МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА

К. В. Плахотніков

КОМП'ЮТЕРНІ МЕРЕЖІ

КОНСПЕКТ ЛЕКЦІЙ

(для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122 – Комп'ютерні науки)

Харків
ХНУМГ ім. О. М. Бекетова
2023

УДК 004 – 77

Плахотніков К. В. Комп’ютерні мережі : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122 – Комп’ютерні науки / К. В. Плахотніков ; Харків. нац. ун-т міськ. госп. ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2023. – 156 с.

Автор
канд. техн. наук К. В. Плахотніков

Рецензент
Н. Д. Сізова, доктор фізико-математичних наук, професор, професор кафедри комп’ютерних наук та інформаційних технологій (Харківський національний університет міського господарства імені О. М. Бекетова)

Рекомендовано кафедрою комп’ютерних наук та інформаційних технологій, протокол № 9 від 27 січня 2023 р.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AD (Admin Distance) – адміністративна відстань

ARP (Address Resolution Protocol) – протокол визначення адреси

Arpanet (Advanced Research Projects Agency Network) – комп'ютерна мережа, створена в 1969 році

ASCII (American Standard Code For Information Interchange) – назва таблиці, в якій деякими друкованим і недрукованим символам зіставлені числові значення коду

BPDU (Bridge Protocol Data Unit) – кадр (одиниця даних) протоколу управління мережними мостами

CAN (Controller Area Network) – мережа контролерів

DARPA (Defense Advanced Research Projects Agency) – управління Міністерства оборони США

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузла

DT-комутатори (Distributed Trunking Switch) – комутатор мережний

EIGRP (Enhanced Interior Gateway Routing Protocol) – пропрієтарний протокол маршрутизації

FOIRL (Fiber Optic Inter Repeater Link) – це перший стандарт комітету 802.3 щодо використання оптоволокна в мережах Ethernet

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертексту

HTTPS (Hyper Text Transfer Protocol Secure) – розширення протоколу HTTP

ICMP (Internet Control Message Protocol) – протокол мережних керуючих повідомлень

IEEE 802.11 (Institute of Electrical and Electronics Engineers) – набір стандартів зв'язку для комунікації в бездротовій локальній мережній

IEEE 802.1Q (Institute of Electrical and Electronics Engineers) – відкритий стандарт, який описує процедуру тегування трафіку

IPv6 (Internet Protocol version 6) – нова версія Інтернет – протоколу

IP-адреса (Internet Protocol Address) – це ідентифікатор (унікальний числовий номер) мережного рівня

ISO 8583 – стандарт ISO, що описує процес передачі та формат фінансових повідомлень системами, що обробляють дані банківських платіжних карток

L3 – 3-й рівень мережної моделі OSI

LACP (Link Aggregation Control Protocol) – стандартний протокол управління канальною агрегацією

LAN (Local Area Network) – локальна обчислювальна мережа

MAC-адреса (Media Access Control) – унікальний ідентифікатор, який присвоюється кожній одиниці мережного обладнання

NAT (Network Address Translation) – перетворення мережних адрес

NCP (Network Control Program) – мережний протокол, який був першим стандартом мережевого протоколу в ARPANET.

NSFNET (National Science Foundation Network) – комп'ютерна мережа Національного фонду науки США

OSI (The Open Systems Interconnection model) – мережна модель стека мережних протоколів

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації

PAgP (Port Aggregation Protocol) – протокол агрегування каналів

PAT (Port Address Translation) – це NAT з перевантаженням

RIR (Regional Internet Registry) – організація, яка займається питаннями адресації та маршрутизації в інтернеті

SSID (Service Set Identifier) – це символьна назва бездротової точки доступу Wi-Fi , що служить для ідентифікації її серед інших точок користувачами або пристроями, що підключаються до мережі

STP (Spanning Tree Protocol) – канальний протокол

TCP/IP (Transmission Control Protocol / Internet Protocol) – набір протоколів мережі Інтернет

UDP (User Datagram Protocol) – протокол користувальницьких датаграм

VLAN (Virtual Local Area Network) – віртуальна локальна комп’ютерна мережа

VLSM (Variable Length Subnet Mask) – безкласова адресація, що ґрунтується на змінній довжині маски підмережі

WAN (Wide Area Network) – комп’ютерна мережа, що охоплює величезні території

WEP (Wired Equivalent Privacy) – алгоритм забезпечення безпеки мереж Wi-Fi

Wi-Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11

WPA, WPA2 (Wi-Fi Protected Access) – програми сертифікації бездротових пристроїв, розроблені об’єднанням Wi-Fi Alliance для захисту бездротової Wi-Fi мережі

БД – база даних

ГІ – Глобальна інформаційна інфраструктура

ОЗП (Оперативний запам’ятовуючий пристрій) – технічний пристрій, що реалізує функції оперативної пам’яті

ВСТУП

Інформатизація суспільства та активний розвиток сучасних інформаційних технологій супроводжуються збільшенням ролі комунікаційних систем різного призначення та комп'ютерних мереж, що в свою чергу сприяє розвитку в області формування сучасного інформаційного простору.

Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі і навчальної, для якої важливе значення мають час та оперативність її доставки до користувачів.

Однією з основних тенденцій розвитку сучасних комп'ютерних мереж стає розширення доступності інформаційних та обчислювальних ресурсів мереж для окремих абонентів.

У зв'язку з цим окремі абоненти комп'ютерних мереж стають все більш активними споживачами їх ресурсів і учасниками створення баз даних, що безпосередньо володіють технікою доступу до інформаційних ресурсів комп'ютерних мереж.

З іншого боку підвищення активності окремих абонентів комунікаційних мереж обумовлене розподілом інформаційних та обчислювальних ресурсів сучасних комп'ютерних мереж, у зв'язку з чим в розподілених системах різко зростає роль комунікацій як на рівні баз даних і прикладних завдань, так і на рівні технічних систем.

В період пандемії та дії військового стану роль комп'ютерних мереж значно зросла як на рівні роботи сучасних підприємств та організацій, так і на рівні освіти.

Все частіше використовуються в процесі навчання та роботи сервіси обміну документами (електронна пошта), хмарні сховища, сервіси обміну повідомленнями в on-line, електронні бібліотеки тощо, що значно збільшує ефективність як навчання так і роботи.

Особливе місце займають сучасні технології комп'ютерних мереж, серед яких слід виділити локальні та глобальні мережі. Це пояснюється необхідністю використання корпоративної інформації, що міститься в корпоративних базах

даних, що можуть розташовуватися як в окремих підрозділах організації, так й за її межами.

Сучасні технології оброблення документів різного призначення базуються на засобах телекомунікаційного зв’язку й стандартів комп’ютерних мереж, які виступають як транспортні системи передачі даних.

Для підвищення ефективності функціонування мереж підприємств та організацій повинні використовуватися засоби їх модернізації у випадку збільшення кількості робочих станцій та користувачів.

Це призводить до необхідності більш детальнішого вивчення та використання спеціальних пристроїв та відповідних стандартів для об’єднання окремих локальних мереж в єдину.

Важливу роль в підготовці фахівців, що мають відповідні знання та навички відіграє вивчення освітньої компоненти «Комп’ютерні мережі» з використанням в навчальному процесі спеціальних програм.

1 ІСТОРІЯ РОЗВИТКУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Комп'ютерна мережа – від початку до сьогодення

З появою персональних комп'ютерів питання обміну даними набули глобального характеру. Завдяки спеціальним програмним та апаратним засобам стало можливим організувати взаємодію між людьми, відокремленими один від одного на відстань у десятки тисяч кілометрів.

Створення комп'ютерних мереж викликано потребою спільного використання інформації на віддалених один від одного комп'ютерах. Мережі надають персональним комп'ютерам можливість не тільки обмінюватися інформацією, а й спільно використовувати обладнання для одночасної роботи з документами.

Комп'ютери вже не так давно увійшли в сучасний світ, в усі сфери людської діяльності, тим самим, створюючи необхідність у забезпеченні різним програмним забезпеченням.

Об'єднання комп'ютерів у мережі дозволило значно підвищити продуктивність праці. Комп'ютери використовуються для виробничих або офісних потреб, для навчання в навчальних закладах тощо.

В наш час комп'ютерні мережі набули широкого поширення.

Якщо в одній будівлі або комплексі будівель є кілька комп'ютерів, користувачі яких повинні спільно вирішувати завдання, обмінюватися даними чи використовувати загальні дані, то ці комп'ютери доцільно об'єднати в комп'ютерну мережу.

Використання комп'ютерних мереж дозволяє забезпечити колективну обробку даних користувачами, підключеними до мережі комп'ютерів, організовувати обмін даними між ними та спільне використання програм, принтерів та інших пристроїв.

Тому практично всі підприємства, що мають більше одного комп'ютера, об'єднують свої комп'ютери в комп'ютерні мережі. Багато користувачів портативних комп'ютерів підключаються до комп'ютерної мережі фірми або приходячи в офіс, з'єднуються з комп'ютером фірми по каналам зв'язку.

Процес розвитку комп’ютера рухається з постійно швидким прискоренням, у зв’язку з чим, комп’ютери стали обов’язковим і незамінним атрибутом підприємства, офісу чи організації.

Однією з найбільш перспективних на даний момент областей дослідження є розробка так званих нейрокомп’ютерів, здатних зберігати великі обсяги інформації щодо сучасного комп’ютера при мінімальних розмірах самих носіїв інформації.

Великого успіху останнім часом набули віртуозні технології, які дозволяють з великою точністю моделювати фізичні явища, процеси, предмети, їх взаємодію тощо. Такі технології використовуються в різних галузях діяльності людини.

В наш час більшість організацій зберігає і спільно використовує в мережному середовищі величезні обсяги життєво важливих даних. Ось чому мережі зараз так необхідні.

Одна з перших мереж виникла з розвитком обчислювальної техніки, що зажадала створення мережі хоча б з двох комп’ютерів і потребувала забезпечення багато разів більшою, ніж могла дати в той час одна машина, надійності при управлінні відповідальним процесом у режимі реального часу.

Так, при запуску космічного апарату необхідні темпи реакції на зовнішні події перевершують можливості людини, і вихід з ладу керуючого комп’ютера загрожує жахливими наслідками.

У простій схемі роботу цього комп’ютера дублює другий, при збої активної машини вміст її процесу і оперативного запам’ятовуючого пристрою дуже швидко перекидається на другу, яка підхоплює управління (у реальних системах все, звичайно, відбувається істотно складніше).

Незабаром після появи на початку 80-х років XX століття персональних комп’ютерів їх стали об’єднувати в мережі, що дозволило спільно використовувати файли, бази даних і апаратні ресурси, такі як принтери. До середини 80-х років XX століття мережі стали настільки великими і складними, що управляти ними стали відділи інформаційного забезпечення.

Крім того, мережі часто виходять за рамки однієї установи, стають глобальними. Це вже вимагає кваліфікованого персоналу з телефонних мережах, мікрохвильового або супутникового зв'язку.

Мережі, що складаються з комп'ютерів, сприяли появі нових технологій обробки інформації, таких як мережні технології. У найпростішому випадку мережні технології дозволяють спільно виключати ресурси, такі як накопичувачі великої ємності, друкуючі пристрої, доступ до Інтернету, бази даних тощо.

Звичною стала можливість обміну електронними повідомленнями між користувачами комп'ютерної мережі.

В умовах організації електронна пошта забезпечує електронний управлінський документообіг.

Найбільш сучасні і перспективні підходи до мереж пов'язані з використанням колективного поділу праці при спільній роботі з інформацією, а саме розробці різних документів і проєктів, спільне використання баз даних, управління установою або підприємством.

Завдяки відносно великим довжинам ліній зв'язку можна передавати інформацію в цифровому вигляді з високою швидкістю передачі.

На невеликих відстанях такий спосіб передачі неприйнятний через неминуче загасання високочастотних сигналів. В цих випадках доводиться вдаватися до додаткових технічних рішень (протоколів корекції помилок). При підключенні комп'ютера до мережі він стає вузлом мережі і називається робочою станцією.

Після запуску в 1957 році штучного супутника Землі, Міністерство оборони США вирішило, що на випадок війни потрібна надійна система передачі інформації, яка повсюдно б поширювалася.

Агентство передових дослідницьких проєктів Defense advanced research projects agency (DARPA) запропонувало розробити для цього комп'ютерну мережу.

Розробка такої мережі була доручена університету в Лос-Анджелесі. Комп'ютерні мережа була названа «Advanced research projects agency network» (ARPANET) і в 1969 році в рамках проєкту об'єднала чотири наукові установи. Всі роботи фінансувалися за рахунок Міністерства оборони США, мережа ARPANET почала активно розвиватися, після чого її почали використовувати вчені працівники з різних галузей науки.

Перший сервер ARPANET було встановлено 1 вересня 1969 року в Каліфорнійському університеті. Цей комп'ютер Honeywell 516 мав 12 кілобайт оперативної пам'яті.

До 1971 року була розроблена перша програма для відправки електронної пошти через мережу, де відразу стала дуже популярна і практична. У 1973 році до мережі були підключені, через телефонний кабель, перші організації з Великобританії та Норвегії, де мережа стала міжнародною.

У 70-х роках XX століття мережа в основному використовувалась для відправки електронної пошти, тоді ж з'явилися перші списки поштової розсилки, новини і дошка оголошень.

В ті часи мережа ще не могла взаємодіяти з іншими мережами, побудованими на інших технічних стандартах.

До кінця 70-х років XX століття почали швидко розвиватися протоколи передачі даних, які були стандартні в 1983 році.

Активну роль в розробці і стандартизації мережних протоколів відігравав Джон Постел. 1 січня 1983 року мережа ARPANET перейшла на Transmission control protocol / internet protocol (TCP/IP), що застосовується до сьогодні для об'єднання (або, як ще кажуть, «нашарування») мереж. Саме у 1983 році термін «інтернет» закріпився за мережею ARPANET.

У 1984 році у мережі ARPANET з'явився суперник. Національний науковий фонд США заснував велику мережу «National science foundation network» (NSFNET), яка була сформована з нерозвинених мереж і мала набагато більшу здатність, ніж ARPANET.

До цієї мережі за рік підключилися приблизно 15000 комп'ютерів, назва «Інтернет» почало плавно переходити до NSFNET.

У 1988 році був винайдений протокол «Internet relay chat», завдяки чому в Інтернеті стало можливе спілкування в реальному вигляді.

У 1989 році в Європейській раді з ядерних досліджень, народилася концепція всесвітньої павутини.

Всесвітнє павутиння це глобальний інформаційний простір, заснований на структурі Інтернету і протоколі передачі даних «Hyper text transfer protocol» (HTTP).

Для позначення всесвітньої павутини також використовують термін «веб».

У 1990 році мережа ARPANET припинила своє існування, програвши конкуренцію NSFNET та зафіксовано перше підключення до Інтернету по телефонній лінії.

У 1991 році всесвітня павутина стала розвинена і доступна в Інтернеті і набирала популярність. У 1995 році NSFNET повернулася до ролі дослідницької мережі, планом всього трафіку Інтернету тепер займались мережні провайдери, а не суперкомп'ютери Національного наукового фонду.

Також, у 1995 році, всесвітня павутина стала головним постачальником інформації в комп'ютерні мережі, обігнавши по об'єму трафіку протокол пересилки файлів, був створений консорціум всесвітньої павутини.

Можна сказати, що всесвітня павутина придбала Інтернет і створила його національне обличчя.

З 1996 року всесвітня павутина в деякій мірі підміняє собою поняття «Інтернет». У 1990 році Інтернет об'єднав у собі більшість існуючих у той час мереж (хоча деякі, як Фідонет, залишилися такими ж).

З'єднання виглядало привабливим завдяки відсутності єдиного керівництва, а також завдяки відкритості технічних стандартів Інтернету, що робило локальні мережі незалежними від бізнесу чи компаній.

До 1997 року в Інтернеті нараховувалось близько 15 мільйонів комп'ютерів, було зареєстровано більше 1 мільйону доменних імен. Інтернет став дуже популярним засобом обміну інформацією.

В даний час підключитися до локальних мереж можна через супутники зв'язку, кабельне телебачення, радіосигнал, телефон, стільниковий зв'язок, спеціальні оптиковолоконні лінії або кабель.

Всесвітня мережа стала невід'ємною частиною життя у розвинутих країнах.

Народження комп'ютерних мереж було викликано нагальною потребою мати можливість для спільного використання даних.

Якби користувач підключив свій комп'ютер до інших, він зміг би працювати з їх даними та їх принтерами.

Мережею називається група з'єднаних комп'ютерів та інших пристроїв.

Комп'ютерна мережа – набір апаратних засобів і алгоритмів, що забезпечують з'єднання комп'ютерів, периферійних пристроїв і дозволяють їм спільно використовувати загальну дискову пам'ять, периферійні пристрої, обмінюватися даними тощо.

Комп'ютери, підключені до локальної мережі, називаються станціями.

На сьогодні понад 130 мільйонів комп'ютерів, тобто більше 80%, об'єднані в комп'ютерні мережі, починаючи від малих локальних мереж до глобальних мереж Internet.

Тенденція до об'єднання комп'ютерів у мережі обумовлена низкою причин, таких як необхідність одержання і передачі повідомлень не відходячи від робочого місця, необхідність швидкого обміну інформацією між користувачами, можливість швидкого отримання різноманітної інформації, незалежно від її місцезнаходження тощо.

До середини 2008 року число користувачів, які регулярно використовували комп'ютерну мережу, склало близько 1,4 мільярда осіб.

В даний час комп'ютерні мережі об'єднуються у глобальні мережі, охоплюючи цілі країни і континенти.

1.2 Класифікація комп’ютерних мереж

На сьогоднішній день широко використовується загальноприйнята класифікація комп’ютерних мереж, а саме за масштабами, типом функціональної взаємодії та типом мережної топології.

За розміром, охопленою територією (за масштабами) комп’ютерні мережі поділяються на наступні:

– локальна мережа, що організовує спільне підключення декількох окремих комп’ютерів до єдиного каналу передачі даних. Дана мережа діє в межах однієї організації, установи, фірми. Розмір локальних мереж не перевищує десять кілометрів;

– об’єднання декількох будівель;

– міська або регіональна мережа, яка діє в межах міста і регіону, в якій абоненти можуть знаходиться на відстані від десяти до ста кілометрів. В даний час така мережа є частиною деякої глобальної мережі;

– глобальна обчислювальна мережа, що з’єднує країни, континенти. У загальному випадку комп’ютер може знаходитися в будь-якій точці земної кулі. Ця обставина робить економічно неможливою прокладку ліній зв’язку, наприклад, телефонні лінії та супутникові лінії зв’язку.

За типом функціональної взаємодії комп’ютерні мережі поділяються на наступні:

– між клієнтом та сервером відбувається виконання специфічних дій за запитами клієнта, при цьому сам сервер не ініціює жодної взаємодії з клієнтом;

– змішана мережа, що забезпечує зв’язок з різними користувачами, які дозволяють спільно використовувати файли, жорсткі диски, принтери тощо;

– тимчасова мережа, що забезпечує зв’язок персональних комп’ютерів кінцевих користувачів і дозволяє спільно використовувати жорсткі диски, принтери тощо;

– багаторангова мережа , що забезпечує різноманітність користувачів.

За типом мережної топології комп’ютерні мережі поділяються на наступні:

– шина це пристрій, що підключається до кабелю послідовно, обмеження на довжину визначає максимальну відстань між станціями. Недоліком є те, що при використанні топології шини складно визначити несправність кабельної системи;

– зірка це топологія, при якій кожен пристрій підключається до центрального пристрою. Передача даних відбувається тільки через центральний пристрій. Перевага в тому, що при з’єднанні зоряного типу легко шукати несправність в мережі. Недоліком є те, що цей тип не завжди надійний, тому що вихід з ладу центрального вузла може призвести до зупинки мережі;

– кільце це топологія, при якій до кабельного сегменту послідовно з’єднуються всі станції мережі, щоб вийшло кільце. Дані передаються тільки в одному напрямку;

– комірчаста (змішана) топологія використовується в регіональних мережах. При виході будь-якого сегменту існує маршрут, за яким дані можуть, передані заданому вузлу і володіє високою точністю перезавантаження мережі.

1.3 Структура комп’ютерних мереж

Якщо підрозділи підприємства розташовані не дуже далеко один від одного (наприклад, в межах одного міста), можна прокласти власні лінії зв’язку між підрозділами, але це коштує дуже дорого.

Частіше доцільно орендувати наявні лінії зв’язку у постачальників телекомунікаційних послуг.

При цьому потрібно прокласти кабель тільки від кожного підрозділу підприємства до найближчого до цього підрозділу вузла мережі постачальника телекомунікаційних послуг.

Якщо обсяг даних, переданих і прийнятих підрозділом підприємства, незначний, то з вузлом мережі постачальника телекомунікаційних послуг можна зв’язуватися по телефонних лініях за допомогою модему.

У всіх випадках для створення розподіленої мережі необхідно відповідне обладнання (модеми, маршрутизатори тощо).

В Україні створення розподілених мереж ускладнено, бо більшість розгалужених мереж передачі даних низькошвидкісні аналогові мережі, малопридатні для передачі великих масивів.

Також прокладка кабелів зв'язку дуже дорого коштує і процес стикається з численними бюрократичними перешкодами.

Для ефективної роботи користувачів у комп'ютерній мережі застосовується допоміжне програмне забезпечення, а саме:

– електронна пошта, яка забезпечує доставку листів (довільних файлів, голосових повідомлень) від одних користувачів комп'ютерної мережі іншим, а іноді дозволяє спілкуватися і з віддаленими користувачами;

– засоби віддаленого доступу, які дозволяють підключатися до комп'ютерної мережі за допомогою спеціальних пристроїв і працювати на комп'ютері, як ніби він безпосередньо підключений до мережі;

– засоби групової роботи, що дозволяють спільно працювати над документами, забезпечують узгодженість версій документів у різних користувачів, надають кошти для організації документообігу підприємства тощо;

– програми резервування, які дозволяють створювати резервні копії даних, що зберігаються на комп'ютерах комп'ютерної мережі, а при необхідності відновлювати дані з їх резервної копії;

– засоби управління локальною мережею, що дозволяють керувати ресурсами комп'ютерної мережі з одного робочого місця.

1.4 Нові можливості комп'ютерних мереж

У документах 1998 року фахівці прогнозували, що 4 мільярди IP-адрес (Internet protocol) закінчаться до 2018 року. У 2000 році говорили, що їх вистачить до 2013 року, а у 2005 році стало очевидно, що до настання перших проблем залишилося декілька років.

Щоб приблизно уявити, скільки приладів зараз реально претендують на IP-адреси, досить згадати, що в 1996 році в світі діяло 300 мільйонів персональних комп'ютерів, у 2000 році ця цифра вже наблизилася до 600 мільйонів, а у 2010 року вже 1,3 мільярда.

До них варто додати сервери, мережне обладнання, яке становить фізичну основу Інтернету, мобільні телефони та інші пристрої з виходом в мережу.

У цілому, як показала практика, вартість обробки даних у комп'ютерних мережах, за рахунок розширення можливостей обробки даних, краще завантаження ресурсів і підвищення надійності функціонування системи, не менш ніж у півтора рази нижче в порівнянні з обробкою аналогічних даних на автономних комп'ютерах.

При об'єднанні комп'ютерів в мережу система повинна зберігати надійність, тобто відмова будь-якого комп'ютера не повинна призводити до зупинки роботи системи, і більше того, повинна забезпечуватися передача функцій призупиненого комп'ютера на інший комп'ютер мережі.

У 2004 році в світі було зареєстровано 63 мільйони доменних імен.

У 2002 році компанія LG представила перший холодильник з виходом в Інтернет, а станом на 2022 рік вже кожен прилад має вихід до Інтернету.

У популярній пресі згадується, що розрядності IPv6 (Internet protocol version 6) вистачить більш ніж на одну тисячу адрес на кожний квадратний метр поверхні нашої планети. Наші власні обчислення показують, що це цифра занижена на кілька порядків. Площа поверхні Землі до речі, 510 073 квадратних кілометрів.

Бурхливий розвиток комп'ютерних мереж та підключення все більшого числа персональних комп'ютерів до мереж, привело в останні десятиліття до формування основ концепції мережного комп'ютера.

Слідуючи з того, якого прогресу змогли мережні технології досягти за останні роки, не важко здогадатися, що найближчим часом швидкість передачі даних з комп'ютерної мережі зросте щонайменше вдвічі.

Контрольні запитання

1. Що ви знаєте про ARPANET?
2. Коли і за яких умов виник протокол HTTP?
3. Наведіть класифікацію мереж за типом мережної топології.
4. Скільки комп’ютерів на вашу думку об’єднані у мережі у 2022 році?
5. У чому різниця глобальної та локальної мережі?
6. Які засоби віддаленого доступу вам відомі?
7. Яка кількість IP-адрес у світ станом на початок 2023 року?
8. Які причини об’єднання комп’ютерів у мережі?

2 ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Основна термінологія та поняття

Комп'ютерна мережа – сукупність комп'ютерів та інших пристроїв, що з'єднані лініями зв'язку та обмінюються інформацією між собою відповідно до певних правил, а саме протоколів.

Основна мета мережі полягає в забезпеченні користувачам можливості спільного використання мережних ресурсів. Мережними ресурсами називають інформацію, програмне та апаратне забезпечення. Щоб організувати локальну комп'ютерну мережу з невеликою кількістю комп'ютерів найчастіше використовується одна з типових топологій (звичайна шина, кільцева, зірка тощо). Ці топології мають властивість однорідності, коли всі комп'ютери володіють однаковими правами на доступ до інших комп'ютерів (за винятком центрального комп'ютера в топології зірки).

Однорідність структури дозволяє легко збільшити кількість комп'ютерів, полегшує технічне обслуговування та експлуатацію мережі.

Однак ці топології накладають певні обмеження на довжину лінії зв'язку між двома вузлами, кількість вузлів в мережі та інтенсивність трафіку.

Для зняття цих обмежень використовуються спеціальні методи структурування мережі та спеціальне мережне обладнання, а саме повторювачі (ретранслятори), концентратори, вузли, мости, комутатори, маршрутизатори. Це обладнання називається комунікаційним, з його допомогою окремі сегменти мережі взаємодіють один з одним.

Ретранслятор – найпростіший пристрій зв'язку, який використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної довжини мережі. Ретранслятор покращує якість сигналу, що передається (відновлює потужність, амплітуду сигналу і т. д.). Ретранслятор який має кілька портів і з'єднує кілька фізичних сегментів, часто називають концентратором або хабом.

Міст (bridge) ділить середовище передачі в мережі на частини (логічні сегменти), передаючи інформацію з одного сегмента мережі на інший тільки в

тому випадку, коли така передача є необхідною, тобто якщо адреса комп'ютера призначення належить іншій підмережі. Міст ізолює трафік однієї підмережі від трафіку іншої, покращуючи загальну продуктивність передачі даних в мережі.

Комутатор (switch) за принципом обробки кадрів практично не відрізняється від моста. Єдина відмінність полягає в тому, що він є свого роду комунікаційним мультипроцесором, оскільки кожен з його портів оснащений мікросхемою, яка обробляє кадри за алгоритмом моста незалежно від мікросхем інших портів. Завдяки цьому загальна продуктивність комутатора, як правило, вища від продуктивності традиційного моста, що має один процесор.

Маршрутизатор (router) це спеціалізований мережний пристрій, який має два або більше мережних інтерфейсів та пересилає пакети даних між різними сегментами мережі. Маршрутизатор може зв'язувати неоднорідні мережі різної архітектури. Для прийняття рішень про пересилку пакетів він використовує інформацію про топологію мережі та правила, встановлені адміністратором.

Шлюз використовується для об'єднання мереж з різними типами програмного та апаратного забезпечення.

Зазначимо, що з кожним роком підсилюється тенденція зближення комп'ютерних і телекомунікаційних мереж різних видів. Намагаються створити універсальну, так звану мультисервісну мережу, здатну надавати послуги як комп'ютерних, так і телекомунікаційних мереж.

До телекомунікаційних мереж відносяться телефонні мережі, радіомережі й телевізійні мережі. Головне, що поєднує їх з комп'ютерними мережами – те, що в якості ресурсу, який надається клієнтам, виступає інформація. Однак ці мережі, як правило, представляють інформацію у різному вигляді. Так, споконвічно комп'ютерні мережі розроблялися для передачі цифрової інформації, що часто називають просто даними, у результаті в комп'ютерних мереж є інша назва, а саме мережі передачі даних, у той час як телефонні мережі й радіомережі були створені для передачі тільки голосової інформації, а телевізійні мережі передають і голос, і зображення.

