МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Лабораторний практикум
для студентів напряму підготовки
6.050101 «Комп'ютерні науки»

VIVERE!
VINCERE!
CREARE!

Київ 2014

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Лабораторний практикум
для студентів напряму підготовки
6.050101 «Комп'ютерні науки»

Київ 2014

УДК 004.415 (076.5)
ББК З 973ю202 я7
К688

Укладачі: *Т. В. Холявкіна, В. А. Василенко*

Рецензент *М. А. Віноградов* – д-р техн. наук, проф. (Національний авіаційний університет).

Затверджено методично-редакційною радою Національного авіаційного університету (протокол № 8/13 від 19.12.2013)

К688 **Корпоративні інформаційні системи**: лабораторний практикум / уклад. : Т. В. Холявкіна, В. А. Василенко. – К.: НАУ, 2014. – 28 с.

Викладено сутність створення корпоративних інформаційних систем, основні методи динамічної маршрутизації і відповідні маршрутизатори для інтеграції автономних систем у рамках корпоративної інформаційної системи. Розглянуто принципи розрахунку базових характеристик функціонування корпоративних інформаційних систем.

Для студентів напряму підготовки 6.050101 «Комп'ютерні науки».

ВСТУП

Лабораторні роботи виконуються відповідно до навчальної програми з дисципліни «Корпоративні інформаційні системи», яка призначена для підготовки спеціалістів та магістрів спеціальності 7/8.05010101 «Інформаційні управляючі системи та технології». Мета виконання робіт – набуття студентами практичних навичок та закріплення теоретичних знань для розробки проектних рішень при створенні корпоративних інформаційних систем і мереж комп'ютерів.

Викладення матеріалів дисципліни побудовано відповідно до вимог кредитно-модульної системи. Програмою дисципліни передбачено виконання чотирьох лабораторних робіт у модулі. Метою проведення лабораторних робіт є поглиблення та закріплення знань із розділу дисципліни «Проектування корпоративних систем». У процесі виконання лабораторних робіт студенти ознайомлюються з методами створення корпоративних інформаційних систем та методами динамічної маршрутизації автономних систем у рамках корпоративної інформаційної системи. Проводять аналіз розрахунку базових характеристик функціонування корпоративних інформаційних систем. На виконання та захист кожної роботи відводиться чотири академічні години, крім четвертої роботи першого модуля, на яку заплановано п'ять академічних годин. За цей час студент повинен одержати у викладача варіант завдання і виконати його; зробити висновки щодо лабораторної роботи; підготувати протокол звіту про лабораторну роботу; відповісти на контрольні запитання.

Звіт про виконання лабораторної роботи має містити титульний аркуш; мету роботи; порядок виконання лабораторної роботи; висновки.

До оформлення звіту висуваються такі вимоги: робота оформлюється на аркушах формату А4 або в окремому зошиті з лабораторних робіт; на титульному аркуші мають бути вказані тема роботи, назва дисципліни, ким виконано роботу (ПІБ, номер групи, інститут), ким прийнята робота; звіт про роботу повинен містити вихідні дані, отримані результати, висновки.

Лабораторна робота 1

ПРОЕКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ КОМП'ЮТЕРІВ НА БАЗІ АВТОНОМНИХ СИСТЕМ

Мета роботи: вивчити спосіб адресації вузлів, прийнятий в IP-мережах, ознайомитися з класами IP-адрес із використанням масок підмережі.

Основні теоретичні відомості

Автономна система (AS) — це система IP-мереж і маршрутизаторів, керованих одним або декількома операторами, що мають єдину політику маршрутизації з Інтернетом.

Автономні системи можна згрупувати в три категорії, залежно від їх з'єднань і режиму роботи.

Багатоінтерфейсна (multihomed) AS — це AS, яка має з'єднання з більш ніж одним інтернет-провайдером. Така AS залишається підключеною до Інтернету в разі виходу з ладу з'єднання із одним з інтернет-провайдерів. Крім того, AS цього типу не передає транзитний трафік від одного інтернет-провайдера до іншого.

Обмежена (stub) AS — це AS, що має єдине підключення до однієї зовнішньої автономної системи. Це розцінюється як недоцільне використання номера AS, оскільки мережа розміщується повністю під одним інтернет-провайдером і, отже, не потребує унікальної ідентифікації.

Транзитна (transit) AS — це AS, яка пропускає через себе транзитний трафік мереж, підключених до неї. Таким чином, мережа A може використовувати транзитну AS для зв'язку з мережею B.

IP-адреса

Нагадаємо, що **порт** – це номер, який точно вказує серверну програму на вибраному комп'ютері. Клієнтська програма використовує порт для того, щоб вказати, до якого сервера на вибраному комп'ютері вона хоче під'єднатися. Для зручності в мережі кожної програми, призначеної для роботи в мережі Інтернет, відведені свої порти. **Протокол** – це спосіб передачі даних, а **маршрутизатор (router)** – система, що відповідає за ухвалення рішень про вибір одного з декількох шляхів передачі мережевого трафіку.

Переважна більшість комп'ютерів, що існують сьогодні, об'єднані в мережі. Оскільки комп'ютер підключений до мережі, повинен існувати спосіб обміну даними з іншими машинами. Причому цей спосіб обміну має бути єдиним для всіх комп'ютерів у мережі, щоб не виникало труднощів при передачі інформації. Набір правил, за якими інформація передається від власника до споживача, називається протоколом. Протоколів існує безліч. Розглянемо той, що дозволяє ідентифікувати (адресувати) кожен пристрій, під'єднаний до мережі. У цьому сенсі Інтернет як всесвітня глобальна комп'ютерна мережа підпорядкований законам IP (*Internet Protocol*, міжмережевий протокол), що входить до сімейства протоколів TCP/IP. IP передбачає, що інформація передається не від користувача до користувача, а від пристрою до пристрою, наприклад, від комп'ютера до комп'ютера або до стільникового телефону. Відповідно, кожен пристрій повинен мати свою унікальну адресу, виражену мовою цифр, яка складається з певного набору нулів і одиниць. Великі мережі отримують адреси класу A, середні – класу B, а невеликі – класу C.

