Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

на тему: **" Безпека мережевих протоколів Internet "**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки»)

ПЛАН ЛЕКЦІЇ

1. Протоколи прикладного рівня.
2. Транспортні протоколи.
3. Протоколи IP.
4. Протоколи керування мережею.

ЛІТЕРАТУРА

1. **Анин Б.** Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.

2. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.

3. **Kahn D.** The Codebreakers: The Story of Secret Writing. - N.Y.: MacMillan, 1967. – 1164 p.

4. **Мельников В.В.** Защита информации в компьютерных системах. – М.: Финансы и статистика: Эмектроинформ, 1997. – 368 с.

1. Протоколи прикладного рівня.

Аналізуючи безпеку протоколів, слід чітко розуміти різницю між протоколами та їх реалізаціями. Протокол - це набір правил і домовленостей, яких дотримуються сторони під час взаємодії через мережу. Ці правила мають бути оформлені у вигляді документа, який визнають розробники програмного забезпечення. Документ може мати силу стандарту, а може бути поданий як пропозиції або рекомендації. Документи, на основі яких побудовано Інтернет і згідно з якими він функціонує, називають RFC (Request For Comments - запит коментарів). Кожний документ RFC має свій унікальний номер. Організація, яка координує діяльність із вцрішення технічних проблем, пов'язаних з Інтернетом, має назву IETF (Internet Engineering Task Force - комітет з інженерних питань Інтернету). Саме ця організація і веде облік RFC.

Реалізація протоколу - це програма з усіма притаманними їй вадами: неточною або неповною реалізацією специфікацій протоколу, документованими або недокументованими додатковими функціями, помилками в алгоритмах і в реалізаціях алгоритмів (помилками програмування).

Передусім потрібно зауважити, що дві найважливіші служби Інтернету- глобальну гіпертекстову систему (Веб), реалізовану на протоколі HTTP, та електронну пошту, основними протоколами якої є SMTP, POP3, IMAP4, - не буде описано під час розгляду безпеки протоколів прикладного рівня. Безпеці цих служб присвячено окремий розділ.

Протокол Telnet

Почнемо з класичних протоколів Інтернету і насамперед із Telnet – протоколу взаємодії, що підтримує двосторонній обмін окремими символами (байтами) і віртуальні термінали. Стандарт протоколу Telnet описано в RFC-854-86.

Термінал, яким він був на початку своєї еволюції, - це апаратний пристрій, що складався з пристрою введення інформації (клавіатури) і пристрою виведення інформації (телетайпа, який у подальшому замінив монітор). Телетайп – це дистанційно керований пристрій друкування, фактично - електромеханічна друкарська машинка, здатна друкувати послідовність символів, що надходить до неї через інформаційний кабель. Саме від телетайпів успадковано терміни «переведення рядка» (Line Feed, LF) і «повернення каретки» (Carriage Return, CR). Монітор спочатку використовували лише як телетайп, тому основною його функцією також було послідовне друкування інформації, хоча користувачі могли вже видаляти помилково надруковані символи, виконувати спрощені операції переведення курсору (який замінив каретку пристрою друкування) у будь-яку позицію на екрані. Згодом з'явилися додаткові можливості, на кшталт змінення кольору і фону шрифту та його кодової таблиці, завантаження додаткових наборів символів і багато інших (про графічні термінали зараз не йдеться). При цьому термінал продовжує бути байт-орієнтованим (символьним) пристроєм, який передає комп'ютеру послідовність байтів (кодів натиснутих клавіш) і приймає від нього послідовність байтів (кодів символів для виведення на екран). Коди символів було стандартизовано. До кожного стандартного набору крім латинської абетки входили ще й деякі спеціальні (службові) символи. Зі стандартних наборів кодів символів найбільшого поширення набув код ASCII (American Standard Code for Information Interchange - американський стандартний код для обміну інформацією). Також поширеним є код EBCDIC, що застосовують здебільшого на великих комп'ютерах (мейнфреймах).

