. Ці публічні адреси відомі як пул адрес NAT. Коли внутрішній

пристрій відправляє трафік за межі мережі, маршрутизатор з підтримкою NAT перетворює внутрішню IPv4 -адресу пристрою в публічну адресу з пулу NAT. Зовнішнім пристроям здається, що увесь трафік, що входить в мережу і виходить з неї, використовує публічні IPv4-адреси з наданого пулу адрес.



Існують три механізми перетворення мережевих адрес.

- Статичне перетворення мережевих адрес (статичний NAT) - це взаємнооднозначна відповідність між локальною і глобальною адресами.
- Динамічне перетворення мережевих адрес (динамічний NAT) - це зіставлення адрес за схемою «багато до багатьох» між локальними і глобальними адресами.
- Перетворення адрес портів (PAT) - це зіставлення адрес за схемою «багато до одного» між локальними і глобальною адресами. Цей метод також називається NAT з перевантаженням.

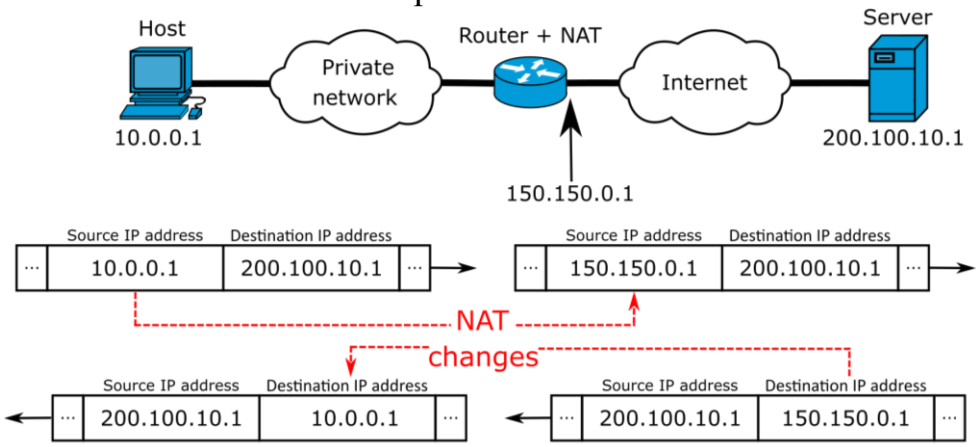


Рис. 5 Перетворення мережевих адрес

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою «один в один». Ці відповідності задаються адміністратором мережі і залишаються незмінними.

Метод статичного перетворення мережевих адрес особливо корисний для веб-серверів або пристроїв, які повинні мати постійну адресу, доступну з Інтернету, – наприклад, для вебсервера компанії. Статичний NAT також підходить для пристроїв, які мають бути доступні авторизованому персоналу, що працює поза офісом, але при цьому залишатися закритими для загального доступу через інтернет. Наприклад, мережевий адміністратор може з ПК підключитися за допомогою SSH до внутрішньої глобальної адреси 209.165.200.226.

Маршрутизатор перетворить цю внутрішню глобальну адресу у внутрішню локальну адресу і підключає сеанс адміністратора до

209.165.200.226. Для статичного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

Метод динамічного перетворення мережевих адрес (динамічний NAT) використовує пул публічних адрес, які привласнюються у порядку живої черги. Коли внутрішній пристрій просить доступ до зовнішньої мережі, динамічний NAT привласнює доступну публічну IPv4-адресу з пулу.

Перетворення адрес портів (PAT) зіставляє багато приватних IPv4-адрес одній або декільком публічним IPv4-адресам. Саме цей метод реалізується більшістю домашніх маршрутизаторів. Інтернет-провайдер призначає маршрутизатору одну адресу, але декілька членів сім'ї можуть одночасно діставати доступ в Інтернет. NAT з навантаженням – це найбільш поширений метод перетворення мережевих адрес.

За допомогою цього методу багато адрес можуть бути зіставлені одній або декільком адресам, оскільки кожна приватна адреса також відстежуються за номером порту. Якщо пристрій починає сеанс TCP/IP, він створює значення порту TCP або UDP для джерела, щоб унікальним чином визначити сеанс. Коли маршрутизатор NAT отримує пакет від клієнта, він використовує свій номер порту джерела, щоб унікальним чином визначити конкретне перетворення NAT.

PAT гарантує, що пристрої використовуватимуть різні номери портів TCP для кожного сеансу взаємодії з сервером в Інтернеті. При поверненні відповіді від сервера номер порту джерела, яке стає номером порту призначення при зворотній передачі, визначає, якому пристрою маршрутизатор перешле відповідні пакети. Процес PAT також переконується в тому, що вхідні пакети дійсно були запрошені, підвищуючи таким чином міру безпеки сеансу.

