МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять
з навчальної дисципліни «Мережеві технології»
вибіркових компонент
освітньо-професійної програми першого (бакалаврського) рівня вищої освіти

125 «Кібербезпека (поліцейська діяльність у кіберсфері)»

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.10.2020 № 10

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 21.10.2020 № 6

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 22.10.2020 № 6

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 20.10.2020 № 19)

Розробники:
1. Доцент кафедри, к.т.н., доцент Євстрат Д. І.

Рецензенти:
1. Завідувач кафедри інформаційних технологій Харківського національного університету Повітряних Сил імені Івана Кожедуба, к.т.н., доцент Соловйова О. І.
2. Провідний науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій ХНУВС, к.т.н., доцент Мордвинцев М. В.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Семестр № 7								
Тема № 1: Основи побудови комп'ютерних мереж.	60	12		6	12	30	Конспект лекцій. Література 7-14	
Тема №2. Локальні комп'ютерні мережі.	60	12		6	12	30	Конспект лекцій. Література 7-14	
Всього за семестр № 7:	120	24		12	24	60		Залік
Семестр № 8								
Тема №3. Глобальні комп'ютерні мережі.	90	12		6	12	60	Конспект лекцій. Література 7-17	
Тема №4. Intemet/Intranet технології.	90	12		6	12	60	Конспект лекцій. Література 7-14	
Всього за семестр № 8:	180	24		12	24	120		Екзамен
Всього по дисципліні	300	48		24	48	180		Екзамен

3. Методичні вказівки практичних занять

Тема№1: Основи побудови комп'ютерних мереж.

Практичне заняття 1: Утиліти для комп'ютерних мереж (Windows)

Навчальна мета заняття: освоїти роботу з утилітами TCP/IP, що використовується в наступних роботах..

Час: 2 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **Вправа 1. Здобуття довідкової інформації по командах**
2. **Вправа 2. Здобуття імені хоста**
3. **Вправа 3. Вивчення утиліти ipconfig**
4. **Вправа 4. Тестування зв'язку за допомогою утиліти ping**
5. **Вправа 5. Визначення дороги IP-пакета**
6. **Вправа 6: Перегляд ARP-^ша**
7. **Вправа 7. Здобуття інформації про поточні мережеві з'єднання і**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.

2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

1. Діагностичні утиліти TCP/IP.

До складу TCP/IP входять діагностичні утиліти, призначені для перевірки конфігурації стека і тестування мережевого з'єднання.

Утиліта	**Вживання**
arp	Виводить для перегляду і зміни таблицю трансляції адрес, використовувану протоколом дозволу адрес ARP (Address Resolution Protocol - визначає локальна адреса по IP-адресу)
hostname	Виводить ім'я локального хоста. Використовується без параметрів.
ipconfig	Виводить значення для поточної конфігурації стека TCP/IP: IP-адрес, маску підмережі, адреса шлюзу за умовчанням, адреси WINS (Windows Internet Naming Service) і DNS (Domain Name System)
nbtstat	Виводить статистику і поточну інформацію по NETBIOS, встановленому поверх TCP/IP. Використовується для перевірки стану поточних з'єднань NETBIOS.
netstat	Виводить статистику і поточну інформацію по з'єднанню TCPЯP.
nslookup	Здійснює перевірку записів і доменних псевдонімів хостов, доменних сервісів хостов, а також інформації операційної системи, шляхом запитів до серверів DNS.
ping	Здійснює перевірку правильності конфігурації TCP/IP і перевірку зв'язку з видаленим хостом.
route	Модифікує таблиці маршрутизації IP. Відображує вміст таблиці, додає і видаляє маршрути IP.
tracert	Здійснює перевірку маршруту до видаленого комп'ютера шляхом відправки ехо-камера-пакетів протоколу ICMP (Internet Control Message Protocol). Виводить маршрут проходження пакетів на видалений комп'ютер.

2. Перевірка правильності конфігурації TCPЯP.

При усуненні несправностей і проблем в мережі TCP/IP слід спочатку перевірити правильність конфігурації TCP/IP. Для цього використовується утиліта ipconfig.

Ця команда корисна на комп'ютерах, що працюють з DHCP (Dynamic Host Configuration Protocol), оскільки дає користувачам можливість визначити, яка конфігурація мережі TCP/IP і які величини були встановлені за допомогою DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter]| /release]

Параметри:

all видає весь список параметрів. Без цього ключа відображується лише IP-адрес, маска і шлюз за умовчанням;

renew[adapter] оновлює параметри конфігурації DHCP для вказаного мережевого адаптера;

release[adapter] звільняє виділену IP-адрес DHCP;

adapter - ім'я мережевого адаптера;

displaydns виводить інформацію про вміст локального кеша клієнта DNS, використовуваного для дозволу доменних імен.

Таким чином, утиліта ipconfig дозволяє з'ясувати, чи ініціалізувала конфігурація і чи не дублюються IP-адреса:

- якщо конфігурація ініціалізувала, то з'являється IP-адрес, маска, шлюз;
- якщо IP-адреса дублюються, то маска мережі буде 0.0.0.0;
- якщо при використанні DHCP комп'ютер не зміг отримати IP-адрес, то він дорівнюватиме 0.0.0.0 .

3. Тестування зв'язку з використанням утиліти ping.

Утиліта ping (Packet Internet Grouper) використовується для перевірки конфігурації TCP/IP і діагности помилок з'єднання. Вона визначає доступність і функціонування конкретного хоста. Використання ping кращий спосіб перевірки того, що між локальним комп'ютером і мережевим хостом

існує маршрут. Хостом називається будь-який мережевий пристрій (комп'ютер, маршрутизатор), що обмінюється інформацією з іншими мережевими пристроями по TCP/IP.

Команда ping перевіряє з'єднання з видаленим хостом шляхом посилки до цього хосту ехо-камера-пакетів ICMP і прослухування ехо-камера-відповідей. Ping чекає кожен посланий пакет і друкує кількість переданих і прийнятих пакетів. Кожен прийнятий пакет перевіряється відповідно до переданого повідомлення. Якщо зв'язок між хостами поганий, з повідомлень ping стане ясно, скільки пакетів втрачено.

Утиліта ping використовується наступними способами:

1) Для перевірки того, що TCP/IP встановлений і правильно конфігурований на локальному комп'ютері, в команді ping задається адреса петлі зворотного зв'язку (loopback address): ping 127.0.0.1

Якщо тест успішно пройден, то ви отримаєте наступну відповідь:

Reply from
127.0.0.1 Reply
from 127.0.0.1
Reply from
127.0.0.1 Reply
from 127.0.0.1

2) Аби переконатися в тому, що комп'ютер правильно доданий в мережу і IP-адрес не дублюється, використовується IP-адрес локального комп'ютера:

ping IP-адреслокальногохоста

3) Аби перевірити, що шлюз за умовчанням функціонує і що можна встановити з'єднання з будь-яким локальним хостом в локальній мережі, задається IP-адрес шлюзу за умовчанням:

ping IP-адресшлюза

4) Для перевірки можливості встановлення з'єднання через маршрутизатор в команді ping задається IP-адрес видаленого хоста:

ping Ш-адреСиУдаленного хоста

Синтаксис утиліти ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметри:

-t виконує команду ping до переривання. Control-Break - поглянути статистику і продовжити. CONTROL-C - перервати виконання команди;

-a дозволяє визначити доменне ім'я видаленого комп'ютера по його IP-адресу;

-n count посилає кількість пакетів ECHO, вказану параметром count;

-l length посилає пакети завдовжки length байт (максимальна довжина 8192 байти);

-f посилає пакет зі встановленим прапором «не фрагментувати». Цей пакет не фрагментуватиметься на маршрутизаторах по шляху свого дотримання;

-i ttl встановлює час життя пакету у величину ttl (кожен маршрутизатор зменшує ttl на одиницю);

-V tos встановлює типа поля «сервіс» у величину tos;

-r count записує дорогу пакету, що виходить, і пакету, що повертається, в полі запису дороги. Count - від 1 до 9 хостов;

-s count дозволяє обмежити кількість переходів з однієї підмережі в іншу (хопов). Count задає максимально можливу кількість хопов;

-j host-list направляє пакети за допомогою списку хостов, визначеного параметром host-list. Послідовні хосты можуть бути відокремлені проміжними маршрутизаторами (гнучка статична маршрутизація). Максимальна кількість хостов в списку, дозволене IP, рівне 9;

-до host-list направляє пакети через список хостов, визначений в host- list. Послідовні хосты не можуть бути розділені проміжними маршрутизаторами (жорстка статична маршрутизація). Максимальна кількість хостов - 9;

-w timeout вказує час чекання (timeout) відповіді від видаленого хоста в мілісекундах (за умовчанням - 1сек);

destination-list вказує видалений хост, до якого треба направити пакети ping.

