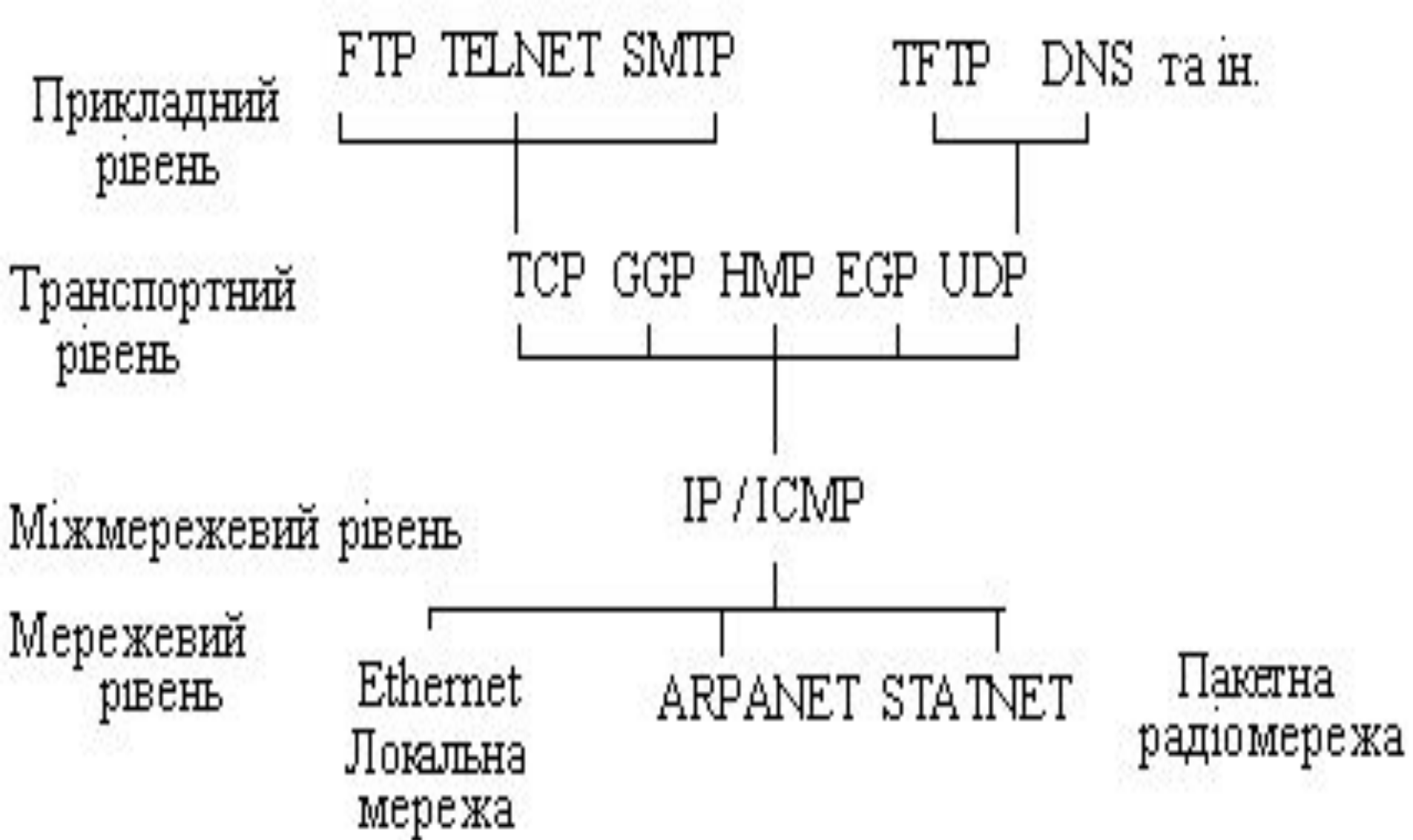


Стек протоколів TCP/IP

В основу роботи мережі Інтернет покладено сім'ю протоколів TCP/IP (Transmission Control Protocol / Інтернет protocol). Це стандартний промисловий набір протоколів, розроблений для глобальних обчислювальних мереж. TCP/IP – це технологія міжмережної взаємодії.