Мережі класу A

Перший октет (вісім біт) IP-адреси будь-якого пристрою, підключеного до такої мережі, позначає номер мережі. Тому мереж класу A можна побудувати $2^8 = 256$. Перший, а точніше нульовий біт двійкової IP-адреси в такій мережі завжди дорівнює **0**.

Три октети (24 розряди), що залишилися, позначають номер окремого пристрою. Таким чином, у такій мережі можна об'єднати до $2^{24} = 16\,777\,216$ окремих пристроїв (рис. 1).

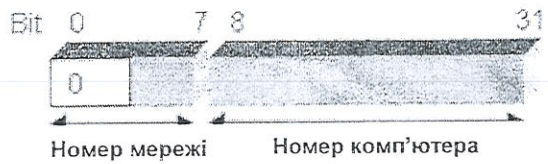

Рис. 1. Позначення мережі класу A

Мережі класу B

Під номер мережі відводиться два октети (16 біт) IP-адреси. Отже, таких мереж можна побудувати 2^{16}=65 536. Перші два біти IP-адреси будь-якого пристрою, підключеного до мережі класу B дорівнює **10**.

Ще два октети дозволяють адресувати до 2^{16} окремих пристроїв, тобто ті ж 65 536 (рис. 2).

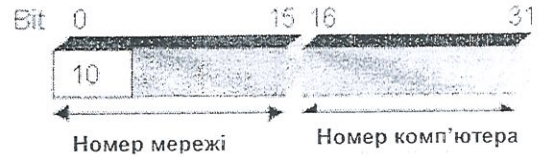

Рис. 2. Позначення мережі класу B

Мережі класу C

У таких мережах 24 розряди описують номер мережі. Всього таких мереж може бути 2^{24} = 16 777 216. Перші три біти адреси дорівнюють **110**.

Лише один октет залишається для ідентифікації пристроїв, підключених до такої мережі. Їх може бути не більше 256 (рис. 3).

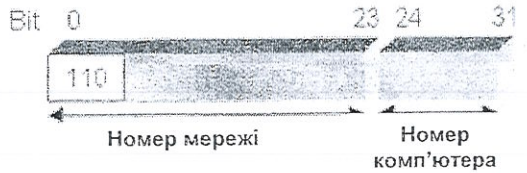

Рис. 3. Позначення мережі класу C

У комп'ютерних мережах, як і в повсякденному житті, неприпустимо відправлення інформації «на село дідусеві». Необхідна точніша адресація, що виключає будь-які невизначеності.

У табл. 1. наведено характеристики адрес різних класів.

Таблиця 1

Характеристика адрес різного класу

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервований

Класи D і E не пов'язані безпосередньо з мережами

Маска мереж

Для правильного функціонування протоколу IP необхідно визначити, який діапазон IP-адрес надано певній локальній мережі. Для цього використовується так звана маска мережі: чотири трійки цифр, що мають значення від 0 до 255. Кінцевий користувач зазвичай має маску 255.255.255.???, де замість знаків питання стоять цифри, які визначають розмір мережі. Ці параметри має повідомити провайдер.

Для стандартних класів мереж маски мають такі значення:

Клас A – 11111111.00000000.00000000.00000000 (255.0.0.0);

Клас B – 11111111.11111111.00000000.00000000 (255.255.0.0);

Клас C – 11111111.11111111.11111111.00000000 (255.255.255.0).

Порядок виконання роботи

1. Згідно із заданими варіантами (табл. 2) для стандартних класів мереж за масками визначити:

а) кількість підмереж;

б) кількість хостів;

в) кількість бітів.

Таблиця 2

Таблиця варіантів завдання

№ з/п	Маски стандартних класів мереж		
1	Маска 255.255.255.128 клас C	Маска 255.255.254.0 клас B	Маска 255.255.255.240 клас A
2	Маска 255.255.255.224 клас B	Маска 255.192.0.0 клас A	Маска 255.255.255.128 клас C
3	Маска 255.224.0.0 клас A	Маска 255.255.224.0 клас B	Маска 255.255.255.224 клас C
4	Маска 255.255.255.240 клас C	Маска 255.255.128.0 клас B	Маска 255.240.0.0 клас A
5	Маска 255.255.255.128 клас A	Маска 255.255.255.252 клас C	Маска 255.255.255.254 клас B
6	Маска 255.255.248.0 клас B	Маска 255.255.192.0 клас A	Маска 255.255.255.240 клас C
7	Маска 255.255.255.248 клас C	Маска 255.255.255.224 клас B	Маска 255.255.255.192 клас A
8	Маска 255.255.192.0 клас B	Маска 255.255.255.224 клас C	Маска 255.255.224.0 клас A
9	Маска 255.255.255.224 клас B	Маска 255.255.255.240 клас A	Маска 255.255.255.128 клас C

Закінчення табл. 2

№ з/п	Маски стандартних класів мереж		
10	Маска 255.255.255.192 клас С	Маска 255.255.255.248 клас В	Маска 255.255.128.0 клас А
11	Маска 255.255.255.240 клас В	Маска 255.255.255.254 клас С	Маска 255.255.248.0 клас А
12	Маска 255.255.255.224 клас А	Маска 255.255.255.128 клас С	Маска 255.255.255.0 клас В
13	Маска 255.255.255.240 клас С	Маска 255.255.255.252 клас В	Маска 255.255.252.0 клас А
14	Маска 255.255.240.0 клас В	Маска 255.254.0.0 клас А	Маска 255.255.255.252 клас С
15	Маска 255.255.248.0 клас А	Маска 255.255.255.252 клас С	Маска 255.255. 255.192 клас В

Звіт. Звіт має містити результати виконання п.п. 2.1 (а,б,в).