4. Вивчення маршруту між мережевими з'єднаннями за допомогою утиліти tracert.

Tracert - це утиліта трасування маршруту. Вона використовує поле TTL (time-to-live, час життя) пакету IP і повідомлення про помилки ICMP для визначення маршруту від одного хоста до іншого.

Утиліта tracert може бути змістовнішою і зручнішою, чим ping, особливо в тих випадках, коли видалений хост недосяжний. За допомогою її можна визначити район проблем із зв'язком (у Internet-провайдера, в опорній мережі, в мережі видаленого хоста) по тому, наскільки далеко буде відстежений маршрут. Якщо виникли проблеми, то утиліта виводить на екран зірочки (*), або повідомлення типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утиліта tracert працює таким чином: посилається по 3 пробних exo-камера-пакету на кожен хост, через який проходить маршрут до видаленого хоста. На екран при цьому виводиться час чекання відповіді на кожен пакет (Його можна змінити за допомогою параметра -w). Пакети посилаються з різними величинами часу життя. Кожен маршрутизатор, що зустрічається по дорозі, перед перенаправлениям пакету зменшує величину TTL на одиницю. Таким чином, час життя є лічильником точок проміжної доставки (хопов). Коли час життя пакету досягне нуля, передбачається, що маршрутизатор пошле в комп'ютер-джерело повідомлення ICMP “Time Exeeded” (Час витік). Маршрут визначається шляхом посилки першого exo-камера-пакету з TTL=1. Потім TTL збільшується на 1 в кожному подальшому пакеті до тих пір, поки пакет не досягне видаленого хоста, або буде досягнута максимально можлива величина TTL (за умовчанням 30, задається за допомогою параметра -h).

Маршрут визначається шляхом вивчення повідомлень ICMP, які присилаються назад проміжними маршрутизаторами.

Примітка: деякі маршрутизатори просто мовчки знищують пакети з минулим TTL і не будуть видні утиліті tracert Синтаксис: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имяцелевого хоста

Параметри:

-d вказує, що не потрібно розпізнавати адреси для імен хостов;

-h maximumhops вказує максимальне число хопов для того, щоб шукати мету;

-j host-list вказує нежорстку статичну маршрутизацію відповідно до host-list;

-w timeout вказує, що потрібно чекати відповідь на кожен ехо-камеру-пакет задане число мсек.

5. Утиліта ARP.

Основне завдання протоколу ARP - трансляція IP-адресов у відповідні локальні адреси. Для цього ARP-протокол використовує інформацію з ARP-таблицы (ARP-кэша). Якщо необхідний запис в таблиці не знайдений, то протокол ARP відправляє широкомовний запит до всіх комп'ютерів локальної підмережі, намагаючись знайти власника даної IP-адреса. У кеші можуть міститися два типи записів: статичні і динамічні. Статичні записи вводяться уручну і зберігаються в кеші постійно. Динамічні записи поміщаються в кеш в результаті виконання широкомовних запитів. Для них існує поняття часу

життя. Якщо протягом певного часу (за умовчанням 2 мин.) запис не зажадався, то вона віддаляється з кеша.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметри:

-s занесення в кеш статичних записів;

-d видалення з кеша запису для певної IP-адреса;

-a перегляд вмісту кеша для всіх мережевих адаптерів локального комп'ютера;

inet_addr - IP-адрес;

eth_addr - MAC-адрес.

6. Утиліта netstat.

Утиліта netstat дозволяє отримати статичну інформацію по деяких з протоколів стека (TCP, UDP, IP, ICMP), а також виводить відомості про поточні мережеві з'єднання. Особливо вона корисна на брандмауерах, з її допомогою можна виявити порушення безпеки периметра мережі.

Синтаксис:

netstat [-a] [-i] [-n] [-s] [-p protocol] [-r]

Параметри:

-a виводить перелік всіх мережевих з'єднань і портів локального комп'ютера, що прослухуються;

-e виводить статистику для Ethemet-интерфейсов (наприклад, кількість отриманих і відправлених байт);

-n виводить інформацію по всіх поточних з'єднаннях (наприклад, TCP) для всіх мережевих інтерфейсів локального комп'ютера. Для кожного з'єднання виводиться інформація про IP-адресах локального і видаленого інтерфейсів разом з номерами використовуваних портів;

-s виводить статистичну інформацію для протоколів UDP, TCP, ICMP, IP. Ключ «/more» дозволяє проглянути інформацію посторінковий;

-г виводить вміст таблиці маршрутизації.

Завдання на практичну роботу

Оформите звіт по практичної роботі, описавши виконання вправ і давши короткі відповіді на контрольні питання.

Вправа 1. Здобуття довідкової інформації по командах

Виведіть на екран довідкову інформацію по утилітах ipconfig, ping,

tracert, hostname. Для цього в командному рядку введіть ім'я утиліти без параметрів або з /?. Вивчите ключі, використовувані при запуску утиліт.

Вправа 2. Здобуття імені хоста

Виведіть на екран ім'я локального хоста за допомогою команди hostname.

Вправа 3. Вивчення утиліти ipconfig

Перевірте конфігурацію TCP/IP за допомогою утиліти ipconfig. Заповните таблицю:

Ім'я хоста	Ws21
IP-адрес	192.168.12.21
Маска підмережі	255.255.255.0
Основний шлюз	192.168.12.1
Чи використовується DHCP (адреса DHCP-сервера)	no
Опис адаптера	PCI FAST ETHERNET realtek rtl8139
Фізична адреса мережевого адаптера	00-c0-26-2b-66-fe
Адреса DNS-сервера	no
Адреса WINS-сервера	no

Вправа 4. Тестування зв'язку за допомогою утиліти ping

1. Перевірте правильність установки і конфігурації TCP/IP на локальному комп'ютері.
2. Перевірте, чи правильно доданий в мережу локальний комп'ютер і чи не дублюється IP-адрес.
3. Перевірте функціонування шлюзу за умовчанням, пославши 5 exo-камера-пакетів завдовжки 64 байти.
4. За допомогою команди ping перевірте перераховані нижче адреси і для кожного з них відмітьте час відгуку. Спробуйте збільшити час відгуку.

4. ВАРІАНТИ ЗАВДАНЬ

1	www.informika.ru www.rfbr.ru www.ras.ru	www.strezhi.ru www.catalog.tomsk.ru www.kvadro.net
2	www.gpntb.ru www.rusmedserv.com www.nsc.ru	auction.tom.ru www.ripn.net www.shpl.ru
3	www.chemnet.ru www.rsl.ru www.philosophy.ru	www.kolesnica.com shema.tomsk.ru ragnarok.tomsk.ru
4	www.auditorium.ru www.membrana.ru www.osi.ru	www.scsml.rssi.ru www.sscc.ru www.nlr.ru
5	www.viniti.ru www.sostav.ru www.ioffe.ru	www.jinr.ru uic.nnov.ru www.ruthenia.ru
6	www.fegi.ru www.elibrary.ru www.extech.ru	www.scsml.rssi.ru www.sscc.ru www.nlr.ru

Мета роботи: Вивчити правила адресації мережевого рівня, навчитися розподіляти адреси між учасниками мережі передачі даних і організовувати маршрутизацію між сегментами мережі.

Устаткування: персональний комп'ютер, включений в мережу IP, Microsoft Windows **Мережевий рівень моделі OSI**

Мережевий рівень відповідає за можливість доставки пакетів по мережі передачі даних - сукупності сегментів мережі, об'єднаних в єдину мережу будь-якої складності за допомогою вузлів зв'язку, в якому є можливість досягнення з будь-якої крапки мережі в будь-яку іншу.