Незважаючи на це, конвергенція телекомунікаційних і комп'ютерних мереж йде за декількома напрямками.

Еволюційні процеси в галузі зв'язку можна спостерігати як у вдосконаленні рівнів технологічного розвитку, так і в зміні термінології.

Так, загальноприйнятий термін «електрозв'язок» поступово трансформувався в міжнародний термін «телекомунікації». Сучасні мережі зв'язку є, мабуть, найскладнішими штучними системами, які вдалося створити сучасній цивілізації. Вивчення таких систем вимагає комплексних знань у багатьох сферах інтелектуальної діяльності людини.

Комунікація це поняття, що означає сполучення, зв'язок, а також засоби сполучення і зв'язку.

Телекомунікації – сукупність засобів, що забезпечують можливість організації зв'язку на значній відстані.

Засобами, визначеними загальним поняттям «засоби телекомунікацій», є лінії зв'язку, пристрої з'єднання середовищ, системи передачі, комунікаційні пристрої мережі, обладнання сигналізації, синхронізації та ін.

Телекомунікаційна мережа – це системоутворююча сукупність засобів телекомунікацій, що надає територіально віддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо).

Телекомунікаційна мережа (мережа зв'язку) є базовим зв'язуючим компонентом будь-якої територіально розподіленої системи. Поняття система характеризує складність об'єкта (численність і неоднорідність елементів, зв'язків між ними), а поняття розподілена його мережну структуру.

Транспортування (transfer) інформації в мережній термінології означає перенесення інформації, перетвореної в сигнал від джерела до одержувача.

Його слід відрізняти від терміна «передача» (transmission), під яким розуміється процес поширення сигналу у фізичному середовищі між двома суміжними пунктами мережі.

Територіально віддаленими об’єктами у мережі зв’язку можуть виступати як термінальні пристрої користувачів так і кінцеві системи мережі,так і окремі мережі.

Обслуговування користувачів з боку телекомунікаційної мережі здійснюється шляхом надання послуг і додатків.

Послуга (service) це те, що пропонується мережею користувачеві з метою задоволення його комунікаційних потреб.

Телекомунікаційні послуги (telecommunication service) – результат функціонування телекомунікаційної мережі, при якому задовольняється запит на доставку (транспортування) даних або на встановлення зв’язку.

Додаток (application) є подібний до поняття послуги, але, на відміну від останньої, надається користувачеві як кінцевий продукт, який може багаторазово ним використовуватися. Наприклад, придбання спеціального пакета програм для реалізації послуг мультимедіа з їхньою інсталяцією на смартфоні, є прикладом додатків.

Службою мережі (service network) називається організаційно-технічний комплекс, який забезпечує надання мережею конкретного виду послуг.

Платформою надання послуг називається сукупність об’єднаних ресурсів.

2.2 Інформаційна та інфокомунікаційна мережі

Поняття інформаційна мережа (information network) передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об’єктами. У такому розумінні інформаційна мережа це навантажена телекомунікаційна мережа.

У загальному випадку під інформаційною мережею будемо розуміти сукупність територіально розосереджених кінцевих систем і об’єднуючої їх телекомунікаційної мережі, що забезпечує доступ прикладних процесів будь-якої з цих систем до всіх ресурсів інформаційної мережі і їхнє спільне використання.

Інформаційна мережа, на відміну від телекомунікаційної мережі, є більш узагальненою і відображає множину інформаційних процесів, які протікають в мережі. Ці процеси виникають у результаті взаємодії кінцевих систем, під'єднаних до телекомунікаційної мережі. Інформаційні мережі призначені для надання користувачам послуг, пов'язаних з обміном інформацією, її споживанням, а також обробкою, зберіганням і накопиченням (рис. 2.1).

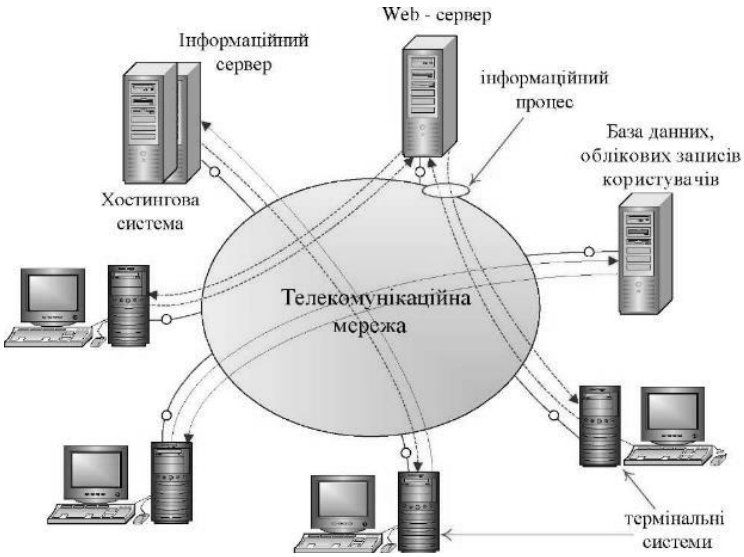

Рисунок 2.1 – Приклад інформаційної мережі

Споживач інформації, що одержав доступ до інформаційної мережі, стає її користувачем (user). Користувачами можуть бути як фізичні, такі юридичні особи (фірми, організації, підприємства).

Телекомунікаційна мережа у складі інформаційної мережі виконує функції транспортувальної системи.

Інформаційна мережа (information network) – системоутворююча сукупність територіально розосереджених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечується взаємодія прикладних процесів, що активізуються в кінцевих системах, і колективний доступ до їх інформаційних і обчислювальних ресурсів.

Базовим компонентом, ядром інформаційної мережі, є телекомунікаційна мережа.

Інформаційні технології (information technologies) – методи і способи накопичення, обробки, зберігання, відображення, пошуку і забезпечення цілісності інформації.

Метою інформаційної технології є виробництво інформації для її аналізу та прийняття рішення для виконання певної дії.

Користувач отримує інформацію з мережі у вигляді контенту (content), тобто деякого обсягу, що забезпечує сприйняття його смислового змісту. У цьому контексті інформаційні послуги ще називають контент послугами.

Під контентом (content) розуміють дані, призначені для зберігання з метою подальшої можливості перетворення в будь-яку необхідну форму.

Інформаційна послуга (information service) – це задоволення інформаційного запиту користувача, сформованого в результаті цілеспрямованого пошуку інформації в розподіленій системі інформаційних ресурсів, шляхом доставки засобами телекомунікацій затребуваної копії контенту.

Конвергенція на рівні мереж, технологій і послуг інформаційної та телекомунікаційної сфер породила нове концептуальне поняття «інфокомунікацій».

Інфокомунікації – порівняно новий термін, що означає нерозривний зв’язок інформаційних і телекомунікаційних елементів інформаційного обміну, які розвиваються в процесі конвергенції,тобто взаємного проникнення.

Інфокомунікації це об’єднання телекомунікацій з інформаційними, комп’ютерними технологіями та радіо технологіями

Інфокомунікації (infocommunication) це сукупність засобів обробки, накопичення, зберігання інформації та перенесення її в просторі, імплементованих в єдину мережну структуру, за допомогою якої забезпечується доступність інформаційних ресурсів та інформаційний обмін.

Інфокомунікаційна мережа (infocommunication network) це сукупність територіально розосереджених інформаційних, обчислювальних ресурсів, програмних комплексів управління, що розміщуються в кінцевих системах

мережі та термінальних системах користувачів, взаємодія між якими забезпечується за допомогою телекомунікацій і які спільно утворюють єдину мультисервісну платформу.

Інфокомунікаційна послуга (infocommunication service) це мультипослуга, що забезпечує задоволення телекомунікаційних або інформаційних, або тих та інших одночасно потреб споживача з наданням йому можливості керувати процесом реалізації цієї послуги.

Під інфокомунікаційними службами розуміються всі існуючі системи передачі й обробки інформації: телефонія, телеграфія, передача даних, телебачення, а також служби, такі як телеметрія, телекерування, теленаведення, телеконтроль, телеосвіта, телемагазин, телебіржа, телеаукціон, телереклама, дистанційна аварійна сигналізація тощо. Наведемо схему інфокомунікаційної мережі, де КінП – кінцевий пункт, КЗ – канал зв'язку, ВЗ – вузол зв'язку, ДІ – джерело інформації, ОІ – одержувач інформації (рис. 2.2).

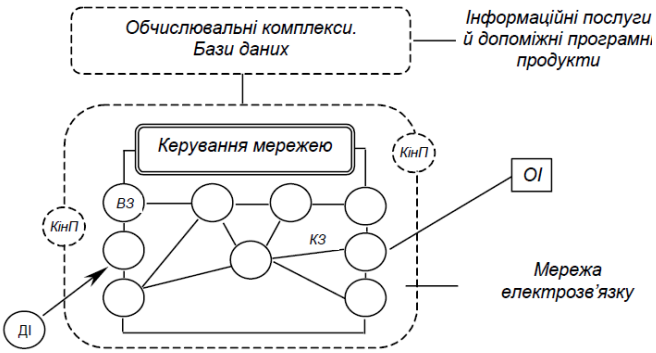

Рисунок 2.2 – Схема інфокомунікаційної мережі

Інформацію, як і речовину та енергію, можна збирати і зберігати, обробляти і змінювати. Але, крім того, інформація може створюватися і зникати, тиражуватися, бути правдивою і помилковою. Є в неї також ще одна особливість і полягає в тому, що вона не витрачається при використанні.

Інформація як відображення деякого об'єкта чи суб'єкта матеріальної системи може існувати незалежно від того, буде вона колись відновлена, чи ні. Цінність інформації та її споживча вартість залежать від споживача і творця інформації, тобто людини чи процесу обробки комп'ютером.

Інформація ж має високу цінність тоді, коли її творець стає джерелом інформації і передає її за допомогою засобів зв'язку, тобто споживча вартість інформації створюється в процесі зв'язку.

Щоб одержати економічний ефект (або політичний чи соціальний), необхідно передати інформацію за допомогою засобів зв'язку.

Отже, роль зв'язку в процесі інформатизації дуже велика, оскільки вона пронизує інформаційний процес від об'єкта спостереження і формування початкової інформації (сприйняття) через її обробку (квантування, кодування, модуляцію), передачу й обробку в приймачі доставки інформації до одержувача в обробленому вигляді.

У підсумку, інфокомунікаційну мережу можна уявити як велику систему, до якої входять користувачі, засоби різних видів зв'язку, обладнання для надання послуг і системи керування.

2.3 Глобальна інформаційна інфраструктура

Глобальна інформаційна інфраструктура (ГІІ) надає користувачам набір комунікаційних послуг, які забезпечують множину застосувань, що охоплює усі види інформації та надає можливість її отримання в будь-якому місці, в будь-який час, за прийнятною ціною і з прийнятною якістю.

На Урядовій конференції країн «Великої сімки», що провадилась Комісією з Європейської Економічної Співдружності, було прийнято основні принципи, на яких має базуватися розвиток ГІІ, у числі яких: прийнятність, елемент культури, керованість, мінімалізм, мобільність, номадизм, ефективність, портативність, взаємодія, якість, надійність, сумісність, ефективність (масштабованість), практичність та захист даних (безпека). Мінімальний набір принципів при створенні ГІІ наведено на рисунку 2.3.

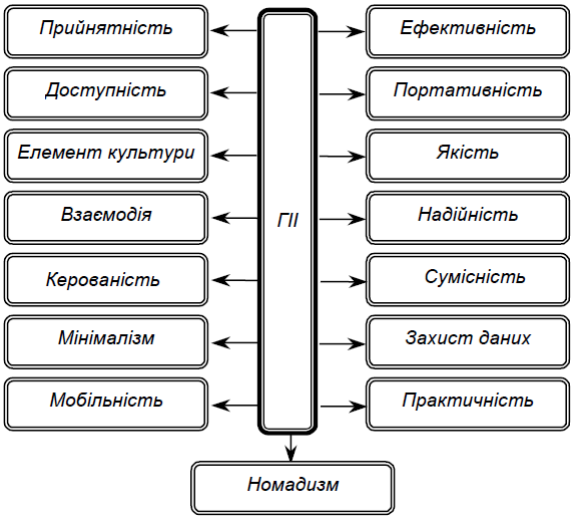

Рисунок 2.3 – Мінімальний набір принципів при створенні ГІІ

Прийнятність – економічна ефективність використання ресурсів підприємствами, організаціями і споживачами у визначений період часу.

Доступність – ступінь доступності до визначеного ресурсу чи групи ресурсів.

Елемент культури – спеціальні характеристики мов і загальноприйнятих правил їх вживання (особливо писемною формою), що властиві визначеним суспільствам і географічним регіонам.

Керованість – можливість для кожного підприємства, організації і визначеного споживача контролювати розміщення й використання своїх ресурсів.

Мінімалізм – методологія або підхід, який забезпечує приєднання з мінімальною кількістю вимог.

Ефективність – ступінь виконання системою або підсистемою своїх функцій, характеризується часом доступу, пропускною здатністю, кількістю операцій за секунду, швидкістю відеоінформації.

Портативність – ступінь легкості, з якою програмне забезпечення і дані можуть бути передані з однієї системи в іншу.

Мобільність – можливості доступу до послуг із різних місць і під час руху. При цьому визначення й локалізація джерела надходження запитів мають забезпечуватися мережею.

Номадизм – можливості переміщення з одного місця в інше, зберігаючи при цьому доступ до послуг незалежно від доступності чи не доступності цих послуг у місцевому середовищі, тобто безперервність доступу в просторі й часі.

Надійність – імовірність того, що продукт або система будуть функціонувати належним чином протягом визначеного проміжку часу.

Сумісність – здатність працювати з різними за швидкістю, ємністю і ціною прикладними платформами і середовищами.

Інтероперабельність – здатність систем мережі обмінюватися інформацією та спільно її використовувати.

Якість – забезпечення рівня якості, який очікує користувач.

Масштабованість – властивість сервісів та систем ефективно виконувати свої функції при широкому діапазоні параметрів, що визначають технічні та ресурсні характеристики підтримуючого середовища.

Практичність – ступінь легкості використання продукту чи системи.

Безпека – захист ресурсів (апаратних, програмних, інформаційних) від випадкових або навмисних дій, що призводять до несанкціонованого доступу до ресурсів і порушення конфіденційності їх використання, модифікації та руйнуванню ресурсів, а також розкриття інформації. Схематично глобальна інформаційна інфраструктура наведена на рисунку 2.4.

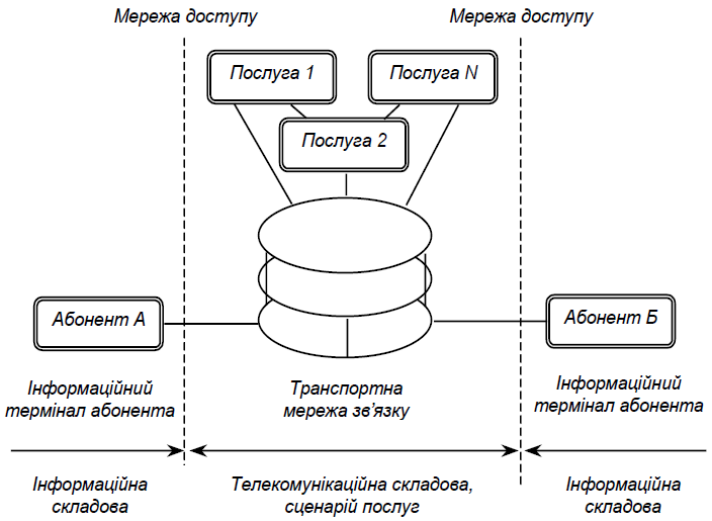

Рисунок 2.4 – Глобальна інформаційна інфраструктура

Таким чином, ГІІ можна вважати сукупністю термінального обладнання, за допомогою якого користувач має доступ до різних (1,2,...,N послуг і мереж доступу, транспортних та інших засобів, в тому числі інформаційних ресурсів). Основою є сучасна інфокомунікаційна мережа.

Модель – це формалізований опис об'єкта, що дозволяє досліджувати його основні елементи, не відволікаючись на несуттєві, з точки зору поставленої мети, деталі. Рівні абстрагування зазвичай розташовуються в ієрархічному порядку (під порядкування за старшинством).

Мережам зв'язку властиво мати всі ознаки складних систем і підпорядковуватися відповідним їм закономірностям. Зазначимо деякі з них.

Ієрархічність – розташування частин та елементів цілого в порядку від вищого до нижчого. Дотримуючись цієї закономірності, ми можемо розчленовувати мережу на окремі підмережі (сегменти) нижчого порядку. Наприклад, глобальна мережа може бути представлена сукупністю територіальних мереж різного масштабу: континентальних, регіональних, міських, локальних та ін.

Комунікаційність – закономірність, що вказує на велику кількість зв'язків (комунікацій) системи, а саме зовнішніх з середовищем і внутрішніх з підсистемами та елементами.

Емержентність – закономірність, яка полягає у виявлені системою інтегрованої якості, тобто цілісності, невластивої окремим її елементам. Так, наприклад, у мережі ми можемо виділити такі функціонально важливі й відносно незалежні підсистеми, як мережа доступу, транспортна мережа, система керування мережею та ін. Жодну із зазначених систем неможна ототожнити з мережею зв'язку в цілому, і тільки їх взаємозв'язок відображає це поняття. З іншого боку, розглядаючи та вивчаючи структури окремих підсистем, ми поглиблюємо своє уявлення про систему.

Процес побудови ряду окремих структур системи називається структуризацією. Структуризація складної системи ототожнюється з архітектурою.

Отже, архітектура – багаторівневий опис системи, отриманий шляхом структуризації. Поняття архітектури характеризує цілісне уявлення про побудову мережі і, відбиває її емержентність. Архітектурою називається системний опис мережі, що відображає всю множину її елементів, зв'язків між ними і правил взаємодії [5, с. 10].

Контрольні запитання

1. Що таке комп'ютерна мережа?
2. Яке призначення повторювачів?
3. Дайте визначення поняттю ретранслятора.
4. Який принцип роботи комутатора?
5. Для чого у комп'ютерній мережі необхідний маршрутизатор?
6. Які мережі відносяться до телекомунікаційних?
7. Яка різниця між комунікацією та телекомунікацією?
8. Наведіть поняття інформаційної мережі.
9. Яка основна мета інформаційної послуги?
10. Яка різниця між передачею та транспортуванням інформації?
11. Наведіть приклади інфокомунікаційних служб.
12. За яких умов інформація має найбільшу цінність?
13. У чому полягає різниця між прийнятність та ефективністю?
14. Надайте визначення поняттю комунікаційність.

3 МЕРЕЖНА МОДЕЛЬ «THE OPEN SYSTEMS INTERCONNECTION MODEL»

Мережна модель «The open systems interconnection model» (OSI) – мережна модель стека мережних протоколів. За допомогою цієї моделі різні мережні пристрої можуть взаємодіяти один з одним. Модель визначає різні рівні взаємодії систем. Кожен рівень виконує певні функції за такої взаємодії.

3.1 Історія виникнення та розвитку мережної моделі

Модель OSI була розроблена наприкінці 70-х років XX століття для підтримки різноманітних методів комп'ютерних мереж, які в цей час конкурували за застосування у великих національних мережних взаємодіях у Франції, Великій Британії та США.

У 1980 році вона стала робочим продуктом групи взаємодії відкритих систем Міжнародної організації зі стандартизації.

Модель не змогла дати повний опис мережі і не отримала підтримки архітекторів на зорі Інтернету, який згодом знайшов відображення в TCP/IP, в основному під керівництвом Інженерної ради Інтернету.

Напочатку і в середині 70-х років XX століття мережа в основному або спонсорувалася державою (NPLnetwork у Великій Британії, ARPANET у США), або розроблялася з використанням власних стандартів, таких як «IBM Systems Network Architecture та Digital Equipment Corporation». Громадські мережі передачі лише починали з'являтися.

Експериментальна система комутації пакетів у Великій Британії приблизно в 1975 році виявила необхідність визначення протоколів вищого рівня. Після публікації британського Національного обчислювального центру статті «Для чого потрібні розподілені обчислення», що стала результатом великих досліджень майбутніх конфігурацій комп'ютерних систем, Великобританія представила аргументи на користь створення Міжнародної комісії зі стандартів для охоплення цієї галузі на нараді Міжнародної організації зі стандартизації в Сіднеї в березні 1977 року.

З 1977 року Міжнародна організація зі стандартизації реалізувала програму з розробки загальних стандартів та методів мережної взаємодії. Аналогічний процес розвивався у Міжнародному консультаційному комітеті з телеграфії та телефонії. Обидва органи розробили документи, що визначають схожі мережні моделі.

Модель OSI була вперше визначена у вихідному вигляді у Вашингтоні в лютому 1978 року французом Х'юбертом Циммерманом, трохи доопрацьований проєкт стандарту був опублікований Міжнародною організацією зі стандартизації в 1980 році.

Розробникам моделі довелося зіштовхнутися з конкуруючими пріоритетами та інтересами.

Темпи технологічних змін зумовили необхідність визначення стандартів, яких нові системи могли б сходитися, а чи не стандартизувати процедури постфактум, тоді як традиційний підхід до розробки стандартів був протилежним.

Хоча це і не був сам стандарт, він був основою, на базі якої можна було б визначити майбутні стандарти.

У 1983 році була сформована базова еталонна модель взаємозв'язку відкритих систем, зазвичай і звана еталонною моделлю взаємозв'язку відкритих систем OSI або просто моделлю OSI. Об'єднаний документ був опублікований в 1984 році як стандарт ISO-7498, і перейменованим у Міжнародному консультаційному комітеті з телеграфії та телефонії (нині сектор стандартизації електрозв'язку Міжнародного союзу електрозв'язку) як стандарт X.200.

OSI складалася з двох основних компонентів: абстрактної моделі мережі, яка називається базовою еталонною моделлю або семишаровою моделлю, і набору мережних протоколів. Грунтуючись на ідеї узгодженої моделі рівнів протоколів, що визначає взаємодію між мережевими пристроями та програмним забезпеченням, еталонна модель OSI стала великим досягненням у стандартизації концепцій мережної взаємодії.

Концепція семишарової моделі була описана в роботі американця Чарльза Бахмана з компанії Honeywell Information Systems.

У цій моделі система мережної взаємодії була поділена на шари. Усередині кожного шару один чи кілька об'єктів реалізовували його функціональність. Кожна сутність взаємодіяла безпосередньо тільки з шаром, що знаходиться прямо під нею, і надавала засоби для використання шаром, що знаходиться над нею.

OSI у такий спосіб стала спробою учасників галузі узгодити загальні мережні стандарти для забезпечення сумісності з обладнанням різних виробників.

Для великих мереж часто підтримувалися кілька наборів мережних протоколів, причому багато пристроїв не могли взаємодіяти з іншими пристроями саме через відсутність загальних протоколів.

Наприкінці 80-х років XX століття і на початку 90-х років XX століття у плані побудови максимально надійних комп'ютерних мереж з моделлю OSI став активно конкурувати набір протоколів TCP/IP, який широко використовувався в мережах з обладнанням різних виробників для роботи в мережі Інтернет.

Тим не менш, модель OSI досі використовується як зразок для навчання та документації.

3.2 Основні принципи, стандарти та рівні моделі

Протоколи зв'язку дозволяють структурі на одному хості взаємодіяти з відповідною структурою того ж рівня на іншому хості.

На кожному рівні N-об'єкти обмінюються блоками даних (PDU) за допомогою протоколу даного рівня на відповідних пристроях. Кожен PDU містить блок службових даних (SDU), пов'язаний з верхнім чи нижнім протоколом.

Обробка даних двома взаємодіючими OSI-сумісними пристроями відбувається так:

– передані дані складаються на верхньому рівні передавального пристрою (рівень N) протокольний блок даних (PDU);

– PDU передається рівень N-1, де він стає сервісним блоком даних (SDU);

– на рівні N-1 SDU поєднується з верхнім, нижнім або обома рівнями, створюючи шар N-1 PDU. Потім він передається у шар N-2;

– процес триває до досягнення нижнього рівня, з якого дані передаються на пристрій;

– на приймальному пристрої дані передаються від найнижчого рівня до найвищого у вигляді серії SDU, послідовно віддаляючись з верхнього або нижнього колонтитула кожного шару до досягнення верхнього рівня, де приймаються останні дані.

Розглянемо в таблиці 3.1 рівні моделі OSI.

Таблиця 3.1 – Рівні моделі OSI

Модель					
Рівень (layer)		Тип даних (PDU)	Функції	Приклади	Устат-кування
1	2	3	4	5	6
Host layers	7 Прикладний (application)	Дані	Доступ до мережних служб	HTTP, FTP, POP3, SMTP, WebSocket	Хости (клієнти мережі), міжме-режний екран
	6 Подання (presentation)		Подання та шифрування даних	ASCII, MIDI, EBCDIC, JPEG	
	5 Сеансовий (session)		Управління сеансом зв’язку	RPC, PAP, L2TP, gRPC	

Продовження таблиці 3.1

1	2	3	4	5	6
	4 Транспортний (transport)	Сегменти, дата-грами	Прямий зв’язок між кінцевими пунктами та надійність	TCP, UDP, SCTP, порти	
Media layers	3 Мережний (network)	Пакети (packet)	Визначення маршруту та логічна адресація	IPv4, IPv6, IPsec, AppleTalk, ICMP	Маршрутизатор, мережний шлюз, міжмережний екран
	2 Канальний (data link)	Біти (bit)/ Кадри (frame)	Фізична адресація	PPP, IEEE 802.22, Ethernet, DSL, ARP,	Мережний міст комутатор, точка доступу
	1 Фізичний (physical)	Біти (bit)	Робота з середовищем передачі, сигналами та двійковими даними	USB, RJ («вита пара», коаксіальний, оптоволоконний), радіоканал	Концентратор , повторювач (мережне обладнання)

У літературі найчастіше прийнято починати опис рівнів моделі OSI з 7-го рівня, званого прикладним, на якому додатки користувача звертаються до мережі. Модель OSI закінчується 1-м рівнем, фізичним, на якому визначені стандарти, які пред'являються незалежними виробниками до середовищ передачі даних, а саме до типу передавального середовища (мідний кабель, оптоволокно, радіоефір тощо), типу модуляції сигналу та сигнальні рівні логічних дискретних станів (нулі та одиниці).

Довільний протокол моделі OSI повинен взаємодіяти або з протоколами свого рівня, або з протоколами на одиницю вище або нижче за свій рівень. Взаємодії з протоколами свого рівня називаються горизонтальними, а з рівнями на одиницю вищими або нижчими вертикальними. Довільний протокол моделі OSI може виконувати лише функції свого рівня і не може виконувати функції іншого рівня, що не виконується в протоколах альтернативних моделей.

Кожному рівню з деякою часткою умовності відповідає свій операнд, тобто логічно неподільний елемент даних, яким на окремому рівні можна оперувати в рамках моделі і протоколів, що використовують фізично дрібну одиницю біт, на канальному рівні інформація об'єднана в кадри, на мережному в пакети (датаграми), на транспортному у сегменти. Довільний фрагмент даних, логічно об'єднаний при передачі, а саме кадр, пакет чи датаграма вважається повідомленням. Саме повідомлення у загальному вигляді є операндами сеансового уявлення та прикладного рівнів.

До базових мережних технологій належать фізичний та канальний рівні.

Прикладний рівень (рівень додатків, application layer) – верхній рівень моделі, що забезпечує взаємодію додатків користувача з мережею та дозволяє додаткам використовувати мережні служби (віддалений доступ до файлів та баз даних, пересилання електронної пошти), відповідає за передачу службової інформації, надає додаткам інформацію про помилки та формує запити до рівня подання.

До протоколів прикладного рівня відносяться: RDP, HTTP, SMTP, SNMP, POP3, FTP, XMPP, OSCAR, Modbus, SIP, TELNET та інші.

Визначення протоколу прикладного рівня та рівня подання дуже розмиті, і належність протоколу до того чи іншого рівня, наприклад протоколу «Hyper text transfer protocol secure» (HTTPS) залежить від кінцевого сервісу, який надає додаток.

Якщо протокол, наприклад HTTPS, використовується для перегляду простої Інтернет сторінки через браузер, то його можна розглядати як протокол прикладного рівня.