Контрольні запитання та завдання

1. Що таке автономні системи? Назвіть типи автономних систем.
2. Дайте визначення маршрутизатора. Що таке порт?
3. Що таке протокол?
4. Що таке IP-адреса? Що таке маска мережі?

Лабораторна робота 2

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ В КОРПОРАТИВНИХ СИСТЕМАХ

Мета роботи: дослідити основні методи динамічної маршрутизації і відповідні маршрутизатори для інтеграції автономних систем у рамках корпоративної інформаційної системи.

Основні теоретичні відомості

Маршрутизатор – це пристрій мережевого рівня еталонної моделі OSI, що використовує одну або більше метрик для визначення оптимального шляху передачі мережевого трафіку на підставі інформації мережевого рівня. Маршрутизатор, передусім, необхідний для визначення подальшого шляху даних, відправлених у велику і складну мережу. Користувач такої мережі відправляє свої дані в мережу і зазначає адресу свого абонента. Дані передаються по мережі і в точках із розгалуженням маршрутів надходять на маршрутизатори, які і встановлюються в таких точках. Маршрутизатор вибирає подальший найкращий шлях. Який шлях буде кращий, визначається кількісними показниками, які називаються ***метриками.*** Кращий шлях – це шлях із найменшою метрикою. У метриці може враховуватися декілька показників, наприклад, довжина шляху, час проходження тощо.

Таблиця маршрутизації містить інформацію, на основі якої маршрутизатор приймає рішення про подальше пересилання пакетів. Таблиця складається з деякої кількості записів маршрутів, у кожному з яких міститься адреса мережі одержувача, адреса наступного вузла, якому слід передавати пакети, і деяка вага запису (метрика). Метрики записів у таблиці потрібні для обчислення найкращих маршрутів до різних одержувачів.

Таблиця маршрутизації зазвичай містить:

- адресу мережі або вузла призначення, або вказівку, що маршрут є *маршрутом за замовчуванням;*
- маску мережі призначення (для IPv4-мереж маска /32 (255.255.255.255) дозволяє вказати одиничний вузол мережі);
- шлюз, що позначає адресу маршрутизатора в мережі, на який необхідно переслати пакет, наступний до вказаної адреси призначення;
- інтерфейс (залежно від системи, це може бути порядковий номер, GUID або символьне ім'я пристрою);
- метрику — числовий показник, що вказує перевагу маршруту. Що менше число, то кращий маршрут.

Таблиця маршрутизації може складатися двома способами.

Статична маршрутизація – це така маршрутизація, в якій записи в таблиці вводяться і змінюються вручну. Такий спосіб вимагає втручання адміністратора щоразу, коли відбуваються зміни в топології мережі. З іншого боку, він є найбільш стабільним і потребує мінімуму апаратних ресурсів маршрутизатора для обслуговування таблиці.

При заданні статичного маршруту зазначається:

- адреса мережі (на яку маршрутизується трафік), маска мережі;
- адреса шлюзу (вузла), який відповідає за подальшу маршрутизацію (або підключений до мережі, що маршрутизується безпосередньо);
- (опціонально) метрика (інколи іменується також «ціною») маршруту. За наявності декількох маршрутів на одну й ту ж мере-

жу деякі маршрутизатори вибирають маршрут із мінімальною метрикою (проте, наприклад, ядро Linux просто ігнорує параметр metric у таблиці маршрутизації, і призначається він лише для протоколів маршрутизації на зразок RIP).

Основні переваги статичної маршрутизації:

- легкість налагодження і конфігурації в малих мережах;
- відсутність додаткових накладних витрат (через відсутність протоколів маршрутизації);
- миттєва готовність (не потрібний інтервал для конфігурації/підстроювання);
- низьке навантаження на процесор маршрутизатора;
- передбаченість у кожен момент часу.

Недоліки:

- погане масштабування (при додаванні N + 1 мережі необхідно зробити 2*(N + 1) записів про маршрути, причому на більшості маршрутизаторів таблиця маршрутів буде різною, при N > 3 – 4 процес конфігурації стає доволі трудомістким);
- низька стійкість до пошкоджень ліній зв'язку (особливо в ситуаціях, коли обрив відбувається між пристроями другого рівня і порт маршрутизатора не отримує статус down);
- відсутність динамічного балансування навантаження;
- необхідність у веденні окремої документації до маршрутів, проблема синхронізації документації і реальних маршрутів.

У реальних умовах статична маршрутизація використовується за наявності шлюзу за замовчуванням (вузла, що володіє зв'язністю з рештою вузлів) і 1–2 мережами. Окрім цього статична маршрутизація використовується для «вирівнювання» роботи протоколів, що маршрутизують, в умовах наявності тунелю (для того, щоб маршрутизація трафіку, що створюється тунелем, не проводилася через сам тунель).