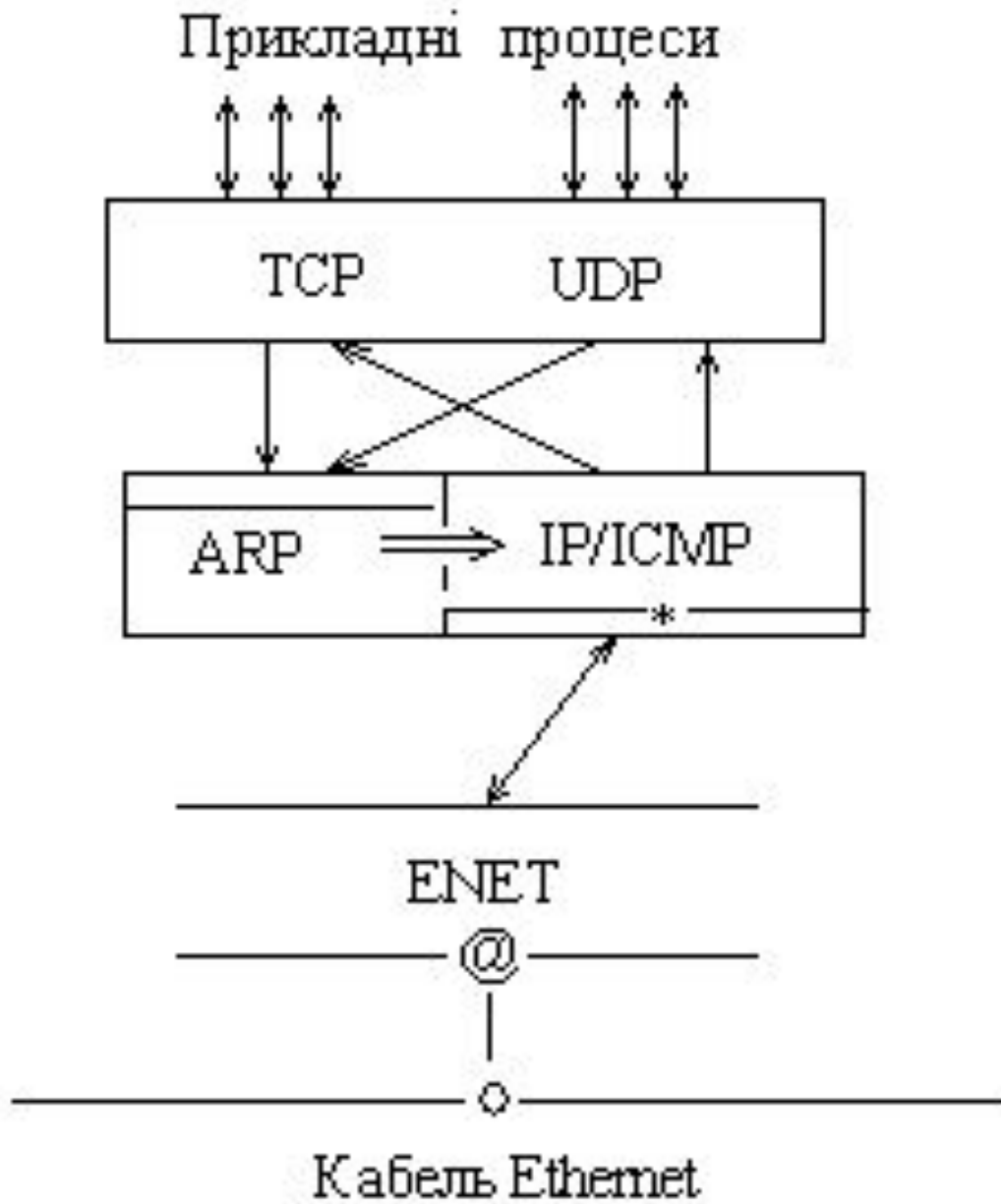
Назва сім'ї протоколів утворилася від найбільш часто використовуваних протоколів TCP та IP. До складу сім'ї протоколів TCP/IP входять протоколи: ARP, TCP, UDP, IP, ICMP, FTP, TELNET, SMTP й ін.



Взаємозалежність протоколів сім'ї TCP/IP

Рівні моделі OSI	IBM/Microsoft	TCP/IP		Novell	Стек OSI
Прикладний	SMB	Telnet, FTP, SMTP, NNTP, HTTP, SNMP		NCP, SAP	X.400, X.500, VTP, FTAM
Представницький					Протокол подання OSI
Сеансовий	NetBIOS	TCP			Сеансовий протокол OSI
Транспортний			UDP	SPX	Транспортний протокол OSI
Мережний	—	IP, ICMP, RIP, OSPF	IPX, RIP, NLSP	IS-IS	
Канальний	Ethernet (802.3), Token Ring (802.5), FDDI, SLIP, PPP, X.25, ATM, LAP-B, LAP-D				
Фізичний					

Стеки протоколів



Структура протоколів та модулів у вузлі мережі TCP/IP

У випадку використання протоколу TCP (Transmission Control Protocol – протокол керування передачею) дані передаються між прикладним процесом і модулем TCP. Типовим прикладним процесом, що використовує протокол TCP, є модуль FTP (File Transfer Protocol – протокол передачі файлів). *Стек протоколів* у цьому випадку буде таким: FTP/TCP/IP/ENET.

При використанні протоколу UDP (User Datagram Protocol – протокол датаграм користувача) дані передаються між прикладним процесом і модулем UDP. Наприклад, SNMP (Simple Network Management Protocol – простий протокол керування мережею) користується транспортними послугами UDP. Його *стек протоколів* має такий вигляд: SNMP/UDP/IP/ENET.

Модулі TCP, UDP і драйвер ENET є **мультиплексорами**. Діючи як мультиплексори, вони перемикають кілька входів на один вихід. Вони також є **демультиплексорами**. Як демультиплексори вони перемикають один вхід на один з багатьох виходів відповідно до поля типу в заголовку протокольного блоку даних.

Коли Ethernet-кадр потрапляє в драйвер мережного інтерфейсу ENET, він може бути спрямований або в модуль ARP (Address Resolution Protocol – адресний протокол), або в модуль IP (Internet Protocol – міжмережевий протокол). Про те, куди повинен бути спрямований Ethernet-кадр, свідчить значення поля типу в заголовку кадру.

Якщо IP-пакет потрапляє в модуль IP, то дані, які містяться в ньому, можуть бути передані або модулю TCP, або модулю UDP, це визначається полем "протокол" у заголовку IP-пакета.

Якщо UDP-датаграма потрапляє в модуль UDP, то на підставі значення поля "порт" у заголовку UDP-датаграми визначається прикладна програма, якій повинне бути передане прикладне повідомлення. Якщо TCP-повідомлення попадає в модуль TCP, то вибір прикладної програми, якій повинне бути передане повідомлення, здійснюється на основі значення поля "порт" у заголовку TCP-повідомлення.

Мультиплексування даних у зворотний бік здійснюється досить просто, тому що з кожного модуля існує тільки один шлях униз. Кожен протокольний модуль додає до пакета свій заголовок, на підставі якого машина, що прийняла пакет, виконує демупльтиплексування.

Дані від прикладного процесу проходять через модулі TCP або UDP, після чого потрапляють у модуль IP і звідти – на рівень мережного інтерфейсу.