У тому ж разі, якщо протокол HTTPS використовується як низькорівневий протокол для передачі фінансової інформації, наприклад, за протоколом ISO-8583, то протокол HTTPS буде протоколом рівня подання, а протокол ISO-8583 буде протоколом рівня програми. Те саме стосується інших протоколів прикладного рівня.

Рівень подання (Presentation layer) забезпечує перетворення протоколів та кодування чи декодування даних. Запити програм, отримані з сеансового рівня, на рівні подання перетворюються на формат передачі мережі, а отримані з мережі дані перетворюються на формат програм. На цьому рівні може здійснюватися стиснення чи розпакування або шифрування чи дешифрування, а також перенаправлення запитів іншому мережному ресурсу, якщо вони не можуть бути локально оброблені.

Цей рівень зазвичай є проміжний протокол для перетворення інформації з сусідніх рівнів. Це дозволяє здійснювати обмін між програмами на різнорідних комп’ютерних системах прозорим для програм чином. Рівень уявлень забезпечує форматування та перетворення коду. Форматування коду використовується для того, щоб гарантувати додатку надходження інформації для обробки, яка б мала для нього сенс. За потреби цей рівень може виконувати переклад із одного формату даних до іншого. Даний рівень має справу не лише з форматами та поданням даних, він також займається структурами даних, що використовуються програмами. Таким чином, рівень 6 забезпечує організацію даних при їх пересиланні.

Щоб зрозуміти, як це працює, уявімо, що є дві системи. Одна використовує для представлення даних розширений двійковий код обміну інформацією, наприклад, це може бути мейнфрейм IBM, а інша американський стандартний код обміну інформацією ASCII (його використовує більшість інших виробників комп'ютерів). Якщо цим двом системам необхідно обмінятися інформацією, то необхідний рівень уявлень, який виконає перетворення та здійснить переклад між двома різними форматами.

Іншою функцією, що виконується на рівні уявлень, є шифрування даних, яке застосовується в тих випадках, коли необхідно захистити інформацію, що передається, від доступу несанкціонованими одержувачами. Щоб вирішити це завдання, процеси та коди, що знаходяться на рівні уявлень, повинні виконати перетворення даних. На цьому рівні існують інші підпрограми, які стискають тексти і перетворюють графічні зображення в бітові потоки, так що вони можуть передаватися по мережі.

Стандарти рівня подання визначають способи представлення графічних зображень. Для цього можна використовувати формат зображень (pict), що використовується для передачі графіки QuickDraw між програмами.

Іншим форматом уявлень є тегований формат файлів зображень tiff , який зазвичай використовується для растрових зображень з високою роздільною здатністю. Наступним стандартом рівня уявлень, який можна використовувати для графічних зображень, є стандарт, розроблений Об'єднаною експертною групою з фотографії, який у повсякденному користуванні називають jpeg.

Існує інша група стандартів рівня подання, яка визначає уявлення звуку та кінофрагментів. Сюди входять інтерфейс електронних музичних інструментів (Musical instrument digital interface) для цифрового представлення музики, розроблений Експертною групою з кінематографії стандарт mpeg , що використовується для стиснення та кодування відеороликів на дисках, зберігання в цифрованому вигляді та передачі зі швидкостями до 1,5 мегабіт за секунду, і QuickTime, що описує звукові та відео елементи для програм, що виконуються на комп'ютерах.

Сеансовий рівень (Session layer) моделі забезпечує підтримку сеансу зв’язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень управляє створенням сеансу, завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права передачі даних і підтримкою сеансу у періоди не активності додатків.

Протоколи сеансового рівня H.245 (call control protocol for multimedia communication), ISO-SP (OSI session layer protocol (X.225, ISO 8327)), iSNS (Internet storage name service), L2F (Layer 2 forwarding protocol), L2TP (Layer 2 tunneling protocol), NetBIOS (Network basic input output system), PAP (Password authentication protocol), PPTP (Point-to-point tunneling protocol), RPC (Remote procedure call protocol), RTCP (Realtime transport control protocol), SMPP (Short message peer-to-peer), SCP (Session control protocol), ZIP (zone information protocol), SDP (Sockets direct protocol).

Транспортний рівень (Transport layer) моделі призначений для забезпечення надійної передачі даних від відправника до одержувача. При цьому рівень надійності може змінюватись у широких межах. Існує безліч класів протоколів транспортного рівня, починаючи від протоколів, що надають лише основні транспортні функції (наприклад, функції передачі даних без підтвердження прийому), і закінчуючи протоколами, які гарантують доставку до пункту призначення декількох пакетів даних у належній послідовності, мультиплексують кілька потоків даних, забезпечують механізм управління потоками даних та гарантують достовірність прийнятих даних. Наприклад, UDP обмежується контролем цілісності даних у межах однієї датаграми та не виключає можливості втрати пакета повністю або дублювання пакетів, порушення порядку отримання пакетів даних. TCP забезпечує надійну безперервну передачу даних, що виключає втрату даних або порушення порядку їх надходження або дублювання, може перерозподіляти дані, розбиваючи великі порції даних на фрагменти і, склеюючи фрагменти в один пакет.

Протоколи транспортного рівня ATP (Appletalk transaction protocol), CUDP (Cyclic udp), DCCP (Datagram congestion control protocol), FCP (Fibre channel protocol), IL (IL protocol), NBF (Netbios frames protocol), NCP (Netware core protocol), SCTP (stream control transmission protocol), SPX (sequenced packet exchange), SST (Structured stream transport), TCP (Transmission control protocol), UDP (User datagram protocol).

Мережний рівень (Network layer) моделі призначений для визначення шляху передачі. Відповідає за трансляцію логічних адрес та імен у фізичні, визначення найкоротших маршрутів, комутацію та маршрутизацію, відстеження неполадок та заторів у мережі.

Протоколи мережного рівня маршрутизують дані джерела до одержувача. Пристрої (маршрутизатори), що працюють на цьому рівні, умовно називають пристроями третього рівня (за номером рівня в моделі OSI).

Протоколи мережного рівня: IP/IPv4/IPv6 (Internet protocol), IPX (Internetwork packet exchange, протокол міжмережного обміну), X.25 (частково цей протокол реалізовано на рівні 2), CLNP (мережний протокол без організації з'єднань), IPsec (Internet protocol security). Протоколи маршрутизації RIP (Routing information protocol), OSPF (Open shortest path first).

Канальний рівень (Data link layer) призначений для забезпечення взаємодії мереж на фізичному рівні та контролю помилок, які можуть виникнути. Отримані з фізичного рівня дані, представлені в бітах, він пакує в кадри, перевіряє їх на цілісність і, якщо потрібно, виправляє помилки (або формує повторний запит пошкодженого кадру) і відправляє на мережний рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи та керуючи цією взаємодією.

Специфікація IEEE-802 поділяє цей рівень на два підрівні, а саме MAC (Media access control) регулює доступ до фізичного середовища, що розділяється та LLC (Logical link control), що забезпечує обслуговування мережевого рівня.

На цьому рівні працюють комутатори, мости та інші пристрої. Ці пристрої використовують адресацію другого рівня (за номером рівня моделі OSI).

Протоколи канального рівня Arcnet, ATM, Controller area (CAN), Econet, IEEE 802.3 (Ethernet), Ethernet automatic protection switching (EAPS), Fiber distributed data interface (FDDI), Frame relay, High–level data link control (HDLC), IEEE 802.2 (надає функції LLC для підрівня IEEE-802 MAC), link access procedures, D channel (LAPD), IEEE-802.11 Wireless LAN, Localtalk, Multiprotocol label switching (MPLS), Point-to-point protocol (PPP), Point-to-point protocol over ethernet (PPPoE), Serial line internet protocol (SLIP, застарілий), Starlan, Token ring, Unidirectional link detection (UDLD), x.25, ARP.

При розробці стеків протоколів на цьому рівні вирішуються завдання стійкого до перешкод кодування. До таких способів кодування відноситься код Хеммінга, блочне кодування, код Ріда – Соломона .

У програмуванні цей рівень є драйвером мережної плати, в операційних системах є програмний інтерфейс взаємодії канального і мережевого рівнів між собою. Не новий рівень, а просто реалізація моделі для конкретної операційної системи. Приклади таких інтерфейсів: ODI, NDIS, UDI.

Фізичний рівень (Physical layer) – нижній рівень моделі, який визначає метод передачі даних, поданих у двійковому вигляді, від одного пристрою (комп’ютера) до іншого. Складання таких методів займаються різні організації, у тому числі: Інститут інженерів з електротехніки та електроніки, Альянс електронної промисловості, Європейський інститут телекомунікаційних стандартів та інші. Здійснюють передачу електричних або оптичних сигналів в кабель або радіоефір і, відповідно, їх прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів.

На цьому рівні також працюють концентратори, повторювачі сигналу та медіа конвертери.

Функції фізичного рівня реалізуються усім пристроях, підключених до мережі. З боку комп’ютера функції фізичного рівня виконуються мережним

адаптером чи послідовним портом. До фізичного рівня належать фізичні, електричні та механічні інтерфейси між двома системами. Фізичний рівень визначає такі види середовищ передачі даних як оптоволокно, вита пара, коаксіальний кабель, супутниковий канал передач даних і т.д. Стандартними типами мережних інтерфейсів, що відносяться до фізичного рівня є: V.35, RJ-11, RJ-45.

Під час розробки стеків протоколів цьому рівні вирішуються завдання синхронізації і лінійного кодування. До таких способів кодування відноситься код NRZ, код RZ, MLT-3, PAM5, Манчестер II .

Протоколи фізичного рівня IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi radio interface, ITU і ITU-T, TransferJet, ARINC 818, G.hn/G.9960, Modbus Plus.

3.3 Відповідність моделі до інших моделей мережної взаємодії

Оскільки найбільш затребуваними та практично використовуваними стали протоколи, наприклад TCP/IP, розроблені з використанням інших моделей мережної взаємодії, далі необхідно описати можливе включення окремих протоколів інших моделей різних рівнів моделі OSI.

Родина TCP/IP має три транспортні протоколи, а саме TCP, що повністю відповідає OSI, що забезпечує перевірку отримання даних, User datagram protocol (UDP), що відповідає транспортному рівню тільки наявністю порту, що забезпечує обмін датаграмами між додатками, але не гарантує отримання даних та SCTP, розроблений для усунення деяких недоліків TCP, який додано деякі нововведення. У сімействі TCP/IP є ще близько двохсот протоколів, найвідомішим у тому числі є службовий протокол ICMP.

У родині IPX/SPX порти з’являються у протоколі мережевого рівня IPX, забезпечуючи обмін датаграмами між додатками (операційна система резервує частину сокетів собі).

Протокол SPX, у свою чергу, доповнює IPX рештою можливостей транспортного рівня в повній відповідності з OSI. В якості адреси хосту ICX

використовує ідентифікатор, утворений із чотирибайтного номера мережі (призначається маршрутизаторами) та MAC-адреси мережного адаптера.

Незважаючи на те, що модель OSI досі використовується як зразок для навчання та документації, протоколи OSI, спочатку задумані для цієї моделі, не набули популярності. Деякі інженери стверджують, що еталонна модель OSI все ще є актуальною для хмарних обчислень.

Контрольні запитання

1. Що таке мережна модель OSI?
2. З яких компонентів складається OSI?
3. З протоколами якого рівня може взаємодіяти протокол рівня 2?
4. Що ви знаєте про горизонтальну та вертикальну взаємодію?
5. Що відносять до базових мережних технологій?
6. Надайте своє визначення поняттю протоколу прикладного рівня.
7. Що Ви знаєте про стандарт jpeg?
8. Наведіть поняття датаграми.
9. Які пристрої реалізують фізичний рівень?

4 ОСНОВИ VIRTUAL LOCAL AREA NETWORK

Virtual local area network (VLAN) – група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережних комутаторів. І навпаки, пристрої, що знаходяться в різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв’язок між цими пристроями можливий тільки на мережному та вищому рівнях.

У сучасних мережах VLAN – головний механізм створення логічної топології мережі, яка залежить від її фізичної топології. VLAN використовується для скорочення широкомовного трафіку в мережі. Мають велике значення з погляду безпеки, зокрема як засіб боротьби з ARP-spoofing.

Як правило, одному VLAN відповідає одна підмережа. Пристрої, що знаходяться у різних VLAN, будуть знаходитися у різних підмережах. Але в той же час VLAN не прив’язаний до розташування пристроїв і тому пристрої, що знаходяться на відстані один від одного, все одно можуть бути в одному VLAN незалежно від розташування.

Кожен VLAN це окремий широкомовний домен. Наприклад, комутатор це пристрій другого рівня моделі OSI. Всі порти на комутаторі з одним VLAN знаходяться в одному широкомовному домені.

Створення додаткових VLAN на комутаторі означає розбиття комутатора на кілька широкомовних доменів. Якщо один і той же VLAN налаштований на різних комутаторах, то порти різних комутаторів утворюватимуть один широкомовний домен.

Коли мережа розбита на VLAN, спрощується завдання застосування політик та правил безпеки. З VLAN політики можна застосовувати до цілих підмереж, а не до окремого пристрою. Крім того, перехід з одного VLAN в інший передбачає проходження через пристрій 3-го рівня, на якому зазвичай застосовуються політики, що дозволяють або забороняють доступ з VLAN в VLAN.

Комп’ютер при відправці трафіку в мережу навіть не здогадується, в якому VLAN він розміщений. Про це думає комутатор. Комутатор знає, що комп’ютер, який підключений до певного порту, знаходиться у відповідному VLAN. Трафік, що приходить на порт певного VLAN, нічим особливим не відрізняється від трафіку іншого VLAN. Іншими словами, ніякої інформації про належність трафіку певному VLAN в ньому немає.

Однак, якщо через порт може прийти трафік різних VLAN, комутатор повинен його якось розрізняти. Для цього кожен кадр трафіку, має бути позначений якимось особливим чином. Позначка повинна говорити про те, якому VLAN трафік належить.

Найбільш поширений зараз спосіб ставити таку позначку описаний у відкритому стандарті IEEE-802.1Q.

4.1 Комутатор та Virtual local area network

VLAN можуть бути налаштовані на комутаторах, маршрутизаторах, інших мережних пристроях та на хостах. Однак для пояснення VLAN найкраще підійде комутатор.

Комутатор – пристрій 2-го рівня, і спочатку, всі порти комутатора знаходяться, як правило, в VLAN 1 і, отже, в одному широкомовному сегменті.

Це означає, що якщо один із пристроїв, який підключений до порту комутатора, відправить широкомовний кадр, то комутатор перенаправить цей кадр на всі інші порти, до яких підключені пристрої, і вони отримають цей кадр.

Щоб передавати кадри, комутатор використовує таблицю комутації (табл. 4.1).

Спочатку, після включення комутатора, таблиця порожня. Коли комутатор отримує фрейм від хоста, він спочатку передає його відповідно до своїх правил, а потім запам’ятовує MAC-адресу відправника у фреймі і ставить його у відповідність порту на якому він був отриманий.

Таблиця 4.1 – Таблиця комутації

Порт комутатора	MAC-адреса хоста
1	A
2	B
3	C
4	D

Наприклад, для рисунку 4.1, підсумкова таблиця комутації матиме вигляд (табл. 4.1) (після того, як всі хости передавали якийсь трафік).

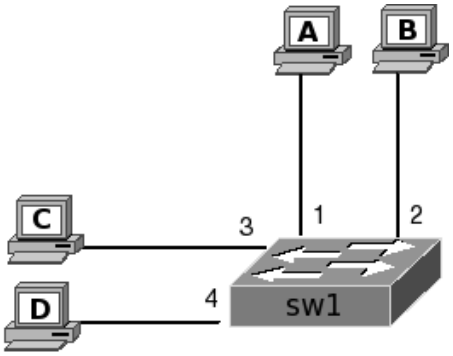

Рисунок 4.1 – Приклад підключення комутатора

Коли таблиця заповнена, комутатор знає на яких портах у нього є якісь хости і передає кадри на відповідні порти.

Для того, щоб передавати кадри, комутатор використовує три базові механізми:

– flooding це кадр, отриманий одним з портів, передається іншим портам комутатора. Комутатор виконує цю операцію у двох випадках, а саме при отриманні широкомовного або multicast (якщо не налаштована підтримка multicast) кадру та при отриманні unknown unicast кадру. Це дозволяє комутатору доставити фрейм хосту (за умови, що хост можна досягти і існує), навіть коли він не знає, де хост знаходиться;

– forwarding це передача кадру, отриманого одним портом через інший порт відповідно до запису у таблиці комутації;

– filtering, коли комутатор отримує кадр через певний порт, і MAC-адреса одержувача доступна через цей порт (це вказано в таблиці комутації), то комутатор відкидає кадр. Тобто комутатор вважає, що в цьому випадку хост вже отримав цей кадр, і не дублює його.

Розглянемо приклад мережі для демонстрації використання механізмів передачі кадрів (рис. 4.2).

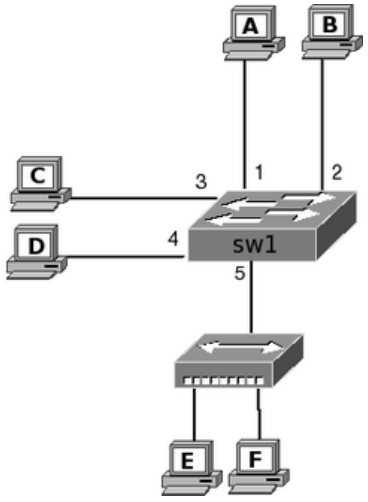

Рисунок 4.2 – Приклад мережі

На рисунку 4.2. зображено комутатор sw1 і повторювач (hub) до якого підключено два хости. Спочатку до комутатора були підключені три хости A, B і C. Відповідно у комутатора буде наступна таблиця комутації (табл. 4.2):

Таблиця 4.2 – Таблиця комутації для комутатора sw1

Порт комутатора	MAC-адреса хоста
1	A
2	B
3	C

Коли хост A відправляє кадр хосту B, комутатор використовує механізм forwarding, тому що йому відомо де знаходяться обидва хоста і хости знаходяться на різних портах комутатора.

Далі до комутатора підключили хост D. Якщо хост A відправляє кадр хосту D, то для комутатора це unknown unicast кадр, тому що в таблиці комутації немає запису про MAC-адресу D. Відповідно до своїх правил

комутатор виконує flooding і передає кадр на всі порти, крім 1 (з якого кадр був отриманий).

Після того, як комутатор отримає кадр від хоста D, він запам’ятовує його адресу і створить відповідний запис у таблиці комутації.

До комутатора підключили повторювач із двома хостами і комутатор вивчив їхні адреси. Відповідна таблиця комутації наведена в таблиці 4.3.

Таблиця 4.3 – Таблиця комутації для повторювача з двома хостами

Порт комутатора	MAC-адреса хоста
1	A
2	B
3	C
4	D
5	E
5	F

Якщо після цього хост E передаватиме кадр хосту F, то комутатор отримає його, але не передаватиме далі.

У цій ситуації комутатор використовує механізм filtering, тому що MAC-адреса одержувача доступна через той же порт, що і відправник.

4.2 Хости в Virtual local area network

Раніше розглядалася схема хосту в одному VLAN на одному комутаторі (рис. 4.1).

До комутатора підключено 4 хости. Для спрощення вважатимемо, що A, B, C та D це відповідні MAC-адреси хостів.

Відповідна таблиця комутації наведена далі (табл. 4.1).

Розглянемо схему хосту в різних VLAN на одному комутаторі (рис. 4.3).

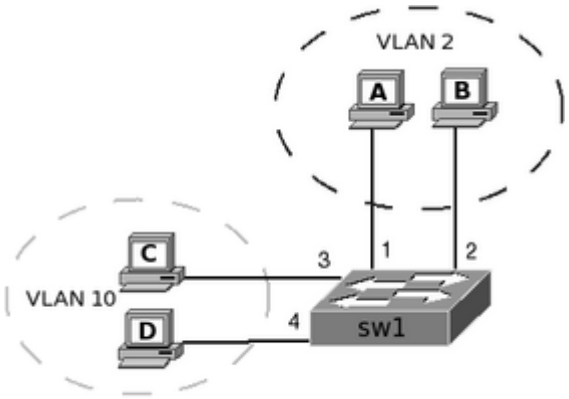

Рисунок 4.3 – Схема хосту в різних VLAN на одному комутаторі

Зазвичай всі порти комутатора вважаються нетегованими членами VLAN. У процесі налаштування або роботи комутатора вони можуть переміщатися в інші VLAN. На комутаторі, зображеному на рисунку вище налаштовані два VLAN, всі порти у відповідних VLAN налаштовані як нетеговані, тобто не використовують теги IEEE 802.1Q при передачі кадрів (access-порти в термінології Cisco). Після цього на комутаторі є дві таблиці комутації (табл. 4.4, 4.5).

Таблиця 4.4 – Таблиця комутації для VLAN 2

Порт комутатора	MAC-адреса хоста
1	A
2	B

Таблиця 4.5 – Таблиця комутації для VLAN 10

Порт комутатора	MAC-адреса хоста
3	C
4	D

Всі базові механізми комутатора залишаються такими ж, як і до поділу на VLAN, але вони використовуються тільки в межах відповідного VLAN. Наприклад, якщо хост з VLAN 10 відправляє широкомовний кадр, він буде відправлений лише порти у цьому VLAN.

Виходить, що нетеговані порти це звичайні порти комутатора. Це просто можливість повідомити комутатор про те, якому VLAN належать порти. Потім комутатор використовує цю інформацію під час передачі кадрів.

Як правило, реально в таблиці комутації в комутаторах вказується порт, MAC-адреса та VLAN. Тобто для зазначеного прикладу таблиця комутації буде наступною (табл. 4.6):

Таблиця 4.6 – Таблиця комутації з указанням параметрів

Порт комутатора	VLAN	MAC-адреса хоста
1	2	A
2	2	B
3	10	C
4	10	D

Однак, для спрощення використовується запис таблиці комутації у вигляді відповідності між портами і MAC-адресами. Розглянемо хости різних VLAN на різних комутаторах (пояснення тегованих портів). Для початку додаємо комутатор sw2 і два хоста E і F в VLAN 2 (рис. 4.4).

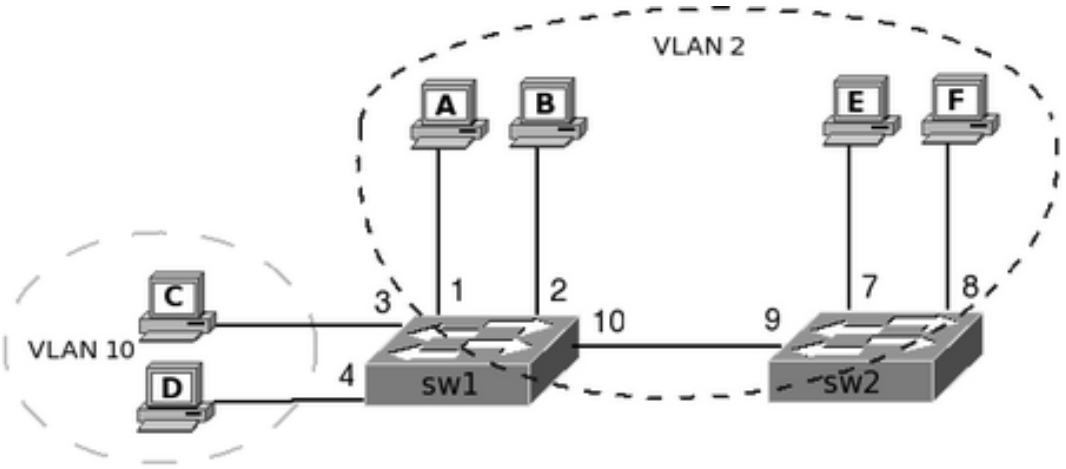

Рисунок 4.4 – Схема з двома комутаторами

Якщо розглядати два комутатора окремо, то виходить, що на комутаторі sw1 залишилася колишня таблиця комутації, а на комутаторі sw2 таблиця (табл. 4.7) (поки що комутатори не з’єднані).

Таблиця 4.7 – Таблиця комутації для sw2

Порт комутатора	MAC-адреса хоста
7	E
8	F

Тепер необхідно, щоб хости A, B, E, F «побачили» один одного. Вони повинні знаходитись в одному VLAN. Тобто необхідно якимось чином вказати комутатору, що ще на одному порту є хости у відповідному VLAN.

Для зазначеного прикладу достатньо додати на комутаторі sw1 порт 10 у VLAN 2, а на комутаторі sw2 порт 9 у VLAN 2. Приналежність до VLAN вказується налаштуванням порту нетегованим у VLAN 2 (поки що). Після цього на комутаторах у таблицях комутації додадуться нові порти та відповідні MAC-адреси хостів. Наведемо таблиці комутації sw1 для VLAN 2 (табл. 4.8) та sw2 для VLAN 2 (табл. 4.9).

Таблиця 4.8 – Таблиця комутації sw1 для VLAN 2

Порт комутатора	MAC-адреса хоста
1	A
2	B
10	E
10	F

Таблиця 4.9 – Таблиця комутації sw2 для VLAN 2

Порт комутатора	MAC-адреса хоста
7	E
8	F
9	A
9	B

Далі до комутатора sw2 додані два хоста G і H VLAN 10 (рис. 4.5).

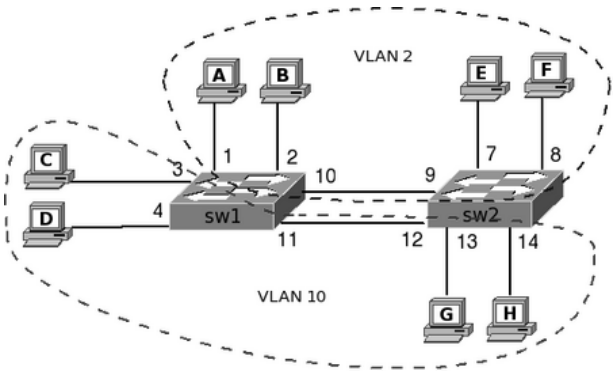

Рисунок 4.5 – Додавання двох хостів G і H VLAN 10 до комутатора sw2

Для того, щоб хости C і D в VLAN 10 на комутаторі sw1, могли обмінюватися інформацією з хостами VLAN 10 на комутаторі sw2, доданий лінк між комутаторами. Логіка аналогічна додавання хостів до VLAN 2.

Наведемо таблиці комутації sw1 для VLAN 10 (табл. 4.10) та sw2 для VLAN 10 (табл. 4.11).

Таблиця 4.10 – Таблиця комутації sw1 для VLAN 10

Порт комутатора	MAC-адреса хоста
3	C
4	D
11	G
11	H

Таблиця 4.11 – Таблиця комутації sw2 для VLAN 10

Порт комутатора	MAC-адреса хоста
13	G
14	H
12	C
12	D

Створимо тегований порт між комутаторами (рис. 4.6).

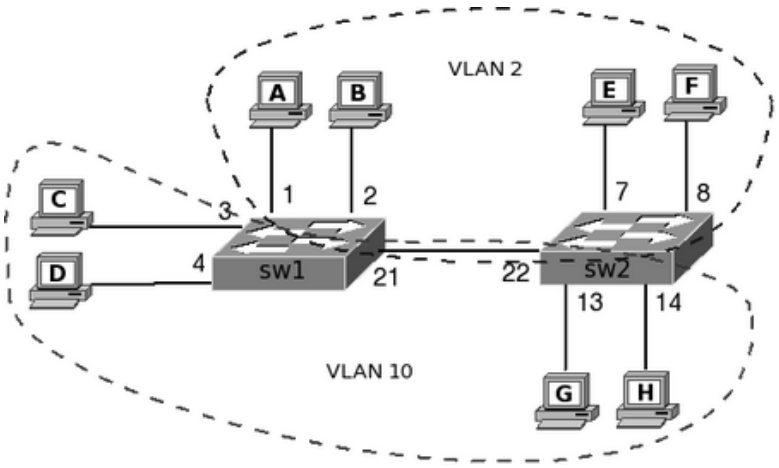

Рисунок 4.6 – Створення тегованого порту між комутаторами

Коли потрібно передати трафік одного чи двох VLAN між комутаторами, то схема, яка використовувалася вище, виглядає припустимо. Однак, коли кількість VLAN зростає, то схема явно стає дуже незручною, тому що для кожного VLAN треба буде додавати лінк між комутаторами для того, щоб об’єднати хости в один широкомовний сегмент.