Динамічна маршрутизація – така маршрутизація, коли записи в таблиці оновлюються автоматично за допомогою одного або декількох протоколів маршрутизації RIP, OSPF, EIGRP, IS-IS, BGP тощо. Крім того, маршрутизатор будує таблицю оптимальних шляхів до мереж призначення на основі різних критеріїв: кількості проміжних вузлів, пропускної здатності каналів, затримки передачі даних тощо. Критерії визначення оптимальних маршрутів найчастіше залежать від протоколу маршрутизації, а також задаються конфігурацією маршрутизатора. Такий спосіб побудови таблиці дозволяє автоматично тримати таблицю маршрутизації в актуальному стані й визначити оптимальні маршрути на основі поточної топології мережі. Проте динамічна маршрутизація надає додаткове навантаження на пристрої, а висока нестабільність мережі може призводити до ситуацій, коли маршрутизатори не встигають синхронізувати свої таблиці, що призводить до суперечливих відомостей про топологію мережі в різних її частинах і до втрати даних.

Обслуговуючи великі мережі з великою кількістю маршрутизаторів, складно заповнювати таблиці маршрутів і особливо їх оперативно змінювати, якщо, наприклад, який-небудь із каналів не працює.

Для створення динамічної маршрутизації необхідно, щоб маршрутизатори самі обмінювалися маршрутною інформацією. Для цього були створені спеціальні протоколи.

У маршрутизаторі з динамічним протоколом резидентно завантажена програма (демон – gated або routed для UNIX) змінює таблиці маршрутизації на основі інформації, отриманої від сусідніх маршрутизаторів.

Динамічні протоколи поділяють на дві групи:

- **EGP (External Gateway Protocol)** – зовнішній протокол маршрутизації для використання між AS. До групи входять RIP, OSPF, IGRP (CISCO), IS-IS;
- **IGP (Interior Gateway Protocol)** – внутрішній протокол маршрутизації для використання всередині AS. До групи входять BGP, IDPR.

RIP (Routing Information Protocol) – протокол маршрутної інформації, який використовує алгоритм Белмана–Форда. Вибирається найкоротший маршрут (distance-vector).

Перший стандарт **RIP RFC1058** (Routing Information Protocol C.L. Hedrick Jun-01-1988).

Остання версія **RIPv2 RFC2453** (RIP Version 2 G. Malkin November 1998).

Використовується транспортний протокол **UDP**.

Порт сервера за замовчуванням 520.

Маршрут характеризується **вектором відстані** до місця призначення.

Описи зібраних маршрутів зберігаються в **таблиці маршрутів** (не плутати з таблицею маршрутизації), з якої потім вибирається найкращий маршрут і розміщується в таблиці маршрутизації, яку ще називають **первинною таблицею маршрутизації**.

Таблиця маршрутів повинна містити для кожного маршруту:

- IP-адресу місця призначення (напрям вектора);
- метрику маршруту (від 1 до 15; кількість кроків до місця призначення, модуль вектора);
- IP-адресу найближчого маршрутизатора на шляху до місця призначення;
- позначку, що маршрутну інформацію було змінено;
- різні таймери маршруту (наприклад, актуальність інформації).

Протокол RIP використовують найчастіше (переважно тому, що його було включено в стандартне постачання популярної ОС BSD UNIX 4.x). Принцип роботи протоколу такий.

Кожен маршрутизатор повідомляє своїх сусідів про видимі ним мережі, пересилаючи їм свою таблицю маршрутизації. У таблицях «кращі» маршрути йдуть першими. «Кращим» маршрутом вважається не найшвидший маршрут, а той, що містить найменшу кількість хопів. Тим самим зовсім не береться до уваги пропускна здатність каналів, яка впливає на швидкість передачі даних. Для подолання цієї проблеми в таблиці маршрутизації додають ваги дуг (каналів), які обернено пропорційні пропускній здатності каналу. При формуванні маршруту дані ваги підсумовуються, і найкращим буде маршрут, біля якого сума вагів є найменшою.

Даному протоколу притаманні такі недоліки:

- не передбачено захист від циклічних маршрутів. Тому системний адміністратор повинен перевірити їх відсутність у таблицях;
- максимальна кількість хопів у маршруті 15, що робить його непридатним для використання у великих мережах із великою кількістю роутерів.

Протокол має таку властивість, як Slow Convergence. Повільне перебудування таблиць маршрутизації на роутерах при зміні топології мережі. Це пов'язано з тим, що роутери пересилають всю таблицю маршрутизації, і перед сеансами зв'язку є деякі проміжки часу. Тому може виникнути ситуація, що далеко розташовані роутери пересилатимуть пакети за маршрутом, до якого входить вимкнений канал (зменшити час перебудування таблиць, було обмежено число хопів 15).

Можливі варіанти вирішення цієї проблеми

Зачекати певний час, поки всі роутери в мережі отримають повідомлення про вимкнення каналу і перебудують свої таблиці маршрутизації (чекати доводиться досить довго). «Розмежування горизонтів» – роутер запам'ятовує ім'я інтерфейсу, з якого прийшло повідомлення про вимкнення каналу, і перестає пересилати на цей інтерфейс пакети. При подальшому пересиланні таблиць маршрутизації не пересилати повідомлення про можливість проходження пакетів за маршрутами через цей інтерфейс (тут виникають проблеми у з'єднанні між фреймами мережі).

OSPF (Open Shortest Path First) – відкрити найкоротший маршрут першим (алгоритм Дейкстри), є протоколом стану каналу (link-state).

Перший стандарт OSPF – RFC1131 (OSPF specification J. Moy Oct-01-1989).

Остання версія **OSPFv2** – RFC2328 (OSPF Version 2 J. Moy April 1998).

Повідомлення OSPF інкапсулюється прямо в IP-пакет (поле даних), тобто протоколи транспортного рівня не використовуються.

Поле protocol = 89 (у заголовку IP).