Принципи адресації в Інтернет

Кожна машина, під'єднана до мережі, повинна мати своє унікальне ім'я, що прийнято називати *IP-адресою*. ***IP-адреса – це унікальне 32-бітне число (4-байтне), що має вигляд сукупності чотирьох чисел від 0 до 255, розділених між собою крапками.***

Наприклад:

134.30.0.17

192.168.1.56

IP-адресація комп'ютерів у мережі Інтернет побудована на концепції мережі, що складається з *хостів* та інших мереж. ***Хост являє собою об'єкт мережі, що може передавати й приймати IP-пакети***, наприклад, комп'ютер робочої станції або маршрутизатор. Зазвичай помилково розуміють під хостом який-небудь сервер, однак у рамках концепції IP-мережі і робочі станції, і сервери – всі є хостами.

Хости з'єднані один з одним через одну або кілька мереж. **IP-адреса** кожного з хостів складається з адреси мережі й адреси хоста в цій мережі. IP-адресація, на відміну, наприклад, від IPX-адресації, використовує один ідентифікатор, що поєднує адресу мережі і адресу хоста. Як відзначалося вище, адреса подана чотирма десятковими числами, розділеними крапками. Кожне із цих чисел не може перевищувати 255 і являє собою один байт з 4-байтної IP-адреси. Довжина IP-адреси становить 32 біти, розділених на дві або три частини. Перша частина позначає *адресу мережі*, друга (якщо вона є) – *адреса підмережі*, третя – *адреса вузла*. Нагадаємо, по-перше, що *адреса підмережі* наявна тільки у тому випадку, коли адміністратор мережі ухвалив рішення щодо поділу мережі на підмережі; по-друге, *IP-адреса вузла* ідентифікує точку доступу модуля IP до мережного інтерфейсу, а не всю машину.

Довжина полів адреси мережі, підмережі та хоста є змінними величинами. Менеджер мережі (адміністратор або програма) привласнює IP-адреси машинам відповідно до того, до яких IP-мереж вони під'єднані.

Для того, щоб показати, яка частина IP-адреси є ідентифікатором мережі (Network ID), а яка – ідентифікатором хоста (Host ID), вводять поняття “*маска мережі*”.

Маска мережі – це шаблон, що накладається на IP-адресу для встановлення, яка частина IP-адреси є ідентифікатором мережі (Network ID), а яка – ідентифікатором хоста (Host ID). Наприклад, для адреси 197.200.12.5 і маски підмережі 255.255.255.0 Network ID буде 197.200.12, а Host ID – 5.

Маска мережі використовується при обміні даними між двома хостами. Якщо хост-комп'ютери **A** і **B** належать одній мережі, хост **A** безпосередньо звертається до хосту **B**, однак якщо хост **B** належить іншій мережі, хост **A** буде звертатися через шлюз, і спосіб, яким хост **A** може повідомити про свою належність даної мережі, – це використання маски мережі. Наприклад, нехай маємо три хости

вузол **A** з IP-адресою 200.163.10.5

вузол **B** 200.163.10.9

вузол **C** 200.163.199.11

і маску мережі 255.255.255.0

Припустимо хост **A** з'єднується з хостом **B**, оскільки обидва вони мають Network ID 200.163.10, то хост **A** звертається до хосту **B** безпосередньо. Якщо ж хост **A** з'єднується з хостом **C**, а вони перебувають у різних мережах (200.163.10 й 200.163.199 відповідно), то хост **A** буде надсилати запит через шлюз.

Клас	Діапазон значень першого октету	Маска мережі за замовчуванням	Можлива кількість мереж	Можлива кількість вузлів
A	1 -	255.	126	1677
B	126	0.0.0	1638	7214
C	128 -	255.	2	6553
D	191	255.	2097	4
E	192 -	0.0	150	254

Адреси класу А призначені для використання у великих мережах загального користування. Вони допускають велику кількість номерів вузлів. Адреси класу В використовуються в мережах середнього розміру, наприклад, в мережах університетів і великих компаній. Адреси класу С використовуються в мережах з невеликим числом комп'ютерів. Адреси класу D – при звертаннях до груп машин, а адреси класу E зарезервовані на майбутнє.

Характеристики IP-адрес різних класів

Клас	Старші біти	Найменший номер мережі	Найбільший номер мережі	Примітка
A	0	1.0.0.0	126.0.0.0	
B	10	128.0.0.0	191.255.0.0	
C	110	192.0.1.0	223.255.255.0	
D	1110	224.0.0.0	239.255.255.255	Групові адреси
E	11110	240.00.0	247.255.255.255	Зарезервовані

Розглядають *глобальні* (IP-) і *локальні* (Ethernet-) адреси.

Ethernet-адреса – це унікальне 6-байтне число, що має вигляд сукупності шести чисел в 16-й системі числення, розділених між собою двокрапкою або тире.

Якщо локальна адреса привласнюється машині постачальником послуг Інтернет, то Ethernet-адреса є унікальним для кожного мережного адаптера й розпізнається драйвером. Іншими словами, Ethernet-адреса відома машині, коли тільки у неї вставили мережну плату або інший мережний адаптер. Ethernet-адреса «вшита» у мережний адаптер виробником.

Машина, яка працює в глобальній мережі, завжди має свої IP- та Ethernet- адреси.

Протокол ARP

Розглянемо те, як при пересиланні IP-пакета визначається Ethernet-адреса призначення. Для відображення IP-адрес в Ethernet-адреси використовується протокол ARP (Address Resolution Protocol – адресний протокол). Відображення виконується *тільки для IP-пакетів*, які відправляються, тому що тільки в момент відправлення створюються IP- і Ethernet- заголовки.

Перетворення адрес виконується шляхом пошуку відповідності в таблиці. Ця таблиця, називана ARP-таблицею, зберігається в пам'яті комп'ютера й містить рядки для кожного вузла мережі.