Для вирішення цієї проблеми використовуються теговані порти. Тегований порт дозволяє комутатору передати трафік декількох VLAN через один порт і зберегти при цьому інформацію про те, в межах якого VLAN передається кадр. На комутаторах sw1 та sw2 порти 21 та 22, відповідно, це теговані порти. Для того, щоб комутатори розуміли якому VLAN належить кадр, що прийшов, і використовували відповідну таблицю комутації для його обробки, виконується тегування кадру (рис. 4.7).

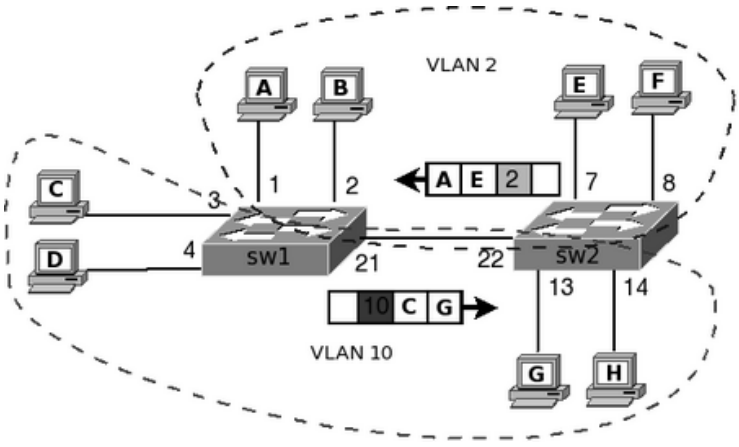

Рисунок 4.7 – Тегування кадру

Наприклад, якщо хост E передає кадр хосту A, то комутатор sw2 перевіряє свою таблицю і бачить, що хост A доступний через порт 22. Оскільки порт налаштований як тегований, то коли кадр виходить з порту 22 в ньому проставляється тег, який вказує якому VLAN належить цей кадр. В даному випадку проставляється тег із VLAN 2.

Реальна структура кадру з тегом описана у 802.1Q. Комутатор sw1 отримує тегований кадр через тегований порт 21. Щоб визначити який порт його передає далі sw1 використовує таблицю комутації для VLAN 2 (оскільки цей VLAN було вказано у тезі). На комутаторі sw1 порт 21 має бути налаштований як тегований для того, щоб комутатор не відкидав теговані кадри, а зчитував інформацію тега. І відповідно щоб він також позначав кадр тегом, коли передаватиметься трафік комутатору sw2.

Інші порти комутатора залишаються нетегованими. І для хостів операція тегування, яку виконують комутатори, абсолютно прозора. Хости нічого не знають про теги та отримують звичайні фрейми.

Аналогічні дії виконуються, наприклад, під час передачі кадру від хоста C хосту G.

4.3. Приналежність Virtual local area network

Порти комутатора, що підтримують VLAN (з деякими припущеннями) можна розділити на дві множини, а саме теговані порти (або транкові порти, trunk-порти в термінології Cisco) та нетеговані порти (або порти доступу, access-порти в термінології Cisco).

Теговані порти потрібні для того, щоб через один порт була можливість передавати дані, що належать до різних VLAN і, відповідно, отримувати трафік кількох VLAN на один порт. Інформація про належність трафіку до конкретного VLAN, як було зазначено вище, вказується у спеціальному тегу. Без тега комутатор зможе розрізняти трафік різних VLAN.

Якщо порт нетегований і належить до будь-якого VLAN, то трафік для цього VLAN передається без тега. На Cisco нетегований порт (access-порт)

може бути лише в одному VLAN, на деяких інших комутаторах (наприклад, ZyXEL, D-Link та Planet) реалізація інша.

Якщо порт тегований для кількох VLAN, то в цьому випадку весь нетегований трафік прийматиметься спеціальним рідним VLAN (native VLAN). Із цим параметром (native, PVID, port VID) виникає багато плутанини. Наприклад, деякі свічі для правильної роботи нетегованого порту вимагають помістити порт у VLAN, задати режим порту untagged (нетегований), і прописати номер цього VLAN в PVID цього порту. На комутаторах HP ProCurve тегований порт починає працювати як тегований, тільки якщо поставити його PVID в «None».

Якщо порт належить лише одному VLAN як нетегований, то тегований трафік, що надходить через такий порт, повинен видалятися. Насправді ця поведінка зазвичай налаштовується.

Найпростіше це зрозуміти, якщо забути всю внутрішню структуру комутатора і відштовхуватися лише від портів. Припустимо, є VLAN з номером 111, є два порти, які належать до VLAN 111. Вони спілкуються тільки між собою, з untagged access-порту виходить нетегований трафік, з tagged trunk-порту виходить трафік тегований у VLAN 111. Всі необхідні перетворення прозоро у собі робить комутатор.

Зазвичай всі порти комутатора вважаються нетегованими членами VLAN. У процесі налаштування або роботи комутатора вони можуть бути переміщені в інші VLAN.

Існують два підходи до призначення порту до певного VLAN, а саме статичне призначення, коли належність порту VLAN задається адміністратором у процесі налаштування та динамічне призначення, коли приналежність порту VLAN визначається під час роботи комутатора за допомогою процедур, описаних у спеціальних стандартах, таких, наприклад, як 802.1X.

При використанні 802.1X для отримання доступу до порту комутатора, користувач проходить аутентифікації на сервері. За результатами

аутентифікації порт комутатора розміщується у тому чи іншому VLAN [7, с. 296].

Контрольні запитання

1. Надайте поняття комутатора з точки зору моделі OSI.
2. Що таке широкомовний домен?
3. Що вам відомо про механізм filtering?
4. Які порти вважаються нетегованими?
5. Надайте визначення тегованого порту.
6. Що таке фрейм?
7. Наведіть кратку характеристику стандарту 802.1X.

5 SPANNING TREE PROTOCOL

5.1 Основи Spanning tree protocol

Spanning tree protocol (STP) – це канальний протокол. Основним завданням STP є усунення петель у топології довільної мережі Ethernet, у якій є один або більше мережних мостів, пов'язаних надлишковими з'єднаннями. STP вирішує це завдання, автоматично блокуючи з'єднання, які в даний момент для повної зв'язності комутаторів є надмірними.

Необхідність усунення топологічних петель у мережі Ethernet випливає з того, що їх наявність у реальній мережі Ethernet з комутатором з високою ймовірністю призводить до нескінченних повторів передачі одних і тих же кадрів Ethernet одним і більше комутатором, через що пропускна здатність мережі виявляється майже повністю зайнятою цими марними повторами. В цих умовах, хоча формально мережа може продовжувати працювати, на практиці її продуктивність стає настільки низькою, що може бути повною відмовою мережі.

STP відноситься до другого рівня моделі OSI. Протокол описаний у стандарті IEEE-802.1D, виробленому робочою групою IEEE-802.1 з міжмережної взаємодії. Заснований на однойменному алгоритмі, який розробила Перлман.

Якщо в мережі з мостовими підключеннями (в сегменті мережі з комутаторів) є кілька шляхів, можуть утворитися циклічні маршрути, і дотримання простих правил пересилання даних через міст (комутатор) призведе до того, що один і той же пакет буде нескінченно передаватися з одного мосту на інший (передатися по кільцю з комутаторів).

Алгоритм сполученого дерева дозволяє при необхідності автоматично відключати передачу через міст (у сучасних мережах комутатори) в окремих портах (блокувати порти комутатора), щоб запобігти зациклюванню в топології маршрутів пересилання пакетів. Для використання алгоритму острівного дерева в мережному мосту ніякого додаткового налаштування не потрібно.

Алгоритм острівного дерева є основою протоколу, що динамічно відключає надлишкові зв’язки в мережі стандарту Ethernet (для утворення деревоподібної топології). Протокол STP стандартизований і підтримується багатьма моделями керованих комутаторів, зокрема включений за замовчуванням на всіх комутаторах Cisco.

Суть роботи протоколу полягає в тому, що комутатори мережі Ethernet, що його підтримують, обмінюються один з одним інформацією про себе. На підставі певних умов (зазвичай відповідно до налаштувань) один з комутаторів вибирається кореневим (root), після чого всі інші комутатори за алгоритмом острівного дерева вибирають для роботи порти, найближчі до кореневого комутатора (враховується кількість посередників та швидкість ліній). Всі інші мережні порти, що ведуть до кореневого комутатора, блокуються. Таким чином утворюється дерево з коренем у вибраному комутаторі.

У комутаторах Cisco із підтримкою VLAN протокол STP за замовчуванням виконується незалежно для кожної віртуальної мережі.

Крім STP, в комутаторах можуть застосовуватися інші методики виявлення та усунення петель, наприклад, порівнянням таблиць комутації (списків MAC-адресів) різних портів, або порівнянням контрольних сум пакетів, що проходять (збіг вказує на однакові пакети, які з’являються через виникнення петель). Порівняно з описаними методами, випадково (або грунтуючись на якихось здогадах) блокуючими «дублюючі» порти, протокол STP забезпечує деревоподібну структуру всього сегмента, при будь-якій кількості резервних ліній між довільними комутаторами, що підтримують STP.

5.2 Принцип дії, правила та алгоритм Spanning tree protocol

Наведемо основні принципи дії STP. Спочатку вибирається один кореневий міст (Root bridge). Далі кожен комутатор прораховує найкоротший шлях до кореневого. Відповідний порт називається кореневим портом. Будь-який некореневий комутатор може мати лише один кореневий порт. Після цього для кожного сегмента мережі, до якого приєднано більш ніж один міст

(або кілька портів одного мосту), прораховується найкоротший шлях до кореневого мосту (порту). Міст, через який проходить цей шлях, стає призначеним для цієї мережі (Designated bridge), а відповідний порт стає призначеним портом.

Наприкінці у всіх сегментах, з якими з'єднано більше одного порту моста, всі мости блокують всі порти, що не є кореневими та призначеними. У результаті виходить деревоподібна структура (математичний граф) з вершиною, як у кореневого комутатора (рис. 5.1). Пронумеровані квадрати означають мости, а хмари означають мережні сегменти.

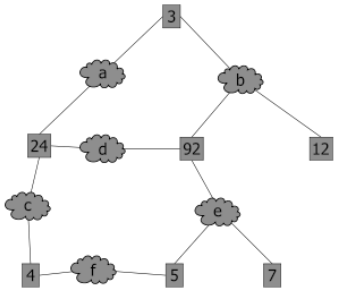

Рисунок 5.1 – Приклад мережі деревоподібної структури

Далі розглянемо основні правила при роботі з STP. Кореневим (root) портом призначається порт із найнижчою вартістю шляху (path cost). Виходячи з рисунку вище найменший ID дорівнює 3. Отже, міст 3 стає кореневим. Можливі випадки, коли вартість шляху у двох і більше портах комутатора буде однакова, тоді вибір кореневого (root) порту відбуватиметься на підставі отриманих від сусідів пріоритету та порядкового номера порту (Lowest sender port id), наприклад, fa0/1, fa0/2, fa0/3 та кореневим (root) стане порт із найменшим номером.

Комутатори, за замовчуванням, не вимірюють стан завантаження мережі в реальному часі і працюють відповідно до вартості інтерфейсів в момент побудови дерева STP. Кожен порт має свою вартість (cost), обернено пропорційну пропускній спроможності (bandwidth) порту і яку можна налаштовувати вручну.

Всі порти в STP послідовно проходять чотири стани: blocking (прослуховують Bridge protocol data unit (BPDU) без передачі), listening (прослуховують і ретранслюють BPDU), learning (отримують дані, оновлюють MAC-таблиці), forwarding (робочий стан порту). З інтервалами за замовчуванням робота порту починається через 30 секунд. Розглянемо алгоритм дії STP. Після включення комутаторів до мережі за замовчуванням кожен комутатор вважає себе кореневим (root). Кожен комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз на 2 секунди.

Якщо міст отримує BPDU з ідентифікатором моста (bridge ID) меншим, ніж власний, він припиняє генерувати свої BPDU і починає ретранслювати BPDU з цим ідентифікатором. Таким чином в цій мережі Ethernet залишається лише один міст, який продовжує генерувати та передавати власні BPDU. Він стає кореневим мостом (root bridge). Інші мости ретранслюють BPDU кореневого моста, додаючи в них власний ідентифікатор та збільшуючи лічильник вартості шляху (path cost). Для кожного сегмента мережі, до якого приєднано два і більше портів мостів, відбувається визначення designated port, тобто порту, через який BPDU, що надходять від кореневого мосту, потрапляють у цей сегмент. Після цього всі порти в сегментах, до яких приєднано два і більше портів моста, блокуються за винятком root port і designated port. Кореневий міст продовжує посилати свої Hello BPDU раз на 2 секунди. Rapid STP (RSTP) є значним удосконаленням STP. Насамперед необхідно відзначити зменшення часу збіжності та більш високу стійкість. Неабиякою мірою це досягнуто за рахунок ідей, використаних Cisco Systems як пропрієтарні розширення STP.

Rapid STP сумісний із STP. Якщо якийсь пристрій використовує STP, то Rapid STP теж використовуватиме STP з цим пристроєм, але у цьому режимі може бути, що наявність Rapid STP інших пристроях не дає переваг проти STP.

Per-VLAN STP (PVSTP) відповідно до назви розширює функціональність STP для використання VLAN. В рамках цього протоколу в кожному VLAN працює окремий екземпляр STP і є пропрієтарним розширенням Cisco.

Multiple STP це варіація протоколу STP, яку можна класифікувати за кількістю екземплярів STP у разі, коли число VLAN більше одиниці. Є варіації протоколів, де на всі VLAN припадає єдиний екземпляр STP.

Деяка надмірність варіацій з окремим екземпляром STP для кожної VLAN полягає в тому, що якщо топологія кількох VLAN збігається, то відповідні екземпляри STP повністю повторюють роботу один одного. У такому разі в принципі непотрібна робота по суті дублюючих один одного екземплярів STP обертається непотрібним додатковим навантаженням на процесор комутатора, і в кінцевому рахунку може змусити конструкторів обладнання для забезпечення його стійкої роботи вибирати потужніший процесор з великим енергоспоживанням, що може спричинити додаткові витрати на електроживлення та охолодження як при виготовленні обладнання, так і експлуатації.

У цьому плані окремо стоїть Multiple STP. В один екземпляр Multiple STP можуть входити кілька віртуальних мереж за умови, що їхня топологія однакова (в сенсі комутаторів, що входять до VLAN, і з'єднань між ними). Мінімальна кількість екземплярів Multiple STP відповідає кількості топологічно унікальних груп VLAN у домені другого рівня (на рівні комутаторів та з'єднань між ними). Multiple STP накладає важливе обмеження: всі комутатори, що беруть участь у Multiple STP, повинні мати однаково налаштовані групи VLAN, що обмежує гнучкість при зміні конфігурації мережі.

Контрольні запитання

1. Надайте поняття та основне призначення протоколу STP.
2. До якого рівня моделі OSI відноситься STP?
3. Що вам відомо про стандарт IEEE-802.1D?
4. Наведіть основні принципи дії STP.
5. Опишіть основні 4 стани, які проходять порти в STP.
6. Що таке BPDU?
7. Наведіть поняття та властивості топологічних груп.

6 АГРЕГУВАННЯ КАНАЛІВ

6.1 Основні принципи та термінологія

Агрегування каналів (агрегація каналів, link aggregation) – технологія, що дозволяє об’єднати кілька фізичних каналів в один логічний. Таке об’єднання дозволяє збільшувати пропускну здатність та надійність каналу. Агрегування каналів може бути налаштовано між двома комутаторами, комутатором та маршрутизатором, між комутатором та хостом.

Для агрегування каналів існують інші назви, такі як:

– port trunking (trunk називається тегований порт, тому з цим терміном плутанини найбільше);

– etherchannel (агрегування каналів, це може стосуватися як налаштування статичних агрегованих каналів, так і з використанням протоколів «Link aggregation control protocol» (LACP) або «Port aggregation protocol» (PAgP);

– інші, а саме магістраль Ethernet, об’єднання мережних карток, канал портів, об’єднання портів, об’єднання каналів, багатоканальні канали, об’єднання мережних карток, відмовостійкість мережі, швидкий EtherChannel тощо.

Агрегування каналів дозволяє вирішити дві задачі, а саме підвищити пропускну спроможність каналу та забезпечити резерв у разі виходу з ладу одного з каналів.

Більшість технологій з агрегування дозволяють об’єднувати лише паралельні канали, тобто такі, які починаються на тому самому пристрої і закінчуються на іншому (рис. 6.1).

Рисунок 6.1 – Агрегування каналів

Якщо розглядати надмірні з’єднання між комутаторами, то без використання спеціальних технологій для агрегування каналів, дані будуть

передаватися тільки через один інтерфейс, який не заблокований STP. Такий варіант дозволяє забезпечити резервування каналів, але не дозволяє збільшити пропускну здатність (рис. 6.2).

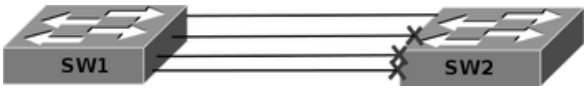

Рисунок 6.2 – Забезпечення резервування каналів

Технології агрегування каналів дозволяють використовувати всі інтерфейси одночасно. При цьому пристрої контролюють поширення широкомовних кадрів (а також multicast і unknown unicast), щоб вони не зациклювалися. Для цього комутатор при отриманні широкомовного кадру через звичайний інтерфейс відправляє його в агрегований канал тільки через один інтерфейс. А при отриманні широкомовного кадру з агрегованого каналу не відправляє його назад.

Хоча агрегування каналів дозволяє збільшити пропускну здатність каналу, не варто розраховувати на ідеальне балансування навантаження між інтерфейсами в агрегованому каналі. Технології з балансування навантаження в агрегованих каналах, як правило, орієнтовані на балансування за такими критеріями: MAC-адреси, IP-адреси, порти відправника або одержувача (по одному критерію або їх комбінації).

Тобто реальна завантаженість конкретного інтерфейсу ніяк не враховується. Тому один інтерфейс може бути завантажений більше за інші. Більше того, при неправильному виборі методу балансування (або якщо недоступні інші методи) або в деяких топологіях, може скластися ситуація, коли всі дані будуть передаватися, наприклад, через один інтерфейс.

Деякі пропрієтарні розробки дозволяють агрегувати канали, які з’єднують різні пристрої. Таким чином резервується не тільки канал, а й сам пристрій. Такі технології загалом, як правило, називаються розподіленим агрегуванням каналів (у багатьох виробників є своя назва цієї технології).

Для агрегування каналів, наприклад у Cisco, може бути використаний один із трьох варіантів LACP протокол, PAgP та статичне агрегування без використання протоколів.

Оскільки LACP і PAgP вирішують одні й самі завдання (з невеликими відмінностями за можливостями), краще використовувати стандартний протокол. Фактично залишається вибір між LACP та статичним агрегуванням.

Перевага статичного агрегування в тому, що не вноситься додаткова затримка під час підняття агрегованого каналу або зміни його налаштувань. Недоліком є те, що немає узгодження налаштувань із віддаленою стороною. Помилки в налаштуванні можуть призвести до утворення петель

До переваг агрегування за допомогою LACP відноситься узгодження налаштувань з віддаленою стороною, що дозволяє уникнути помилок та петель у мережі та підтримка standby-інтерфейсів, яка дозволяє агрегувати до шістнадцяти портів, вісім з яких будуть активними, а решта в режимі standby. Недоліком агрегування за допомогою LACP є внесення додаткової затримки під час підняття агрегованого каналу або зміни його налаштувань.

6.2 Налаштування каналів

При настроюванні агрегування каналів на обладнанні використовується Etherchannel, тобто технологія агрегування каналів, port-channel, тобто логічний інтерфейс, який поєднує фізичні інтерфейси та channel-group команда, яка вказує на який логічний інтерфейс належить фізичний інтерфейс і який режим використовується для агрегування.

Ці терміни використовуються при налаштуванні в командах перегляду незалежно від того, який варіант агрегування використовується (який протокол, якого рівня Etherchannel) (рис. 6.3).

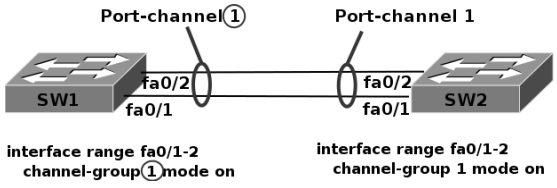

Рисунок 6.3 – Налаштування агрегування каналів

На схемі число після команди channel-group вказує який номер буде у логічного інтерфейсу port-channel. Номери логічних інтерфейсів із двох сторін агрегованого каналу не обов'язково мають збігатися. Номери використовуються для того, щоб відрізняти різні групи портів в межах одного комутатора.

LACP та PAgP групують інтерфейси з однаковою швидкістю (speed), режимом дуплекса (duplex mode), native VLAN, діапазоном дозволених VLAN, станом транкінгу, типом інтерфейсу.

6.3 Налаштування Etherchannel

Так як для об'єднання в Etherchannel на інтерфейсах повинні збігатися багато параметрів, простіше об'єднувати їх, коли вони налаштовані за замовчуванням. А потім налаштовувати логічний інтерфейс. Перед об'єднанням інтерфейсів краще вимкнути їх. Це дозволить уникнути блокування інтерфейсів STP (або переведення їх у стан err-disable). Щоб видалити налаштування Etherchannel, достатньо видалити логічний інтерфейс. Команди channel-group видаляються автоматично.

Створення Etherchannel для портів рівня 2 та портів рівня 3 відрізняється:

– для інтерфейсів 3-го рівня вручну створюється логічний інтерфейс командою port-channel;

– для інтерфейсів 2-го рівня логічний інтерфейс створюється динамічно;

– для обох типів інтерфейсів необхідно вручну призначати інтерфейс Etherchannel. Для цього використовується команда channel-group у режимі налаштування інтерфейсу. Ця команда пов'язує разом фізичні та логічні порти.

Після налаштування Etherchannel зміни, які застосовуються до port-channel інтерфейсу, застосовуються до всіх фізичних портів, які присвоєно цьому port-channel інтерфейсу. Також зміни, які застосовуються до фізичного порту впливають тільки на порт, на якому були зроблені ці зміни.

Розглянемо налаштування статичного Etherchannel 2-го рівня (рис. 6.4).

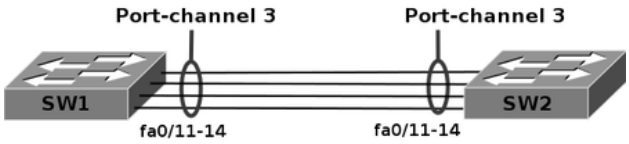

Рисунок 6.4 – Налаштування статичного Etherchannel 2-го рівня

Особливості налаштування агрегування на маршрутизаторі:

– підтримується лише статичне агрегування без використання протоколів;

– можна створити лише два агреговані інтерфейси;

– максимальна кількість інтерфейсів у Etherchannel 4 штуки;

– метод балансування використовує IP-адреси відправника та одержувача, включений за замовчуванням і не може бути змінено;

– агрегувати можна лише ті інтерфейси, що знаходяться на модулях однакового типу.

Розглянемо взаємодію Etherchannel з іншими функціями:

– dynamic trunking protocol та cisco discovery protocol відправляють та отримують пакети через фізичні інтерфейси до Etherchannel;

– trunk ports відправляють та отримують PAgP та LACP через VLAN з найменшим номером;

– spanning tree відправляє пакети через перший інтерфейс EtherChannel;

– MAC-адреса EtherChannel 3-го рівня це MAC-адреса першого порту в port-channel;

– PAgP відправляє та отримує тільки з інтерфейсів на яких PAgP включений у режимі auto або desirable;

– LACP відправляє та отримує тільки з інтерфейсів, на яких LACP включений у режимі active або passive.

6.4 Розподілене агрегування

У комутаторах, наприклад, HP серій 5400, 3500, 8200, підтримується розподілене агрегування портів. Розподілене агрегування дозволяє об’єднувати

порти, що знаходяться на різних комутаторах. За допомогою повідомлень пропрієтарного протоколу, пара комутаторів узгоджує налаштування і для інших пристроїв, розподілений транк виглядає як транк з одним комутатором.

На кожному з пари комутаторів, між якими налаштовується розподілений транк, повинні бути налаштовані два спеціальні інтерфейси:

1. ISC-інтерфейс (Inter switch connect), через який комутатори обмінюються інформацією для того, щоб пара комутаторів для інших пристроїв виглядала як один комутатор. Це може бути один фізичний інтерфейс чи транк.
2. Keepalive-інтерфейс це інтерфейс 3-го рівня, який використовується для передачі повідомлень keepalive при падінні ISC-інтерфейсу, для того щоб визначити вийшов з ладу ISC-інтерфейс або весь комутатор.

Але накладаються і обмеження розподіленого агрегування:

– розподілений транк можна налаштувати лише між двома комутаторами;

– на кожному з комутаторів в одному розподіленому транці може бути не більше чотирьох портів;

– розподілений транк може бути налаштований лише як статичний транк за допомогою LACP або протоколу.

Для того, щоб розподілений транк працював коректно, повинні бути узгоджені такі налаштування комутаторів:

– у комутаторів мають бути однакові версії операційної системи;

– Inter switch connect інтерфейс має бути налаштований на обох комутаторах з однаковими VLAN;

– всі інтерфейси, які об’єднуються в розподілений транк, повинні бути налаштовані з однаковими VLAN;

– ім’я транку та тип транку мають бути однаковими;

– налаштування DHCP snooping на комутаторах мають бути однаковими. Inter Switch Connect інтерфейс має бути довіреним на обох комутаторах при цьому час має бути синхронізований;

– налаштування loop protection повинні бути однаковими;

Відповідно використовується наступна термінологія:

– Distributed trunking switch-комутатори (DT-комутатори), що беруть участь в організації розподіленого транку;

– DT-інтерфейси, що належать розподіленому транку;

– Distributed trunking device-пристрої (DTD), що підключаються до розподіленого транку (комутатори, сервера).

DT-комутатори вибирають між собою основний пристрій та вторинний. Той комутатор у якого менша системна MAC-адреса стає основним пристроєм.

Ці ролі визначаються для того, щоб визначити який пристрій передаватиме трафік, якщо ISC-інтерфейс вимкнений.

Якщо Inter Switch Connect інтерфейс падає, кожен комутатор запускає таймер hold. У цей час не надсилаються повідомлення keepalive.

Коли таймер закінчується, обидва комутатори починають обмінюватися keepalive повідомленнями.

Якщо протягом інтервалу timeout повідомлення keepalive не прийшли, комутатор вважає, що сусід не працездатний і передає трафік самостійно.

Якщо після падіння Inter Switch Connect інтерфейсу на вторинний комутатор прийшли повідомлення keepalive від основного, то вторинний комутатор відключає всі DT-інтерфейси.

Основний комутатор завжди передає трафік, незалежно від того отримав він keepalive повідомлення від вторинного чи ні.

При відновленні ISC-інтерфейсу комутатори відновлюють нормальний режим роботи.

Контрольні запитання

1. Надайте поняття агрегування каналів.
2. Назвіть основні переваги та недоліки статичного агрегування.
3. Які особливості налаштування агрегування на маршрутизаторі?
4. Які варіанти агрегування каналів вам відомі?

5. Назвіть переваги та недоліки агрегування за допомогою LACP.
6. У чому полягає метод балансування?
7. Що вам відомо про ISC-інтерфейс?
8. Наведіть принцип використання розподіленого агрегування.
9. Чим відрізняються створення EtherChannel для портів рівня 2 та 3?

7 КОМУТАТОРИ ТРЕТЬОГО РІВНЯ

7.1 Технології комутації та модель «The open systems interconnection model»

Комутатори локальних мереж можна класифікувати відповідно до рівня моделей OSI, на яких вони передають, фільтрують і комутують кадри. Розрізняють комутатори 2-го рівня (Layer 2 Switch), комутатори 2-го рівня з властивостями рівня 3-го (Layer 3 Switch) і багаторівневі комутатори.

Комутатори рівня 2-го аналізують вхідні кадри, приймають рішення про їх подальшу передачу та передають їх пунктам призначення на основі MAC-адресу канального рівня моделі OSI. Основна перевага комутаторів 2-го рівня полягає у прозорості для протоколів верхнього рівня.