Основні переваги OSPF:

- відсутність обмеження на розмір мережі;
- автономна система може бути поділена на області маршрутизації;
- висока швидкість встановлення маршрутів;
- маршрутизація враховує тип сервісу IP (type-of-service – TOS), тобто для різних сервісів можуть бути різні маршрути;
- кожному інтерфейсу може бути призначена метрика на підставі пропускної здатності, часу повернення – надійності, завантаженості (черга пакетів) – розміру максимального блока даних, який може бути переданий через канал. Окрема ціна може бути призначена для кожного типу сервісу IP. Якщо маршрути мають однакову

ціну, OSPF розподіляє трафік порівну між цими маршрутами. Це називається балансуванням навантаження (Load balancing);

- підтримує підмережі (маску);
- підтримка без адресних мереж (unnumbered) – канали точка-точка між маршрутизаторами, що не мають IP-адрес. Такий підхід дозволяє заощадити IP-адреси;
- використання аутентифікації;
- використовується групова (multicast) адресація замість широкомовної.

На відміну від RIP, цей протокол не «розповідає сусідам про світ», навпаки «світу розповідає про сусідів», пересилаючи не всю таблицю маршрутизації, а лише маленькі повідомлення про стан довколишніх каналів (Link State Advertisement). Роутери, отримуючи повідомлення про зміну топології мережі, перебудовують базу даних із топологією мережі, що зберігається у них. При проходженні пакета через роутер для нього вибирається найшвидший маршрут відповідно до бази даних, що зберігається. Використовуючи цей протокол для синхронізації, мережа менше навантажується системним трафіком, виграючи на обсязі інформації, що передається, і частоті сеансів. Протокол має певні недоліки, наприклад, у великій мережі (близько сотні роутерів) зміна топології мережі спричинить породження тисяч повідомлень LSA про внесені зміни.

Порядок виконання роботи

1. На рис. 4 наведено мережі джерел і одержувачів.

2. Створити таблицю переходів для шести маршрутів згідно з варіантом із табл. 3. Наприклад, варіант 1 – із мережі 10.2.0.0 у мережу 10.1.0.0 – 3 довільних маршрути, і з мережі 10.2.0.0 у мережу 192.168.120.0 – 3 довільних маршрути.

3. На основі таблиці переходів створити таблиці маршрутизації кожного задіяного маршрутизатора (табл. 4).

4. Із кожних груп створених маршрутів (2–3 маршрути) обрати оптимальні за метрикою кількості Hop. (табл. 5).

5. Із кожних груп створених маршрутів (2–3 маршрути) обрати оптимальні за метрикою згідно з варіантом із табл. 3. Наприклад: 10 Мб/с/120/10/230 – швидкість з'єднання 10 Мб; надійність – 120; завантаження – 10; затримка – 230) (табл. 6).

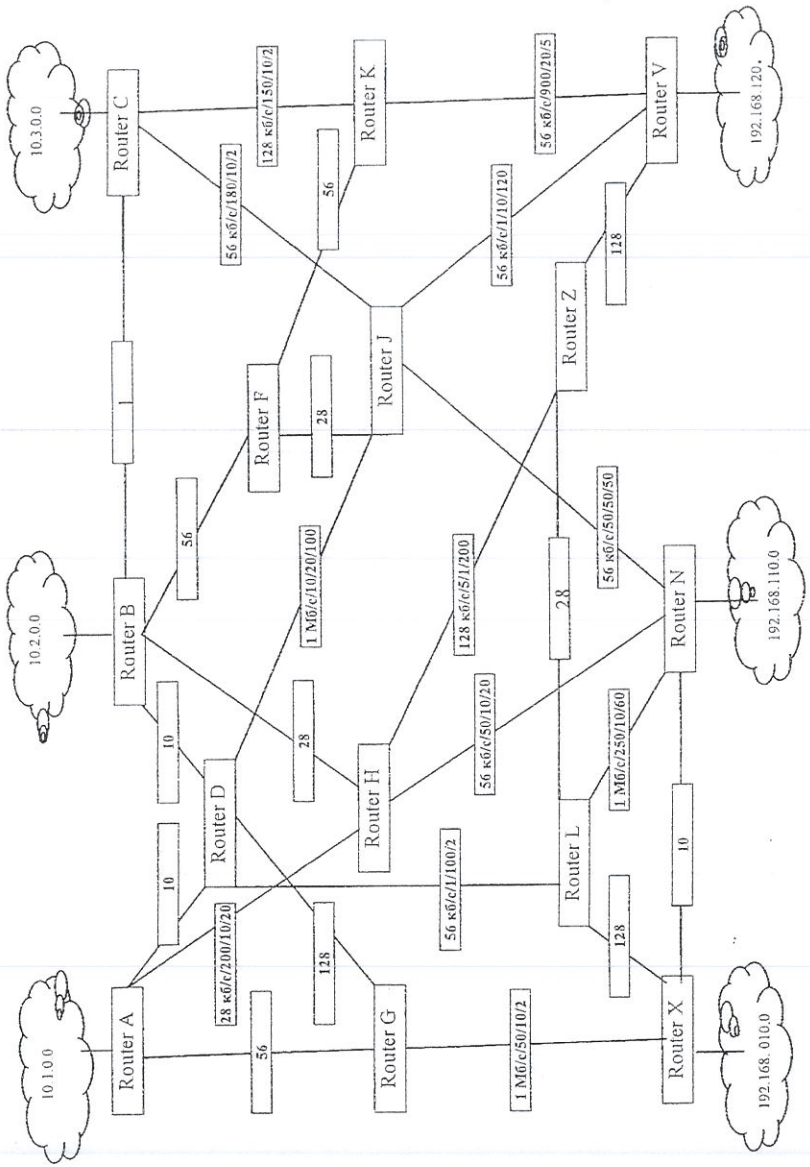

Рис. 4. Мережі джерел і одержувачів

Таблиця 3

Таблиця варіантів завдання

Мережі джерела і одержувача	10.1.0.0	10.2.0.0	10.3.0.0	192.168.100.0	192.168.110.0	192.168.120.0
10.1.0.0		1/5	2/6	3/7	4/8	5/9
10.2.0.0	6/10		7/11	8/12	9/13	10/14
10.3.0.0	11/15	12/16		13/17	14/18	15/19
192.168.100.0	16/20	17/21	18/22		19/23	20/24
192.168.110.0	21/25	22/26	23/27	24/28		25/29
192.168.120.0	26/30	27/1	28/2	29/3	30/4	