Команди термінала передавалися в основному потоці виведення, а щоб їх можна було відрізнити від символів, які мали бути надрукованими, команди оформлювалися в так звані ESC-послідовності (ескейп-послідовності). ESC-послідовність починається зі службового символу ESC, за яким розташовано один чи кілька символів, що складають команду, яка може мати параметри. У результаті розвитку систем команд терміналів виникла потреба в їх стандартизації, відтак 'явилася низка стандартів терміналів: ANSI, VT52, VT100 та інші.

Зв'язок термінала з комп'ютером не потребує великої швидкості обміну даними, і тому здебільшого його реалізовували на основі стандартного інтерфейсу послідовного передавання даних RS-232. Підключення віддаленого термінала з використанням модемів і звичайних аналогових телефонних ліній жодних проблем не викликало.

Коли комп'ютери почали об'єднувати у мережу, постало питання: як забезпечити взаємодію комп'ютерів за максимального використання наявних технологій? І тут дуже зручним виявився протокол Telnet, який забезпечував двосторонній обмін байтами, аналогічний обміну термінала з комп'ютером. Клієнт Telnet - це програма, яка підтримує інтерфейс командного рядка і систему команд деякого стандартного термінала (або навіть багатьох різних стандартних терміналів). Як правило, у багатовіконних графічних середовищах клієнт Telnet запускається в інтерфейсі командного рядка (який часто не зовсім коректно називають консоллю). Сервер Telnet за стандартом займає TCP-порт 23.

Telnet - дуже давній протокол; його було розроблено ще наприкінці 60-х років минулого століття. Тоді це був, напевно, найважливіший з усіх прикладних протоколів. Хоча протокол Telnet зараз не є таким значущим, його використовують і дотепер, зокрема для віддаленого керування UNIX-серверами і мережним обладнанням.

Протокол FTP

Протокол FTP (File Transfer Protocol - протокол передавання файлів) є одним із найдавніших протоколів стека TCP /IP і найпоширеніших в Інтернеті. Якщо приблизно десять років тому традиційно писали, що «протокол FTP не менш поширений в Інтернеті, ніж Telnet~, то сьогодні можна впевнено говорити про те, що протокол FTP є набагато популярнішим, позаяк не має адекватної альтернативи (на відміну від Telnet). Інша річ, що на зміну традиційним інтерфейсам і прийомам роботи з FTP прийшли нові. До певної міри частину функціональності FTP реалізують за допомогою протоколу HTTP, але доступ до FTP-серверів зручніше здійснювати з клієнтів FTP. Протокол FTP описано у RFC-959.

Обмін даними у протоколі FTP здійснюється з використанням транспортного протоколу TCP. Обмін побудовано за принципом технології клієнт-сервер. На рис. 1 зображено модель протоколу FTP.

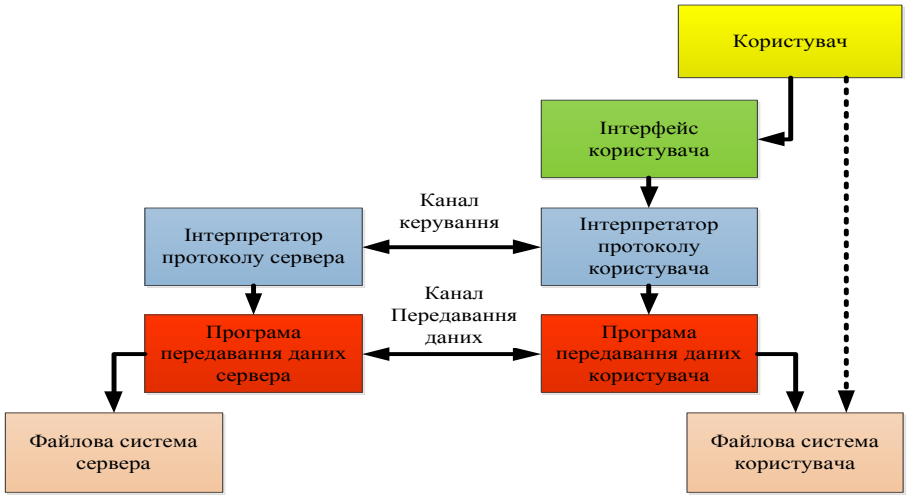

Рис. 1. Модель протоколу FTP

2. Транспортні протоколи.