Комутація 2-го рівня апаратна. Вона має високу продуктивність, оскільки пакет даних не зазнає змін. Передача кадру в комутаторі може здійснюватись спеціалізованим контролером, званим Application Specific Integrated Circuits. Ця технологія, розроблена для комутаторів, дозволяє забезпечувати високу швидкість комутації з мінімальними затримками.

Існують дві основні причини використання комутаторів 2-го рівня, а саме сегментація мережі та об’єднання робочих груп. Висока продуктивність комутаторів дозволяє розробникам мереж значно зменшити кількість вузлів у фізичному сегменті. Розподіл великої мережі на логічні сегменти підвищує продуктивність мережі (за рахунок зменшення обсягу даних в окремих сегментах), а також гнучкість побудови мережі, збільшуючи ступінь захисту даних, і полегшує управління мережею.

Незважаючи на переваги комутації 2-го рівня, вона все ж таки має деякі обмеження. Наявність комутаторів у мережі не перешкоджає поширенню широкомовних кадрів (broadcast) по всіх сегментах мережі, зберігаючи її прозорість.

Таким чином, очевидно, що для підвищення продуктивності мережі потрібна функціональність 3-го рівня OSI моделі.

Комутатор локальної мережі 2-го рівня з функціями рівня 3 (або комутатор 3-го рівня) приймає рішення про комутацію на підставі більшої кількості інформації, ніж просто MAC-адреса.

Комутатори 3-го рівня здійснюють комутацію та фільтрацію на основі адрес канального (рівень 2) та мережного (рівень 3) рівнів OSI-моделі. Такі комутатори динамічно вирішують, комутувати (рівень 2) або маршрутизувати (рівень 3) трафік, що входить. Комутатори рівня 3 виконують комутацію в межах робочої групи і маршрутизацію між робочими групами.

Комутатори 3-го рівня функціонально практично нічим не відрізняються від традиційних маршрутизаторів та виконують функції визначення оптимальних шляхів передачі даних на основі логічних адрес (адреса мережного рівня, традиційна IP-адреса), управління широкомовним та багатоадресним трафіком, фільтрація трафіку на основі інформації 3-го рівня та IP-фрагментацію.

Основна відмінність між маршрутизаторами та комутаторами 3-го рівня полягає в тому, що в маршрутизаторах загального призначення прийняття рішення про пересилання пакетів зазвичай виконується програмним чином, а в комутаторах обробляється спеціалізованими контролерами. Це дозволяє комутаторам виконувати маршрутизацію пакетів швидкості каналу зв’язку.

Комутація 4-го рівня вважається технологією апаратної комутації рівня 3, яка може враховувати додаток, що використовується. Комутатори використовують інформацію 4-го рівня (номери портів, що знаходяться в заголовку транспортного рівня) при створенні списків доступу для фільтрації даних протоколів верхнього рівня, програм та додатків.

Багаторівневі комутатори поєднують у собі технології комутації рівнів 2, 3 та 4.

Ухвалення рішення про передачу даних здійснюється в таких комутаторах на основі MAC-адреса джерела чи приймача кадру даних, IP-адреси джерела чи приймача із заголовка мережного (3-го) рівня, типу

протоколу в заголовку мережного рівня та номера порту джерела чи приймача у заголовку транспортного рівня.

7.2 Характеристики, що впливають на продуктивність комутаторів

Продуктивність комутатора – характеристика, на яку мережні інтегратори та досвідчені адміністратори звертають увагу насамперед при виборі пристрою.

Основними показниками комутатора, що характеризують його продуктивність, є швидкість фільтрації кадрів, швидкість просування кадрів, пропускна спроможність та затримка передачі кадру.

Крім того, існує кілька характеристик комутатора, які найбільше впливають на зазначені характеристики продуктивності. До них відносяться тип комутації, розмір буфера кадрів, продуктивність внутрішньої шини, продуктивність процесора чи процесорів та розмір внутрішньої адресної таблиці.

Швидкість фільтрації та просування кадрів – це дві основні характеристики продуктивності комутатора. Ці характеристики є інтегральними показниками і залежить від того, як технічно реалізований комутатор.

Швидкість фільтрації визначає швидкість, з якою комутатор виконує такі етапи обробки кадрів, як прийом кадру до свого буфера, перегляд адресної таблиці з метою знаходження порту адреси призначення кадру та знищення кадру, якщо його порт призначення та порт джерела належать одному логічному сегменту.

Швидкість просування визначає швидкість, з якою комутатор виконує такі етапи обробки кадрів, як прийом кадру до свого буфера, перегляд адресної таблиці з метою знаходження порту адреси призначення кадра, передача кадру до мережі через знайдений за адресною таблицею порт призначення.

Як швидкість фільтрації, швидкість просування вимірюється, зазвичай, у кадрах на секунду. Якщо в характеристиках комутатора не уточнюється, для якого протоколу та якого розміру кадру наведено значення швидкостей

фільтрації та просування, то за умовчанням вважається, що ці показники даються для протоколу Ethernet та кадрів мінімального розміру, тобто кадрів завдовжки 64 байт (без преамбули) з полем даних 46 байт. Застосування в якості основного показника швидкості обробки комутатором кадрів мінімальної довжини пояснюється тим, що такі кадри завжди створюють для комутатора найбільш важкий режим роботи в порівнянні з кадрами іншого формату при рівній пропускній здатності даних, що передаються.

Тому при проведенні тестування комутатора режим передачі кадрів мінімальної довжини використовується як найскладніший тест, який повинен перевірити здатність комутатора працювати за найгіршого поєднання параметрів трафіку.

Пропускна спроможність комутатора вимірюється кількістю даних користувача (у мегабітах або гігабітах в секунду), переданих в одиницю часу через його порти. Так як комутатор працює на канальному рівні, для нього даними користувача є ті дані, які переносяться в поле даних кадрів протоколів канального рівня, а саме Ethernet, Fastethernet тощо.

Максимальне значення пропускної спроможності комутатора завжди досягається на кадрах максимальної довжини, тому що при цьому частка накладних витрат на службову інформацію кадру набагато нижча, ніж для кадрів мінімальної довжини, а час виконання комутатором операцій з обробки кадру, що припадає на один байт інформації користувача, істотно менше. Тому комутатор може бути блокуючим для кадрів мінімальної довжини, але при цьому мати дуже добрі показники пропускної здатності.

Затримка передачі кадру вимірюється як час, що минув з приходу першого байта кадру на вхідний порт комутатора до появи цього байта в його вихідному порту. Затримка складається з часу, що витрачається на буферізацію байт кадру, а також часу, що витрачається на обробку кадру комутатором, а саме перегляду адресної таблиці, прийняття рішення про просування та отримання доступу до середовища вихідного порту. Величина затримки, що вноситься комутатором, залежить від режиму його роботи.

7.3 Загальні принципи проєкту комп'ютерної мережі

Грамотний мережний проєкт ґрунтується на багатьох принципах, основні з яких можна виразити так:

1. Вивчення можливих точок відмови мережі існує для того, щоб поодинока відмова не могла ізолювати якийсь із сегментів мережі, у ній має бути передбачена надмірність. Під надмірністю розуміється резервування життєво важливих компонентів мережі та розподіл навантаження. Так у разі відмови в мережі повинен існувати альтернативний або резервний шлях до будь-якого її сегменту. Розподіл навантаження використовується в тому випадку, якщо до пункту призначення є два або більше шляхів, які можуть використовуватись залежно від завантаженості мережі. Необхідний рівень надмірності мережі змінюється залежно від її конкретної реалізації.

2. Визначення типу трафіку мережі, а саме якщо в мережі використовуються клієнт-серверні програми, то потік трафіку, що виробляється ними, є критичним для ефективного розподілу ресурсів, таких як кількість клієнтів, що використовують певний сервер або кількість клієнтських робочих станцій в сегменті.

3. Аналіз доступної смуги пропускання реалізується коли у мережі не повинно бути великої різниці у доступній смузі пропускання між різними рівнями ієрархічної моделі (опис ієрархічної моделі мережі знаходиться в наступному розділі нижче). Важливо пам'ятати, що ієрархічна модель посилається на концептуальні рівні, які забезпечують функціональність. Фактична межа між рівнями може не проходити фізичним каналом зв'язку, їй може бути і внутрішня магістраль певного пристрою.

4. Створення мережі на базі ієрархічної чи модульної моделі, коли ієрархія дозволяє об'єднати через міжмережні пристрої окремі сегменти, які функціонуватимуть як єдина мережа.

Ієрархічна модель визначає підхід до проєктування мереж і включає три логічні рівні: рівень доступу, рівень розподілу та рівень ядра.

Рівень ядра знаходиться на самій верхівці ієрархії та відповідає за надійну та швидку передачу великих обсягів даних.

Трафік, що передається через ядро, є загальним для більшості користувачів.

Самі дані користувача обробляються на рівні розподілу, який, при необхідності, пересилає запити до ядра.

Для рівня ядра велике значення має його стійкість до відмови, оскільки збій на цьому рівні може призвести до втрати зв'язності між рівнями розподілу мережі.

Рівень розподілу, який іноді називають рівнем робочих груп, є сполучною ланкою між рівнями доступу та ядра.

Залежно від способу реалізації, рівень розподілу може виконувати такі функції, як:

– забезпечення маршрутизації;

– забезпечення якості обслуговування та безпеки мережі;

– агрегування каналів;

– перехід від однієї технології до іншої (наприклад, від 100Base-TX до 1000Base-T);

– об'єднання смуг пропускання низькошвидкісних каналів доступу до високошвидкісних магістральних каналів.

Рівень доступу керує доступом користувачів та робочих груп до ресурсів об'єднаної мережі.

Основним завданням рівня доступу є створення точок входу або виходу користувачів у мережу.

Рівень виконує такі функції, як продовження (починаючи з рівня розподілу) управління доступом та політиками мережі, створення окремих доменів колізій (сегментація), підключення робочих груп до рівня розподілу та рівень доступу використовує технологію комутованих локальних мереж.

7.4 Особливості використання комутаторів третього рівня

Комутатор 3-го рівня це пристрій, який пересилає трафік на основі інформації рівня 3 (головним чином через MAC-адресу).

Комутатор 3-го рівня підтримує всі функції комутації, а також має деякі функції маршрутизації між VLAN.

Він задуманий, як технологія для підвищення продуктивності мережної маршрутизації у великих локальних мережах.

Для комутатора 3-го рівня перенаправлення рівня виконується спеціалізованими ASIC, а це швидше ніж маршрутизатори, але їм зазвичай не вистачає розширених можливостей маршрутизаторів.

На відміну від маршрутизаторів, комутатор 3-го рівня менш схильний до затримки в мережі, оскільки пакетам не потрібно виконувати додаткові дії через маршрутизатор.

Комутатор 3-го рівня виконує функції, як і 2-го рівня, тому, його також називають багаторівневим комутатором, Комутатор 3-го рівня це насамперед пристрій локальної обчислювальної мережі.

Тобто, цей комутатор повинен маршрутизувати трафік локальної мережі між існуючими сегментами. Зазвичай він використовується лише на рівні розподілу в ієрархічної моделі мережі.

Контрольні запитання

1. Які основні переваги комутаторів 2 рівня?
2. Що вам відомо про контролер ASIC?
3. Для чого потрібна функціональність 3-го рівня OSI моделі?
4. Назвіть основні функції комутаторів рівня 3.
5. Які показниками комутатора характеризують його продуктивність?
6. У чому вимірюється пропускна спроможність комутатора?
7. З чого складається затримка передачі кадру?
8. Що таке надмірність?
9. Які три логічні рівні включає ієрархічна модель?

10. Наведіть основні функції рівню розподілу.

11. Що відноситься до сегментів?

12. Які пристрої менш схильні до затримки в мережі?

8 ОСНОВИ МАРШРУТИЗАЦІЇ

8.1 Маршрутизація та класифікація методів маршрутизації

За допомогою маршрутизаторів можна з'єднувати комп'ютери, а також забезпечувати обмін даними між двома мережами, наприклад, між домашньою мережею та Інтернетом. Саме через здатність спрямовувати мережний трафік маршрутизатор має таку назву.

Маршрутизатори можуть бути провідними (з використанням кабелів Ethernet) або безпровідними. Якщо слід лише з'єднати комп'ютери, концентраторів і маршрутизаторів вистачить; проте якщо слід надати доступ до Інтернету для всіх комп'ютерів за допомогою одного модему, необхідно використовувати маршрутизатор або модем із вбудованим маршрутизатором.

Маршрутизатори забезпечують комутацію мереж 3-го (мережного) рівня, засоби з'єднування вузлів різних мереж, що використовують мережні (логічні) адреси вузлів.

Мережі можуть бути віддалені, а шлях передавання пакетів пролягати через інші маршрутизатори. Мережна адреса при цьому трактується як ієрархічний опис розташування вузла. Більш складні мультипротокольні маршрутизатори підтримують одночасно декілька протоколів для гетерогенних мереж. Іноді розрізняють, так звані, Brouter (Bridging router), тобто комбінацію моста та маршрутизатора, що одночасно оперує на мережному та канальному рівнях.

Основні характеристики маршрутизатора:

- тип (однопротокольний, мультипротокольний, LAN або WAN, Brouter);
- підтримувані протоколи;
- пропускна здатність;
- типи мереж, що можуть під'єднуватись;
- інтерфейси (LAN або WAN);
- кількість портів;
- можливість управління та моніторингу мережею.

Маршрутизатор (router) – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (3-й рівень моделі OSI) між різними сегментами мережі.

Для звичайного користувача маршрутизатор (роутер) це мережний пристрій, який підключається між локальною мережею та Інтернетом.

Часто маршрутизатор не обмежується простим пересиланням даних між інтерфейсами, а й виконує і інші функції, а саме захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів Інтернету, роздає IP-адреси, шифрує трафік і багато іншого.

Маршрутизатори працюють на мережному рівні моделі OSI та можуть пересилати пакети з однієї мережі до іншої. Для того, щоб надіслати пакети в потрібному напрямку, маршрутизатор використовує таблицю маршрутизації, що зберігається у пам'яті.

Таблиця маршрутизації може складатися засобами статичної або динамічної маршрутизації.

Крім того, маршрутизатори можуть здійснювати трансляцію адреси відправника й одержувача (NAT), фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування або дешифрування даних, що передаються тощо.

Таблиця складається з деякого числа записів (маршрутів), в кожному з яких міститься адреса мережі одержувача, адреса наступного вузла, якому слід передавати пакети і певна вага запису (метрика). Метрики записів в таблиці грають роль в обчисленні найкоротших маршрутів до різних одержувачів.

Проблема маршрутизації полягає у виборі шляху, яким рухається пакет у багатовузловій мережі. Цей шлях повинен задовольняти певні вимоги, а саме: найшвидше передавання даних з найменшими змінами.

Маршрутизація забезпечується розміщенням у вузлах мережі маршрутної інформації (таблиці маршрутизації) та програм, які реалізують алгоритм маршрутизації.

Загалом методи маршрутизації поділяють на прості і складні (рис. 8.1).

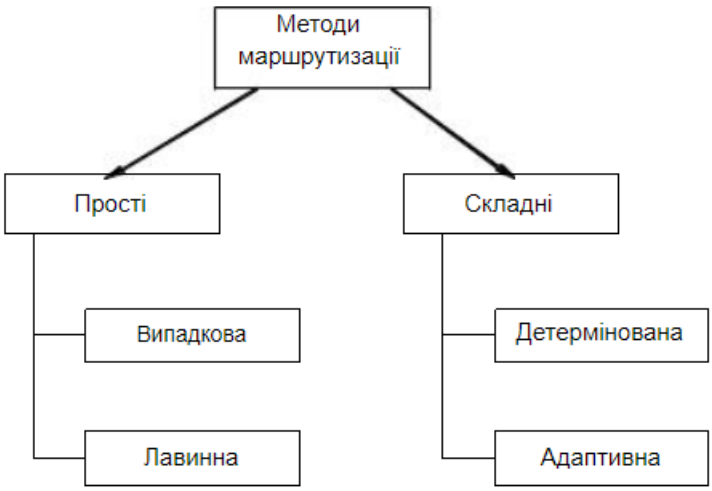

Рисунок 8.1 – Класифікація методів маршрутизації

Прості методи маршрутизації це лише проміжний етап розвитку методів маршрутизації. Ці методи вже практично ніде не використовуються.

Для детермінованого методу маршрутизації характерне ручне складання та коригування таблиць маршрутизації. Метод ефективний для невеликих малозавантажених мереж. Є варіанти цього методу, які враховують можливість виходу каналів з ладу, а також варіанти, які передбачають розщеплення потоку (60% та 40%).

Широко використовуються зараз адаптивні методи маршрутизації, які є найпрогресивнішими з погляду алгоритму маршрутизації.

8.2 Адаптивні методи маршрутизації

Адаптивна маршрутизація передбачає пристосування алгоритму маршрутизації до реального стану мережі. Недоліком методів адаптивної маршрутизації є складність прогнозування стану мережі.

Зараз використовуються наступні основні методи адаптивної маршрутизації:

– маршрутизація за досвідом. Кожний пакет має лічильник пройдених каналів. Транзитні пакети скеровуються у випадкові канали. У вузлах мережі створюється таблиця найближчих вузлів для конкретного адресата;

– метод найшвидшого передавання. Мета – швидше позбутись транзитного пакету. В методі використовується глобальна інформація про наявність та довжину черг до вихідних каналів;

– локально – адаптивна маршрутизація. Вибір напряму передавання здійснюється на підставі локальної інформації про наявність та довжину черг до вихідних каналів;

– розподілена маршрутизація. У кожному вузлі зберігаються таблиці маршрутизації, в яких вказані маршрути до кожного з адресатів з мінімальною затримкою. Спочатку ці таблиці будують на підставі теоретичних обчислень за відомою топологією, а потім ці дані поновлюються з використанням спостережень. В мережі при цьому завжди існує трафік маршрутизації (до 50% трафіку);

– централізована маршрутизація. Таблиця маршрутизації формується на сервері домена і передається на всі вузли. Таблиця маршрутизації будується на основі інформації, яку передають вузли;

– гібридна маршрутизація. Цей метод є комбінацією методів локально – адаптивної і централізованої маршрутизації. Рішення про напрям передавання приймається на основі порівняння оцінок за обома варіантами.

8.3 Маршрутизація в Transmission Control Protocol / Internet Protocol

Головним параметром маршрутизації є IP-адреса. У відповідності з протоколом IP вузли поділяються на маршрутизатори (routers) та хости (hosts).

Маршрутизатор це апаратно – програмний комплекс, який фізично поєднує кілька комп’ютерних мереж, передаючи за допомогою спеціального програмного забезпечення пакети з однієї мережі в іншу (приймає у свій буфер по одному каналу зі своїх вхідних каналів і відправляє по одному зі своїх вихідних каналів).

Маршрутизатор може поєднувати мережі з різною топологією та різними протоколами.

Хост це спільний термін, який описує програмно – апаратний комплекс, який містить ресурси (апаратні, програмні та інформаційні) і надає до них доступ.

Хости не розсилають таблиці маршрутизації, хоча й можуть мати програмне забезпечення для їх створення та для маршрутизації.

Принцип маршрутизації проілюструємо на наступному прикладі (рис. 8.2):

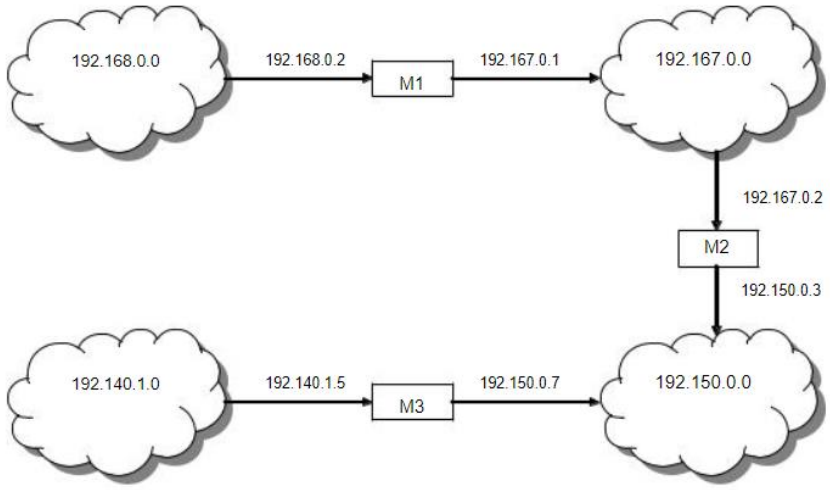

Рисунок 8.2 – Приклад схеми мережі

На цій схемі зображено чотири мережі-адресати, три маршрутизатори і IP-адреси мереж та кожного маршрутизатора зі сторони кожної мережі [6, с. 16].

Для цієї мережі таблиця маршрутизації матиме наступний вигляд (табл. 8.1):

Таблиця 8.1 – Таблиця маршрутизації для маршрутизатора M2

Мережа – адресат	Маршрут
192.167.0.0	пряме передавання
192.150.0.0	пряме передавання
192.168.0.0	через адресу 192.167.0.1
192.140.1.0	через адресу 192.150.0.7

8.4 Алгоритм вибору маршруту

Алгоритм вибору маршруту має наступний вигляд:

1. З пакету зчитується IP-адреса.

2. В IP-адресі виділяється адреса мережі призначення.

3. Якщо адреса мережі призначення відповідає даній локальній мережі, то пакет надсилається безпосередньо адресату.

4. Якщо вказана адреса є в таблиці маршрутизації, то пакет надсилається за відповідним маршрутом.

5. Якщо описаний маршрут за замовчуванням, то пакет надсилається за адресою за замовчуванням.

6. Якщо ні один із варіантів неможливий, то видається повідомлення про помилку маршрутизації.

Графічно цей алгоритм можна зобразити наступним чином (рис. 8.3):

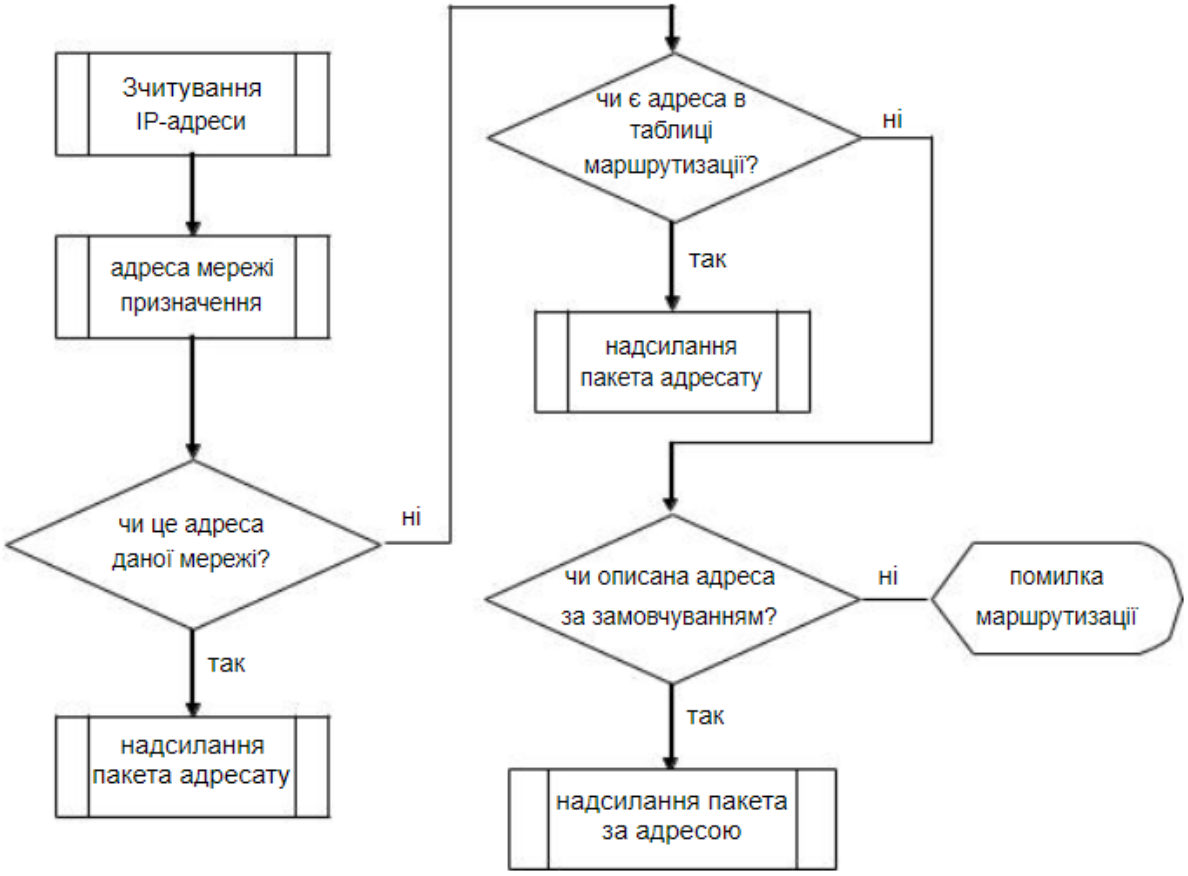

Рисунок 8.3 – Алгоритм вибору маршруту

Контрольні запитання

1. Які пристрої називають маршрутизаторами?
2. Які основні характеристики маршрутизатора?
3. На якому рівні моделі OSI знаходяться маршрутизатори?
4. У чому полягає основна проблема маршрутизації?
5. Яку маршрутизацію називають адаптивною?
6. Наведіть визначення хосту.
7. Який принцип складання таблиці маршрутизації?

9 СТАТИЧНА МАРШРУТИЗАЦІЯ

9.1 Основні переваги та недоліки статичної маршрутизації

Маршрутизація виконується на рівні ядра мережі шляхом передачі даних через об’єднану мережу від джерела до одержувача. Маршрутизатори є пристроями, які відповідають за передачу пакетів з однієї мережі в іншу.

Маршрутизатори отримують дані про віддалені мережі динамічно за допомогою протоколів маршрутизації або вручну за допомогою статичних маршрутів. У багатьох випадках маршрутизатори одночасно використовують протоколи динамічної маршрутизації і статичні маршрути.

Статичні маршрути дуже поширені, при цьому вони не вимагають такої ж кількості обчислень і операцій, як протоколи динамічної маршрутизації. Маршрутизатор можна повідомити про віддалені мережі одним з двох способів: вручну, коли віддалені мережі вручну вводяться в таблицю маршрутизації за допомогою статичних маршрутів і динамічно віддалені маршрути автоматично додаються за допомогою протоколу динамічної маршрутизації.

Статична маршрутизація має свої переваги, в порівнянні з динамічною маршрутизацією в тому, що статичні маршрути не оголошуються по мережі, що робить їх більш безпечними.

Статичні маршрути використовують більш вузьку смугу пропускання, ніж протоколи динамічної маршрутизації (для розрахунку і зв’язку маршрутів цикли центрального процесора не використовуються). Шлях, який використовується статичним маршрутом для відправки даних, відомий.

Використання статичної маршрутизації також має недоліки: початкове налаштування і її підтримка вимагають часових витрат. При налаштуванні часто припускаються помилок, особливо в великих мережах. Для внесення змін до даних маршруту потрібне втручання адміністратора.

Недостатні можливості масштабування для зростаючих мереж, обслуговування при цьому стає досить трудомістким. Для якісного впровадження потрібно доскональне знання всієї мережі.

Статичні маршрути рекомендується використовувати в невеликих мережах, для яких заданий тільки один шлях до зовнішньої мережі. Вони також забезпечують безпеку в великих мережах з певним типом трафіку або в каналах до інших мереж, для яких потрібні розширені функції контролю.

Важливо розуміти, що статична і динамічна маршрутизація не є взаємовиключними. У більшості мереж використовується комбінація протоколів динамічної маршрутизації і статичних маршрутів. Це може привести до того, що для маршрутизатора задається кілька шляхів до мережі призначення за допомогою статичних маршрутів і динамічно одержуваних маршрутів. Однак слід пам’ятати, що значення адміністративної відстані (AD) є критерієм вибору джерел маршруту.

Джерела маршрутів з низькими значеннями AD краще джерел маршрутів з більш високими значеннями AD. Значення AD для статичного маршруту дорівнює 1.

Таким чином, статичний маршрут має пріоритет над усіма динамічно отриманими маршрутами, які будуть мати більш високі значення AD.