У зв'язку з необхідністю перенаправляти пакети з одного сегменту мережі в інший, мережеві адреси повинні задовольняти наступним вимогам:

- адреси мають бути унікальні. У мережі не може бути декількох учасників з однаковими адресами щоб уникнути неоднозначності
- мережева адреса повинна містити інформацію про те, як досягти одержувача по мережі.

Це наводить до структурності адреси - адреса розбивається на частини, що дозволяють визначити місце розташування учасника усередині мережі.

Структура може бути складною багаторівневою, наприклад адреса містить інформацію про країну, область, населений пункт, підприємство, будівлю, відділі і так далі або простій, що містить номер мережі і номер комп'ютера в мережі.

По складній структурі легко побудувати маршрут проходження пакету, але адреса виявляється складною і переобтяженою часто непотрібною інформацією. Прикладом такої адресації може служити доменна адресація в Інтернет, за адресою asu.bru.mogilev.by неважко зрозуміти, де знаходиться даний учасник мережі і як до нього добратися.

2ho.biz

Ibm.com

Kharkovforum.com

5. Задайте різну довжину посиланих пакетів.

Вправа 5. Визначення дороги IP-пакета

За допомогою команди tracert перевірте для перерахованих нижче адрес, через які проміжні вузли йде сигнал. Відзначте їх:

http://www.calcmaster.net/ http://www.idzap.com/
http://www.rrdb.org/rrdbproxy.php?l=en http://www.kproxy.com/
http://www.goproxing.com/ http://www.merletn.org/anonymizer
http://www. cgi -proxy. net/ http://www.proxymouse.com/
http://www.proxywave.com/ http://www.vtunnel.com/ http://www.
freeproxy.ca/

Вправа 6: Перегляд АКР-кзша

За допомогою утиліти агр проглянете ARP-таблицу локального комп'ютера.

Вправа 7. Здобуття інформації про поточні мережеві з'єднання і протоколи стека TCP/IP.

За допомогою утиліти netstat виведіть перелік мережевих з'єднань і статистичну інформацію для протоколів UDP, TCP, ICMP, IP.

За допомогою сайтів 2ip.ru 1-ip.ru, потрібно для двох працездатних Internet-узлов визначити:

a. країну, де знаходиться вузол;

b. діапазон IP-адресов, тобто IP-сеть, до якої належить досліджуваний вузол;

c. клас мережі, до якої належить IP-узел;

d. кому належить дана IP-сеть;

e. якщо є - адміністраторів мережі.

Тема№1: Основи побудови комп’ютерних мереж.

Практичне заняття 2: Вивчення мережевого рівня моделі OSI на прикладі протоколу IP.

Навчальна мета заняття: Вивчити правила адресації мережевого рівня, навчитися
розподіляти адреси між учасниками мережі передачі даних і організовувати маршрутизацію між сегментами мережі.

Час: 2 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. Мережевий рівень моделі OSI.
2. Протокол IP.
3. Визначення діапазону адрес підмережі.
4. Завдання для самостійного вирішення.

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид- во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP,Мїсішой Windows

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорення теоретичного матеріалу

Проста структура дозволяє значно скоротити розмір адреси і зберігає можливість роботи в мережі будь-якої структури, але для цього можуть потрібно складні і, часто, не настільки очевидні алгоритми, як у попередньому випадку.

Протокол IP

Архітектуру мережевого рівня зручно розглядати на прикладі мережевого протоколу IP - найпоширенішого в даний час, основного протоколу мережі Інтернет. Термін «стек протоколів TCP/IP» означає «набір протоколів, пов'язаних з IP і TCP(протоколом транспортного рівня)».

Архітектура протоколів TCP/IP призначена для об'єднаної мережі, що складається із сполучених один з одним шлюзами окремих різнорідних пакетних підмереж, до яких підключаються різнорідні машини.

Кожна з підмереж працює відповідно до своїх специфічних вимог і має свою природу засобів зв'язку. Проте передбачається, що кожна підмережа може прийняти пакет інформації (дані з відповідним мережевим заголовком) і доставити його за вказаною адресою в цій конкретній підмережі.

Таким чином, дві машини, підключені до однієї підмережі, можуть обмінюватися пакетами.

Коли необхідно передати пакет між машинами, підключеними до різних підмереж, то машина-відправник посилає пакет у відповідний шлюз (шлюз підключений до підмережі також як звичайний вузол). Звідти пакет прямує по певному маршруту через систему шлюзів і підмереж, поки не досягне шлюзу, підключеного до тієї ж підмережі, що і машина-одержувач: там пакет прямує до одержувача.

Таким чином, адреса одержувача повинна містити в собі:

- номер (адреса) підмережі;
- номер (адреса) учасника (хоста) усередині підмережі.

IP адреси є 32-ми розрядні двійкові числа. Для зручності їх записують у вигляді чотирьох десяткових чисел, розділених крапками. Кожне число є десятковим еквівалентом відповідного байта адреси (для зручності записуватимемо крапки і в двійковому зображенні).

192.168.200.47 є десятковим еквівалентом двійкової адреси

11000000.10101000.11001000.00101111

Інколи застосовують десяткове значення IP-адреса. Його легко обчислити

$$192*256^3+168*256^2+200*256+47=3232286767$$

або за допомогою методу Горнера :

$$(((192*256)+168)*256+200)*256+47=3232286767$$

Кількість розрядів адреси підмережі може бути різною і визначається маскою мережі.

Маска мережі також є 32-х розрядним двійковим числом. Розряди маски мають наступний сенс: якщо розряд маски дорівнює 1, то відповідний розряд адреси є розрядом адреси підмережі, а якщо 0, то розрядом хоста усередині підмережі. Всі одиничні розряди маски (якщо вони є) знаходяться в старшій (лівою) частині маски, а нульові (якщо вони є) - в правій (молодшою).

Виходячи з вищесказаного, маску часто записують у вигляді числа одиниць в ній що містяться.

255.255.248.0 (11111111.11111111.11111000.00000000) - є правильною маскою підмережі (/21), а

255.255.250.0 (11111111.11111111.11111010.00000000) - є неправильною, недопустимою.

Неважко побачити, що максимальний розмір підмережі може бути лише мірою двійки (двійку треба піднести до ступеня, рівного кількості нулів в масці).

При передачі пакетів використовуються правила маршрутизації, головне з яких звучить так: «Пакети учасникам своєї підмережі доставляються безпосередньо, а останнім - по інших правилах маршрутизації».

Таким чином, потрібно визначити, чи є одержувач членом нашої підмережі чи ні.

Визначення діапазону адрес підмережі.

Визначення діапазону адрес підмережі можна виробити з визначення поняття маски:

— ті розряди, які відносяться до адреси підмережі, у всіх хостов підмережі мають бути однакові;

— адреси хостов в підмережі можуть бути будь-якими.

Двійкове	Десяткове
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Тобто, якщо наша адреса 192.168.200.47 і маска рівна /20, то діапазон можна порахувати:

11000000.10101000.11001000.00101111 - адреса

11111111.11111111.11110000.0 - маска

11000000.10101000.1100XXXX.XXXXXXXX -диапазон адрес

де 0,1 - певні значення розрядів, X - будь-яке значення

Що наводить до діапазону адрес: від 11000000.10101000.11000000.00000000 (192.168.192.0) до 11000000.10101000.11001111.11111111 (192.168.207.255)

Слід враховувати, що деякі адреси є забороненими або службовими і їх не можна використовувати для адрес хостов або підмереж. Це адреси, що містять:

- **0** у першому або останньому байті
- **255** у будь-якому байті (це широкомовні адреси)
- **127** у першому байті (внутрішня петля - ця адреса є в кожному хосте і служить для скріплення компонентів мережевого рівня).

Тому доступний діапазон адрес буде декілька менше.