Таблиця 4

Таблиця переходів

Джерело (Router)	Одержувач (IP)	Наступний перехід	Залишилося переходів (Hop)

Таблиця 5

Таблиця маршрутів конкретного маршрутизатора

Router *A*		
Одержувач (IP)	Наступний перехід	Залишилося переходів (Hop)

Таблиця 6

Затримка	Надійність	Навантаження
1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16	17	18
19	20	21
22	23	24
25	26	27
28	29	30

Звіт. Звіт має містити результати виконання п.п. 2–5.

Контрольні запитання та завдання

1. Розкрийте поняття маршруту і маршрутизації.
2. Які бувають види маршрутизацій?
3. Що таке статична маршрутизація? Назвіть її переваги і недоліки.
4. Що таке динамічна маршрутизація? Назвіть її переваги і недоліки.
5. Розкрийте поняття метрики і її призначення.
6. Які бувають види метрик?

Лабораторна робота 3

СУЧАСНІ АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Мета роботи: ознайомитися з архітектурними особливостями організації безпеки інформаційних ресурсів у корпоративних інформаційних системах.

Основні теоретичні відомості

Класичні криптографічні методи і алгоритми бувають двох основних типів:

- симетричні (з секретним ключем);
- асиметричні (з відкритим ключем).

У **симетричних методах** для шифрування і розшифровування використовується один і той самий секретний ключ.

До переваг симетричних методів відносять високу швидкодію і простоту. Основним недоліком є те, що ключ має бути відомий і відправникові, і одержувачеві. Це істотно ускладнює процедуру призначення і розподілу ключів між користувачами. Цей недолік став причиною розробки методів шифрування з відкритим ключем – асиметричних методів.

Асиметричні методи використовують два взаємозв'язані ключі: для шифрування і розшифровування. Один ключ закритий і відомий лише одержувачеві. Його використовують для розшифровування. Другий ключ відкритий, тобто він може бути загальнодоступним по мережі і опублікований разом із адресою користувача. Його використовують для виконання шифрування.

Опис алгоритму RSA (Rivest, Shamir and Aldeman)

Схема RSA є блоковим шифром, в якому і відкритий текст, і шифрований текст зображуються цілими числами з діапазону від 0 до n–1 для деякого n. Відкритий текст шифрується блоками, кожен із яких містить двійкове значення, менше деякого заданого числа n. На практиці довжина блока вибирається рівною 2^k бітам, де

$$2^k < n \le 2^{k+1}.$$

Ключі обчислюються за такою схемою:

1. Вибір p, q, де p і q мають бути простими.

Як відправник, так і одержувач повинні знати значення n.

2. Обчислення $n = pq$.

У разі простих p і q маємо функцію Ейлера $\varnothing(n)$.

3. Обчислення $\varnothing(n) = (p - 1)(q - 1)$.

4. Вибір цілого e, при якому $gcd(\varnothing(n), e) = 1$, $1 < e < \varnothing(n)$.

5. Обчислення d за формулою – $d \equiv e^{-1} \bmod \varnothing(n)$.

Відправник знає значення e, і лише одержувачеві відоме значення d.

Таким чином, така схема є алгоритмом шифрування з відкритим ключем KU = $\{e, n\}$ і особистим ключем KR = $\{d, n\}$.

Шифрування і дешифрування для блока відкритого тексту M і блока шифрованого тексту C можна зобразити у вигляді таких форм:

Шифрування

Відкритий текст: $M < n$.

Шифрований текст: $C = M^e \pmod n$.

Дешифрування

Відкритий текст: C.

Шифрований текст: $M = C^d \pmod n$.

Шифрування може проводитися за двома варіантами:

- відкритим ключем одержувача (дешифрування закритим ключем одержувача);
- закритим ключем відправника (дешифрування відкритим ключем відправника).

На рис. 5 наведено перший варіант шифрування, на рис. 6 – другий варіант. Тут e і d – відкритий і закритий ключ відправника.

Рис. 5. Шифрування відкритим ключем одержувача:
d – закритий ключ одержувача; e – відкритий ключ одержувача

Рис. 6. Шифрування закритим ключем відправника:
d – закритий ключ відправника; e – відкритий ключ відправника

Наприклад (рис. 7):

1. Вибирається два прості числа $p = 7$ і $q = 17$.
2. Обчислюється $n = p \times q = 7 \cdot 17 = 119$
3. Обчислюється $\varnothing(n) = (p - 1)(q - 1) = 96$.
4. Вибирається e, взаємно просте з $\varnothing(n) = 96$ і менше, ніж $\varnothing(n)$; у даному випадку $e = 5$.
5. Визначається таке d, що $de = 1 \bmod 96$ і $d < 96$. Відповідним значенням буде $d = 77$, оскільки $77 \times 5 = 385 = 4 \times 96 + 1$.