9.2 Завдання та типи статичної маршрутизації

Статична маршрутизація використовується в трьох ситуаціях:

– забезпечення спрощеного обслуговування таблиці маршрутизації в невеликих мережах, які не планується суттєво розширювати;

– маршрутизація до тупикових мереж і від них. Тупикова мережа являє собою мережу, доступ до якої здійснюється через один маршрут, і маршрутизатор має тільки одне сусіднє пристрій;

– використання єдиного маршруту за замовчуванням для подання шляху до довільної мережі, що не має більш точного збігу з іншим маршрутом в таблиці маршрутизації. Маршрути за замовчуванням використовуються для відправки трафіку в довільний пункт призначення за межами наступного маршрутизатора в висхідному напрямку.

На рисунку 9.1 представлений приклад підключення до тупикової мережі і використання маршруту за замовчуванням. Зверніть увагу, що на малюнку у будь-якій мережі, підключеної до маршрутизатора R0, буде тільки один шлях для доступу до інших місць призначення (до мереж, підключеним до маршрутизатора R1, або до місць призначення за межами маршрутизатора R2). Це означає, що мережа 192.168.33.0/24 є тупиковою, а маршрутизатор R0 – тупиковим маршрутизатором.

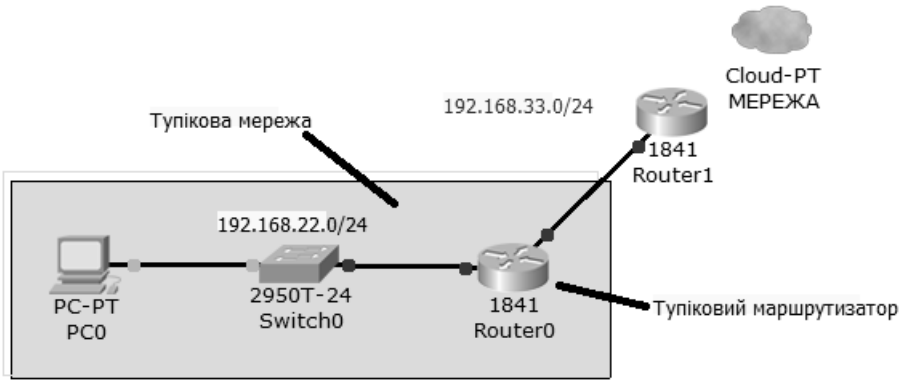

Рисунок 9.1 – Приклад підключення до тупикової мережі.

У цьому прикладі статичний маршрут можна налаштувати на маршрутизаторі R1 для доступу до мережі LAN маршрутизатора R0. Крім того, оскільки для маршрутизатора R0 існує тільки один спосіб відправки нелокального трафіку, статичний маршрут за замовчуванням можна налаштувати на маршрутизаторі R0 для вказівки на маршрутизатор R1 як на наступний перехід для всіх інших мереж.

Як показано на рисунку 9.1, статичні маршрути найчастіше використовуються для підключення до конкретної мережі або надання шлюзу останньої надії для тупикової мережі. Їх також можна використовувати для зменшення числа оголошених маршрутів шляхом об’єднання деяких суміжних мереж в один статичний маршрут та створення резервного маршруту на випадок відмови основного маршруту.

Існують чотири типи статичних маршрутів IPv4 і IPv6, а саме стандартний статичний маршрут, статичний маршрут за замовчуванням, сумарний статичний маршрут та плаваючий статичний маршрут.

Протоколи IPv4 і IPv6 підтримують налаштування статичних маршрутів. Статичні маршрути рекомендується використовувати при підключенні до певної віддаленої мережі. На рисунку 9.1 показано, що маршрутизатор R1 можна налаштувати з використанням статичного маршруту для доступу до тупикової мережі 192.168.22.0/24.

В даному прикладі продемонстровано тупикова мережа, але насправді статичний маршрут можна використовувати для підключення до будь-якої мережі.

Маршрут за замовчуванням це маршрут, який відповідає всім пакетам і використовується маршрутизатором, якщо пакет не відповідає жодному з інших, більш точних маршрутів з таблиці маршрутизації.

Маршрут за замовчуванням можна отримати динамічно або налаштувати статично. Статичний маршрут за замовчуванням це статичний маршрут з IPv4-адресою призначення, рівною 0.0.0.0/0. Під час налаштування статичного маршруту за замовчуванням створюється шлюз останньої надії.

Статичні маршрути за замовчуванням використовуються при відсутності інших маршрутів в таблиці маршрутизації, які збігаються з IP-адресою призначення пакета.

Статичні маршрути часто використовуються при підключенні прикордонного маршрутизатора компанії до мережі Інтернет провайдера. Якщо маршрутизатор підключений тільки до одного маршрутизатора.

Ще одним типом статичного маршруту є плаваючий статичний маршрут. Плаваючі статичні маршрути це статичні маршрути, які використовуються для надання резервного шляху основного статичному маршруту або динамічному маршруту на випадок збою в роботі каналу. Плаваючий статичний маршрут використовується тільки тоді, коли основний маршрут недоступний. Для цієї мети плаваючий статичний маршрут налаштовується за більш високим значенням адміністративного відстані, ніж основний маршрут.

Адміністративна відстань визначає надійність маршруту. При наявності декількох шляхів до адреси призначення маршрутизатор вибирає шлях з найнижчим значенням адміністративного відстані.

Процес повторного пошуку маршрутизатором в таблиці маршрутизації перед пересиланням пакета відомий як рекурсивний пошук. Оскільки рекурсивний пошук витрачає ресурси маршрутизатора, рекомендується по можливості уникати його. Рекурсивний статичний маршрут є допустимим (може бути доданий в таблицю маршрутизації), тільки якщо зазначений наступний перехід безпосередньо чи опосередковано пов’язаний з допустимим вихідним інтерфейсом. Якщо для вихідного інтерфейсу встановлений параметр down (відключений), то статичний маршрут не буде доданий в таблицю маршрутизації.

Статичний маршрут за замовчуванням це маршрут, яким відповідають всі пакети. Замість зберігання маршрутизаторами маршрутів для всіх мереж в Інтернеті вони можуть зберігати один маршрут за замовчуванням, що представляє всі мережі, що не додані в таблицю маршрутизації.

Маршрутизатори зазвичай використовують маршрути за замовчуванням, налаштовані локально або отримані від іншого маршрутизатора за протоколом динамічної маршрутизації. Вони використовуються в тому випадку, коли жоден маршрут не відповідає IP-адресі призначення в таблиці маршрутизації. Іншими словами, при відсутності більш точних збігів в якості «шлюзу останньої надії» використовується маршрут за замовчуванням.

Статичні маршрути за замовчуванням зазвичай використовуються при підключенні прикордонного маршрутизатора до мережі Інтернет провайдера, маршрутизатора, для якого існує сусідній маршрутизатор тільки в вихідному напрямку та у випадку, якщо маршрутизатор не має інших сусідніх пристроїв і, отже, вважається тупиковим маршрутизатором.

Плаваючі статичні маршрути це статичні маршрути, адміністративна дистанція яких більше, ніж адміністративна дистанція інших статичних маршрутів або динамічних маршрутів. Подібні маршрути рекомендується

використовувати в якості резервного каналу для основного каналу. За замовчуванням статичні маршрути мають значення адміністративного відстані, що дорівнює 1, тому вони мають пріоритет перед маршрутами, отриманими від протоколів динамічної маршрутизації.

Адміністративну дистанцію статичного маршруту можна збільшити і, таким чином, зробити цей маршрут менш пріоритетним, ніж інший статичний маршрут або маршрут, отриманий через протокол динамічної маршрутизації.

Таким чином, статичний маршрут плаває і не використовується в той час, коли маршрут з більш короткою адміністративною відстанню працює. Однак, якщо кращий маршрут втрачений, плаваючий статичний маршрут може бути використаний, і трафік буде вставлений альтернативним маршрутом.

Дистанційні мережі являють собою мережі, доступ до яких можливий тільки шляхом пересилання пакета на інший маршрутизатор. Статичні маршрути легко налаштувати. Однак у великих мережах виконання таких операцій вручну може бути дуже трудомістким.

Статичні маршрути і раніше використовуються навіть в разі впровадження протоколу динамічної маршрутизації. Статичні маршрути можна налаштувати з використанням IP-адреси наступного переходу, який, як правило, є IP-адресою маршрутизатора наступного вузла.

Якщо використовується IP-адреса наступного переходу, процес таблиці маршрутизації повинен перетворити цю адресу в вихідний інтерфейс. На послідовних каналах з конфігурацією типу «точка-точка» краще налаштовувати статичний маршрут з вихідним інтерфейсом. У мережах множинного доступу, наприклад, Ethernet, можна одночасно налаштувати IP-адреса наступного переходу і вихідний інтерфейс на статичному маршруті. Адміністративне відстань за замовчуванням для статичних маршрутів дорівнює 1. Адміністративне відстань також застосовується для статичних маршрутів, налаштованих як з використанням адреси наступного переходу, так і з вихідним інтерфейсом.

Контрольні запитання

1. За яких умов маршрутизатор вважають тупиковим?
2. Де використовуються статичні маршрути?
3. Наведіть визначення маршруту за замовчуванням.
4. Наведіть типи статичних маршрутів IPv4 і IPv6.
5. Наведіть переваги та недоліки статичних маршрутів.
6. Що вам відомо про плаваючий статичний маршрут?
7. Який статичний маршрут називають рекурсивним?
8. Наведіть характеристики статичного маршруту за замовчуванням.
9. Які статичні маршрути називають плаваючими?
10. Які мережі вважать дистанційними?

10 DYNAMIC HOST CONFIGURATION PROTOCOL

10.1 Походження Dynamic host configuration protocol

Протокол «Dynamic host configuration protocol» (DHCP) створений на основі протоколу Bootstrap Protocol. Цей протокол був розроблений для того, щоб забезпечити можливість бездисковим робочим станціям завантажитися, отримати IP-адресу і підключити операційну систему до мережі.

Протокол DHCP значно досконаліший, ніж Bootstrap Protocol. З його допомогою адміністратор може конфігурувати параметри TCP/IP та встановлювати терміни оренди адрес. У протоколі DHCP передбачено динамічне виділення адрес. Іноді сервери DHCP конфігурують на підтримку клієнтів Bootstrap Protocol.

Протокол DHCP не орієнтований на певну операційну систему. Його можна використовувати з різними популярними операційними системами. Однак конкретні реалізації постачальників DHCP можуть дещо відрізнятись один від одного. Наприклад, сервери DHCP для Windows інтегровані з Active Directory. Це дозволяє адміністраторам запобігти виділенню IP-адрес несанкціонованими (так званими шулерськими) серверами DHCP.

10.2 Основні поняття Dynamic host configuration protocol

DHCP (протокол динамічної конфігурації вузла) – це мережний протокол, що дозволяє комп’ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP/IP.

Протокол DHCP є клієнт-серверним, тобто у його роботі беруть участь клієнт DHCP та сервер DHCP. Передача даних здійснюється за допомогою протоколу UDP, при цьому сервер приймає повідомлення від клієнтів і відправляє повідомлення клієнтам.

Під областю DHCP розуміється адміністративна група, що ідентифікує повні послідовні діапазони можливих IP-адрес для всіх DHCP-клієнтів у фізичній підмережі. Області визначають логічну підмережу, для якої повинні надаватися послуги DHCP, і дозволяють серверу задавати параметри

конфігурації, які видаються всім DHCP-клієнтам у підмережі. Область повинна бути визначена, перш ніж DHCP-клієнти зможуть використовувати DHCP-сервер для динамічної конфігурації TCP/IP.

Безліч областей, згрупованих в окремий адміністративний об'єкт, є суперобластю. Суперобласті корисні для вирішення різних завдань служби DHCP.

Якщо визначено область DHCP і задані діапазони виключення, то частина адрес, що залишилася, називається пулом доступних адрес (у межах області). Ці адреси можуть бути динамічно призначені клієнтам DHCP у мережі.

Діапазон виключення – обмежена послідовність IP-адрес у межах області, які мають бути виключені з надання службою DHCP.

Резервування дозволяє призначити клієнту постійну адресу та гарантувати, що вказаний пристрій у підмережі може завжди використовувати ту саму IP-адресу.

Під періодом оренди розуміється відрізок часу, протягом якого клієнтський комп'ютер може використовувати виділену IP-адресу. У момент закінчення половини терміну дії оренди клієнт повинен відновити оренду, звернувшись до сервера із повторним запитом. Слід пам'ятати про те, що тривалість періоду оренди впливає на частоту оновлення оренди.

Опції DHCP є додатковими параметрами налаштування клієнтів, які DHCP-сервер може призначати одночасно з виділенням IP-адреси. Сервер DHCP підтримує більше 30 опцій DHCP відповідно до RFC 2132. Як приклад опції DHCP можна навести такі параметри, як IP-адреси стандартного шлюзу, DNS-сервера, адреси серверів DNS, ім'я домену DNS тощо. Опції можуть бути визначені як для кожної області окремо, так і для всіх галузей, розміщених на DHCP-сервері. Крім стандартних опцій, описаних у специфікації протоколу DHCP, адміністратор може визначити власні опції.

Деякі постачальники програмного забезпечення можуть визначити власні, додаткові опції DHCP.

10.3 Призначення протоколу Dynamic host configuration protocol

Для кожного пристрою, підключеного до мережі, потрібна унікальна IP-адреса. Мережні адміністратори привласнюють статичні IP-адреси маршрутизаторам, серверам, принтерам та іншим мережевим пристроям, чиє фізичне і логічне розташування, швидше за все, не зміниться.

В більшості випадків йдеться про пристрої, що надають служби користувачам і пристроям в мережі. Таким чином, привласнюванні ними адреси мають бути постійними. Крім того, статичні адреси дозволяють адміністраторам управляти цими пристроями віддалено.

Мережним адміністраторам простіше дістати доступ до пристрою, якщо його IP-адресу легко визначити. Проте в організації часто змінюється фізичне і логічне місце розташування користувачів і комп'ютерів. Привласнення нових IP-адрес при кожному переміщенні співробітника може бути складним і трудомістким процесом.

При ручному налаштуванні параметрів мережі для співробітників, що працюють з віддалених місць, адміністратор також може зіткнутися з рядом труднощів. Крім того, привласнення IP-адрес вручну і налаштування іншої інформації про адресацію для комп'ютерів також вимагає зусиль і витрат часу системного адміністратора, особливо у разі розширення мережі.

Впровадження сервера з протоколом динамічної конфігурації вузла (DHCP) в локальну мережу спрощує процес привласнення IP-адрес як стаціонарним, так і мобільним пристроям.

Використання централізованого сервера DHCP дозволяє організації управляти привласненням усіх динамічних IP-адрес з одного сервера. Подібна практика робить управління IP-адресацією ефективнішою і забезпечує послідовність процесів і узгодженість даних по усій організації, включаючи філії.

Протокол DHCP доступний як для IPv4 (DHCPv4), так і IPv6 (DHCPv6). DHCPv4 привласнює IPv4-адреси та інші мережні параметри динамічно. Оскільки стаціонарні комп'ютери зазвичай складають основну частину

мережних вузлів, протокол DHCPv4 є украй корисним інструментом, що дозволяє мережним адміністраторам значно економити час.

Протокол DHCPv4 має три різні механізми призначення адреси, що забезпечують гнучкість при привласненні IP-адрес:

– ручний розподіл, при якому адміністратор привласнює клієнтові заздалегідь виділену IPv4-адресу, тоді як DHCPv4 тільки передає IPv4-адресу до пристрою

– автоматичний розподіл, при якому DHCPv4 автоматично привласнює пристрою постійну статичну IPv4-адресу, вибираючи його з пулу доступних адрес. При автоматичному розподілі відсутнє поняття оренди, і пристрою виділяється адреса на постійне використання;

– динамічний розподіл DHCPv4 привласнює або видає в оренду IPv4-адресу з пулу адрес на обмежений період часу за вибором сервера або до тих пір, поки у клієнта є необхідність в адресі.

Протокол DHCPv4 зазвичай використовує механізм динамічного розподілу. При використанні динамічного розподілу клієнти орендують дані від сервера на заданий адміністратором термін. Адміністратори настроюють сервери DHCPv4 так, щоб термін оренди збігав в різний час. Термін оренди зазвичай складає від 24-х годин до тижня або більше. Після закінчення терміну оренди клієнт повинен запросити іншу адресу, хоча в більшості випадків клієнтові повторно призначається та ж адреса.

10.4 Операція Dynamic host configuration protocol версії чотири

DHCPv4 працює згідно моделі клієнт-сервер. Коли клієнт підключається до сервера DHCPv4, сервер привласнює або здає йому в оренду IPv4-адресу. Клієнт з орендованою IP-адресою підключається до мережі до закінчення терміну оренди. Періодично клієнт повинен зв’язуватися з DHCP-сервером для продовження терміну оренди. Завдяки подібному механізму клієнти, що «переїхали» або відключилися, не займають адреси, яких вони більше не потребують.

Після закінчення терміну оренди сервер DHCP повертає адресу в пул, з якого адреса може бути повторно отримана при необхідності.

При початковому завантаженні клієнта (чи іншому способі підключення до мережі) починається чотири кроковий процес отримання адреси в оренду (рис. 10.1).

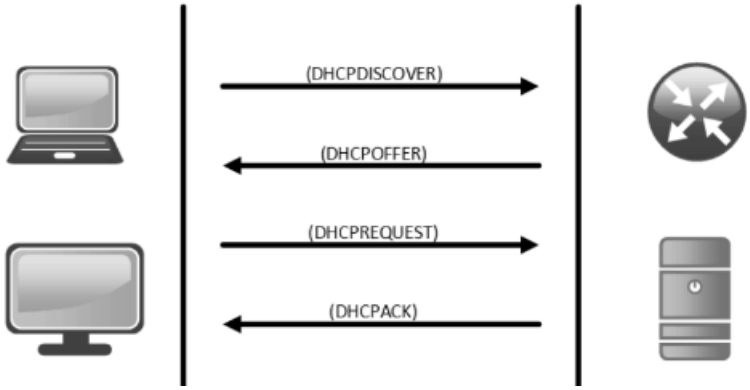

Рисунок 10.1 – Процес отримання адреси

Наведемо основні елементи процесу отримання адреси.

1. Виявлення DHCP (DHCPDISCOVER), коли повідомлення DHCPDISCOVER знаходиться в мережі DHCPv4-сервери. Оскільки під час завантаження у клієнта немає вірної IPv4 інформації, для зв’язку з сервером використовуються широкомовні адреси рівня 2 і рівня 3.

2. Пропозиція DHCP (DHCPOFFER), коли сервер DHCPv4 отримує повідомлення DHCPDISCOVER, він резервує доступні IPv4-адреси для видачі в оренду клієнтові. Сервер також створює запис ARP, що складається з MAC-адреси потребуючого клієнта і виданої клієнтові IPv4-адреси. DHCPv4-сервер посилає повідомлення прив’язки DHCPOFFER клієнтові, що потребує. Адресою джерела одно адресної розсилки повідомлення DHCPOFFER є MAC-адреса 2-го рівня 2-го сервера, адресою призначення – MAC-адреса 2-го рівня клієнта.

3. Запит DHCP (DHCPREQUEST): коли клієнт отримує від сервера повідомлення DHCPOFFER, він відправляє у відповідь повідомлення DHCPREQUEST. Це повідомлення використовується як для первинної оренди адреси, так і для її продовження. Коли повідомлення використовується при

первинній оренді, DHCPREQUEST служить повідомленням про прийняття пропозиції прив'язки до запропонованим сервером параметрам і непрямим відхиленням для усіх інших серверів, які могли надати клієнтові пропозицію прив'язки. У корпоративних мережах часто використовується декілька DHCPv4-серверів. Повідомлення DHCPREQUEST вирушає у формі широкомовної розсилки з метою інформування цього DHCPv4-сервера та інших DHCPv4-серверів про те, що пропозиція була прийнята.

4. Підтвердження DHCP (DHCPACK): при отриманні повідомлення DHCPREQUEST, сервер перевіряє, чи не використовується видавана в оренду IP-адреса за допомогою відправки запиту за протоколом ICMP на цю адресу. Після цього сервер створює новий запис ARP для клієнтської оренди і відповідає повідомленням одно адресної розсилки DHCPACK. Повідомлення DHCPACK є копією повідомлення DHCPOFFER, за винятком зміни в полі типу повідомлення. При отриманні повідомлення DHCPACK клієнт завантажує інформацію про конфігурацію і виконує ARP-перевірку присвоєної адреси. Якщо ARP-відповіді немає, значить, IPv4-адреса доступна, і клієнт починає використовувати її як власну адресу.

Продовження оренди та запит DHCP (DHCPREQUEST), коли оренда закінчується, клієнт посилає повідомлення DHCPREQUEST безпосередньо DHCPv4-серверу, який спочатку запропонував IPv4-адресу. Якщо повідомлення DHCPACK не отримане за певний період часу, клієнт відправляє інше повідомлення DHCPREQUEST широкомовною розсилкою, щоб інший DHCPv4-сервер міг продовжити термін оренди.

Підтвердження DHCP (DHCPACK): при отриманні повідомлення DHCPREQUEST сервер підтверджує інформацію про оренду повідомленням у відповідь DHCPACK.

У порівнянні з ручним присвоєнням IP-адрес служба DHCP має суттєві переваги. Адміністратору не потрібно витрачати час на ручну конфігурацію властивостей кожного комп'ютера. Робота мережі стає більш упорядкованою, тому що всі необхідні адреси постійно присвоєні і адміністратору не потрібно

стежити за тим, які адреси зайняті або вільні і чи не закінчується термін терміну оренди.

Послугами DHCP можна скористатися і в тому випадку, якщо комп'ютери повинні мати ту саму IP-адресу (часто це потрібно для серверів). Такі комп'ютери слід налаштувати на використання зарезервованої адреси. Клієнту, який замовив резервування, сервер DHCP завжди надає ту саму адресу. Резервування здійснюється на основі MAC-адреси клієнта (фізичної адреси).

Контрольні запитання

1. Для яких пристроїв застосовують статичні IP-адреси?
2. З чого складається запис ARP при реалізації протоколу DHCP?
3. Що називають протоколом ICMP?
4. У чому полягають основні переваги DHCP?
5. Надайте визначення DHCP.
6. Що розуміється під терміном область?
7. Які області називають суперобластями?
8. Що відносять до пулу адрес?
9. Які три способи розподілу ip адрес надає протокол DHCP?
10. В чому різниця IPv4 (DHCPv4) від IPv6 (DHCPv6)?

11 ТЕХНОЛОГІЯ «NETWORK ADDRESS TRANSLATION»

11.1 Актуальність використання технології

Усі публічні IPv4-адреси, що підключаються до Інтернету, мають бути занесені в Регіональний Інтернет реєстратор (RIR). Організації можуть орендувати публічні адреси у постачальника послуг, але тільки зареєстрований власник публічної Інтернет адреси може призначити цю адресу мережному пристрою. Теоретично, максимально допустима кількість IPv4-адрес складає 4,3 мільярда, що строго обмежує адресний простір IPv4. Коли в 1981 році Боб Кан (Bob Kahn) і Вінт Серф (Vint Cerf) розробили пакет протоколів TCP/IP, включаючи IPv4, вони не мали уявлення про те, на що перетвориться Інтернет. З поширенням персональних комп'ютерів і настанням ери Всесвітньої мережі стало очевидно, що 4,3 мільярда IPv4-адрес буде недостатньо.

Поява протоколу IPv6 стала довгостроковим рішенням, проте разом з цим знадобилися швидші способи усунення проблеми вичерпання адресного простору. IETF розробила ряд короткострокових рішень, у тому числі перетворення мережних адрес (NAT) і приватні IPv4-адреси відповідно до RFC 1918.

Кількості публічних IPv4-адрес недостатньо, щоб призначити унікальні адреси усім пристроям, підключеним до Інтернету. В більшості випадків, мережі реалізуються з використанням приватних IPv4-адрес відповідно до RFC 1918.

Ці приватні адреси використовуються у рамках організації або об'єкту з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію або організацію, приватні IPv4-адреси не можна використовувати для маршрутизації через Інтернет. Для того, щоб дозволити пристрою з приватною IPv4-адресою доступ до пристроїв і ресурсів поза локальною мережею, приватну адресу спочатку необхідно перетворити в публічну адресу. NAT забезпечує перетворення приватних адрес в публічні адреси. Це дозволяє пристрою з приватною IPv4-адресою діставати доступ до ресурсів поза своєю приватною мережею, включаючи ресурси,

знайдені в Інтернеті. У поєднанні з приватними IPv4-адресами, NAT продемонстрував свою доцільність відносно економії публічних IPv4-адрес. Одна публічна IPv4-адреса може спільно використовуватися сотнями, навіть тисячами пристроїв, для кожного з яких налагоджена унікальна приватна IPv4-адреса.

Без використання NAT адресний простір IPv4 був би вичерпаний задовго до настання 2000 року. Незважаючи на свої переваги, NAT має ряд обмежень. Вирішенням проблеми вичерпання простору IPv4-адрес і обмежень NAT є остаточний перехід на IPv6.

Перетворення мережних адрес NAT використовується в різних цілях, проте основним завданням цього механізму є збереження публічних IPv4-адрес. Це досягається шляхом дозволу мережам використовувати приватні IPv4-адреси для внутрішньої взаємодії і перетворення їх в публічні адреси тільки у разі потреби.

Додаткова перевага NAT полягає у підвищенні міри конфіденційності і безпеки мережі і пояснюється тим, що цей механізм приховує внутрішні IPv4-адреси від зовнішніх мереж. Для маршрутизатора з підтримкою NAT можна налаштувати одну або декілька діючих публічних IPv4-адрес. Ці публічні адреси відомі як пул адрес NAT. Коли внутрішній пристрій відправляє трафік за межі мережі, маршрутизатор з підтримкою NAT перетворює внутрішню IPv4-адресу пристрою в публічну адресу з пулу NAT.

Зовнішнім пристроям здається, що увесь трафік, що входить в мережу і виходить з неї, використовує публічні IPv4-адреси з наданого пулу адрес. Маршрутизатор NAT зазвичай працює на межі тупикової мережі. Тупикова мережа це мережа, що використовує єдине з’єднання з сусідньою мережею, один вхідний маршрут і один вихідний маршрут.

Коли пристрою в тупиковій мережі потрібне з’єднання з пристроєм поза його мережею, пакет пересилається пограничному маршрутизатору. Пограничний маршрутизатор виконує процес NAT, перетворюючи внутрішню приватну адресу пристрою в публічну, зовнішню адресу, яка маршрутизується.

11.2 Термінологія

У термінології NAT під внутрішньою мережею мається на увазі набір мереж, задіяних у перетворенні. Зовнішня мережа відноситься до усіх інших мереж.

При використанні NAT, IPv4-адреси представляють різні точки призначення залежно від того, чи знаходяться вони в приватній або в публічній мережі (Інтернет), а також від того, чи є трафік вхідним або вихідним.

У NAT передбачено 4 типи адрес:

– внутрішня локальна адреса;

– внутрішня глобальна адреса;

– зовнішня локальна адреса;

– зовнішня глобальна адреса.

При визначенні типу адреси важливо пам’ятати, що термінологія NAT завжди застосовується з точки зору пристрою з перетворюваною адресою.

Внутрішня адреса – це адреса пристрою, що перетворюється механізмом NAT.

Зовнішня адреса – це адреса пристрою призначення.

У рамках NAT по відношенню до адрес також використовується поняття локальності або глобальності.

Локальна адреса – це довільна адреса, що з’являється у внутрішній частині мережі.

Глобальна адреса – це довільна адреса, що з’являється в зовнішній частині мережі.

Внутрішня локальна адреса – це адреса джерела, видима з внутрішньої мережі.

Внутрішня глобальна адреса – це адреса джерела, видима із зовнішньої мережі.

Зовнішня глобальна адреса – це адреса призначення, видима із зовнішньої мережі.

Зовнішня локальна адреса – це адреса призначення, видима з внутрішньої мережі.

11.3 Механізми перетворення мережних адрес

Існують три механізми перетворення мережних адрес:

1. Статичне перетворення мережних адрес (статичний NAT) це взаємно однозначна відповідність між локальним і глобальним адресами.

2. Динамічне перетворення мережних адрес (динамічний NAT) це зіставлення адрес за схемою «багато до багатьох» між локальними і глобальними адресами.

3. Перетворення адрес портів (PAT) це зіставлення адрес за схемою багато до одного між локальними і глобальним адресами. Цей метод також називається NAT з перевантаженням.