Протоколами транспортного рівня у стеку TCP /IP є UDP (User Datagrams Protocol - протокол користувацьких дейтаграм) і TCP (Transmission Control Protocol - протокол керування передаванням). Протокол UDP - дуже простий протокол, який працює без встановлення з'єднання, не гарантує доставлення даних, не має засобів ідентифікації відправника. Протокол TCP встановлює віртуальний канал передавання даних і забезпечує базові функції контролю за потоком даних.

Обидва протоколи на своєму рівні ідентифікують програму-відправника пакета і програму-одержувача. Така ідентифікація здійснюється через так звані номери портів. Слід розуміти, що порти на транспортному рівні не мають нічого спільного з апаратними портами введення-виведення. Це два незалежні набори 16-розрядних числових ідентифікаторів, один - для UDP, другий - для TCP. Для спрощення процедури встановлення з'єднань за багатьма прикладними службами закріплено добре відомі номери портів. Їх облік веде організація IANA (Internet Assigned Numbers Autority - Центр присвоєння номерів Інтернету)

Протокол UDP

UDP - це дуже простий дейтаграмний протокол, стандарт якого визначено у RFC 768. Основні функції протоколу - мультиплексування і демультиплексування інформаційних потоків. Тобто цей протокол дає змогу передавати в мережу дані одночасно від різних програм і приймати з мережі дані для різних програм. Ідентифікація програм-відправників і програм-одержувачів здійснюється за номерами UDP-портів. Заголовок пакета (дейтаграми) UDP має довжину 8 байт. На рис. 2 наведено формат заголовка.

16 біт	**16 біт**
Номер порту відправника	Номер порту одержувача
16 біт	**16 біт**
Довжина повідомлення	Контрольна сума

Рис. 2. Формат заголовка UDP-пакета

Протокол TCP

Протокол TCP, на відміну від UDP, є протоколом із встановленням логічного з'єднання; його описано в RFC 793. У межах з'єднання здійснюються реєстрація послідовності пакетів, підтвердження доставлення кожного пакета, керування потоком пакетів, повторне передавання спотворених пакетів. Деякі із зазначених функцій надають сервіс із захисту від підміни суб'єктів з'єднання. Саме тому деякі протоколи прикладного рівня, зокрема FTP, Telnet, HTTP, що надають користувачам віддалений доступ, застосовують саме TCP як транспортний протокол. Більше того, TCP як транспортний протокол використовується одним з основних протоколів маршрутизації в Інтернеті - BGP. Деякі служби, наприклад DNS, можуть використовувати як транспорт і UDP, і TCP. Проте рекомендують застосовувати саме протокол TCP для підвищення стійкості служби проти атак. Далі ми розглянемо переваги та недоліки протоколу TCP.

За прийнятою термінологією, порцію даних, що передається як одне ціле, у протоколі TCP називають сегментом. Але ми використовуватимемо більш вживаний термін пакет. Пакет TCP має заголовок мінімум 20 байтів завдовжки, після якого розміщуються дані. На рис. 3 наведено формат такого заголовка.

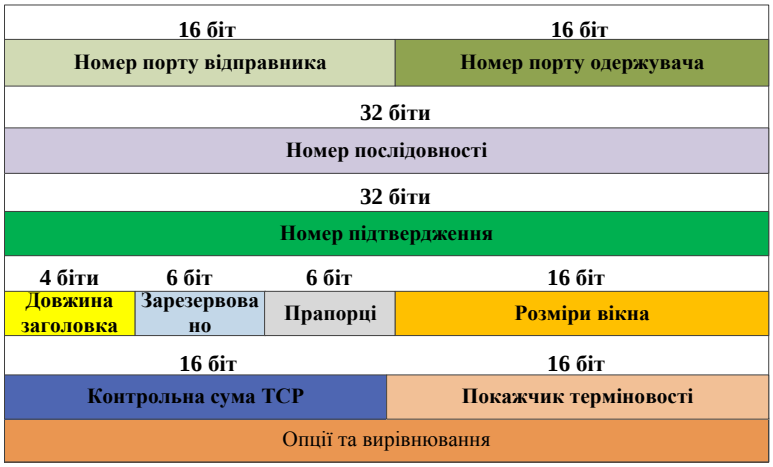

Рис. 3. Формат заголовка TCP-пакета

В заголовку присутні командні біти - прапорці, за допомогою яких здійснюється керування з'єднанням. Передбачено 6 прапорців:

- URG (Urgent Pointer Field Significant) - термінове повідомлення;
- ACK (Acknowledgment Fi~ld Significant) - квитанція на сегмент, який було прийнято;
- PSH (Push Function) - запит на відправлення повідомлення без очікування заповнення буфера;
- RST (Reset the eonnection) - запит на розірвання з'єднання;
- SYN (Synchronize Sequence Number) - повідомлення, яке використовується для синхронізації лічильників даних, що передаються, під час встановлення з'єднання;
- FIN (No More Data from Sender) - ознака передавання останнього байта переданих даних.

Найбільше значення для керування потоком інформації через TCP-з'єднання мають два 32-розрядні поля: Номер послідовності та Номер підтвердження. Ці поля виконують роль ідентифікаторів пакета, з'єднання і суб'єкта з'єднання; їх також використовують як лічильники пакетів.

3. Протоколи IP.

До мережного рівня належить базовий протокол IP (Internet Protocol), який, власне, і відповідає за доставлення пакета (дейтаграми) кінцевому адресату в глобальній мережі. Пакет проходить через різні мережі, що у загальному випадку можуть базуватися на різних технологіях. Окрім протоколу IP у стеку TCP /IP до мережного рівня належать протокол керування ICMP, а також протоколи маршрутизації.

Сьогодні співіснують дві версії протоколу: IPv4 і та IPv6. Протокол IPv4 активно використовують уже понад 20 років. Саме на ньому побудовано Інтернет, який ефективно працює й дотепер. Слід визнати, що протокол IPv4 має суттєві недоліки, які роблять можливими деякі атаки в Інтернеті. Протокол IPv6 сильно відрізняється від IPv4, і тому перехід на нього є непростою задачею.

Призначення й можливості протоколу IPv4

Основним завданням протоколу IP як протоколу мережного рівня моделі OSI є передавання і маршрутизація повідомлень між вузлами Інтернету. Протокол описано в RFC 791. На рівні протоколу IP відпрацьовується передавання пакета між мережами, для чого передбачено низку засобів. По-перше, це система глобальної адресації, по-друге - здійснення контролю за часом життя пакета, що дає змогу виявити та відкинути пакети, які через помилки у маршрутизації надто довго блукають мережею, і по-третє - можливість динамічної фрагментації пакетів.

І ще одне - підтримка якості обслуговування, що дає можливість задати для пакета бажані пріоритети під час його передавання: мінімальний час затримки, максимальну швидкість каналу, найвищі гарантії щодо успішного доставлення. Слід визнати, що останню можливість тривалий ·час не використовували, вона й наразі не має достатньої підтримки.

Зауважимо, що IP-протокол відповідає лише за притаманні йому функції. Так, для передавання пакета всередині кожної з мереж, через які відбувається його доставляння, IP-протокол звертається до засобів нижчого (канального) рівня. А щодо таких питань, як гарантоване доставлення пакета, його повторне передавання, - то це справа засобів вищого (транспортного) рівня.

Формат заголовка

На рис. 5 показано формат заголовка IPv4.

