Лекція 16

Тема № 6: Глобальні комп’ютерні мережі

Протоколи стеку TCP/IP

План лекції.

1. Міжмережний протокол IP
2. Протокол TCP
3. Інші протоколи стеку
4. Команди контролю з'єднань та маршрутизації
5. Система доменних імен

1. Міжмережний протокол IP

Internet Protocol (IP) створений для використання в об'єднаних системах комп'ютерних комунікаційних мереж з комутацією пакетів.

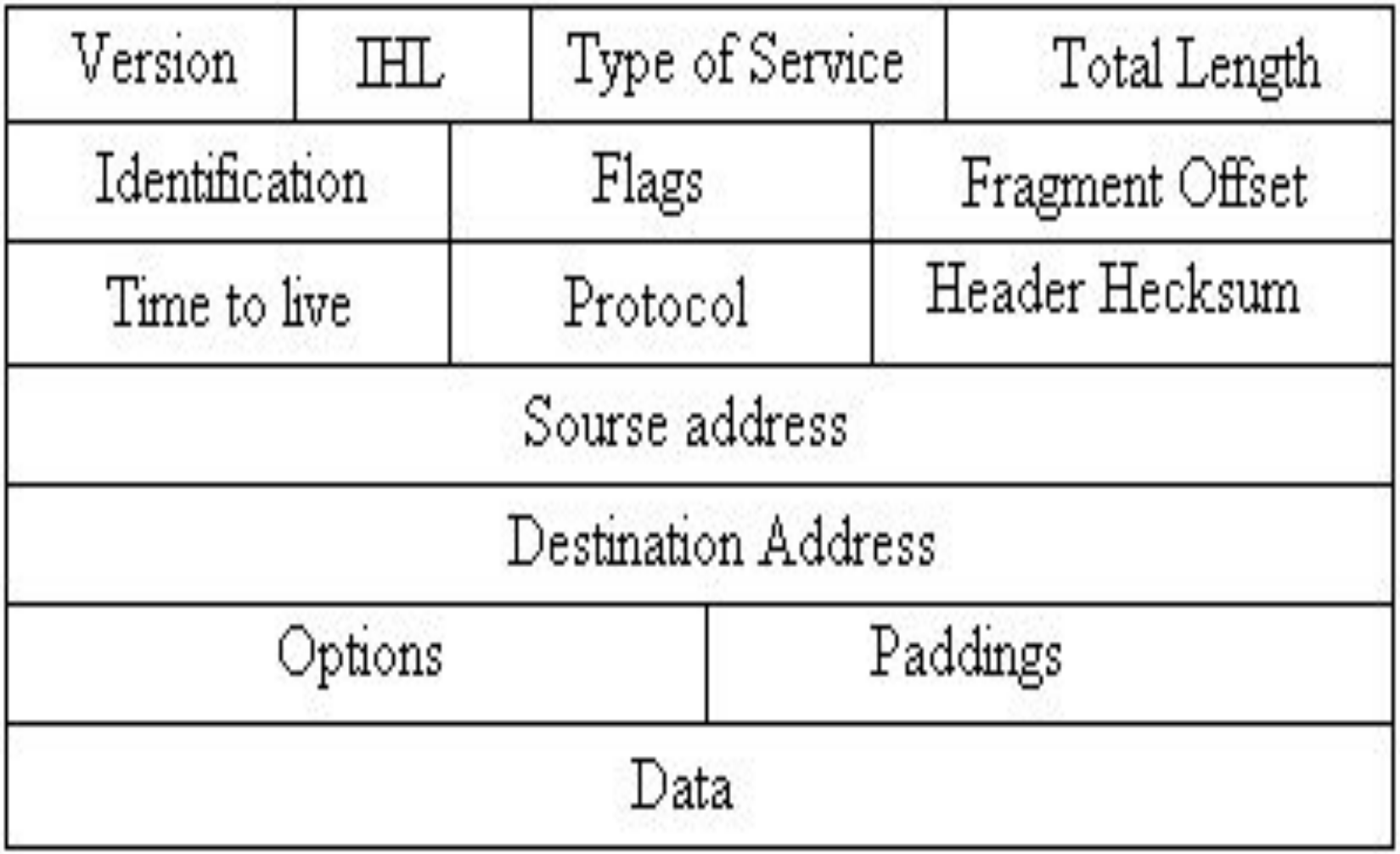
Він *забезпечує передачу блоків даних*, ***датаграм*** *від відправника до одержувачів*, де відправник та одержувач є хост-комп'ютерами, які ідентифікуються адресами фіксованої довжини.

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.

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.

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.

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 утворять 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.

2. Протокол TCP

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

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

TCP займає в багаторівневій архітектурі протоколів нішу безпосередньо над IP-протоколом, що дозволяє протоколу TCP відправляти й одержувати сегменти інформації змінної довжини, укладені в оболонку IP-датаграм.