IP-адреса	Ethernet-адреса
223.1. 2.1	08:00:39:00:2F:C3
223.1. 2.3	08:00:5A:21:A7:22
223.1. 2.4	08:00:10:99:AC:54

Якщо за допомогою ARP-таблиці не вдається відразу здійснити перетворення адрес, то IP-пакет ставиться в чергу, а необхідна для перетворення інформація надходить за допомогою запитів і відповідей протоколу ARP, після чого IP-пакет передається за призначенням.

Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде й не буде запису в ARP-таблиці. Протокол IP буде знищувати IP-пакети, що направляються за зазначеною IP-адресою. Зазначимо, що протоколи верхнього рівня не можуть відрізнити випадок ушкодження мережі Ethernet від випадку відсутності машини із шуканою IP-адресою.

Деякі реалізації IP- й ARP- протоколів не ставлять у чергу IP-пакети на той час, поки вони чекають ARP-відповідей. Замість цього IP-пакет просто знищується, а його відновлення покладається на модуль TCP або прикладний процес, що працює через UDP. Таке відновлення виконується за допомогою таймаутів і повторних передач. Повторна передача повідомлення відбувається успішно, тому що перша спроба вже викликала заповнення ARP-таблиці.

Міжмережний протокол IP

Internet Protocol (IP) створений для використання в об'єднаних системах комп'ютерних комунікаційних мереж з комутацією пакетів. Він забезпечує *передачу блоків даних, датаграм від відправника до одержувачів*, де відправник та одержувач є хост-комп'ютерами, які ідентифікуються адресами фіксованої довжини. IP-протокол забезпечує *за необхідності також фрагментацію та дефрагментацію датаграм для передачі даних через мережі з малим розміром пакетів.*

Таким чином, IP-протокол виконує дві **головні функції: адресацію і фрагментацію.**

Вся інформація передається в мережі Інтернет за допомогою IP-датаграм (Internet-датаграм), причому кожна датаграма має заздалегідь певну структуру.

Version	IHL	Type of Service	Total Length
Identification	Flags		Fragment Offset
Time to live	Protocol	Header Hecksum	
Source address			
Destination Address			
Options		Paddings	
Data			

Схема IP-датаграми

Version (версія) – поле, призначене для називання версії, що визначає формат IP-заголовка. Розглянутий заголовок описує версію 4.

IHL – визначає довжину IP-заголовка, виміряється в словах по 32 біти кожне і вказує на початок поля даних. Коректний заголовок може мати мінімальний розмір 5 слів.

Type of Service – визначає тип необхідного сервісного обслуговування. Реально вибір здійснюється між трьома альтернативами:

малою затримкою;

високою вірогідністю;

високою пропускною здатністю.

Для даного поля виділяється 8 бітів:

біти 0-2 визначають пріоритет:

011 – миттєво;

001 – пріоритетно;

000 – звичайний маршрут;

біт 3 визначає затримку:

0 – нормальна затримка;

1 – мала затримка;

біт 4 визначає пропускну здатність:

0 – нормальна пропускна здатність;

1 – висока пропускна здатність;

біт 5 визначає достовірність:

0 – звичайна достовірність;

1 – висока достовірність;

біти 6-7 зарезервовані.

Total Length – визначає загальну довжину IP-датаграми. Загальна довжина – це довжина датаграми, яка вимірюється в октетах (байтах), включаючи IP-заголовок і поле даних. Це поле може задавати довжину датаграми аж до 65535 октетів.

У більшості хост-комп'ютерів і мереж настільки великі датаграми не використовуються. Всі хости повинні бути готові приймати датаграми довжиною 576 октетів, незалежно від того, чи надходять вони єдиним цілим або фрагментами. Хостам рекомендується відправляти датаграми розміром більше 576 октетів, тільки в тому випадку, якщо вони впевнені, що хост, який приймає, готовий обслуговувати датаграми підвищеного розміру.

Значення 576 вибране для того, щоб відповідним чином обмежений блок даних передавався разом з необхідною інформацією в заголовку.

Identification (ідентифікатор) – визначає ідентифікатор, що встановлюється відправником для збирання фрагментів якої-небудь датаграми.

Flags – визначає різні керуючі прапорці.

Біт 1 (DF) – відповідає за фрагментацію датаграми:

0 – можлива фрагментація;

1 – заборона фрагментації.

Біт 2 (MF) – прапорець появи додаткових фрагментів:

0 – останній фрагмент;

1 – будуть ще фрагменти.

Fragment Offset – визначає зсув фрагмента й показує, де в датаграмі перебуває цей фрагмент. Зсув фрагмента змінюється порціями по 8 октетів (64 біти). Перший фрагмент має зсув нуль.

Time to Live (TTL) – визначає максимальний час, протягом якого датаграмі дозволено перебувати в системі Інтернет

Protocol – визначає протокол більш високого (наступного) рівня, що використовує дані з IP-датаграми.

Header Checksum – визначає контрольну суму заголовка. Оскільки деякі поля заголовка змінюють своє значення (наприклад, TTL), це значення перевіряється й повторно перераховується при кожній обробці IP-заголовка.

Source Address – визначає адресу відправника.

Destination Address – визначає адресу одержувача.

- **Options** – поле змінної довжини для службових записів. Опції можуть з'явитися у датаграмах, а можуть і не з'являтися. Вони повинні підтримуватися всіма Інтернет-модулями (хостами й шлюзами). Необов'язково кожна конкретна датаграма має опції, але мати їх все-таки може.
- **Padding** – забезпечує вирівнювання. Вирівнювання Інтернет-заголовка використовується для того, щоб переконатися в тому, чи закінчується Інтернет-заголовок на 32-бітній границі. Вирівнювання здійснюється нулями.
- **Data** – поле, що містить дані, які передаються по мережі Інтернет.