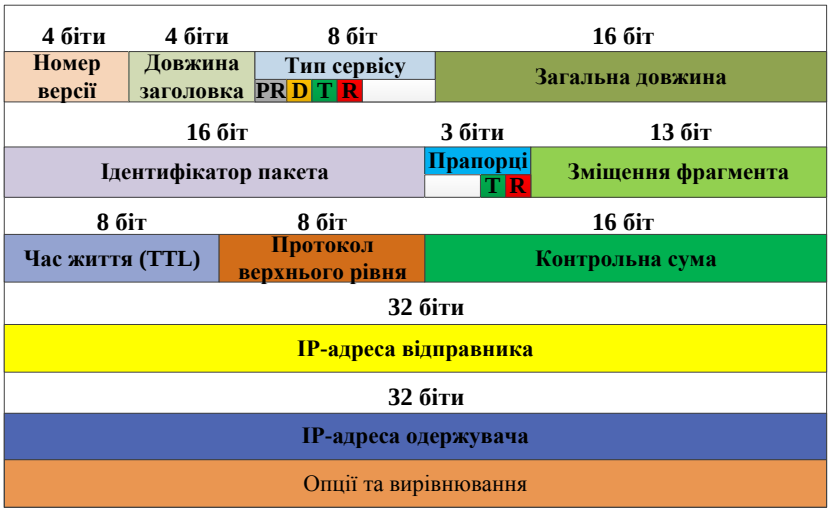

Рис. 5. Формат заголовка IP-пакета

У полі **Номер версії** вказується версія протоколу, а в полі **Довжина заголовка** - довжина заголовка у 32-розрядних словах. Найменша довжина - 20 байт, тобто 5 слів. Найбільша можлива довжина - 60 байт, або 15 слів (максимальне значення, яке можна задати у 4-розрядному полі).

Поле **Опції та вирівнювання** має змінну довжину - від О до 40 байт, причому опції можуть мати будь-яку довжину, а вирівнювання забезпечує заповнення 32-розрядних слів. Поле **Тип сервісу** призначене для керування якістю обслуговування (Quality of Service, QoS). З точки зору безпеки це поле може нас зацікавити тим, що в ньому є два зарезервовані біти, які не задіяні, але саме їх можна використати для організації прихованого каналу витоку інформації (адже за стандартом значення цих бітів мають дорівнювати нулю, проте немає впевненості, що за цим у мережі хтось буде здійснювати контроль).

У полі **Загальна довжина** задається повна довжина пакета у байтах разом із його заголовком. Очевидно, це значення не має перевищувати 65 535 байт. Факт отримання IP-пакета, який перевищує максимально припустиму довжину, може викликати проблеми у системі, про що йтиметься далі. До речі, рекомендована довжина пакета значно менша - 576 байт. Стандарт вимагає, щоб усі хости були здатні приймати пакети такого розміру. У мережах Ethernet довжину кадру обмежено 1500 байтами, тому IP-пакети, що вкладають у кадри Ethernet, мають саме такий розмір.

Далі йдуть поля, дані в яких пов'язані із забезпеченням динамічної фрагментації пакетів.

За полями фрагментації (32 розряди) розміщено такі поля:

- *Час життя* (Time To Live, TTL) - значення цього поля встановлюється у межах 1-255, а далі зменшується на одиницю після проходження пакета через кожний маршрутизатор на його шляху (пакет із TTL=О знищується);
- *Протокол верхнього рівня* (який іноді називають IP-протоколом) – ідентифікатор протоколу, що передав пакет на мережний рівень для доставляння. Значення ідентифікаторів наведено в документі IANA «Protocol Numbers» (раніше ці дані розповсюджувались у спеціальному RFC «Assigned Numbers», останнім з яких був RFC-1700). Приклади: TCP (6), UDP (17), ICMP (1).
- *Контрольна сума* (16 розрядів) - підраховується лише на транзитних вузлах. Оскільки деякі поля заголовка змінюються під час передавання пакета, щоразу перераховується і контрольна сума.

Далі йдуть **IP-адреси джерела і пункту призначення**. За ними в заголовку може бути розміщено необов'язкові опції, які доповнюються нулями для вирівнювання за межею 32-розрядного слова. Саме в них може бути визначено вимоги до керування маршрутизацією та (або) контролю за маршрутом пакета (маршрутизація від джерела, запис фактичного маршруту). Ці можливості протоколу не завжди підтримуються.

Прапорець **DF** (Don't Fragment - не фрагментувати) забороняє фрагментацію пакета на транзитному вузлі, відтак, якщо такий пакет не можна передати у наступну мережу (коли його довжина перевищує відповідне значення MTU), його просто знищують, надсилаючи повідомлення про це вузлу-відправнику.

Прапорець **MF** (More Fragments - додаткові фрагменти) вказує на те, що фрагмент не є останнім, і їх збирання може тривати.