Завдання для самостійного вирішення:

1. Які адреси з приведеного нижче списку є допустимими адресами хостов:

0. **10.10.10**

10.0.10.10

10.10.0. 10
10.10.10.10
127.0. 127.127
127.0. 127.0
255.0. 200.1
1.255.0. 0

2. Перерахуєте всі допустимі маски.
3. Визначите діапазони адрес підмереж (даны адреса хоста і маска підмережі):

10.212.157.12/24
27.31.12.254/31
192.168.0. 217/28
10.7.14.14/16

4. Які з адрес

241.253.169.212
243.253.169.212
242.252.169.212
242.254.169.212
242.253.168.212
242.253.170.212 **242.253.169.211**
242.253.169.213

будуть досягнуті безпосередньо з хоста 242.254.169.212/21

5. Поглянете параметри IP на своєму комп'ютері за допомогою команди ірсопйр. Визначите діапазон адрес і розмір підмережі, в якій Ви знаходитеся. Спробуйте пояснити, чому вибрані такі мережеві параметри і які мережеві параметри вибрали б Ви.

Тема№1: Локальні комп'ютерні мережі.

Практичне заняття 3: Маршрутизація в IP-мережах

Навчальна мета заняття: Вивчити правила адресації мережевого рівня, навчитися розподіляти адреси між учасниками мережі передачі даних і організовувати маршрутизацію між сегментами мережі.

Час: 2 год.

Місце проведення: комп'ютерний клас

Навчальні питання:

1. **Правила маршрутизації.**
2. **Завдання для самостійного вирішення.**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид- во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP,Мїсішой Windows

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорення теоретичного матеріалу

Архітектуру мережевого рівня зручно розглядати на прикладі мережевого протоколу IP - найпоширенішого в даний час, основного протоколу мережі Інтернет. Термін «стек протоколів TCP/IP» означає «набір протоколів, пов'язаних з IP і TCP(протоколом транспортного рівня)».

Архітектура протоколів TCP/IP призначена для об'єднаної мережі, що складається із сполучених один з одним шлюзами окремих різнорідних пакетних підмереж, до яких підключаються різнорідні машини.

Кожна з підмереж працює відповідно до своїх специфічних вимог і має свою природу засобів зв'язку.

Проте передбачається, що кожна підмережа може прийняти пакет інформації (дані з відповідним мережевим заголовком) і доставити його за вказаною адресою в цій конкретній підмережі. Не потрібний, аби підмережа гарантувала обов'язкову доставку пакетів і мала надійний крізний протокол. Таким чином, дві машини, підключені до однієї підмережі, можуть обмінюватися пакетами.

Коли необхідно передати пакет між машинами, підключеними до різних підмереж, то машина-відправник посилає пакет у відповідний шлюз (шлюз підключений до підмережі також як звичайний вузол). Шлюз (gateway) - будь-яке мережеве устаткування з декількома мережевими інтерфейсами і здійснююче просування пакетів між мережами на рівні протоколів мережевого рівня.

З шлюзу пакет прямує по певному маршруту через систему шлюзів і підмереж, поки не досягне шлюзу, підключеного до тієї ж підмережі, що і

Архітектуру мережевого рівня зручно розглядати на прикладі машина-одержувач; там пакет прямує до одержувача.

Таким чином, шлюз виконує маршрутизацію - процедуру знаходження в структурі мережі дороги досягнення одержувача (побудова дороги доставки пакетів).

Якщо хост підключений до декількох мереж, він повинен мати декілька мережевих адрес, як мінімум стільки, скільки каналів до нього підключено.

Таблиця маршрутизації має наступний вигляд:

Мережева адреса	Маска мережі	Адреса шлюзу	Інтерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Мережева адреса — Початкова адреса підмережі, порядок досягнення якої описує правило.

Маска — Маска підмережі, яку описує правило.

Маршрутизація виробляється по правилах маршрутизації, зведених в таблицю маршрутизації.

Навіть якщо хост не є шлюзом між підмережами, все одно в нім присутня таблиця маршрутизації, адже будь-який хост повинен відправляти пакети безпосередньо членам своєї підмережі, через якийсь шлюз іншим підмережам і не передавати в мережу пакети, призначені самому собі (завертати їх по внутрішній петлі 127.0.0.1).

Таблиця 6.4.

мережі

Адреса шлюзу — Показує, на яку адресу будуть послані пакети, що йдуть в мережу призначення. Якщо пакети йтимуть безпосередньо, то вказується власна адреса (точніше та адреса того каналу, через який передаватимуться пакети).

Інтерфейс — Вказує адреса каналу, через який передаватимуться пакети. Інтерфейс завжди належить хосту, на якому знаходиться правило.

Метрика — Визначає час, за який пакет досягне мережі призначення.

Правила застосовуються в порядку зменшення масок.

Правила з рівними масками застосовуються в порядку збільшення метрики.

Вживання правила полягає у визначенні, чи належить хост призначення мережі, вказаної в правилі, і якщо належить, то пакет вирушає на адресу шлюзу через інтерфейс.

Розглянемо наведену вище таблицю маршрутизації, пересортувавши правила:

Мережева адреса	Маска мережі	Адреса шлюзу	Інтерфейс	Метри»
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Звернете увагу на маску мережі в першому правилі.

Вона описує підмережу розміром в 1 хост з адресою 255.255.255.255 - це широкомовна

192.168.200.255 255.255.255.255 192.168.200.47 192.168.200.47 30

адреса. Пакети посилатимуться на адресу 192.168.200.47 через інтерфейс

192.168.200.47 255.255.255.255 127.0.0.1 127.0.0.1 30

192.168.200.47. Це наша адреса, тобто пакети вирушатимуть безпосередньо.

Знову широкомовна адреса. Дивися попередній коментар.

внутрішню петлю.

192.168.192.0 255.255.240.0 192.168.200.47 192.168.200.47 30

А ось і наша підмережа. Відправляємо безпосередньо.

127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1

Все, що починається з 127, відправляємо через внутрішню петлю.

224.0.0.0 240.0.0.0 192.168.200.47 192.168.200.47 30

Клас D - відправляємо безпосередньо.

0.0.0.0 0.0.0.0 192.168.200.1 192.168.200.47 30

Знову така ж маска, але адреса нашого хоста. Відправляти будемо через

Найцікавіше правило. Маска покриває ВСІ можливі адреси! Пакети вирушають через наш інтерфейс на адресу 192.168.200.1. Правило застосовується

останнім, тому його можна озвучити так: по всіх адресах, які

не підійшли по попередніх правилах, пакети відправляємо на адресу 192.168.200.1

Така адреса зазвичай є в будь-якій мережі і називається шлюзом за умовчанням (default gateway). Ця адреса приховує від хостов і користувачів структуру мережі і дозволяє спростити таблиці маршрутизації і зняти навантаження з хостов, перенісши маршрутизацію на спеціально виділені шлюзи - маршрутизатори.

Неважко здогадатися, що всі адреси в колонці Адреса шлюзу повинні досягатися безпосередньо, тобто входити в нашу підмережу.

Для роботи з таблицями маршрутизації у складі ОС є програма route.

Одному з основних завдань, що стоять при проектуванні мереж, є розподіл по підмережах мережевих адрес із заданого діапазону, тобто розділення мережі на підмережі.

При розділенні мережі на підмережі слід враховувати наступні правила:

— розмір підмереж має бути мірою двійки
— є заборонені адреси
— початкова адреса підмережі має бути кратна її розміру

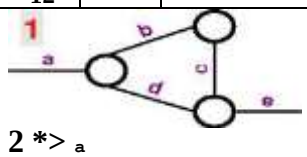
Як шлюз за умовчанням можна використовувати будь-який вузол, але, виходячи із збільшення пропускної спроможності мережі і зменшення часу передачі пакетів, слідує як шлюз за умовчанням використовувати або найближчий вузол, або вузол, сполучений з максимальною кількістю мереж, тобто слід враховувати топологію мережі.

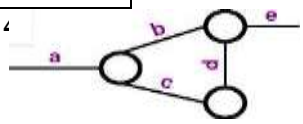
Завдання для самостійного вирішення:

1. За допомогою програми route print поглянете таблицю маршрутизації Вашого комп'ютера. Поясните всі правила.
2. Поглянете таблицю маршрутизації хоста, що має декілька каналів. Поясните всі правила.
3. Поглянете таблицю маршрутизації маршрутизатора. Поясните всі правила.