Маршрутизація пряма й непряма. Правила маршрутизації

Раніше зазначалося, що однією з основних функцій IP-протоколу є адресація. IP-протокол використовує адреси, розміщені в IP-заголовку, для передачі IP-датаграм їх одержувачам. *Вибір шляху передачі даних називається маршрутизацією.*

Центральною частиною протоколу IP є його **таблиця маршрутів**. Протокол використовує цю таблицю при прийнятті всіх рішень про маршрутизацію IP-пакетів. Зміст таблиці маршрутів визначається адміністратором мережі. Помилки при встановленні маршрутів можуть заблокувати передачу даних.

*При **прямій маршрутизації** IP- і Ethernet-адреси відправника відповідають адресам того вузла, що послав IP-пакет, а IP- і Ethernet-адреси місця призначення відповідають адресам одержувача. При **непрямій маршрутизації** IP- і Ethernet-адреси не утворюють таких пар.*

Правила маршрутизації

1. Для IP-пакетів, які надійшли від модулів верхнього рівня для відправлення, модуль IP повинен визначити спосіб доставки – прямий або непрямий – і вибрати мережний інтерфейс. Цей вибір робиться на підставі результатів пошуку в таблиці маршрутів.
2. Для прийнятих IP-пакетів, що надходять від мережних драйверів, модуль IP повинен вирішити, чи потрібно ретранслювати IP-пакет по іншій мережі або передати його модулям верхнього рівня. Якщо модуль IP вирішить, що IP-пакет необхідно ретранслювати, то подальша робота з ним здійснюється так само, як з IP-пакетами, що відправляються (див. пункт 1).
3. Вхідний IP-пакет ніколи не ретранслюється через той самий мережний інтерфейс, яким він був прийнятий.
4. Рішення про маршрутизацію приймається до того, як IP-пакет передається мережному драйверу, і до того, як відбувається звертання до ARP-таблиці.

Протокол ТСР

Протокол керування передачею (Transmission Control Protocol або ТСР) призначений для використання як надійного протоколу спілкування між хост-комп'ютерами в комунікаційних комп'ютерних мережах з комутацією пакетів.

Протокол ТСР забезпечує надійність комунікацій між парами процесів на хост-комп'ютерах, які включені у різні комп'ютерні комунікаційні мережі й об'єднані в єдину систему.

ТСР займає в багаторівневій архітектурі протоколів нішу безпосередньо над ІР-протоколом, що дозволяє протоколу ТСР відправляти й одержувати сегменти інформації змінної довжини, укладені в оболонку ІР-датаграм. Датаграма надає дані для адресації відправника й одержувача ТСР-сегментів у різних мережах. ІР-протокол також здійснює будь-яку фрагментацію й збирання сегментів ТСР, які необхідні для здійснення передачі й доставки через безліч мереж і проміжних шлюзів. ІР-протокол також обробляє інформацію про пріоритет, класифікацію безпеки, а також здійснює розмежування ТСР сегментів. Отже, дана інформація може бути передана прямо через безліч мереж.

Протокол TCP припускає, що він може одержати простий, потенційно ненадійний сервіс для своїх датаграм із боку протоколів нижнього рівня. Отже, він:

- повинен забезпечити надійний сервіс для комунікацій між процесами в багатомережній системі;
- повинен бути загальним протоколом для комунікацій між хост-комп'ютерами в безлічі мереж.

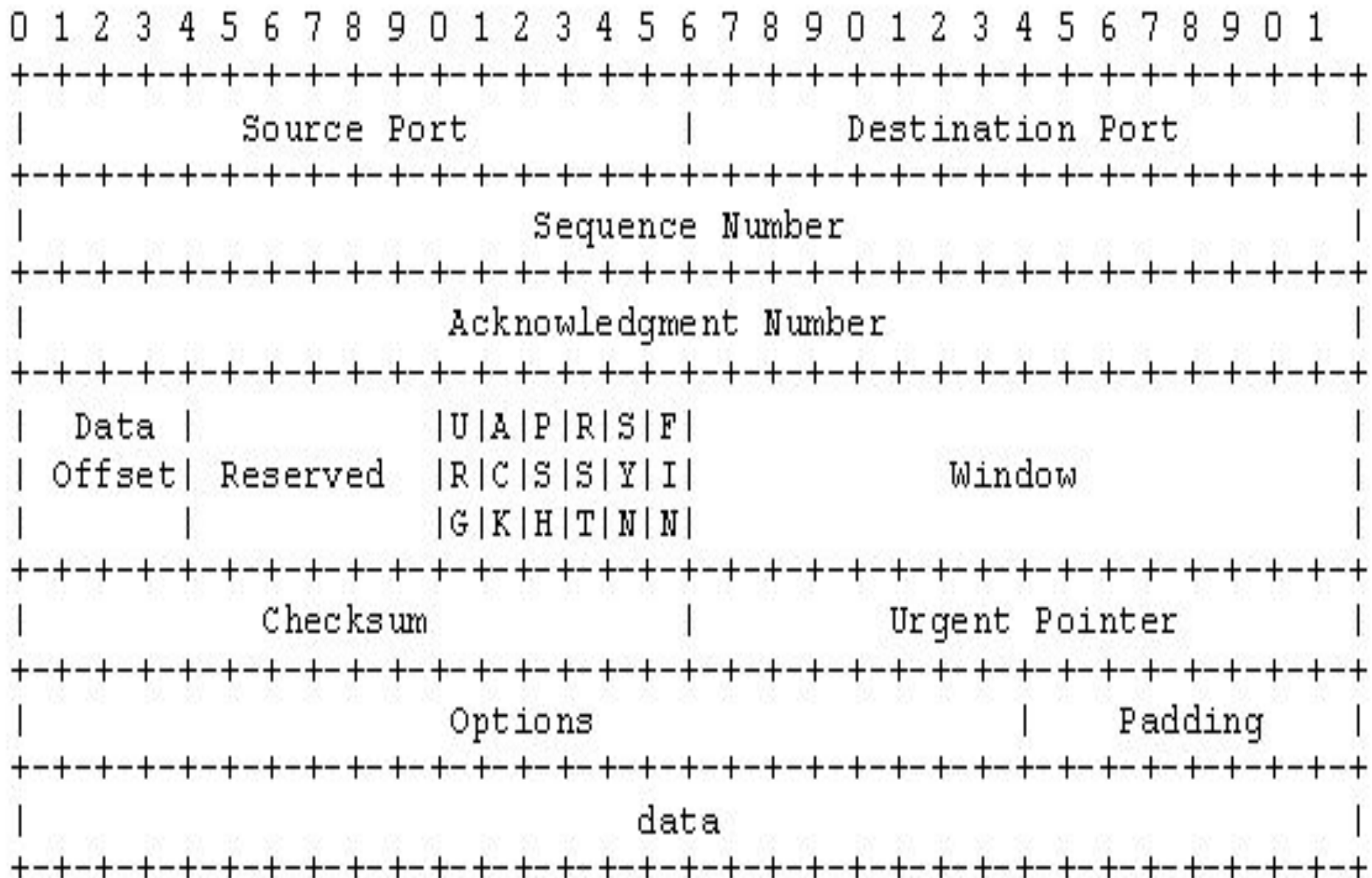
Головною **метою протоколу TCP** є забезпечення надійного, безпечного сервісу для логічних з'єднань між парами процесів. Щоб забезпечити такий сервіс, ґрунтуючись на менш надійних комунікаціях Інтернет, система повинна мати можливості для роботи в таких областях:

- базова передача даних;
- достовірність;
- керування потоком даних;
- поділ каналів;
- робота із з'єднаннями;
- пріоритет і безпека.

Формат ТСР-заголовок

Передавання ТСР сегментів здійснюється у вигляді ІР-датаграм. Заголовок ТСР-сегмента в Інтернет-протоколі має кілька інформаційних полів, включаючи адреси хост-комп'ютерів, що відправляють і приймають дані. ТСР-заголовок іде за ІР-заголовком і доповнює його інформацією, яка є специфічною для ТСР-протоколу. Такий розподіл допускає використання на рівні хост-комп'ютерів протоколів, інших, ніж ТСР.

Щоб дозволити на окремо взятому комп'ютері багатьом процесам одночасно використовувати комунікаційні можливості транспортного рівня, протокол TCP надає на кожному хост-комп'ютері набір адрес або портів. Разом з IP-адресами на комунікаційному рівні Інтернету вони утворюють **сокет** (socket – гніздо). Кожне з'єднання унікальним чином ідентифікується *парою сокетів*. Так, будь-який сокет може одночасно використовуватися в багатьох з'єднаннях.



Формат TCP-заголовка

Source Port – номер порту відправника – 16 бітів.

Destination Port – номер порту одержувача – 16 бітів.

Sequence Number – номер черги для першого октету даних у даному сегменті (за винятком тих випадків, коли наявний прапорець синхронізації SYN). Якщо ж прапор SYN наявний, то номер черги є ініціалізованим (ISN), а номер першого октету даних – ISN+1.

Acknowledgment Number (номер підтвердження) 32 біти. Якщо встановлено контрольний біт ACK, то це поле містить наступний номер черги, який відправник даної датаграми бажає отримати у зворотному напрямку. Номери підтвердження посилають постійно, як тільки з'єднання буде встановлено.

Data Offset – поле, що свідчить про початок поля даних, тобто вказує кількість 32-бітних слів в TCP-заголовку – 4 біти. TCP-заголовок завжди закінчується на 32-бітній межі, навіть якщо він містить опції.

Reserved – резервне поле, яке повинне бути заповнене нулями – 6 бітів.

Control Bits – поле контрольних бітів – 6 бітів. Кожен біт цього поля несе певне смислове навантаження:

Window – поле, яке визначає кількість октетів даних, одержання яких чекає відправник дійсного сегмента.

Checksum – поле контрольної суми – 16 бітів.

Поле контрольної суми – це 16-бітне доповнення суми всіх 16-бітних слів заголовка й тексту.

Urgent Pointer (терміновий покажчик) – поле, що повідомляє поточне значення термінового покажчика – 16 бітів.

Терміновий покажчик є додатною величиною – зсувом щодо номера черги даного сегмента. Її значення повідомляє номер черги для октету, що йде за терміновими даними. Це поле інтерпретується тільки в тому випадку, коли в сегменті виставлений контрольний біт URG.

Options – поле опцій. Опції можуть розміщуватися наприкінці TCP-заголовка, а їх довжина завжди кратна 8 бітам. Всі опції враховуються при розрахунку контрольної суми.

Padding – поле вирівнювання, довжина поля змінна.

Вирівнювання TCP-заголовка здійснюється для того, щоб переконатися в тому, що TCP-заголовок закінчується, а поле сегмента даних починається на 32-бітній межі. Вирівнювання виконується нулями.

Протокол датаграм користувача (UDP)

використовує IP-протокол для передачі повідомлення від однієї машини до іншої та забезпечує ту саму **ненадійну** доставку повідомлень, що й IP. Протокол UDP:

- не використовує підтвердження надходження повідомлень;
- не впорядковує повідомлення, які надходять отримувачу;
- не забезпечує зворотного зв'язку для керування швидкістю передачі інформації між машинами.

Знаходження UDP-протоколу над IP означає, що повні UDP-повідомлення, що включають UDP-заголовок і дані, інкапсулюються в IP-датаграмах при передаванні мережею .

SLIP (Serial Line Internet Protocol - протокол IP для послідовної лінії) дозволяє пристроям, які сполучені послідовною лінією зв'язку працювати по протоколам TCP/IP.