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою один в один. Ці відповідності задаються адміністратором мережі і залишаються незмінними. Метод статичного перетворення мережних адрес особливо корисний для веб-серверів або пристроїв, які повинні мати постійну адресу, доступну з Інтернету, наприклад, для веб-сервера компанії.

Статичний NAT також підходить для пристроїв, які мають бути доступні авторизованому персоналу, що працює поза офісом, але при цьому залишатися закритими для загального доступу через Інтернет. Наприклад, мережний адміністратор може з ПК підключитися за допомогою SSH до внутрішньої глобальної адреси 209.165.200.226. Маршрутизатор перетворить цю внутрішню глобальну адресу у внутрішню локальну адресу і підключає сеанс адміністратора до 209.165.200.226. Для статичного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

Метод динамічного перетворення мережних адрес (динамічний NAT) використовує пул публічних адрес, які привласнюються у порядку живої черги.

Коли внутрішній пристрій просить доступ до зовнішньої мережі, динамічний NAT привласнює доступну публічну IPv4-адресу з пулу.

Перетворення адрес портів (PAT) зіставляє багато приватних IPv4-адрес одній або декільком публічним IPv4-адресам. Саме цей метод реалізується більшістю домашніх маршрутизаторів. Інтернет провайдер призначає маршрутизатору одну адресу, але декілька членів сім'ї можуть одночасно діставати доступ в Інтернет.

NAT з навантаженням це найбільш поширений метод перетворення мережних адрес. За допомогою цього методу багато адрес можуть бути зіставлені одному або декільком адресам, оскільки кожна приватна адреса також відстежуються за номером порту.

Якщо пристрій починає сеанс TCP/IP, він створює значення порту TCP або UDP для джерела, щоб унікальним чином визначити сеанс. Коли маршрутизатор NAT отримує пакет від клієнта, він використовує свій номер порту джерела, щоб унікальним чином визначити конкретне перетворення NAT.

PAT гарантує, що пристрої використовуватимуть різні номери портів TCP для кожного сеансу взаємодії з сервером в Інтернеті. При поверненні відповіді від сервера номер порту джерела, яке стає номером порту призначення при зворотній передачі, визначає, якому пристрою маршрутизатор перешле відповідні пакети. Процес PAT також переконується в тому, що вхідні пакети дійсно були запрошені, підвищуючи таким чином міру безпеки сеансу.

11.4 Порівняння технологій «Network Address Translation» та «Port Address Translation»

NAT перетворює IPv4-адреси, виходячи з схеми один до одного для приватних IPv4-адрес і публічних IPv4-адрес. В той же час, PAT міняє і адресу, і номер порту. NAT пересилає вхідні пакети за їх внутрішнім призначенням, використовуючи IPv4-адресу вхідного джерела, надану вузлом в публічній

мережі. При використанні PAT зазвичай задіюється тільки одна або невелика кількість публічно представлених IPv4-адрес.

Вхідні пакети з публічної мережі спрямовуються адресатам в приватній мережі за допомогою таблиці маршрутизатора NAT. Ця таблиця відстежує пари публічних і приватних портів, що називається відстежуванням з'єднань. Що ж відбувається з пакетами IPv4, що передають дані, що не є сегментом TCP або UDP? Ці пакети не містять номера порту 4-го рівня. PAT перетворить більшість основних протоколів, що передаються за допомогою IPv4 і що не використовують TCP або UDP, в протокол транспортного рівня. Найпоширенішим серед таких протоколів є протокол ICMPv4.

11.5 Переваги і недоліки

NAT забезпечує багато переваг, у тому числі:

– зберігає офіційно зареєстровану схему адресації, дозволяючи приватне використання внутрішніх мереж;

– економить адреси завдяки мультиплексуванню застосувань на рівні портів;

– при використанні NAT з перевантаженням внутрішні вузли можуть використовувати для усіх зовнішніх взаємодій одну публічну IPv4-адресу. При цьому типі конфігурації для підтримки багатьох внутрішніх вузлів потрібна невелика кількість зовнішніх адрес;

– підвищує гнучкість підключень до публічної мережі. Для забезпечення надійних підключень до публічної мережі можна створити множинні пули, резервні пули і пули розподілу навантаження;

– забезпечує узгодженість схем внутрішньої мережної адресації. Якщо в мережі не використовуються приватні IPv4-адреси і NAT, зміна схеми публічних IPv4-адрес зажадає зміни адрес усіх вузлів існуючої мережі. Витрати на зміну адресації вузлів можуть виявитися істотними;

– дозволяє зберегти існуючу схему приватних IPv4-адрес, одночасно підтримуючи простий перехід на нову схему публічної адресації. Це означає,

що організація може змінити Інтернет провайдера, не міняючи налаштувань своїх внутрішніх клієнтів;

– забезпечує безпеку мережі. Оскільки приватні мережі не оголошують ні свої адреси, ні внутрішню топологію, вони залишаються достатньо захищеними при використанні NAT для діставання керованого зовнішнього доступу. Проте, NAT не замінює міжмережні екрани.

Перетворення мережних адрес має ряд недоліків. Той факт, що вузли в Інтернеті взаємодіють безпосередньо з пристроєм, що підтримує NAT, а не з фактичним вузлом приватної мережі, створює ряд проблем.

Один з недоліків використання NAT пов'язаний з продуктивністю мережі, особливо це стосується протоколів реального часу. NAT збільшує затримки комутації, оскільки перетворення кожної IPv4-адреси в заголовках пакетів вимагає часу.

Комутація першого пакету є програмним процесом. Цей пакет завжди проходить повільнішим шляхом. Маршрутизатор повинен аналізувати кожен пакет, щоб вирішити, чи потрібно його перетворювати. Маршрутизатор повинен змінити заголовок IPv4 і, по можливості, змінити заголовок TCP або UDP. При кожному перетворенні має бути перерахована контрольна сума заголовка IPv4, а також контрольна сума TCP або UDP.

Якщо в кеші є відповідний запис, інші пакети проходять по дорозі зі швидкою комутацією. Інакше вони теж затримуються. Іншим недоліком використання NAT є втрата наскрізної адресації. Багато Інтернет протоколів і застосувань залежать від наскрізної адресації від джерела до вузла призначення. Деякі застосування не сумісні з NAT. Наприклад, деякі застосування безпеки, такі як електронні підписи, не працюють з NAT, оскільки IPv4-адреса джерела змінюється, перш ніж пакет встигає досягти вузла призначення. Додатки, що використовують фізичні адреси замість доменних імен, не можуть досягти вузлів призначення, при проходженні через маршрутизатор, що використовує NAT. В деяких випадках цієї проблеми можна уникнути за допомогою статичних зіставлень NAT. Крім того,

втрачається можливість трасування наскрізного з’єднання IPv4. Дуже сильно ускладнюється трасування пакетів, що піддаються численним змінам адреси пакету при проходженні декількох ділянок NAT, що, у свою чергу, ускладнює усунення неполадок. Використання NAT також ускладнює протоколи туннелювання, оскільки NAT змінює значення в заголовках, що заважає перевіркам цілісності, що виконує протокол туннелювання.

11.6 Налаштування статичного і динамічного Network address translation

Статичне перетворення мережних адрес NAT це взаємне зіставлення внутрішньої і зовнішньої адрес. Статичний NAT дозволяє зовнішнім пристроям ініціювати підключення до внутрішніх пристроїв за допомогою статично призначеної публічної адреси. Наприклад, внутрішньому веб-серверу може бути зіставлена внутрішня глобальна адреса, визначена так, щоб він був доступний із зовнішніх мереж.

Налаштування статичного NAT зв’язане з двома основними завданнями, а саме створення відповідності між внутрішньою локальною і внутрішньою глобальною адресами та після налаштування відповідності інтерфейси, що беруть участь у перетворенні, налаштовуються як внутрішні або зовнішні відносно NAT.

Статичне перетворення NAT забезпечує постійну відповідність між внутрішньою локальною і внутрішньою глобальною адресою, динамічне перетворення NAT підтримує автоматичне зіставлення внутрішніх локальних адрес внутрішнім глобальним адресам.

Ці внутрішні глобальні адреси зазвичай являються публічними IPv4-адресами.

Динамічний NAT використовує для перетворення групу або пул публічних IPv4-адрес. Для динамічного NAT, як і для статичного NAT, потрібне налаштування внутрішнього і зовнішнього інтерфейсів, що беруть участь в перетворенні NAT.

Проте, якщо статичне перетворення NAT створює постійне зіставлення з однією адресою, для динамічного NAT використовується пул адрес.

Перетворення між публічними і приватними IPv4-адресами є найпоширенішим застосуванням NAT. Проте, перетворення NAT можуть виникати між будь-якими парами адрес. Пул публічних IPv4-адрес (пул внутрішніх глобальних адрес) доступний довільному пристрою у внутрішній мережі за принципом «першим прийшов і першим обслужили». При динамічному перетворенні NAT одна внутрішня адреса перетвориться в одну зовнішню адресу. Для цього типу перетворення в пулі має бути досить адрес, щоб охопити усі внутрішні пристрої, яким одночасно потрібен доступ до зовнішньої мережі.

Якщо використані усі адреси пулу, пристрій повинен дочекатися доступної адреси, щоб дістати доступ до зовнішньої мережі.

11.7 Налаштування та перевірка

Перетворення адрес портів PAT (NAT з перевантаженням) економить адреси у внутрішньому глобальному пулі, дозволяючи маршрутизатору використовувати одну внутрішню глобальну адресу для декількох внутрішніх локальних адрес. Іншими словами, одна публічна IPv4-адреса може використовуватися для сотень або навіть тисяч внутрішніх IPv4-приватних адрес. Якщо налагоджений цей тип перетворення, маршрутизатор зберігає достатній об’єм інформації протоколів вищих рівнів, наприклад, номери портів TCP або UDP, для зворотного перетворення внутрішньої глобальної адреси в потрібну внутрішню локальну адресу.

При прив’язці декількох внутрішніх локальних адрес до однієї внутрішньої глобальної адреси для розрізнення локальних адрес використовуються номери портів TCP або UDP. Сумарне число внутрішніх адрес, які можуть бути перетворені в одну зовнішню адресу, теоретично може досягати 65536 на одну IP-адресу. Але число внутрішніх адрес, яким можна призначити одну IP-адресу, приблизно складає 4000.

Залежно від того, яким чином Інтернет провайдер виділяє публічні IPv4-адреси, існує два способи налаштування PAT. У першому випадку Інтернет провайдер виділяє організації декілька публічних IPv4-адрес, а в другому випадку виділяється єдина публічна IPv4-адреса, необхідна організації для підключення до мережі Інтернет провайдера. Якщо об'єкту було виділено декілька публічних IPv4-адрес, то ці адреси можуть бути частиною пулу, що використовує PAT. Це аналогічно динамічному NAT, за винятком того, що публічних адрес недостатньо для створення взаємно однозначних відповідностей внутрішніх і зовнішніх адрес.

Невеликий пул адрес спільно використовується великим числом пристроїв. Якщо доступна тільки одна публічна IPv4-адреса, для конфігурації з перевантаженням зазвичай призначається публічна адреса зовнішнього інтерфейсу, яка підключається до Інтернет провайдера. Усі внутрішні адреси в пакетах, що виходять із зовнішнього інтерфейсу, перетворяться в одну IPv4-адресу.

Процес перетворення NAT з перевантаженням є однаковим, як при використанні пулу адрес, так і при використанні однієї адреси. Для перевірки PAT використовуються ті ж команди, що і для перевірки статичного і динамічного NAT.

Переадресація портів (тунелювання) це переадресація мережного порту від одного вузла мережі на інший вузол. Цей метод дозволяє зовнішнім користувачам зовні досягати порту для приватної IPv4-адреси (у локальній мережі), використовуючи маршрутизатор з підтримкою NAT.

Як правило, для роботи однорангових програм обміну файлами і виконання таких операцій, як веб-обслуговування і вихідний FTP, вимагається, щоб порти маршрутизатора були переадресовані або відкриті. Оскільки NAT приховує внутрішні адреси, однорангові застосування працюють тільки зсередини. В цьому випадку NAT може зіставити вихідні запити і вхідні відповіді.

Проблема полягає в тому, що NAT не дозволяє ініціювати запити зовні. Цю ситуацію можна вирішити за допомогою змін, внесених вручну. Можна налаштувати переадресацію портів, щоб визначити конкретні порти, які можуть бути переадресовані на внутрішні вузли. Інтернет додатки працюють з користувацькими портами, які мають бути відкриті або доступні цим застосуванням.

Різні застосування використовують різні порти. Це дозволяє додаткам і маршрутизаторам визначати мережні сервіси.

Переадресація портів дозволяє користувачам досягати внутрішніх серверів з Інтернету, використовуючи адресу WAN-порту маршрутизатора і відповідний номер зовнішнього порту. Внутрішні сервери зазвичай налаштовуються з використанням приватних IPv4-адрес RFC 1918. Коли запит вирушає за IPv4-адресою WAN-порта через Інтернет, маршрутизатор переадресує запит відповідному серверу в локальній мережі. З міркувань безпеки широкосмугові маршрутизатори за замовчуванням не дозволяють переадресацію зовнішніх веб-запитів вузлам внутрішньої мережі.

Реалізація переадресації портів за допомогою команд IOS аналогічна застосуванню команд налаштування статичного NAT. Переадресація портів фактично є статичним перетворенням NAT із заданим номером порту TCP або UDP. Як і для інших типів NAT, для переадресації портів необхідно налаштувати як внутрішній, так і зовнішній інтерфейси NAT.

З початку 1990-х років пріоритетним завданням для IETF стало вирішення проблеми вичерпання адресного простору IPv4. Поєднання приватних IPv4-адрес RFC 1918 і NAT стало інструментом, спрямованим на уповільнення процесу вичерпання. NAT має помітні недоліки, і в січні 2011 було виділено для регіональних Інтернет реєстраторів останні IPv4-адреси. Однією з «ненавмисних» переваг NAT для IPv4 стало те, що ця технологія приховує приватні мережі від публічного Інтернету. Перевагою NAT є забезпечення очевидного рівня безпеки шляхом заборони комп’ютерам з публічного Інтернету доступу до внутрішніх вузлів. Але цю технологію не

можна вважати заміною правильної мережної безпеки, наприклад, як це забезпечує між мережний екран.

Протокол IPv6 з 128-бітовою адресою надає 340 ундециліонів адрес. Таким чином, адресний простір не є проблемою. Протокол IPv6 був розроблений, щоб усунути необхідність в NAT для IPv4 з його перетворенням між публічними і приватними IPv4-адресами. Проте, IPv6 дійсно реалізує певну форму NAT. IPv6 включає і власний простір приватних IPv6-адрес, і перетворення NAT, реалізовані інакше, ніж для IPv4.

Унікальні локальні IPv6-адреси схожі на приватні адреси RFC 1918 в IPv4, але при цьому істотно відрізняються від них. Мета унікальних локальних адрес – забезпечити простір IPv6-адрес для взаємодії в межах локального об'єкту. Це не означає ні надання додаткового простору IPv6-адрес, ні забезпечення рівня безпеки.

Унікальна локальна адреса використовує префікс FC00::/7, і тому перший гекстет знаходиться в діапазоні від FC00 до FDFF. Якщо префікс призначається локально, наступний 1 біт встановлений рівним 1. Сенс значення 0 буде визначений пізніше.

Наступні 40 бітів це глобальний ідентифікатор, за яким йде 16-бітовий ідентифікатор підмережі. Ці перші 64 біта об'єднуються для створення префікса унікальної локальної адреси. Це залишає 64 біта для ідентифікатора інтерфейсу або, згідно термінології IPv4 – вузлової частини адреси.

Унікальні локальні адреси визначені в RFC 4193. Унікальні локальні адреси також називаються локальними IPv6-адресами (не слід плутати з локальними IPv6-адресами типу link – local) і мають ряд характеристик:

– можливість об'єднувати або приватно сполучати об'єкти, без яких-небудь конфліктів адрес або необхідності в зміні нумерації інтерфейсів, що використовують ці префікси;

– незалежність від Інтернет провайдера і можливість застосування з метою взаємодії усередині об'єкту без необхідності в підключенні до Інтернету;

– неможливість маршрутизації через Інтернет, проте при випадковому «витіку» через маршрутизацію або DNS конфлікт з іншими адресами відсутній.

Унікальні локальні адреси не настільки прості, як адреси RFC 1918. На відміну від приватних IPv4-адрес, IETF не прагнула використовувати різновид NAT для перетворення між унікальними локальними адресами і глобальними індивідуальними адресами IPv6. Реалізація і потенційні сфери застосування унікальних локальних IPv6-адрес все ще вивчається Інтернет співтовариством. Наприклад, IETF аналізує можливість створення префікса унікальних локальних адрес локально, використовуючи FC00::/8, або призначення його автоматично сторонньою організацією, починаючи з FD00::/8. NAT для IPv6 використовується в зовсім іншому контексті, ніж NAT для IPv4.

Різноманітні варіанти NAT для IPv6 використовуються з метою надання прозорого доступу між мережами, в яких використовується тільки протокол IPv6, і мережами, в яких використовується тільки протокол IPv4. NAT для IPv6 не застосовується для перетворення приватних IPv6-адрес в глобальні IPv6-адреси.

В ідеалі, IPv6 повинен по можливості використовуватися в початковому форматі. Це означає, що пристрої IPv6 взаємодіють один з одним по мережах IPv6. IETF розробила декілька методів переходу для різних сценаріїв переходу від IPv4 до IPv6, включаючи використання подвійного стека, тунелювання і перетворення.

Подвійний стек застосовується, коли пристрої використовують протоколи, пов’язані як з IPv4, так і з IPv6.

Тунелювання для IPV6 це процес інкапсуляції пакетів IPv6 в пакети IPv4. Цей метод дозволяє передавати пакет IPv6 по мережі, в якій використовується тільки протокол IPv4. NAT для IPv6 слід використовувати не як довгострокову стратегію, а як тимчасовий механізм, що допомагає перейти з IPv4 на IPv6. З часом з’явилося декілька типів NAT для IPv6, включаючи NAT – PT (Network Address Translation – Protocol Translation, перетворення мережних адрес –

перетворення протоколів). IETF визнала технологію NAT – PT застарілою і порекомендувала використовувати її заміну – NAT64 [8, с. 125].

Контрольні запитання

1. Чому виникла необхідність використання технології NAT?
2. Яка термінологія використовується в технології NAT?
3. Які ви знаєте механізми перетворення мережних адрес?
4. У чому полягають відмінності технологій NAT і PAT?
5. Які переваги і недоліки NAT?
6. Які особливості налаштування статичного NAT?
7. Як відбувається налаштування і перевірка динамічного NAT?
8. Як відбувається налаштування та перевірка PAT?
9. У чому полягає процес тунелювання для IPV6?

12 ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL ТА НАЛАШТУВАННЯ OPEN SHORTEST PATH FIRST МАРШРУТИЗАЦІЇ

12.1 Основні характеристики та опис роботи Enhanced interior gateway routing protocol

Enhanced interior gateway routing protocol (EIGRP) це удосконалений дистанційно – векторний протокол динамічної маршрутизації, розроблений компанією Cisco.

Основні характеристики EIGRP:

– швидка збіжність (порівняно з іншими дистанційно – векторними протоколами);

– підтримка VLSM;

– часткові оновлення;

– підтримка різних протоколів мережного рівня;

– однакові налаштування протоколу під час використання різних протоколів канального рівня (наприклад, у OSPF налаштування відрізняються для Ethernet і Frame Relay);

– складна метрика;

– використання multicast адрес (224.0.0.10) та unicast адрес, замість широкомовної розсилки.

RTP керує процесом надсилання та отримання пакетів EIGRP.

RTP забезпечує:

– гарантовану доставка пакетів. Для цього використовується пропрієтарний алгоритм Cisco, reliable multicast. Пакети надсилаються на multicast-адресу 224.0.0.10. Кожен сусід, який отримав такий пакет, відправляє підтвердження відправнику пакета;

– збереження порядку пакетів. У кожному пакеті використовують два номери послідовності (sequence). Кожен пакет включає номер присвоєний йому відправником. Цей номер збільшується на одиницю кожного разу, коли

маршрутизатор надсилає новий пакет. Крім того, відправник поміщає пакет останнього отриманого пакета від одержувача;

– у деяких випадках RTP використовує негарантовану доставку. У таких пакетах не проставляються номери послідовностей і вони не вимагають підтвердження отримання.

Всі повідомлення EIGRP інкапсулюються в IP-пакети, номер EIGRP у полі protocol IP-пакета – 88.

EIGRP використовує 5 типів повідомлень:

– hello, коли маршрутизатори використовують hello-пакети для виявлення сусідів. Пакети надсилаються multicast і не вимагають підтвердження отримання;

– update містить інформацію про зміну маршрутів. Вони надсилаються лише маршрутизаторам, яких стосується оновлення. Ці пакети можуть бути надіслані до конкретного маршрутизатора (unicast) або групи маршрутизаторів (multicast). Отримання update пакета підтверджується відправкою ack;

– query, коли маршрутизатор виконує підрахунок маршруту і в нього немає feasible successor, він відправляє query-пакет своїм сусідам для того щоб визначити чи немає feasible successor для цього destination у них. Зазвичай query-пакети відправляються multicast, але можуть бути й unicast. Отримання query-пакета підтверджується надсиланням ack одержувачем пакета;

– reply, коли маршрутизатор відправляє reply-пакет у відповідь query-пакет. Reply-пакети відправляються unicast тому, хто надіслав query-пакет. Отримання reply-пакета підтверджується надсиланням ack;

– ack це пакет, який підтверджує отримання пакетів update, query, reply. ack-пакети відправляються unicast і містять у собі acknowledgment number. Фактично це hello-пакети, які не передають даних. Використовується негарантована доставка.

Для встановлення відносин сусідства EIGRP використовує пакети hello:

– на ethernet-інтерфейсах та point-to-point інтерфейсах hello-пакети за замовчуванням відправляються кожні 5 секунд, але з невеликим випадковим відхиленням, яке використовується для того, щоб між маршрутизаторами не було синхронізації у відправленні hello-пакетів;

– на multipoint X.25, Frame Relay, та ATM інтерфейсах hello-пакети відправляються unicast за замовчуванням кожні 60 секунд;

– якщо сусід не надсилає hello-повідомлення протягом hold time (за умовчанням 15 секунд, 3 hello-інтервали), то він вважається недоступним.

Для того, щоб маршрутизатори стали сусідами, повинні виконуватися такі умови:

– маршрутизатори повинні пройти аутентифікації;

– маршрутизатори повинні бути в одній операційній системі;

– відносини сусідства повинні встановлюватися на primary-адресах (коли приходить hello-пакет, маршрутизатор перевіряє, чи належить адреса відправника мережі на primary-адресі інтерфейсу);

– повинні збігатися значення K-коефіцієнтів.

Для того, щоб маршрутизатори стали EIGRP-сусідами, у них не зобов’язані збігатися Hello і Hold time. Маршрутизатор використовує значення таймерів, отримані від сусіда.

Якщо на одному з маршрутизаторів змінено Hello або Hold time, сусіди цього маршрутизатора будуть використовувати ці значення. Щоб сам маршрутизатор використовував інші значення, необхідно змінити таймер на відповідному інтерфейсі сусіда. Інформація про всіх виявлених сусідів міститься у таблиці сусідів.

Таблиця сусідів (neighbor table) – список безпосередньо приєднаних маршрутизаторів (на яких працює EIGRP), з якими маршрутизатор встановив відносини сусідства.

EIGRP може анонсувати мережі secondary-адрес, але hello-пакети відправляються з primary-адреси. Після того, як маршрутизатори стали

сусідами, вони починають обмінюватись оновленнями (Update). Ці пакети можуть бути надіслані до конкретного маршрутизатора (unicast) або групи маршрутизаторів (multicast).

Процес обміну оновленнями:

– спочатку відправляються повні оновлення, до яких включені всі маршрути, за винятком тих, які підпадають під правило split horizon;

– після того, як обмін маршрутами завершився, оновлення не надсилаються;

– надалі оновлення відправляються, якщо змінився один чи більше маршрутів;

– якщо відносини сусідства розриваються, та був відновлюються, то відправляються повні оновлення.

Оновлення EIGRP:

– неперіодичні (Nonperiodic) – оновлення відправляються не через регулярні інтервали часу, а за зміни топології чи метрики;

– часткові (Partial), коли в оновленнях передається не вся інформація з таблиці маршрутизації, а лише зміни;

– обмежені (Bounded), коли оновлення надсилаються лише задіяним маршрутизаторам.

Diffusing Update Algorithm – логіка, яку використовує EIGRP для обчислення нових маршрутів.

Наведемо основні визначення:

1. Advertised distance (AD), відома також як reported distance (RD) – вартість відстані між сусіднім маршрутизатором, який анонсує маршрут, та мережею призначення.

2. Feasible distance (FD) – вартість відстані від локального маршрутизатора до мережі призначення дорівнює AD, яке анонсує сусідній маршрутизатор плюс вартість відстані між локальним маршрутизатором та сусіднім маршрутизатором.

3. Successor – сусідній маршрутизатор із шляхом без петель та з найменшою вартістю шляху до мережі призначення.

4. Feasible successor – резервний маршрутизатор за допомогою без петель (AD feasible successor має бути меншим ніж FD поточного маршруту successor).

5. Feasible condition – AD feasible successor має бути менше, ніж FD поточного маршруту successor.

12.2 Характеристики протоколу «Open shortest path first»

Протокол OSPF є протоколом маршрутизації за станом каналу, розробленим як заміна дистанційно – векторному протоколу (RIP). Протокол RIP був прийнятним протоколом маршрутизації на початкових етапах розвитку мережних технологій і Інтернету.

Проте використання протоколом RIP числа переходів як єдиної метрики для визначення оптимального маршруту незабаром привело до ряду труднощів. При використанні цього методу можливості масштабування великих мереж, що містять декілька шляхів з різними швидкостями, обмежені.

Протокол OSPF має ряд значних переваг порівняно з протоколом RIP, забезпечуючи швидшу збіжність і можливість масштабування в цілях реалізації мереж більшого розміру.

Протокол OSPF є безкласовим протоколом маршрутизації, що використовує концепцію розподілу на області в цілях масштабованості. Розробку OSPF в 1987 році почала робоча група OSPF у складі Інженерної групи по розвитку Інтернету (IETF). У той час Інтернет в основному використовувався в учбових закладах і дослідницьких центрах і фінансувався урядом США. У 1989 році специфікація протоколу OSPFv1 була опублікована в запиті для коментарів (RFC) 1131.

Було розроблено дві реалізації. Одна з них була розроблена для роботи з маршрутизаторами, а друга – з робочими станціями під управлінням UNIX. Друга реалізація перетворилася на поширений сервіс UNIX, відомий як

GATED. OSPFv1 був експериментальним протоколом маршрутизації, і його розгортання не виконувалося.

У 1991 році Джон Мой представив протокол OSPFv2. Протокол OSPFv2 пропонував істотні технічні переваги порівняно з протоколом OSPFv1. В той же час, коли був представлений протокол OSPF, робоча група ISO розробляла власний протокол маршрутизації за станом каналу – протоколу маршрутизації проміжних систем (IS-IS).

Інженерна група по розвитку Інтернету (IETF) вибрала протокол OSPF в якості рекомендованого протоколу внутрішньої маршрутизації.

У 1998 році специфікація протоколу OSPFv2 була оновлена в запиті для коментарів (RFC) 2328, який до теперішнього часу залишається актуальним RFC для протоколу OSPF. У 1999 році протокол OSPFv3 для IPv6 був опублікований в RFC 2740.

У 2008 році протокол OSPFv3 був оновлений в запиті для коментарів (RFC) 5340 як протокол OSPF для IPv6.

Протокол OSPF має наступні властивості:

1. Безкласовість, тобто протокол розроблений як безкласовий, отже, він підтримує використання VLSM і маршрутизації CIDR.

2. Ефективність, тобто зміни маршрутизації запускають оновлення маршрутизації (без регулярних оновлень). Протокол використовує алгоритм пошуку найкоротшого шляху SPF для вибору оптимального шляху.

3. Швидка збіжність – швидка трансляція змін мережі.

4. Масштабованість, яка підходить для використання, як в невеликих, так і у великих мережах. Для підтримки ієрархічної структури маршрутизатори можна згрупувати в області.

5. Безпека, яка підтримує аутентифікацію Message Digest 5 (MD5). Якщо ця функція включена, маршрутизатори OSPF приймають лише зашифровані повідомлення маршрутизації від рівноправних вузлів з однаковим заздалегідь заданим паролем.