Поле **Ідентифікатор пакета** - значення цього поля унікальне для кожного окремого пакета, але однакове для всіх його фрагментів. Воно дає змогу виявити і зібрати разом усі фрагменти пакета.

Поле **Зміщення фрагмента** визначає положення фрагмента в пакеті. Необхідно звернути увагу на те, що це поле має 13 розрядів, тоді як довжина всього пакета (65 535 байт) описується 16-розрядним полем. Це свідчить про те, що зміщення фрагмента задається не в байтах, а в так званих параграфах, що мають розмір 8 байт. На жаль, на таку «дрібницю~ часто не звертають увагу, і через це з'явився один із міфів про фактично неіснуючу загрозу, пов'язану з маніпуляціями зі зміщенням фрагментів.

Можливості, закладені у протокол IPv6

Активна робота із створення нової версії протоколу IP розпочалася в 1992 році. Головне, що спонукало суттєво переглянути наявний протокол IPv4, - це вади адресації: недостатній адресний простір і відсутність (точніше сказати, катастрофічна нестача) структурування адреси (яку поділяли лише за номером мережі та номером вузла у мережі) та будь-якої системи в географії адрес.

Стандарти, які визначають специфікації IPv6, було прийнято в 1998 році. Це RFC-2460, що визначає загальну архітектуру IPv6 та низка інших. Деякі з них у подальшому було змінено. Наприклад, чинним наразі документом, що визначає систему адресації IPv6, є RFC-4291, прийнятий у 2006 році.

Адреса IPv6 має 128 розрядів (16 байт). Таку велику довжину адреси було обрано не для того, аби мати у запасі неосяжну кількість адрес, а для того, щоб впровадити ієрархічну систему побудови адреси. Адреса має чотири рівні ієрархії, причому три верхніх рівні призначено для ідентифікації мережі, а останній, нижній, - для ідентифікації вузла у мережі. Завдяки багаторівневій ієрархії адреса IPv6 підтримує технологію агрегації адрес (Classless InterDomain Routing, CIDR). Суттєво вдосконалено також групову адресацію і введено новий тип адрес - anycast (пакет доставляється будь-якому одному вузлу з цією адресою; такі адреси призначають лише інтерфейсам маршрутизаторів).

Отже, в IPv6 визначено адреси трьох основних типів: unicast, multicast, anycast. Тип адреси задається префіксом формату, який визначають кілька старших бітів адреси. Наприклад, глобальна унікальна адреса (основний підтип unicast-адрес) має таку структуру, як на рис. 6.

3	**13**	**8**	**24**	**16**
Префікс формату (FP)	Агрегування верхнього рівня (TLA)	Зарезервовано	Агрегування нижнього рівня (NLA)	Агрегування місцевого рівня (SLA)
64				
Ідентифікатор інтерфейсу (Interface ID)				

Рис. 6. Структура глобальної унікальної адреси IPv6

Агрегація верхнього рівня (TLA) ідентифікує великих провайдерів найвищого рівня (автономні системи Інтернету). Зарезервовані розряди в подальшому може бути використано саме для розширення цього поля, але його розмір (13 розрядів) свідомо було обрано порівняно невеликим для прискорення процесу маршрутизації в магістральних маршрутизаторах.

Агрегація наступного рівня (NLA) ідентифікує середніх або дрібних провайдерів, причому це поле дає змогу провайдерам верхнього рівня впроваджувати багаторівневу ієрархію провайдерів у своїх автономних системах.

Агрегація місцевого рівня (SLA) призначене для адресації підмереж окремої організації (абонента глобальної мережі), наприклад корпоративної мережі. Відтак полем SLA розпоряджається адміністратор локальної мережі.

Нарешті, **поле ідентифікатора інтерфейсу** має достатній розмір для розміщення в ньому MAC-адреси із префіксом, адреси X.25 або інших адрес наявних мережних технологій. Це надає можливість замість локальних адрес на мережному рівні використовувати адреси канального рівня та взагалі відмовитися від протоколу ARP, щоб уникнути притаманних йому вад, а також організувати повністю автоматизовану конфігурацію кінцевих вузлів, оскільки програмне забезпечення вузла отримує MAC-адреси чи інші аналогічні апаратні адреси від апаратури, а мережні префікси їм надсилає маршрутизатор. Повністю змінено також структуру заголовка IP. Ті можливості, одну частину яких у IPv4 було вбудовано в основний

заголовок (фрагментація), а другу - приховано в опціях, які не завжди і не всюди підтримуються (маршрутизація від джерела та багато інших можливостей), тепер оформлено як окремі заголовки (вкладені один в один). Обов'язковим є лише один, основний заголовок, формат якого показано на рис. 7.