Датаграма надає дані для адресації відправника й одержувача TCP-сегментів у різних мережах. IP-протокол також здійснює будь-яку фрагментацію й збирання сегментів TCP, які необхідні для здійснення передачі й доставки через безліч мереж і проміжних шлюзів.

IP-протокол також обробляє інформацію про пріоритет, класифікацію безпеки, а також здійснює розмежування TCP 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.

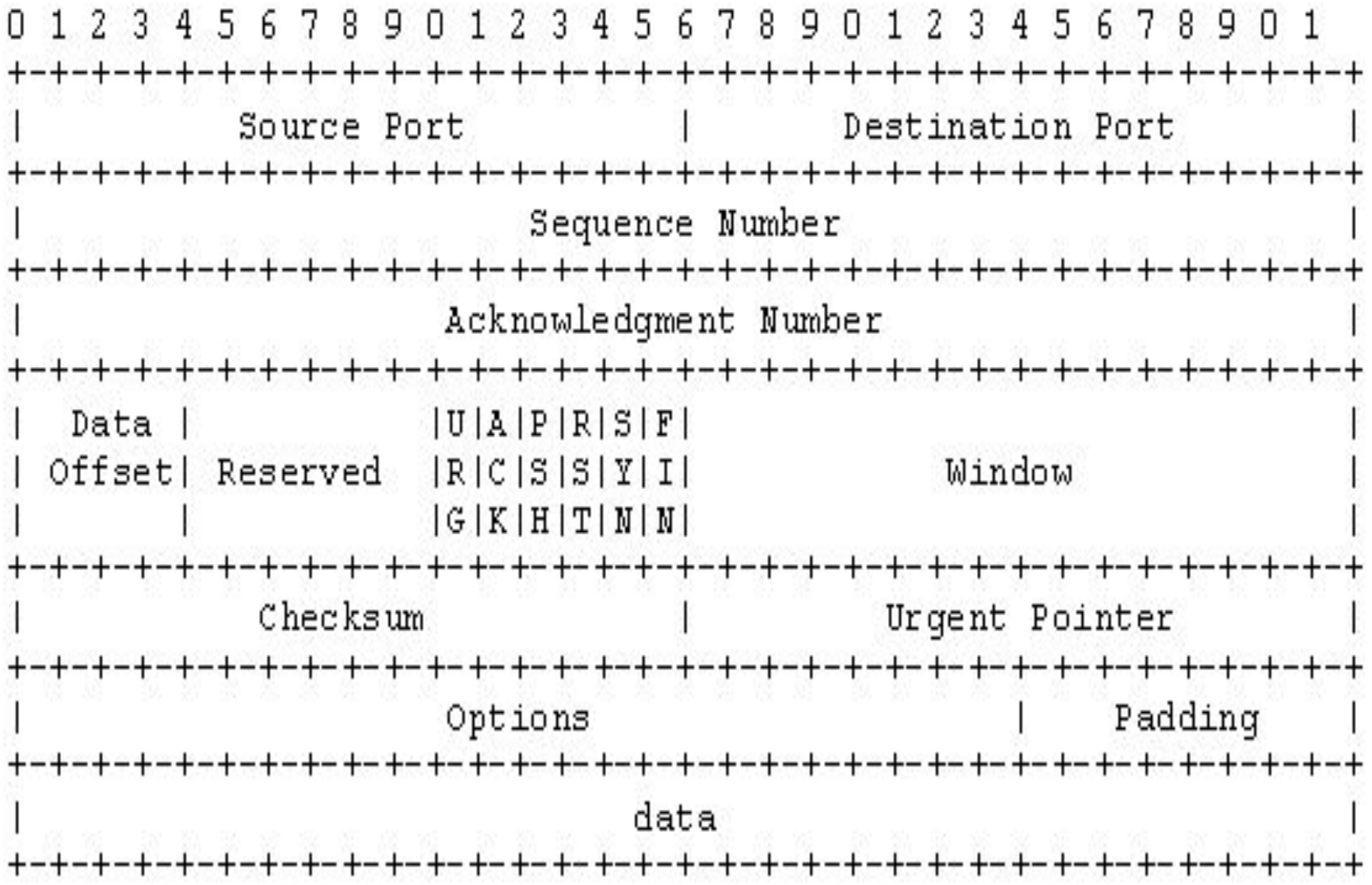
Формат TCP-заголовка

Передавання TCP сегментів здійснюється у вигляді IP-датаграм. Заголовок TCP-сегмента в Інтернет-протоколі має кілька інформаційних полів, включаючи адреси хост-комп'ютерів, що відправляють і приймають дані. TCP-заголовок іде за IP-заголовком і доповнює його інформацією, яка є специфічною для TCP-протоколу.