Для встановлення зв'язку необхідно заздалегідь задати IP-адреси, так як в протоколі SLIP немає системи обміну адресною інформацією.

Відсутня індикація типу інкапсулюемого протоколу - можливе використання тільки IP.

Не передбачена корекція помилок – її необхідно виконувати на верхніх рівнях, рекомендується використовувати протокол TCP.

PPP (Point-to-Point Protocol, протокол точка-точка) розроблений як частина стеку TCP/IP для передачі кадрів інформації по послідовним глобальним лініям зв'язку на заміну застарілого протоколу SLIP.

Протокол PPP досягає погодженої роботи різних пристроїв за допомогою переговорної процедури.

Він оснований на чотирьох принципах:

- Переговорне прийняття параметрів з'єднання (задовольняє відправника і отримувача);
- Багатопротокольна підтримка (на відміну від SLIP, який підтримує тільки IP);
- Розширюваність протоколу (можна вводити нові протоколи в стек PPP);
- Незалежність від глобальних служб (використання будь-якої технології глобальних мереж).

Протокол ICMP

Протокол ICMP (Internet Control Message Protocol - протокол керуючих повідомлень в Інтернеті) було задумано і розроблено як простий та безпечний засіб для повідомлень про помилки і для обміну повідомленнями типу запит-відповідь. У своєму природному вигляді ICMP є простим протоколом з чітко визначеними правилами використання. Але він може бути дещо модифікованим і в такому вигляді використаним порушниками. Тому важливо розрізняти нормальне і нестандартне використання цього протоколу.

Призначення ICMP

Протокол ICMP, який належить до стека протоколів TCP/IP, використовують для передавання коротких повідомлень. Транспортні протоколи цього стека — TCP та UDP потребують наявності призначеного порту сервера, з яким може взаємодіяти клієнт. Для здійснення простого запиту, наприклад для перевірки активності деякого вузла мережі, який називають ping-запитом або echo-запитом, не потрібно мати вільні порти, і надійність доставляння даних не обов'язковою.

Протокол ICMP використовують для обміну інформацією між двома хостами або між хостом і маршрутизатором при виникненні помилок. Маршрутизатори використовують протокол ICMP, щоб повідомити відправника про виникнення проблем під час доставляння повідомлень – наприклад: “заборонено адміністратором” Це повідомлення інформує відправника, що трафік цього типу заборонено згідно із правилом, що є у списку контролю доступу. У цьому випадку очевидно, що повідомлення відправляє маршрутизатор, оскільки саме він забороняє виконувати операцію. Але маршрутизатори також інформують відправника про помилки у випадку, коли доставити повідомлення вказаному адресату не вдається за можливе: наприклад, якщо хост-одержувач недоступний

Незважаючи на те, що пакет ICMP інкапсулюється в пакет IP, протокол ICMP відносять до мережного рівня, оскільки він не має рис, властивих протоколам транспортного рівня стека TCP/IP.

У протоколі ICMP на відміну від TCP або UDP. не використовують номери портів. Для того щоб розрізнити служби, в ICMP указують лише тип повідомлення і код призначення.

Команди контролю з'єднань та маршрутизації

Команда **ping** виконує такі дії: перевірку стану з'єднання з іншим комп'ютером або комп'ютерами відправленням echo-пакетів ICMP і аналіз отриманих відповідних пакетів; очікування до однієї секунди для кожного переданого пакета; виведення числа відправлених і прийнятих пакетів; кожен отриманий пакет порівнюється з відповідним відправленим. Формат команди:

ping [-t] [-a] [-n лічильник] [-l довжина] [-f] [-i ttl] [-v тип] [-r лічильник] [-s число] [[-j список_хостів] | [-k список_хостів] [-w інтервал] список_призначень

Параметри

- t** – повторює запити до віддаленого комп'ютера до того часу, поки програма не буде зупинена.
- a** – дозволяє використовувати ім'я комп'ютера як адресу.
- n лічильник** – задається число echo-пакетів. За замовчуванням – 4.
- l довжина** – відправляються echo-пакети, що містять порцію даних заданої довжини. За замовчуванням – 32 байти, максимум – 65527 байтів.

Traceroute (Tracert)

Команда **tracert** визначає маршрут, який проходять пакети до точки призначення в мережі.

Ця програма намагається відстежити маршрут, яким IP-пакет швидше за все буде йти до деякої машини в мережі, запускаючи пробні UDP-пакети з коротким ttl (time to live - і часом життя) і, потім, слухаючи ICMP відповіді “час перевищений” від шлюзу.

Формат команди

```
tracert [-d] [-h лічильник] [-j host-list] [-w timeout]  
target_name
```

Ключі:

- d** – при перевірках маршруту використовувати тільки IP-адресацію без доменних імен.
- h лічильник** – називається максимальна кількість переходів для визначення шляху проходження по маршруту. За замовчуванням дорівнює 30.
- j host-list** – список хостів передбачуваного маршруту.
- w timeout** – максимальний час очікування відповіді.

Команда ipconfig — для для виведення деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS.

Ключ /all відображає всю інформацію, а ключ /? – довідка.

Команда netstat — для для виведення вмісту структур даних, пов'язаних з мережею. Ключ -? – довідка.