У результаті отримуємо відкритий ключ KU = {5, 119} та особистий ключ KR = {77, 119}.

У даному прикладі показано використання цих ключів із відкритим текстом, що вводиться M = 19. При шифруванні 19 підноситься до п'ятого степеня, що в результаті дає 2 476 099. У результаті ділення на 119 визначається остача, що дорівнює 66. Отже, 195 = 66 mod119, і тому шифрованим текстом буде 66. Для дешифрування з'ясовується, що 6677 19 mod119.

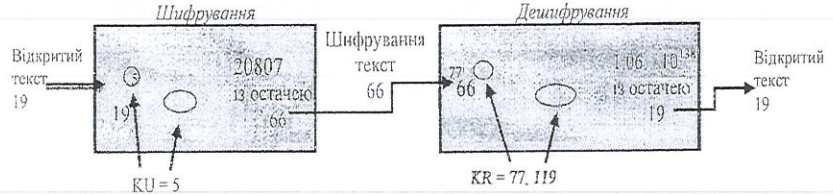

Рис. 7. Приклад використання алгоритму RSA

Порядок виконання роботи

1. Кожен рядок обчислення ключів пояснити прикладом.
2. Написати слово в AsCII-коді (4 букви). Перетворити в двійковий код. Перетворити в десятковий код.
3. Для заданих ключів (e, n), (d, n) навести алгоритм шифрування.
4. Для заданих ключів (e, n), (d, n) навести алгоритм дешифрування прізвища.
5. Написати своє прізвище з чотирьох букв.
6. Для заданих ключів ($e1$, $n1$), ($d1$, $n1$) навести алгоритм для аутентифікації прізвища.
7. Для заданих ключів ($e1$, $n1$), ($d1$, $n1$) навести алгоритм аутентифікації прізвища.

Звіт. Звіт має містити результати виконання п.п. 1–7.

Контрольні запитання та завдання

1. У чому суть класичних криптографічних методів?
2. Що таке шифрування?
3. Що таке дешифрування?
4. Опишіть алгоритм RSA.

Лабораторна робота 4

АНАЛІЗ РОЗРАХУНКУ БАЗОВИХ ХАРАКТЕРИСТИК ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Мета роботи: навчитися розраховувати значення коефіцієнта корисної передачі даних, будувати графіки коефіцієнта корисної передачі даних і часу доставки залежно від доставки різною кількістю пакетів.

Основні теоретичні відомості

Розподілені системи й мережі комп'ютерів припускають наявність безлічі елементів крайового устаткування даних. Ці елементи взаємодіють між собою через мережу комутації пакетів. У кожному вузлі крайового устаткування даних генеруються пакети даних, що складаються з D байтів корисної інформації і h байтів службової інформації (адреси вузлів, тип даних, контрольна сума тощо). Мережа комутації пакетів складається з безлічі комутаторів. При кожному сеансі передачі даних між елементами крайового устаткування даних обирається шлях, який включає певну кількість (r) комутаторів.

Існує багато методів і технологій комутації пакетів. Розглянемо клас завдань комутації пакетів із буферизацією даних у вузлах комутації. Буферизація виконується для виявлення помилок при передачі, зміни службових полів у пакетах тощо. Припустимо, об'єми буферів комутаторів необмежені. У початковому стані ці буфери очищені й готові до прийому даних. Перший крок процесу комутації для кожного вузла полягає в тому, що приймальний буфер заповнюється вхідними даними. Для цього виконується операція PUSH, суть якої полягає в переміщенні даних, що приймаються, до дна буфера. Коли буфер заповнений (тобто прийнято всі байти вхідного пакета), генерується команда «Поворот буферів на 180 градусів».

Продуктивність операції заповнення буфера визначатимемо у відносних одиницях часу – в байт-тактах. Один байт-такт відповідає часу виконання однієї операції PUSH або POP. Іншими словами, один байт-такт дорівнює часу прийому в буфер одного байта інформації. Якщо пакет містить $D+h$ байтів, то час передачі (прийому) цього пакета з буфера (у буфер) дорівнює $D+h$ байт-тактам.

Таким чином, основними параметрами транспортного середовища з комутацією пакетів є кількість комутаторів (r) і довжина заголовка (h), від яких безпосередньо залежить час доставки масиву інформації. Саме величини r і h зумовлюють можливість адаптації часу доставки масиву даних D до конкретних умов функціонування бізнес-додатків. Тому процес вибору необхідного часу доставки масиву даних об'ємом D байтів, виходячи із заданих значень величин r і h, а також із обмежень, що існують як для цих величин, так і для деяких технічних характеристик транспортного середовища з комутацією пакетів, назвемо rh-оптимізацією.

Лема. Нехай пакет даних, який містить D байтів корисної інформації і h байтів заголовка, повинен передаватися в транспортну систему для доставки байтів до приймача інформації. Тоді час доставки пакета даних від джерела **A** до приймача **B** через r комутаторів, кожен із яких вносить затримку пакета на байт-тактів, дорівнюватиме:

$$T^D_{A\to B} = D(r+1) + \sum_{i=1}^{r+1} h_i \quad \text{байт-тактам.}$$

На підставі доведення цієї леми, доведення теореми про мінімальний час передачі D байтів корисної інформації та h_A байтів заголовка між хостом-джерелом і хостом-приймачем n пакетами через обраний маршрут $\boldsymbol{R}$ із r комутаторами, кожен із яких вносить затримку пакета на $h_i \geq 0$ байт-тактів, час доставки дорівнюватиме

$$\min T^D_n = D \div 2\sqrt{Dr * \max\{h_i\}} - \max\{h_i\} + \sum_{i=1}^{r+1} h_i \quad \text{байт-тактам.}$$

Розглянемо окремий випадок передачі масиву даних від **A** до **B**, коли $h_i = h_A \geq 1 \quad \forall i = \overline{1,r}$.