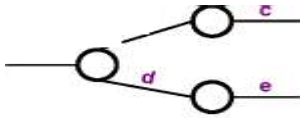
4. Додайте нове правило в таблицю маршрутизації для мережі 192.168.0.0/24 через шлюз у вашій мережі з останнім байтом в адресі 125 і метрикою 12
5. Видалите це правило.
6. Відповідно до таблиці і схем виконаєте завдання на розподіл адрес по підмережах (згідно варіанту). Побудуйте таблиці маршрутизації для всіх шлюзів і для одного хоста для кожного сегменту.

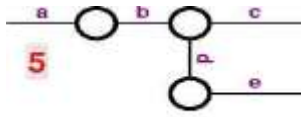
№ варіан Ту	Кількість хостов в підмережі					Діапазон адрес	
	а	**Ь**	**3**	**а**	**Є**	від	до
1	**5**	**10**	**20**	**15**	**50**	**10.0.20.0**	**10.0.20.255**
2	**20**	**15**	**6**	**70**	**25**	**192.168.0.0**	**192.168.0.255**
3	**15**	**25**	**5**	**40**	**5**	**112.38.25.128**	**112.38.25.255**
4	**24**	**32**	**8**	**10**	**2**	**196.13.49.0**	**196.13.49.128**
5	**50**	**16**	**64**	**20**	**15**	**68.76.115.0**	**68.76.115.255**
6	**40**	**6**	**10**	**12**	**5**	**211.3.45.0**	**211.3.45.128**

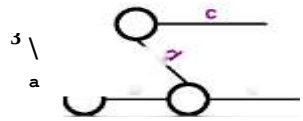


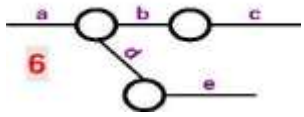


2 *> a









Тема№1: Локальні комп'ютерні мережі.

Практичне заняття 4: Моніторинг мережі

Навчальна мета заняття: навчитися контролювати роботу мережі, монторінг і аналіз мережі.

Час: 2 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **Експертні системи.**
2. **Устаткування для діагностики і сертифікації кабельних систем**
3. **Функції збору статистики аналізатора**
4. **Розподіл використовуваних мережевих протоколів**
5. **Спостереження за трафіком локальних мереж на основі комутаторів**
6. **Аналізатор протоколів CommView**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид- во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу LP,Microsoft Windows

Хід проведення заняття:

І. Порядок проведення вступу до заняття.

Вступ

Обговорення теоретичного матеріалу

Постійний контроль за роботою локальної мережі, складовій основу будь-якої корпоративної мережі, необхідний для підтримки її в працездатному стані. Контроль — це необхідний перший етап, який повинен виконуватися при управлінні мережею. Зважаючи на важливість цієї функції її часто відділяють від інших функцій систем управління і реалізують спеціальними засобами. Таке

розділення функцій контролю і власне управління корисно для невеликих і середніх мереж, для яких установка інтегрованої системи управління економічно недоцільна. Використання автономних засобів контролю допомагає адміністраторові мережі виявити проблемні ділянки і пристрої мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку уручну.

Процес контролю роботи мережі зазвичай ділять на два етапи — моніторинг і аналіз.

На етапі моніторингу виконується простіша процедура — процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і тому подібне

Завдання моніторингу вирішуються програмними і апаратними вимірниками, тестерами, мережевими аналізаторами, вбудованими засобами моніторингу комунікаційних пристроїв, а також агентами систем управління. У даній роботі розглянемо процес моніторингу через роботу аналізатора протоколів локальної мережі.

Під аналізом розуміється складніший і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Завдання аналізу вимагає активнішої участі людини і використання таких складних засобів, як експертні системи, що акумулюють практичний досвід багатьох мережевих фахівців.

1. Класифікація засобів моніторингу і аналізу

Вкажемо місце аналізатора протоколу (Protocol analyzers) в загальній класифікації засобів моніторингу і аналізу.

Агенти систем управління, що підтримують функції одній із стандартних МТВ і що поставляють інформацію по протоколу SNMP або CMIP. Для здобуття даних від агентів зазвичай потрібна наявність системи управління, що збирає дані від агентів в автоматичному режимі.

Вбудовані системи діагностики і управління (Embedded systems). Ці

системи виконуються у вигляді програмно-апаратних модулів, що встановлюються в комунікаційне устаткування, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління лише одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління багатосегментним повторителем Ethernet, що реалізовує функції автосегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам повторителя і деякі інші. Як правило, вбудовані модулі управління «за сумісництвом» виконують роль SNMP-агентов, що поставляють дані про стан пристрої для систем управління.

Аналізатори протоколів (Protocol analyzers). Є програмними або апаратно-програмними системами, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, вживаних в мережах, — звичайні декілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захвату окремих пакетів і виконують повне декодування захоплених пакетів, тобто показують в зручній для фахівця формі вкладеність пакетів протоколів різних рівнів один в одного з розшифровкою вмісту окремих полів кожного пакету.

1. Експертні системи. Цей вигляд систем акумулює знання технічних фахівців про виявлення причин аномальної роботи мереж і можливі способи приведення мережі в працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу і аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів. Простим варіантом експертної системи є контекстно-залежна система допомоги. Складніші експертні системи є, так звані бази знань, що володіють елементами штучного інтелекту. Прикладами таких систем є експертні системи, вбудовані в систему управління Spectrnm

компанії Cabletron і аналізатора протоколів Sniffer компанії Network General. Робота експертних систем полягає в аналізі великого числа подій для видачі користувачеві короткого діагнозу про причину несправності мережі.

2. Устаткування для діагностики і сертифікації кабельних систем. Умовне це устаткування можна поділити на чотири основні групи: мережеві монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери.

2.1. Мережеві монітори (звані також мережевими аналізаторами) призначені для тестування кабелів різних категорій. Мережеві монітори збирають також дані про статистичні показники трафіку — середню інтенсивність загального трафіку мережі, середній інтенсивності потоку пакетів з певним типом помилки і тому подібне Ці пристрої є найбільш інтелектуальними пристроями зі всіх чотирьох груп пристроїв даного класу, оскільки працюють не лише на фізичному, але і на канальному, а інколи і на мережевому рівнях.

2.2. Пристрою для сертифікації кабельних систем виконують сертифікацію відповідно до вимог одного з міжнародних стандартів на кабельні системи.

2.3. Кабельні сканери використовуються для діагностики мідних кабельних систем.

Тестери призначені для перевірки кабелів на відсутність фізичного розриву. Багатофункціональні портативні пристрої аналізу і діагностики. У зв'язку з розвитком технології великих інтегральних схем з'явилася можливість виробництва портативних приладів, які поєднували б функції декількох пристроїв: кабельних сканерів, мережевих моніторів і аналізаторів протоколів.

Що ж є аналізатором протоколів. Розглянемо його детальніше.

2. Аналізатори протоколів

Аналізатор протоколів є або спеціалізованим пристроєм, або персональним комп'ютером, зазвичай переносним, класу Notebook,

оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Вживані мережева карта і програмне забезпечення повинні відповідати технології мережі (Ethernet, Token Ring, FDDI, Fast Ethernet). Аналізатор підключається до мережі точно так, як і звичайний вузол. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, передавані по мережі, тоді як звичайна станція — лише адресовані їй. Для цього мережевий адаптер аналізатора протоколів переводиться в режим «безладного» захвату —promiscuousmode.

Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера і програмного забезпечення, що декодує протокол канального рівня, з яким працює мережевий адаптер, а також найбільш поширені протоколи верхніх рівнів, наприклад IP, TCP, ftp, telnet, HTTP, IPX, NCP, NETBEUI, DECnet і тому подібне До складу деяких аналізаторів може входити також експертна система, яка дозволяє видавати користувачеві рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті або інші результати вимірів, як усунути деякі види несправності мережі.

Аналізатори протоколів мають деякі загальні властивості.

Можливість (окрім захвату пакетів) виміру середньостатистичних показників трафіку в сегменті локальної мережі, в якому встановлений мережевий адаптер аналізатора. Зазвичай вимірюється коефіцієнт використання сегменту, матриці перехресного трафіку вузлів, кількість хороших і поганих кадрів, що пройшли через сегмент.