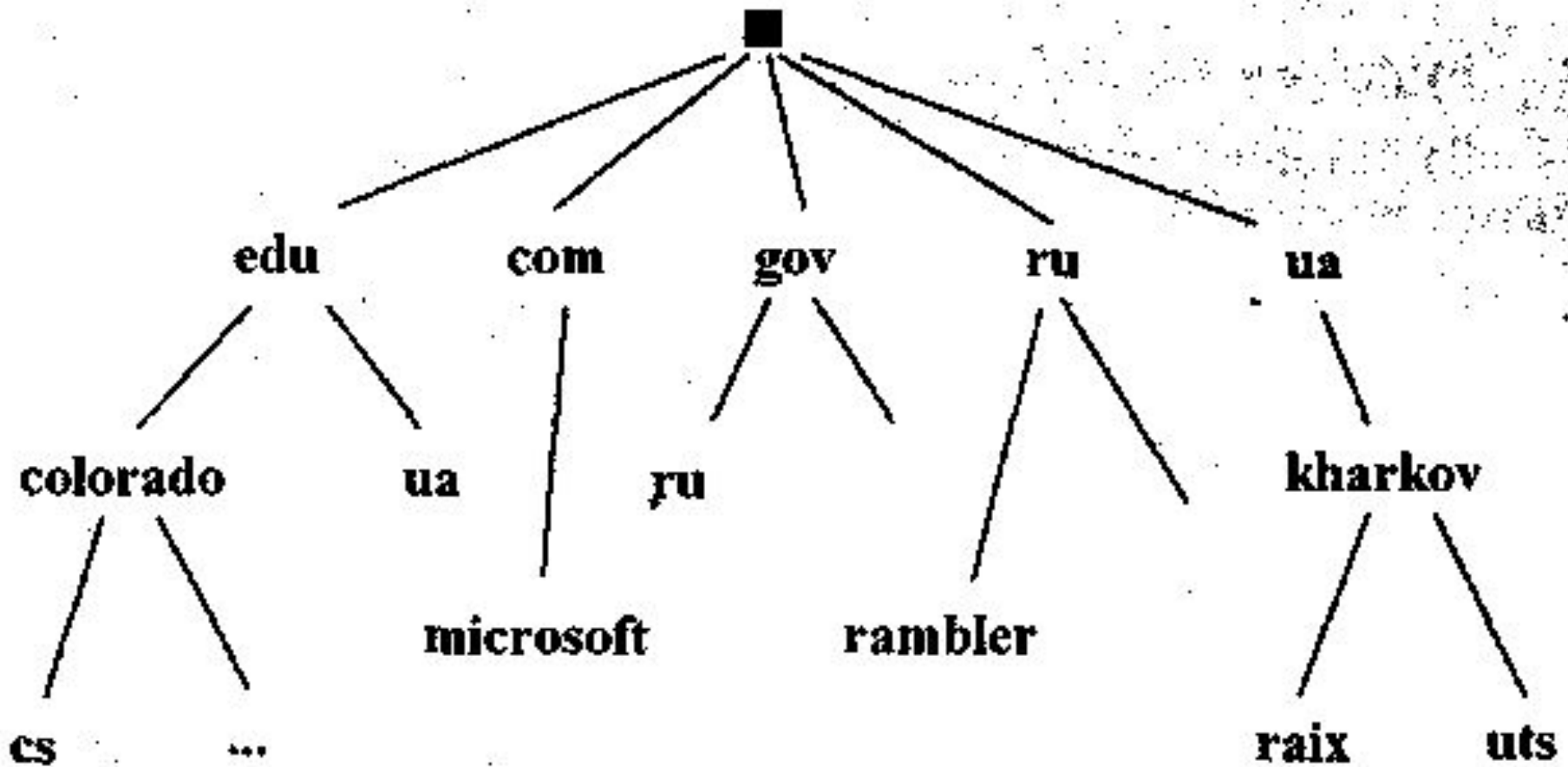
DNS (Domen Name System – система доменних імен)

Ця система для ідентифікації вузлів та мереж у розподіленій комп'ютерній мережі, що об'єднуються у домени. Поняття Домен в системі OSI визначається як зона відповідальності у розподіленій системі DNS. Доменне ім'я - символне ім'я, що служить для ідентифікації областей (одиниць адміністративної автономії в мережі Інтернет) у складі вищестоящої по ієрархії області. Кожна з таких областей називається доменом. Загальний простір імен Інтернету функціонує завдяки DNS - системі доменних імен. Доменні імена дають можливість ідентифікації та адресації інтернет-вузлів і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, інших служб) в зручній для людини текстовій формі.

Для користувача працювати з числовим зображенням IP-адреси незручно, тому йому пропонується більш проста логічна *система доменних імен* DNS (Domain Name System) — послідовність імен доменів, сполучених крапками: microsoft.com, rambler.ru, sumy.a і т. д.

Домен — група вузлів, об'єднаних за деякою ознакою. Система доменів має ієрархічну деревоподібну структуру, тобто кожний домен проміжного рівня містить групу інших доменів. Кореневий домен є умовним, на верхньому рівні розташовано домени різних країн. Ім'я вузла (машини) становить нижній рівень доменного імені та позначається крайнім лівим доменом

Ієрархічна структура доменних імен



IP та DNS — різні форми запису адреси одного й того самого мережного комп'ютера.

Для ідентифікації ресурсів мережі (файлів, Web-сторінок) використовується адреса URL (Uniform Resource Locator — уніфікований покажчик ресурсу), яка складається з трьох частин:

- 1) служба (сервіс), що забезпечує доступ до ресурсу (як правило, це ім'я протоколу). Після імені йдуть двокрапка «:» і два знаки “/” (коса риска): <http://...>;
- 2) DNS ім'я комп'ютера: <http://www.itl.net.ua...>;
- 3) зазначення повного шляху доступу до файлу на даному комп'ютері:
<http://www.itl.net.ua/Files/Archiv/page 1 .html> або <ftp://ftp.netscape.com/pub/book.zip>

Доменні імена не завжди однозначно відповідають IP-адресам. Одній IP-адресі може відповідати кілька різних доменних імен, наприклад, коли різні ресурси фізично розміщені на одному сервері. Може статися, що одне доменне ім'я відповідає кільком IP-адресам, наприклад, коли для деякого ресурсу здійснюється розподіл навантаження між кількома серверами.