Це означає, що розмір заголовка пакетів, що передається (або затримка в комутаторах) на всьому маршруті $\boldsymbol{R}$ залишається величиною сталою. Така ситуація найбільш типова для сучасних мереж із комутацією пакетів. Аналогічні результати можуть бути отримані й для загального випадку. Вважатимемо, що $h_A = h$, тоді:

$$T^D_n = \left(\frac{D}{n} + h\right)(r+n).$$

Якщо $D = 1$ або $Dr < h$, необхідно встановити $n = 1$. Це означає, що при $Dr < h$ масив об'ємом D байтів має бути переданий одним пакетом і тоді час передачі становитиме:

$$T^D_1 = (D+h)(r+1) \quad \text{байт-тактів.}$$

Аналогічно, якщо $D > 1$ і $Dh < r$ (іншими словами, якщо $n > = D$), то $n := D$. У цьому випадку час доставки масиву об'ємом D байтів дорівнюватиме:

$$T^D_D = (1+h)(r+D) \text{ байт-тактів.}$$

Таким чином, час доставки T^D_n буде мінімальним або при $n = 1$, або при $n = D$ (залежно від співвідношення величин h і r) і дорівнюватиме

$$\min T^D_n = \left(\sqrt{hr} + \sqrt{D}\right)^2.$$

Коефіцієнт корисної передачі даних

Теоретичний час доставки масиву інформації буде мінімальним, коли між джерелом і приймачем даних відсутні транзитні вузли (комутатори, маршрутизатори) і пакет не має заголовка. У такому разі час доставки даних об'ємом D байтів дорівнюватиме D байт-тактам. Якщо ж пакет даних містить заголовок розміром h байтів, то мінімальний час його доставки становитиме $D + h$ байт-тактів. Таким чином, за відсутності транзитних вузлів коефіцієнт корисної передачі даних (КПД) визначається як:

$$k_{\text{КПД}} = \frac{\min T^D}{T_n}.$$

Коефіцієнт корисної передачі даних є основним показником транспортної системи з комутацією пакетів. Він дозволяє розраховувати ефективність конкретної системи передачі даних і коректувати її характеристики продуктивності з урахуванням розміру полів фіксованої довжини передаваних пакетів.

Порядок виконання роботи

1. Згідно з таблицею варіантів (табл. 7) провести розрахунки за заданими формулами.
2. Розрахувати значення коефіцієнта корисної передачі даних.

Таблиця 7

Таблиця варіантів завдання та розрахунків

Варіант	D	r	h	min$T$	T_I^D	T_D^D	$T_1^D / T_{\min}$	$T_D^D / T_{\min}$	n_0
	байт	кількість	байт						
1	32	2	2						
2	34	3	4						
3	36	4	6						
4	38	5	8						
5	40	6	10						
6	42	7	12						
7	44	8	14						
8	46	2	16						
9	48	3	2						
10	50	4	4						
11	52	5	6						
12	54	6	8						
13	56	7	10						
15	58	8	12						
16	60	2	14						
17	62	3	16						
18	64	4	2						
19	66	5	4						
20	68	6	6						
21	70	7	8						
22	72	8	10						
23	74	2	12						
24	76	3	14						
25	78	4	16						

3. Побудувати графіки коефіцієнта корисної передачі даних і часу доставки залежно від доставки різною кількістю пакетів. Рекомендується виконувати у додатку MS Excel.

Звіт. Звіт має містити результати виконання п.п. 1–3.

Контрольні запитання та завдання

1. Що таке коефіцієнт корисної передачі даних?
2. Як визначається продуктивність операції заповнення буфера?
3. Розкрийте суть *rh*-оптимізації.
4. Опишіть структуру заголовка пакета даних.

СПИСОК ЛІТЕРАТУРИ

1. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум. – 4-е изд. – Спб. : Питер, 2003. – 992 с.
2. *Столлингс В.* Современные компьютерные сети / В. Столлингс. – СПб. : Питер, 2003, – 783 с.
3. *Столлингс В.* Компьютерные сети, протоколы и технологии Интернета / В. Столлингс. – СПб. : БХВ-Петербург, 2005. – 832 с.
4. *Столлингс В.* Основы защиты сетей. Приложения и структуры / В. Столлингс. – М. : Издательский дом «Вильямс», 2002. – 432 с.
5. *Алишов Н. И.* Развитые методы взаимодействия ресурсов в распределенных системах / Н. И. Алишов. – К. : Сталь, 2009. – 448 с.
6. *Олифер В. Г.* Основы сетей передачи данных / В. Г. Олифер, Н. А. Олифер. – М. : Интернет-университет информационных технологий, 2003. – 248 с.

ЗМІСТ

Навчальне видання

КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Лабораторний практикум
для студентів напряму підготовки
6.050101 «Комп'ютерні науки»

Укладачі: ХОЛЯВКІНА Тетяна Володимирівна
ВАСИЛЕНКО Валерій Андрійович

Редактор *Л. М. Дудченко*
Технічний редактор *А. І. Лавринович*
Коректор *Д. Д. Здірук*
Комп'ютерна верстка *Н. С. Ахроменко*

Підп. до друку 24.06.2014. Формат 60x84/16. Папір офс.
Офс. друк. Ум. друк. арк. 1,63. Обл.-вид. арк. 1,75.
Тираж 100 пр. Замовлення № 129-1.

Видавець і виготівник
Національний авіаційний університет
03680. Київ – 58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002