Можливість роботи з декількома агентами, що поставляють захоплені пакети з різних сегментів локальної мережі. Ці агенти найчастіше взаємодіють з аналізатором протоколів по власному протоколу прикладного рівня, відмінному від SNMP або CMIP.

Наявність розвиненого графічного інтерфейсу, що дозволяє представити результати декодування пакетів з різною мірою деталізації.

Фільтрація захоплюваних пакетів, що відображуються. Умови

фільтрації задаються залежно від значення адрес призначення і джерела, типа протоколу або значення певних полів пакету. Пакет або ігнорується, або записується в буфер захвату. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає захват або перегляд непотрібних в даний момент пакетів.

Використання тригерів. Тригери — це що задаються адміністратором деякі умови початку і припинення процесу захвату даних з мережі. Такими умовами можуть бути: час доби, тривалість процесу захвату, поява певних значень в кадрах даних. Тригери можуть використовуватися спільно з фільтрами, дозволяючи детальніше і тонко проводити аналіз, а також продуктивно витрачати обмежений об'єм буфера захвату.

Многоканальность. Деякі аналізатори протоколів дозволяють проводити одночасний запис пакетів від декількох мережевих адаптерів, що зручно для зіставлення процесів, що відбуваються в різних сегментах мережі.

Можливості аналізу проблем мережі на фізичному рівні в аналізаторів протоколів мінімальні, оскільки всю інформацію вони отримують від стандартних мережевих адаптерів. Тому вони передають і узагальнюють інформацію фізичного рівня, яку повідомляє їм мережевий адаптер, а вона багато в чому залежить від типа мережевого адаптера. Деякі мережеві адаптери повідомляють детальніші дані про помилки кадрів і інтенсивність колізій в сегменті, а деякі взагалі не передають таку інформацію верхнім рівням протоколів, на яких працює аналізатор протоколів.

З поширенням серверів Windows NT усе більш популярним стає аналізатор Network Monitor фірми Microsoft. Він є частиною сервера управління системою SMS, а також входить в стандартне постачання Windows NT Server, починаючи з версії 4.0 (версія з усіченими функціями). Network Monitor у версії SMS є багатоканальним аналізатором протоколів, оскільки може отримувати дані від декількох агентів Network Monitor Agent, що працюють в середовищі Windows NT Server, проте в кожен момент часу аналізатор може працювати лише з одним агентом, так що зіставити дані

різних каналів з його допомогою не удасться. Network Monitor підтримує фільтри захвату (досить прості) і дисплейні фільтри, що відображують потрібні кадри після захвату (складніші). Експертної системи Network Monitor не має в своєму розпорядженні.

3. Функції збору статистики аналізатора

Ці функції дозволяють в реальному масштабі часу простежити за зміною найбільш важливих параметрів, що характеризують «здоров'я» сегментів мережі. Статистика зазвичай збирається з різною мірою деталізації по різних групах.

Мережева статистика

У цій групі зібрані найбільш важливі статистичні показники — коефіцієнт використання сегменту (utilization), рівень колізій, рівень помилок і рівень широкомовного трафіку. Перевищення цими показниками певних порогів в першу чергу говорять про проблеми в тому сегменті мережі, до якого підключений багатофункціональний прилад.

Статистика помилкових кадрів

Ця функція дозволяє відстежувати всіх типів помилкових кадрів для певної технології. Наприклад, для технології Ethernet характерні наступні типи помилкових кадрів.

Укорочені кадри (Short frames). Це кадри, що мають довжину, менше допустимою, тобто менше 64 байт. Інколи цього типа кадрів диференціюють на два класи — просто коротких кадрів (short), в яких є коректна контрольна сума, і «коротунок» (runts), що не мають коректної контрольної суми. Найбільш вірогідними причинами появи укорочених кадрів є несправні мережеві адаптери і їх драйвери.

Подовжені кадри (Jabbers). Це кадри, що мають довжину, що перевищує допустиме значення в 1518 байт з хорошою або поганою контрольною сумою. Подовжені кадри є наслідком тривалої передачі, яка з'являється із-за несправностей мережевих адаптерів.

Кадри нормальних розмірів, але з поганою контрольною сумою (Bad

FCS) і кадри з помилками вирівнювання по кордону байта. Кадри з невірною контрольною сумою є наслідком безлічі причин — поганих адаптерів, перешкод на кабелях, поганих контактів, некоректно працюючих портів повторителей, мостів, комутаторів і маршрутизаторів. Помилка вирівнювання завжди супроводиться помилкою по контрольній сумі, тому деякі засоби аналізу-трафіку не роблять між ними відмінностей. Помилка вирівнювання може бути наслідком припинення передачі кадру при розпізнаванні колізії передавальним адаптером.

Кадри-примари (ghosts) є результатом електромагнітних наведень на кабелі. Вони сприймаються мережевими адаптерами як кадри, що не мають нормальної ознаки початку кадру, — 10101011. Кадри-примари мають довжину більше 72 байт, інакше вони класифікуються як видалені колізії. Кількість виявлених кадрів-примар у великій мірі залежить від точки підключення мережевого аналізатора. Причинами їх виникнення є петлі заземлення і інші проблеми з кабельною системою.

Знання процентного розподілу загальної кількості помилкових кадрів по їх типах може багато що підказати адміністраторові про можливі причини неполадок в мережі. Навіть невеликий відсоток помилкових кадрів може привести до значного зниження корисної пропускної спроможності мережі, якщо протоколи, поновлюючі спотворені кадри, працюють з великими тайм-аутами чекання квитанцій. Вважається, що в нормально працюючій мережі відсоток помилкових кадрів не повинен перевищувати 0,01 %, тобто не більше 1 помилкового кадру з 10 000.

Статистика по колізіях

Ця група характеристик дає інформацію про кількість і види колізій, відмічених на сегменті мережі, дозволяє визначити наявність і місцезнаходження проблеми. Аналізатори протоколів зазвичай не можуть дати диференційованої картини розподілу загального числа колізій по їх окремих типах, в той же час знання переважаючого типа колізій може допомогти зрозуміти причину поганої роботи мережі.

Нижче приведені основні типи колізій мережі Ethernet.

Локальна колізія (Local Collision). Є результатом одночасної передачі два або більш за вузли, що належать до того сегменту, в якому виробляються виміри. Якщо багатофункціональний прилад не генерує кадри, то в мережі на витій парі або волоконно-оптичному кабелі локальні колізії не фіксуються. Дуже високий рівень локальних колізій є наслідком проблем з кабельною системою.

Видалена колізія (Remote Collision). Ці колізії відбуваються на іншій стороні повторителя (по відношенню до того сегменту, в якому встановлений вимірювальний прилад). У мережах, побудованих на багатопортових повторителях (10Base-T, 10Base-FL/FB, 100Base-TX/FX/T4, Gigabit Ethernet), всі вимірювані колізії є видаленими (окрім тих випадків, коли аналізатор сам генерує кадри і може бути винуватцем колізії). Не всі аналізатори протоколів і засобу моніторингу однаковим чином фіксують видалені колізії. Це відбувається через те, що деякі вимірювальні засоби і системи не фіксують колізії, що відбуваються при передачі преамбули.

Пізня колізія (Late Collision). Це колізія, яка відбувається після передачі перших 64 байт кадру (по протоколу Ethernet колізія повинна виявлятися при передачі перших 64 байт кадру). Результатом пізньої колізії буде кадр, який має довжину більше 64 байт і містить невірне значення контрольної суми. Найчастіше це вказує на те, що мережевий адаптер, що є джерелом конфлікту, виявляється не в змозі правильно прослухувати лінію і тому не може вчасно зупинити передачу. Іншою причиною пізньої колізії є дуже велика довжина кабельної системи або дуже велика кількість проміжних повторителей, що наводить до перевищення максимального значення часу подвійного звороту сигналу. Середня інтенсивність колізій в нормально працюючій мережі має бути менше 5 %. Великі сплески (більше 20 %) можуть бути індикатором кабельних проблем.