Такий розподіл допускає використання на рівні хост-комп'ютерів протоколів, інших, ніж TCP.

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.

3. Інші протоколи стеку

Протокол датаграм користувача (UDP)

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 інкапсулюємого 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 пристрої 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 ехо-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, шо 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 видається за можливе: наприклад, якщо хост-одержувач недосяжний.

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

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

4. 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;

порівняння кожного отриманого пакету 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 виведення деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS.

Ключ /all відображає всю інформацію,

а ключ /? – довідка.

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

5. 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.

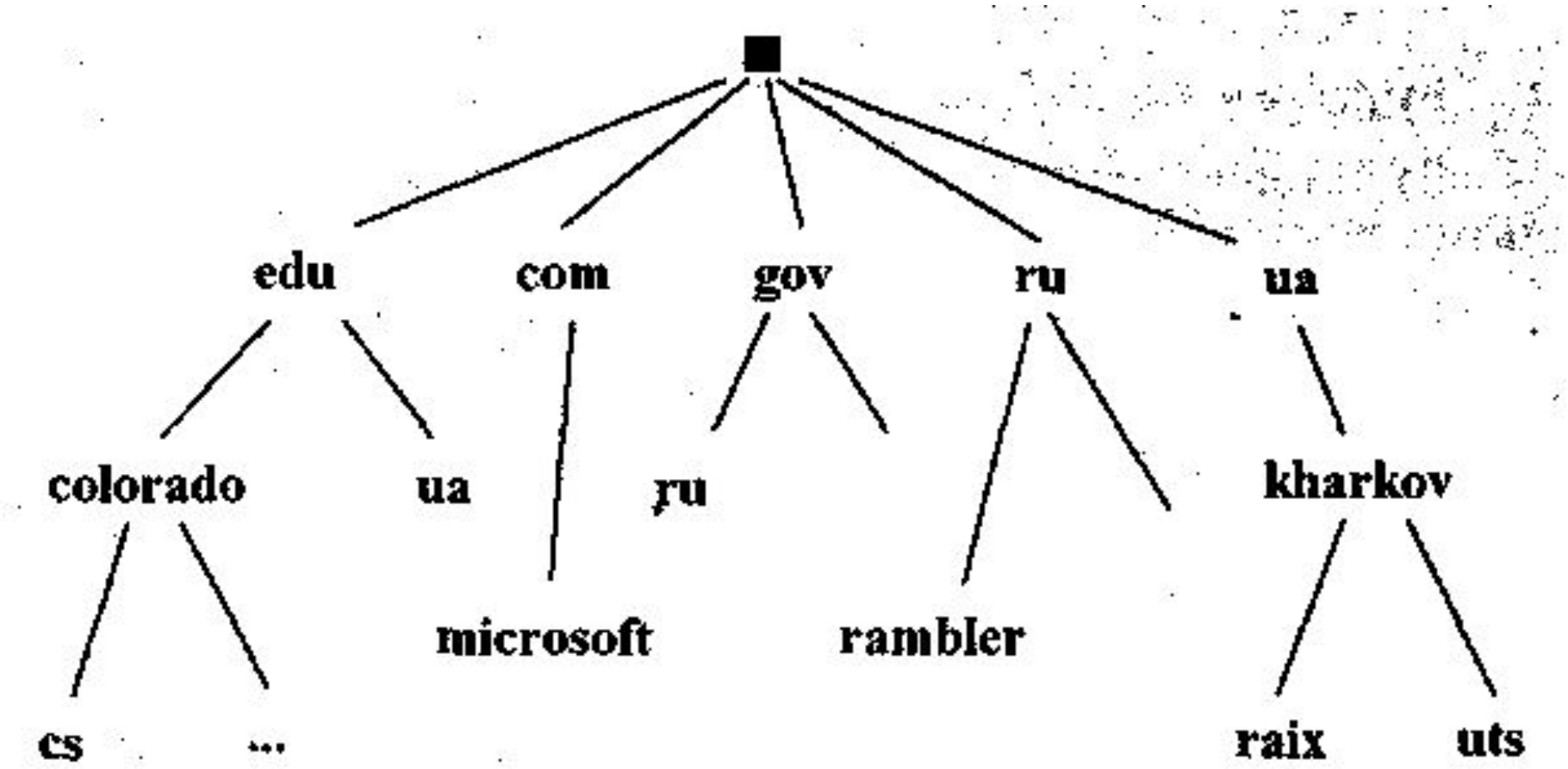
Доменне ім'я - символьне ім'я, що служить для ідентифікації областей (одиниць адміністративної автономії в мережі Інтернет) у складі вищої по ієрархії області. Кожна з таких областей називається доменом.

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.