Цей заголовок має фіксовану довжину - 40 байт. Поле Наступний заголовок (Next Header) визначає тип наступного заголовка. Це може бути інший заголовок IPv6 або заголовок іншого протоколу, як і в IPv4: TCP, UDP, ICMP, OSPF, RIP тощо. Зауважимо, що майже всі додаткові заголовки IPv6 обробляються лише на кінцевих вузлах.

Рис. 7. Формат основного заголовка IPv6

Визначено такі заголовки IPv6:

Routing (Маршрутизація) - заголовок для задавання повного маршруту в разі маршрутизації від джерела;

Fragmentation (Фрагментація) заголовок, що містить інформацію про фрагментацію пакета;

Authentication (Автентифікація) - заголовок, що містить інформацію для автентифікації кінцевих вузлів і забезпечення цілісності повідомлення;

Encapsulation (Інкапсуляція) - заголовок, який містить інформацію, необхідних для забезпечення конфіденційності повідомлення шляхом шифрування;

Hop-by-Hap Options - опції оброблення пакета в режимі Hop-by- Hap;

Destination Options - додаткова інформація для вузла призначення.

Дуже важливою інновацією IPv6 є вбудовані засоби безпеки, шо передбачають інкапсуляцію та автентифікацію. Вони реалізовані у протоколі, який дістав назву IPSec, і хоча останній є складовою IPv6, він у своєму впровадженні значно випереджає IPv6. Якщо

протокол IPv6 ще дуже мало використовують у мережах, то IPSec вже де-факто став стандартом для побудови захищених мереж з передаванням трафіку через глобальну мережу.

4. Протоколи керування мережею.

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.

Протокол описано у RFC 792, деякі доповнення було зроблено у RFC- 4884. 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 та 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 доставлення даних не є обов'язковою.

Саме для відсилання таких нескладних запитів і отримання відповідей і призначений протокол ICMP.

Крім того, ICMP використовують для обміну інформацією між двома хостами або хостом і маршрутизатором у разі виникнення помилок. Дійсно, в протоколах, орієнтованих на встановлення з'єднання, наприклад у TCP (транспортний рівень) або LLC2 (канальний рівень), передбачено механізми сповіщення вузла, що здійснює передавання даних, про виникнення помилок і деякі їхні причини. Але дейтаграмні протоколи (UDP), а також протоколи мережного рівня (IP) таких можливостей не мають, тому й використовують ICMP.

Місце ICMP у моделі OSI та в стеку TCP/IP

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. Власне, спочатку протокол ICMP взагалі розглядали як невід'ємну частину протоколу IP. Протиставляти трафіки ICMP і IP некоректно, тому що пакет ICMP інкапсульовано в пакет IP.

Протокол SNMP

Протокол SNMP (Simple Network Management Protocol - простий протокол керування мережею) і пов'язану з ним концепцію SNMP MIB (Management Information Base - база керуючої інформації) було розроблено як тимчасове рішення для керування маршрутизаторами Інтернету. Але виявилося, що це рішення - простий, ефективний і гнучкий'протокол, який має великий потенціал для розширення.

Через це протокол SNMP набув значного поширення та використовується

й дотепер для керування мережним обладнанням локальних і глобальних мереж майже всіх видів. Хоча під час розроблення цей протокол було однозначно орієнтовано на мережі TCP /IP, зараз його іноді використовують і для телекомунікаційного обладнання (аналогові модеми, модеми ADSL, комутатори ATM тощо), тобто там, де, як правило, перевагу надають альтернативному протоколу CMIP (останній орієнтований на стек ISO та належить до стандартів ITU-T). Також є реалізації SNMP для мереж IPX/SPX, хоча сьогодні такі мережі вже не актуальні.