Розподіл використовуваних мережевих протоколів

Ета статистична група відноситься до протоколів мережевого рівня. На

дисплеї відображується список основних протоколів в убуваючому порядку відносно процентного співвідношення кадрів, що містять пакети даного протоколу до загального числа кадрів в мережі.

Основні відправники (Top Sendes)

Функція дозволяє відстежувати найбільш активні передавальні вузли локальної мережі. Прилад можна набудувати на фільтрацію за єдиною адресою і виявити список основних відправників кадрів для даної станції. Дані відбиваються на дисплеї у вигляді діаграми разом з переліком основних відправників кадрів.

Основні получотели (Top Receivers)

Функція дозволяє стежити за найбільш активними вузлами-одержувачами мережі. Інформація відображується у вигляді, аналогічному приведеному вище.

Основні генератори широкомовного трафіку (Top Broadcasters)

Функція виявляє станції мережі, які більше останніх генерують кадри з широкомовними і груповими адресами.

Генерування трафіку (Traffic Generation)

Аналізатор може генерувати трафік для перевірки роботи мережі при підвищеному навантаженні. Трафік може генеруватися паралельно з активізованими функціями Мережева статистика, Статистика помилкових кадрів і Статистика по колізіях.

Користувач може задати параметри трафіку, що генерується, такі як інтенсивність і розмір кадрів. Для тестування мостів і маршрутизаторів прилад може автоматично створювати заголовки IP- і IPX-пакетов, і все що потрібний від оператора — це внести адреси джерела і призначення.

В ході випробувань користувач може збільшити на ходу розмір і частоту дотримання кадрів за допомогою клавіш управління курсором. Це особливо коштовно при пошуку джерела проблем продуктивності мережі і умов виникнення відмов.

Функції аналізу протоколів

Зазвичай аналізатори підтримують декодування і аналіз лише основних протоколів локальних мереж, таких як протоколи стеків TCP/IP, Novell NetWare, NETBIOS і Banyan VINES.

Наприклад, при аналізі протоколів стека TCP/IP збирається статистика по пакетах протоколу ICMP, за допомогою якого маршрутизатори повідомляють кінцеві вузли про виникнення різного роду помилок. Для ручної перевірки досяжності вузлів мережі в прилади включається підтримка утиліти IP Ping, а також аналогічних за призначенням утиліт NetWare Ping і NETBIOS Ping.

4. Спостереження за трафіком локальних мереж на основі комутаторів

Оскільки перевантаження процесорів портів і інших оброблювальних елементів комутатора можуть наводити до втрат кадрів, то функція спостереження за розподілом трафіку в мережі, побудованій на основі комутаторів, дуже важлива.

Проте якщо сам комутатор не забезпечений вбудованим агентом SNMP для кожного свого порту, то завдання стеження за трафіком, традиційно вирішувана в мережах з середовищами, що розділяються, за допомогою установки в мережу зовнішнього аналізатора протоколів, дуже ускладнюється.

Зазвичай в традиційних мережах аналізатор протоколів або багатофункціональний прилад підключався до вільного порту концентратора, що дозволяло йому спостерігати за всім трафіком, передаваним між будь-якими вузлами мережі.

Якщо ж аналізатор протоколу підключити до вільного порту комутатора, то він не зафіксує майже нічого, оскільки кадри йому передавати ніхто не буде, а чужі кадри в його порт також прямувати не будуть. Єдиний вигляд трафіку, який фіксуватиме аналізатор, — це трафік широкомовних пакетів, які передаватимуться всім вузлам мережі, а також трафік кадрів з невідомими комутатору адресами призначення. У разі коли мережа розділена на віртуальні мережі, аналізатор протоколів фіксуватиме лише

широкомовний трафік своєї віртуальної мережі.

Аби аналізаторами протоколів можна було як і раніше користуватися і в комутованих мережах, виробники комутаторів забезпечують свої пристрої функцією дзеркального відображення трафіку будь-якого порту на спеціальний порт. До спеціального порту підключається аналізатор протоколів, а потім на комутатор подається команда через його модуль SNMP-управлення для відображення трафіку якого-небудь порту на спеціальний порт.

Наявність функції зеркализации портів частково знімає проблему, але залишає деякі питання. Наприклад, як переглядати одночасно трафік двох портів або трафік порту, що працює в повнодуплексному режимі.

Надійнішим способом стеження за трафіком, що проходить через порти комутатора, є заміна аналізатора протоколу на агенти RMON ТВ для кожного порту комутатора.

Агент RMON виконує всі функції хорошого аналізатора протоколу для протоколів Ethernet і Token Ring, збираючи детальну інформацію про інтенсивність трафіку, різних типів поганих кадрів, про втрачені кадри, причому самостійно будуючи тимчасові ряди для кожного параметра, що фіксується. Крім того, агент RMON може самостійно будувати матриці перехресного трафіку між вузлами мережі, які дуже потрібні для аналізу ефективності вживання комутатора.

Оскільки агент RMON, що реалізовує все 9 груп об'єктів Ethernet, коштує вельми дорого, то виробники для зниження вартості комутатора часто реалізують лише перші декілька груп об'єктів RMON MIB. Іншим прийомом зниження вартості комутатора є використання одного агента RMON для декількох портів. Такий агент по черзі підключається до потрібного порту, дозволяючи зняти з нього необхідні статистичні дані.

5. Аналізатор протоколів CommView

Розглянемо програмний засіб CommView (http://www.tamos.com/products/commview/) компанії TamoSoft як аналізатор

протоколів. Для роботи в учбових цілях використовуватимемо 30-денну пробну версію програми. В рамках цього терміну функціонал CommView не обмежений, і програма може реалізувати більшість необхідних функцій аналізатора.

Перед початком роботи аналізатора необхідно вибрати мережевий інтерфейс (мережеву карту) через меню «Налаштування \ установки» і почати захват мережевих пакетів через меню «Файл \ почати захват».

Якщо захват пакетів успішно стартував в головному вікні програми відіб'ється мережева статистика. Приклад наведений на рис. 7.16

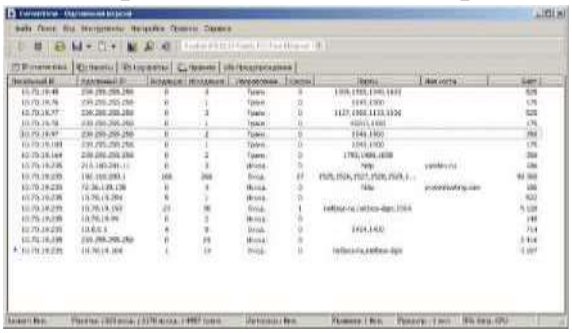


Рис. 7.16 Мережева статистика пакетів ЛВС.

Статистика на мал. 1 відображає одержувачів мережевих пакетів (колонка видалений IP), відправників (локальний IP), число пакетів, напрям, порти по яких відбувається обмін і іншу інформацію по мережевих пакетах.

На вкладці «Пакети» головного вікна програми можна отримати детальну інформацію за змістом мережевого пакету, вибравши його з переліку як на мал. 2. На малюнку вибраний пакет з номером 67 протоколу IP/TCP. У центральній частині вікна вказані основні параметри пакету (внутрішній номер пакету, протокол, мак-адреси і ін.) Справа вказана детальна інформація з декодуванням структури пакету, яка приведена в нижній частині вікна.

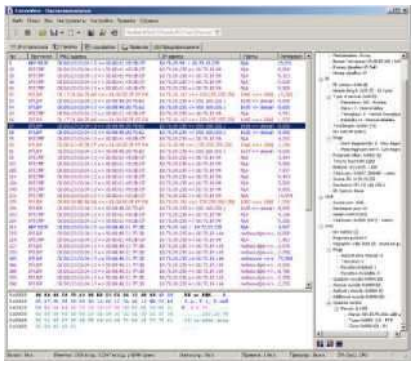


Рис 7.17. Детальне вивчення мережевого пакету.