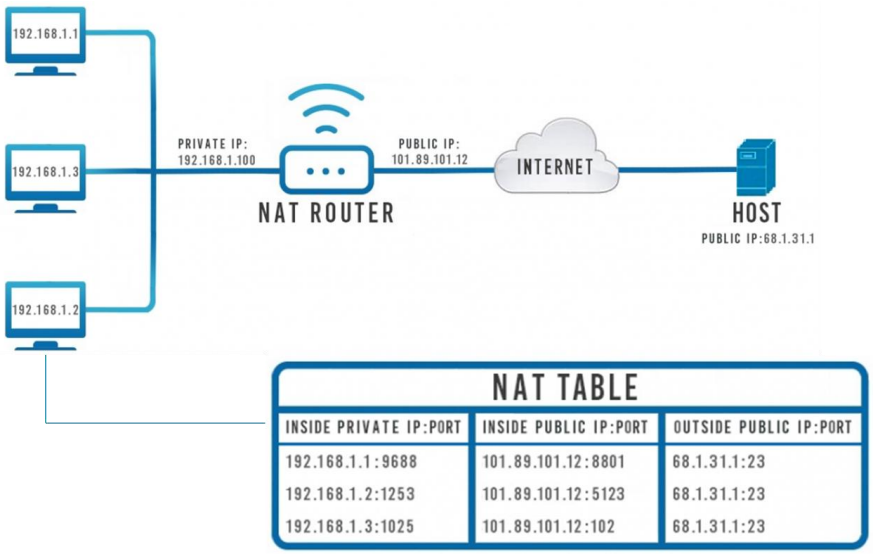


Рис. 6 Перетворення мережевих адрес PAT

Переваги і недоліки NAT наведено в таблиці.

ПЕРЕВАГИ	НЕДОЛІКИ
Збереження IP-адрес: одна «біла» (зовнішня, публічна) IP-адреса обслуговує багато «сірих» (прихованих, внутрішніх) адрес	Не всі протоколи можуть працювати з NAT
Обмеження публічного доступу до внутрішньої мережі (БЕЗПЕКА)	Ускладнення роботи проміжних пристроїв
Приховування внутрішньої архітектури мережі	Додаткові складності ідентифікації користувача
	Кілька підключень з одного IP
	Проблеми доступу до внутрішньої мережі ззовні

VPN

VPN (Virtual Private Network — віртуальна приватна мережа) — загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

Прикладом створення віртуальної мережі використовується інкапсуляція протоколу PPP в будь-який інший протокол — IP (ця реалізація називається також PPTP — Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Деякі інші протоколи так само надають можливість формування захищених каналів (SSH).

Класифікувати VPN рішення можна за кількома основними параметрами.

За типом використовуваної середовища:

Захищені. Найбільш поширений варіант приватних приватних мереж. З його допомогою можливо створити надійну і захищену підмережа на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

Довірчі. Використовуються у випадках, коли передавальне середовище можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN—рішень є: Multi—protocol label switching (MPLS) і L2TP (Layer 2 Tunneling Protocol). (Коректніше сказати, що ці протоколи перекладають завдання забезпечення

безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec)

За способом реалізації:

У вигляді спеціального програмно-апаратного забезпечення. Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

У вигляді програмного рішення. Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегроване рішення. Функціональність VPN забезпечує комплекс, який вирішує також завдання фільтрації зв'язку, організації мережевого екрану і забезпечення якості обслуговування.

За призначенням:

Intranet VPN. Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

Remote Access VPN. Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральною будівлею або філією) та одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера або, перебуваючи у відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

Extranet VPN. Використовують для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти).

Переваги VPN очевидні. Надавши користувачам можливість з'єднуватися через Інтернет, масштабованість досягається в основному збільшенням пропускної здатності каналу зв'язку, коли мережа стає перевантаженою. VPN допомагає заощадити на телефонних витратах, оскільки вам не потрібно мати справу з пулом модемів. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які в звичайній ситуації адміністратори змушені виносити на зовнішнє з'єднання.

Отже, VPN забезпечує:

- захищені канали зв'язку за ціною доступу в Інтернет, що в кілька разів дешевше виділених ліній;
- при установці VPN не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів – все це значна економія;
- забезпечується масштабування, оскільки VPN не створює проблем росту і зберігає зроблені інвестиції;
- незалежність від криптографії і можливість використовувати модулі криптографії будьяких виробників у відповідності з національними стандартами тієї чи іншої країни;
- відкриті інтерфейси дозволяють інтегрувати вашу мережу з іншими програмними продуктами та бізнес-додатками.

До недоліків VPN можна віднести надлишок трафіку.

Питання для самоконтролю

1. Які типи комп'ютерних мереж ви знаєте?
2. Які технології доступу в Інтернет ви знаєте?
3. Чим відрізняються протокольна та еталонна модель?
4. Яке призначення рівнів моделі TCP/IP?
5. Яке призначення рівнів моделі OSI?
6. Для чого використовується мережева і вузлова частини IPv4 – адреси?
7. Що позначає довжина префікса?
8. У чому полягає одноадресна, широкомовна та багатоадресна передача?
9. Яке представлення IPv6?
10. У чому полягають відмінності технологій NAT і PAT?
11. Які переваги і недоліки NAT?
12. Класифікація VPN.

Лекцію склав доцент кафедри ІТтаСЕК Борзов Ю.О.