Часто аналіз всієї статистики малоефективний із-за великого числа не потрібних нам для дослідження пакетів. Це буде потрібно налаштування деяких правил фільтрації мережевих пакетів для спрощення завдання моніторингу і аналізу. Приклад налаштування правил наведений на мал. 3. Як приклад створена правила для ігнорування при зборі мережевих пакетів з широкомовною адресою MAC-. Для цього необхідно перейти на вкладку «Правила», підвкладку «MAC-адреса» далі поставити галочку «Включити правила для MAC-адресов» і ввести MAC-адрес FF FF FF FF FF FF. Вказати «Додати запист» в будь-якому напрямі і як «Дія» ігнорувати. З детальнішим синтаксисом написання правил можна ознайомитися в довідковій системі програми (через головне меню «Довідка») або натискує клавішу F1.

Рис 6.18.. Налаштування правил фільтрації мережевих пакетів.

Інколи виникає необхідність реакції на появу деякої умови, наприклад при адресації від однієї IP-адреса до іншого. В цьому випадку потрібно буде набудувати попередження на відповідній вкладці. Синтаксис попередження цілком аналогічний створенню правила. Так наприклад для виникнення попередження при адресації IP=172.16.4.21 до IP=172.16.4.22 необхідно додати в текст попередження: (sip=172.16.4.21 and dip=172.16.4.22) or (sip=172.16.4.22 and dip=172.16.4.21) і вказати повідомлення для показу (на

малюнку це «Предупрежденіє1»). Таким чином можна відстежувати пакети за деякими умовами і реагувати на них.

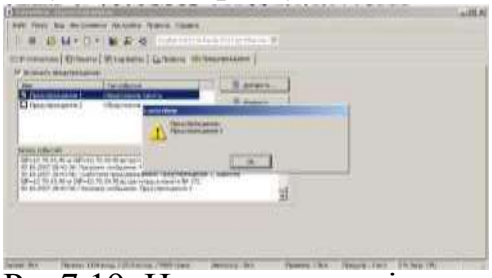


Рис7.19. Налаштування і робота попереджень.

Програма дозволяє набудувати число відбиваних пакетів в головному вікні програми, остання інформація буде записана у файли журналу і поміщена в звідну статистику.

При необхідності перегляду все пакетів це можна зробити через головне меню «Файл \ Перегляд log- файлів». Параметри log-файлов можна набудувати на вкладці log-файлы.

Для віддзеркалення загальної картини по мережевих пакетах можна скористатися розширеною статистикою через головне меню «Вид \ статистика»

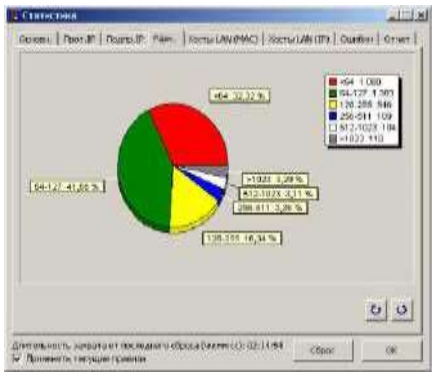
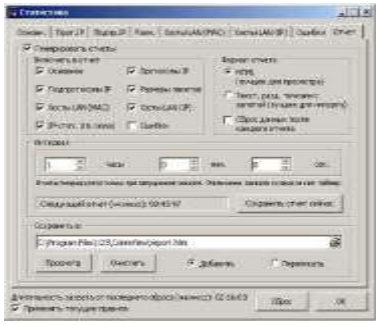


Рис.7.20 Детальна статистика по мережевих пакетах. можливо на основі даних статистики згенерувати HTML-отчет. Для цього у вікні «Статистика» на вкладка «Звіт» необхідно перевірити і при необхідності набудувати параметри звіту і натискувати кнопку «Проглянути». Приклад форми налаштування звіту наведений на рис 7.21..



Ріс 7.21 Налаштування HTML-отчета за статистикою.

Після натиснення кнопки «Перегляду» відкриється HTML-страница з даними статистики з врахуванням вибраних параметрів налаштування. Приклад сторінки наведений на Рис. 7.22.

Рис 7.22. НТМЬ-отчет за мережевою статистикою.

1. Вміст роботи

1.1. Вихідні дані до завдання

Мережеві пакети - трафік ЛВС.

1.2. Перелік досліджуваних завдань аналізатора протоколів (в рамках роботи):

набудувати систему фільтрації мережевих пакетів по умові (фільтр), визначити правила, попередження

досліджувати збір і аналіз статистики по мережевих пакетах ЛВС;

визначити заходи по оптимізації роботи ЛВС.

1.3. Вміст звіту

порядок дій для налаштування захвату пакетів за допомогою фільтру і без нього;

статистика роботи аналізатора за 10 хвилин роботи;

аналіз структури 2-3 пакетів різних протоколів (ICMP, UDP, TCP);

виводи.

1.4 Варіанти завдань (фільтрація

пакетів): по IP- адресам (sip, dip). по

номерах портів (sport, dport). типові

протоколу.

MAC-адресу.

комбінований фільтр по IP і номеру порту. комбінований фільтр за типом протоколу і номером порту.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Закон України “Про Національну програму інформатизації” [Текст] // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.181.
2. Закон України "Про електронні документи та електронний документообіг” [Текст] // Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275.
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Текст] // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.
4. Закон України "Про інформацію" [Текст] // Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650.
5. Закон України “Про Концепцію Національної програми інформатизації” [Текст] // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.182.
6. Указ Президента України „Про першочергові завдання щодо впровадження новітніх інформаційних технологій” [Текст]// Урядовий кур'єр 2005, N207 від 01.11.2005.
7. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
8. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.
9. Кулаков Ю.О., Луцький Г.М. [Текст]: Комп’ютерні мережі. Підручник. - К.: Юніор, 2003. - 400 с.
10. Под редакцией Л.Мелиховой. Интернет. Энциклопедия- СПб: Питер, 2001.528с. ил.
11. Уэнделл Одом. Компьютерные сети. Первый шаг = Computer Networking Firststep. — М.: «Вильямс», 2005. — С. 432.
12. Болілий В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник. - Кіровоград: ЦОП Авангард, 2008.- 146с.
13. Олифер В.Г., Олифер Н.А. Компьютерные сети принципы, технологии, протоколы. - СПб: Питер, 2000.-672с.
14. Кулаков Ю.А., Омельянский С.В. Компьютерные сети. Выбор, установка, использование и администрирование.- К.: Юниор, 1999.- 544с.
15. Гук М. Аппаратные средства локальных сетей. Энциклопедия.- СПб: Питер, 2000.- 576 с.
16. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации - СПб.: Питер, 2002.

Допоміжна

17. Новиков Ю.В., Кондратенко С.В. Локальные сети: архитектура, алгоритмы, проектирование. - М.: ЭКОМ, 2001. - 312 с.

18.Інформатика: Комп’ютерна техніка. Комп’ютерні технології: Підручник для студентів вищих навчальних закладів / За ред. Пушкаря. - К.: Видавничій центр «Академія», 2002. - 704 с. ISBN 966-580-135-X

19. Вуль В.А., Электронные издания. - М.. -СПб.: Издательство «Петербургский институт печати», 2001. - 308 с., илл. ISBN 5-93422-015-2

20. Капелюх С.А. Электронная почта. Самоучитель. - СПб.: БХВ-Петербург, 2006. - 144 с.: ил. ISBN 5-94157-813-X

21. Вирусы и средства борьбы с ними. ЗАО «Лаборатория Касперского»., Учебный курс. М. - 2005

22. Мюллер С. Модернизация и ремонт ПК, 16-е издание.: Пер. с англ. - М.: Издательский дом “Вильямс”, 2006. - 1328 с.: ил. ISBN 5-8459-0819-1

23. Microsoft. Комп'ютерні мережі. Учбовий курс/Пер. з англ. - М.: Видавничий відділ “Російська редакція” ТОО “Channel Trading Ltd.”. - 1998. - 696 с.

24. Високопродуктивні мережі. Енциклопедія користувача: Пер. з англ./Марк А. Спортак і ін. - К.: Видавництво «Діасофт», 1998. - 432 с.

25. Скляров А.Я., Пономаренко л.А., Щелкунов в.І., Інструментальні засоби проектування, імітаційного моделювання і аналізу комп'ютерних мереж. Навчальний посібник. - До: Нук. Думання, 2002. - 508 с.