Адміністративна дистанція (AD) є значенням надійності джерела маршруту.

12.3 Принцип роботи протоколу «Open shortest path first»

Усі протоколи маршрутизації використовують аналогічні компоненти. Усі протоколи використовують повідомлення протоколу маршрутизації для обміну даними маршрутизації. Повідомлення дозволяють вибудовувати структури даних, які згодом обробляються за допомогою алгоритму маршрутизації.

Протокол OSPF створює і обслуговує три БД:

1. БД суміжності – створює таблицю сусідніх пристроїв.
2. БД про стан каналів (LSDB, link state database) створює таблицю топології.
3. БД пересилки створює таблицю маршрутизації.

Ці таблиці містять список сусідніх маршрутизаторів, між якими виконується обмін даними маршрутизації. Протокол OSPF здійснює обмін повідомленнями для передачі даних маршрутизації, використовуючи для цього п’ять типів пакетів.

До таких пакетів відносяться:

- пакет вітання;
- пакет опису БД;
- пакет стану каналу;
- пакет оновлення стану каналу;
- пакет підтвердження стану каналу.

Ці пакети використовуються для виявлення сусідніх маршрутизаторів, а також для обміну даними маршрутизації в цілях надання точних даних про мережу. ЦП обробляє таблиці сусідніх пристроїв і таблиці топології, використовуючи алгоритм пошуку найкоротшого шляху Дейкстри.

Алгоритм пошуку найкоротшого шляху ґрунтується на даних про сукупну вартість доступу до точки призначення. Алгоритм пошуку

найкоротшого шляху створює дерево найкоротших шляхів SPF шляхом розміщення кожного маршрутизатора у корені дерева і розрахунку найкоротших шляхів до кожного з вузлів.

Після цього дерево найкоротших шляхів SPF використовується для розрахунку оптимальних маршрутів. Протокол OSPF вносить оптимальні маршрути в БД пересилки, яка застосовується для створення таблиці маршрутизації.

Для надання даних маршрутизації маршрутизатори, що використовують протокол OSPF, виконують наступні кроки процесу маршрутизації за станом каналу для досягнення стану збіжності:

1. Встановлення стосунків суміжності з сусідніми пристроями, коли маршрутизатори з підтримкою OSPF повинні виконати виявлення один одного в мережі, щоб обмінюватися даними. Маршрутизатор, що використовує OSPF, відправляє пакети вітання з усіх інтерфейсів з включеним OSPF для визначення усіх сусідніх пристроїв у межах цих каналів. За наявності сусіднього пристрою маршрутизатор, що використовує OSPF, намагається встановити з ним стосунки суміжності.

2. Обмін оголошеннями про стан каналу, коли після встановлення стосунків суміжності маршрутизатори виконують обмін оголошеннями про стан каналу (LSA). LSA містять стан і вартість кожного безпосередньо підключеного каналу. Маршрутизатори відправляють свої LSA суміжним пристроям. При отриманні LSA суміжні пристрої миттєво відправляють свої LSA безпосередньо підключеним сусідам; цей процес триває до тих пір, поки усі маршрутизатори області не отримають усі LSA.

3. Створення таблиці топології, коли після отримання оголошень про стан каналу (LSA) маршрутизатори, що використовують OSPF, створюють БД топології на базі отриманих пакетів. У цій БД збирається уся інформація про топологію мережі.

4. Виконання алгоритму пошуку найкоротшого шляху SPF. Після цього маршрутизатори виконують алгоритм пошуку найкоротшого шляху.

Оптимальні маршрути вносяться в таблицю маршрутизації з дерева найкоротших шляхів SPF. Рішення з маршрутизації приймаються на основі записів в таблиці маршрутизації.

Для забезпечення більшої ефективності і масштабованості протокол OSPF підтримує ієрархічну маршрутизацію з розподілом на області. Область OSPF є групою маршрутизаторів, що використовують однакові дані про стан каналу у своїх базах цих станів каналів.

Протокол OSPF можна реалізувати одним з наступних способів:

1. OSPF для однієї області, коли усі маршрутизатори знаходяться в одній області, що називається магістральною або нульовою областю (область 0).

2. OSPF для декількох областей, коли протокол OSPF реалізується за допомогою декількох областей в ієрархічному порядку.

Усі області мають бути підключені до магістральної області (область 0). Маршрутизатори, за допомогою яких здійснюється з'єднання між областями, називаються пограничними маршрутизаторами (ABR, Area Border Router).

У OSPF для декількох областей протокол може розділяти одну велику автономну систему на дрібніші області в цілях забезпечення ієрархічної маршрутизації. При використанні ієрархічної маршрутизації виконується маршрутизація між областями (міжобласна маршрутизація), але багато операцій маршрутизації, що споживають ресурси процесора (наприклад, повторний розрахунок БД), виконується у межах однієї області.

Кожного разу, коли маршрутизатор отримує нові дані про зміну топології в межах області (включаючи додавання, видалення або зміну каналу), маршрутизатор повинен повторно виконати алгоритм пошуку найкоротшого шляху, створити нове дерево найкоротших шляхів SPF і відновити таблицю маршрутизації.

Алгоритм пошуку найкоротших шляхів споживає великий об'єм ресурсів центрального процесора. Час, що витрачається на розрахунки, залежить від розміру області. Зміни топології розподіляються по маршрутизаторах в інших областях в дистанційно – векторному форматі. Тобто ці маршрутизатори

оновлюють тільки свої таблиці маршрутизації і не повинні повторно виконувати алгоритм пошуку найкоротших шляхів.

За наявності великого числа маршрутизаторів в одній області, БД про стан каналу мають занадто великий розмір, і навантаження на центральний процесор, таким чином, збільшується. Тому розподіл маршрутизаторів по областях ефективно розділяє потенційно великі БД на БД меншого розміру, тим самим забезпечуючи можливість ефективнішого управління.

Можливості ієрархічної топології OSPF для декількох областей забезпечують ряд наступних переваг:

1. Таблиці маршрутизації меншого розміру – менше число записів в таблицях маршрутизації, оскільки мережні адреси можуть об'єднуватися між областями. Функція об'єднання маршрутів відключена за замовчуванням.

2. Зниження навантаження, викликаного оновленнями стану каналу – мінімізація вимог до ресурсів процесора і пам'яті.

3. Зниження частоти розрахунків найкоротшого шляху – локалізація дії змін топології в межах області. Таким чином, скорочується дія оновлень маршрутизації, оскільки лавинна розсилка оголошень LSA припиняється на межі області.

12.4 Інкапсуляція та типи пакетів протоколу «Open shortest path first»

Повідомлення OSPF, що передаються по каналу Ethernet, містять наступні дані:

– заголовок кадру каналу даних Ethernet визначає групову MAC-адресу призначення 01-00-5E-00-00-05 або 01-00-5E-00-00-06;

– заголовок IP-пакета визначає поле 89 протоколу IPv4, що вказує, що цей пакет є пакетом OSPF. Він також визначає одну з двох групових адрес OSPF (224.0.0.5 або 224.0.0.6);

– заголовок пакету OSPF визначає тип пакету OSPF, ідентифікатор маршрутизатора і ідентифікатор області.

Дані залежно від типу пакету OSPF містять дані про тип пакету OSPF. Вміст може відрізнятися залежно від типу пакету. У даному випадку це заголовок IPv4. Протокол OSPF використовує пакети стану каналу для встановлення і підтримки стосунків суміжності та обміну оновленнями маршрутизації.

Існує п’ять різних типів пакетів стану каналу, що використовуються протоколом OSPF. Кожен тип пакету виконує певне завдання у процесі маршрутизації OSPF.

Тип 1 (пакет вітання) використовується для встановлення і підтримки стосунків суміжності з маршрутизаторами OSPF.

Тип 2 (пакет опису бази даних) містить скорочений список бази цих станів каналів відправляючого маршрутизатора. Використовується приймаючими маршрутизаторами для звіряння з локальною БД про стан каналу. Для побудови точного дерева найкоротших шляхів SPF маршрутизатори з маршрутизацією за станом каналу в межах області повинні використовувати ідентичну базу цих станів каналів.

Тип 3 (пакет запиту стану каналу LSR) приймаючі маршрутизатори можуть запросити додаткові дані про будь-який запис в пакеті опису БД, відправивши пакет запиту стану каналу (LSR).

Тип 4 (пакет оновлення стану каналу LSU) використовується для відправки відгуку на пакети запиту стану каналу (LSR) та оголошення нових даних. Пакети оновлення стану каналу (LSU) містять сім різних типів LSA.

Тип 5 (пакет підтвердження стану каналу LSAck) при отриманні LSU маршрутизатор відправляє LSAck для підтвердження прийому LSU. Поле даних LSAck є порожнім.

Повідомлення OSPF, що передаються по каналу Ethernet, містять наступні дані:

1. Заголовок кадру каналу даних Ethernet визначає групову MAC-адресу призначення 01-00-5E-00-00-05 або 01-00-5E-00-00-06.

2. Заголовок IP-пакета визначає поле 89 протоколу IPv4, що вказує, що цей пакет є пакетом OSPF. Він також визначає одну з двох групових адрес OSPF (224.0.0.5 або 224.0.0.6).

3. Заголовок пакету OSPF визначає тип пакету OSPF, ідентифікатор маршрутизатора і ідентифікатор області.

4. Дані залежно від типу пакету OSPF містять дані про тип пакету OSPF. Вміст може відрізнятися залежно від типу пакету. У даному випадку це заголовок IPv4.

Протокол OSPF використовує пакети стану каналу для встановлення і підтримки стосунків суміжності та обміну оновленнями маршрутизації.

Пакети вітання використовуються для виявлення сусідніх пристроїв OSPF і встановлення стосунків суміжності з ними та для оголошення параметрів, при яких два маршрутизатори зобов’язано погодитися встановити стосунки суміжності. У мережах з множинним доступом (Ethernet і Frame Relay) необхідно вибрати виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR). Для каналів типу «точка-точка» наявність DR або BDR не потрібно.

До найбільш важливих полів пакету вітання відносяться наступні. Тип – визначає тип пакету. Число 1 означає пакет вітання. Значення 2 означає пакет DBD, 3 – пакет LSR, 4 – пакет LSU, а 5 – пакет LSAck.

Ідентифікатор маршрутизатора – 32-бітове значення, виражене в десятковому форматі з розподілом точкою (IPv4-адрес), використовується для унікального позначення початкового маршрутизатора.

Ідентифікатор області – область, в якій створений пакет.

Маска підмережі – маска підмережі, пов’язана з відправляючим інтерфейсом.

Інтервал вітання – інтервал (у секундах), після закінчення якого маршрутизатором вирушає наступний пакет вітання.

У мережах з множинним доступом інтервал вітання за замовчуванням заданий зі значенням 10 секунд. У сусідніх маршрутизаторах повинен

використовуватися один і той же таймер, інакше стосунки суміжності не встановлюються.

Пріоритет маршрутизатора використовується при виборі DR/BDR. За замовчуванням для усіх маршрутизаторів OSPF заданий пріоритет 1, проте його можна змінити вручну, вибравши значення в діапазоні від 0 до 255.

Чим вище це значення, тим більше вірогідність того, що маршрутизатор використовуватиметься як виділений маршрутизатор (DR) на цьому каналі.

Інтервал простою (Router dead interval) – інтервал (у секундах) очікування маршрутизатором сигналу від сусіднього пристрою, після закінчення якого сусідній маршрутизатор оголошується «мертвим», тобто недіючим. Як правило, значення інтервалу простою дорівнює чотирикратному значенню інтервалу вітання. У сусідніх маршрутизаторах повинен використовуватися один і той же таймер, інакше стосунки суміжності не встановлюються.

Виділений маршрутизатор (DR) – ідентифікатор маршрутизатора DR.

Резервний виділений маршрутизатор (BDR) – ідентифікатор маршрутизатора BDR.

Список сусідніх пристроїв – список, що визначає ідентифікатори усіх суміжних маршрутизаторів.

Контрольні запитання

1. Які ви знаєте характеристики протоколу OSPF?
2. Які компоненти та принцип роботи протоколу OSPF?
3. Як відбувається інкапсуляція пакетів OSPF?
4. Які є типи пакетів OSPF?
5. Як відбувається встановлення стосунків суміжності?
6. Як відбувається синхронізація баз даних OSPF?
7. Як відбувається налаштування процесу OSPF?
8. Як відбувається перевірка даних процесу OSPF?

13 СПЕЦИФІКАЦІЇ ФІЗИЧНОГО СЕРЕДОВИЩА ETHERNET

Історично перші мережі технології Ethernet були створені на коаксіальному кабелі діаметром 0,5 дюйми.

Надалі були визначені інші специфікації фізичного рівня для стандарту Ethernet, що дозволяють використовувати різні середовища передачі даних як загальної шини.

Метод доступу CSMA/CD і всі часові параметри Ethernet залишаються одними й тими самими будь-якої специфікації фізичного середовища.

Фізичні специфікації технології Ethernet на сьогоднішній день включають такі середовища передачі даних:

1. 10Base-5 – коаксіальний кабель діаметром 0,5 дюйма, званий «товстим» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента 500 метрів (без повторювачів).

2. 10Base-2 – коаксіальний кабель діаметром 0,25 дюйма, званий «тонким» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента – 185 метрів (без повторювачів).

3. 10Base-T – кабель на основі неекранованої кручений пари (Unshielded Twisted Pair, UTP). Утворює зіркоподібну топологію із концентратором. Відстань між концентратором та кінцевим вузлом – не більше 100 метрів.

4. 10Base-F – оптоволоконний кабель. Топологія аналогічна стандарту на кручений парі. Є кілька варіантів цієї специфікації – FOIRL (відстань до 1000 метрів), 10Base–FL (відстань до 2000 метрів), 10Base–FB (відстань до 2000 метрів).

Число 10 позначає бітову швидкість передачі цих стандартів – 10 мегабіт за секунду, а слово Base – метод передачі однієї базової частоті 10 мегагерц (на відміну стандартів, використовують кілька несучих частот, які називаються Broadbend – широкосмуговими).

Останній символ у назві стандарту фізичного рівня позначає тип кабелю.

13.1 Стандарт 10Base-5

Стандарт 10Base-5 відповідає експериментальній мережі Ethernet фірми Xerox і може вважатися класичним Ethernet. Він використовує, як середовище передачі даних, коаксіальний кабель з діаметром центрального мідного дроту 2,17 міліметрів та зовнішнім діаметром близько 10 міліметрів («товстий» Ethernet). Такими характеристиками володіють кабелі марок RG-8 та RG-11.

Кабель використовується як моноканал для всіх станцій. Сегмент кабелю має максимальну довжину 500 метрів (без повторювачів) і повинен мати на кінцях узгоджувальні термінатори опором 50 Ом, що поглинають сигнали, що поширюються по кабелю і перешкоджають виникненню відбитих сигналів. За відсутності термінаторів у кабелі виникають стоячі хвилі, отже одні вузли отримують потужні сигнали, інші – настільки слабкі, що й прийом стає неможливим.

Станція повинна підключатися до кабелю за допомогою приймача трансівера (Transmitter та receiver утворюють trnsceiver). Трансівер встановлюється безпосередньо на кабелі та живиться від мережевого адаптера комп’ютера. Трансівер може приєднуватися до кабелю як методом проколювання, що забезпечує безпосередній фізичний контакт, і безконтактним методом.

Трансівер – це частина мережного адаптера, яка організовує прийом та передача даних з кабелю на кабель, проводить визначення колізій на кабелі електрична розв’язка між кабелем та іншою частиною адаптера, організовує захист кабелю від некоректної роботи адаптера.

Останню функцію часто називають контролем балакучості (jabber control). При виникненні несправностей адаптера може виникнути ситуація, коли на кабель безперервно видаватиметься послідовність випадкових сигналів. Оскільки кабель це загальне середовище для всіх станцій, то робота мережі буде заблокована одним несправним адаптером. Щоб цього не сталося, на виході передавача ставиться схема, яка перевіряє кількість бітів, переданих у пакеті. Якщо максимальна довжина пакета перевищується, ця схема просто

від’єднує вихід передавача від кабелю. Максимальний час передачі кадру (разом з преамбулою) дорівнює 1221 мікросекунд, а час jabber-контролю встановлюється рівним 4000 мікросекунд.

Детектор колізій визначає наявність колізії у коаксіальному кабелі за підвищеним рівнем постійної складової сигналів. Якщо постійна складова перевищує певний поріг (близько 1,5 ватт), це означає, що на кабель працює більш ніж один передавач.

Стандарт дозволяє використання в мережі не більше чотирьох повторювачів і відповідно не більше п’яти сегментів кабелю. При максимальній довжині сегмента кабелю в 500 метрів це дає максимальну довжину мережі 10Base-5 в 2500 метрів. Тільки три сегменти з п’яти можуть бути навантаженими, тобто такими, до яких підключаються кінцеві вузли. Між навантаженими сегментами мають бути ненавантажені сегменти, отже максимальна конфігурація мережі є два навантажених крайніх сегмента, які з’єднуються ненавантаженими сегментами з одним центральним сегментом.

Правило застосування повторювачів у мережі Ethernet 10Base-5 називається «правило 5-4-3»: п’ять сегментів, чотири повторювачі, три навантажені сегменти. Обмежена кількість повторювачів пояснюється додатковими затримками поширення сигналу, що вони вносять. Застосування повторювачів збільшує час подвійного поширення сигналу, яке для надійного розпізнавання колізій не повинно перевищувати час передачі кадру мінімальної довжини, тобто кадру 72 байт або 576 біт.

Кожен повторювач підключається до сегмента одним своїм трансівером, тому до навантажених сегментів можна підключити не більше 99 вузлів.

До переваг стандарту 10Base-5 відносяться хороша захищеність кабелю від зовнішніх впливів та порівняно велика відстань між вузлами. До недоліків слід віднести високу вартість кабелю, складність його прокладки через велику жорсткість, наявність спеціального інструменту для закладення кабелю. Також при пошкодженні кабелю або поганому з’єднанні відбувається зупинка роботи

всієї мережі. Зазначимо, що необхідно передбачити підведення кабелю до всіх можливих місць встановлення комп'ютерів.

13.2 Стандарт 10Base-2

Стандарт 10Base-2 використовує, як передавальне середовище, коаксіальний кабель з діаметром центрального мідного дроту 0,89 міліметрів і зовнішнім діаметром близько 5 міліметрів («тонкий» Ethernet, хвильовий опір кабелю 50 Ом). Такі характеристики мають кабелі марок RG–58/U, RG–58A/U, RG–58C/U.

Максимальна довжина сегмента без повторювачів становить 185 метрів, сегмент повинен мати на кінцях узгоджувальні термінатори 50 Ом. Тонкий коаксіальний кабель дешевше товстого, через що мережі 10Base-2 іноді називають мережами Cheapernet (від cheaper – дешевший). Але за дешевизну кабелю доводиться розплачуватися якістю, бо «тонкий» коаксіал має найгіршу поміхо захищеність, найгіршу механічну міцність і вужчу смугу пропускання.

Станції підключаються до кабелю за допомогою високочастотного BNC Т-конектора, який є трійником, один відвід якого з'єднується з мережним адаптером, а два інших з двома кінцями розриву кабелю. Максимальна кількість станцій, що підключаються до одного сегменту, 30 одиниць. Мінімальна відстань між станціями становить 1 метр. Стандарт 10Base-2 також передбачає використання повторювачів, застосування яких також має відповідати правилу «5-4-3». У цьому випадку мережа матиме максимальну довжину 925 метрів (5 помножити на 185 метрів). Очевидно, що це обмеження є сильнішим, ніж загальне обмеження 2500 метрів.

Цей стандарт дуже близький до стандарту 10Base-5, але трансівери в ньому об'єднані з мережевими адаптерами за рахунок того, що більш гнучкий тонкий коаксіальний кабель може бути підведений безпосередньо до вихідного роз'єму плати адаптера мережі, встановленої в шасі комп'ютера. Кабель у разі «висить» на мережному адаптері, що утрудняє фізичне переміщення комп'ютерів.

Реалізація цього стандарту практично призводить до найпростішого рішення для кабельної мережі. Однак цей вид кабельних з'єднань найбільш сильно схильний до аварій і збоїв, бо кабель сприйнятливий до перешкод, в моноканалі, є велика кількість механічних з'єднань (кожен Т-конектор дає три механічні з'єднання, два з яких мають життєво важливе значення для всієї мережі), користувачі мають доступ до рознімання і можуть порушити цілісність моноканалу. Крім того, естетика та ергономічність цього рішення залишають бажати кращого, тому що від кожної станції через Т-конектор відходять два досить помітні дроти, які під столом часто утворюють моток кабелю – запас, необхідний на випадок навіть невеликого переміщення робочого місця.

Загальним недоліком стандартів 10Base-5 та 10Base-2 є відсутність оперативної інформації про стан моноканалу. Пошкодження кабелю виявляється відразу (мережа перестає працювати), але для пошуку кабелю, що відмовив, необхідний спеціальний прилад – кабельний тестер.

13.3 Стандарт 10Base–t

Стандарт прийнятий у 1991 році як додаток до існуючого набору стандартів Ethernet та має позначення 802.3i.

Використовує як середовище подвійну неекрановану кручену пару (Unshielded Twisted Pair, UTP). Багатопарний кабель на основі неекранованої кручений пари категорій 3 (категорія визначає смугу пропускання кабелю, величину перехресних наведень та деякі інші параметри його якості) телефонні компанії вже давно використовували для підключення телефонних апаратів усередині будівель.

Ідея пристосувати цей популярний вид кабелю для побудови локальних мереж виявилася дуже плідною, оскільки багато будинків вже було оснащено потрібною кабельною системою. Залишалося розробити спосіб підключення мережних адаптерів та іншого комунікаційного обладнання до крученої пари таким чином, щоб зміни в мережних операційних системах були б мінімальними порівняно з мережами Ethernet на коаксіалі. Це вдалося, тому

перехід на кручену пару вимагає лише заміни трансівера мережного адаптера або порту маршрутизатора, а метод доступу і всі протоколи канального рівня залишилися тими ж, що і в мережах Ethernet на коаксіалі.

З'єднання станцій здійснюються за топологією точка-точка зі спеціальним пристроєм – багатопортовим повторювачем за допомогою двох кручених пар. Одна кручена пара використовується передачі даних від станції до повторювачу (вихід Tx-сітьового адаптера), іншу – передачі даних від повторювача станції (вхід Rx-сітьового адаптера). Повторювач приймає сигнали від однієї з кінцевих вузлів і синхронно передає в інші порти, крім того, з якого надійшли сигнали, де Tx – передавач, Rx – приймач (рис. 13.1).

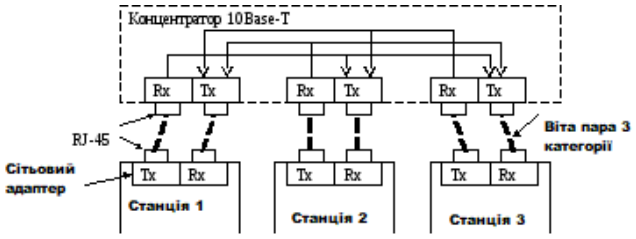

Рисунок 13.1 – Структура мережі стандарту 10Base–T

Багатопортові повторювачі у разі зазвичай називаються концентраторами (англомовні терміни – hub чи concentrator). Концентратор здійснює функції повторювача сигналів на всіх відрізках кручених пар, підключених до його портів, так що утворюється єдине середовище передачі даних – моноканал (шина). Стандарт визначає бітову швидкість передачі даних 10 мегабіт за секунду і максимальну відстань відрізка витої пари між двома безпосередньо зв'язаними вузлами (станціями та концентраторами) не більше 100 метрів при використанні витої пари якості не нижче категорії 3. Ця відстань визначається смугою пропускання витої пари – на довжині 100 метрів вона дозволяє передавати дані зі швидкістю 10 мегабіт за секунду під час використання манчестерського коду.

Концентратори 10Base-t можна з'єднувати один з одним за допомогою тих портів, які призначені для підключення кінцевих вузлів. При цьому потрібно подбати про те, щоб передавач та приймач одного порту були з'єднані відповідно до приймача та передавача іншого порту.

Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD та надійного розпізнавання станціями колізій у стандарті визначено максимальну кількість концентраторів між двома станціями мережі, а саме чотири. Це правило носить назву «правила 4-х хабів» і воно замінює «правило 5-4-3», що застосовується до коаксіальних мереж. При створенні мережі 10Base-t з великою кількістю станцій концентратори можна з'єднувати один з одним ієрархічним способом, утворюючи деревоподібну структуру.

Петлеподібне з'єднання концентраторів у стандарті 10Base-t заборонено, оскільки воно призводить до некоректної роботи мережі. Резервування зв'язків можливе лише за рахунок переведення одного з паралельних зв'язків у неактивний (заблокований) стан. Наведемо ієрархічну сполуку концентраторів Ethernet (рис. 13.2).

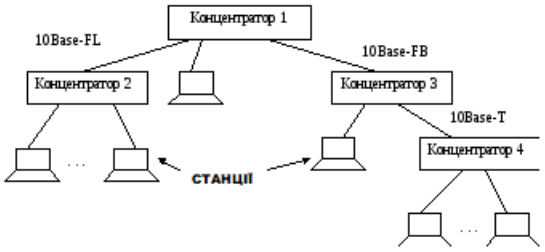

Рисунок 13.2 – Ієрархічна сполука концентраторів Ethernet

Загальна кількість станцій в мережі 10Base-t не повинна перевищувати 1024 і для цього типу фізичного рівня ця кількість дійсно можна досягти. Для цього достатньо створити дворівневу ієрархію концентраторів, розташувавши їх на нижньому рівні достатньо концентраторів із загальною кількістю портів 1024. Кінцеві вузли потрібно підключити до портів концентраторів нижнього рівня. Правило 4-х хабів при цьому виконується – між будь-якими кінцевими вузлами дорівнюватиме 3-м концентратори.

Максимальна довжина мережі тут розуміється як максимальна відстань між двома довільними кінцевими вузлами мережі (часто застосовується термін «максимальний діаметр мережі»). Вочевидь, що й між будь-якими двома вузлами мережі має бути більше 4-х повторювачів, то максимальний діаметр мережі 10Base-t становить 500метрів (5 по 100 метрів).

Мережі, побудовані на основі стандарту 10Base-t, мають у порівнянні з коаксіальними варіантами Ethernet багато переваг. Ці переваги пов'язані з поділом загального фізичного кабелю на окремі кабельні відрізки, підключені до центрального комунікаційного пристрою, адаптер на індивідуальній основі. Ця обставина істотно полегшує експлуатацію великих мереж Ethernet, оскільки концентратор зазвичай автоматично виконує такі функції, повідомляючи при цьому адміністратора мережі про проблему.

У стандарті 10Base-t визначено процедуру тестування фізичної працездатності двох відрізків крученої пари, що з'єднують трансівер кінцевого вузла і порт повторювача. Якщо тест не проходить, порт блокується і відключає проблемний вузол від мережі.

Поява між кінцевими вузлами активного пристрою, який може контролювати роботу вузлів та ізолювати від мережі некоректно працюючі, є головною перевагою технології 10Base-t порівняно зі складними в експлуатації коаксіальними мережами. Завдяки концентраторам мережа Ethernet набула деяких рис від стійкої до відмови системи.

13.4 Оптоволоконний Ethernet

В якості середовища передачі даних 10-и мегабітний Ethernet використовує оптичне волокно. Оптоволоконні стандарти, як основний тип кабелю, рекомендують досить дешеве багатомодове оптичне волокно, що має смугу пропускання 500 – 800 Мегагерц при довжині кабелю 1 кілометр. Допустимо і дорожче одномодове оптичне волокно зі смугою пропускання кілька гігагерц, але при цьому потрібно застосовувати спеціальний тип трансівера.

Функціонально мережа Ethernet на оптичному кабелі складається з тих же елементів, що і мережа стандарту 10Base-t, а саме мережних адаптерів, багатопортового повторювача і відрізків кабелю, що з'єднують адаптер з портом повторювача. Одне з'єднує вихід Tx адаптера із входом Rx повторювача, а інше – вхід Rx адаптера із виходом Tx повторювача.

Стандарт FOIRL (Fiber optic inter repeater link) являє собою перший стандарт 802.3 для використання оптоволокна в мережах Ethernet. Він гарантує довжину оптоволоконного зв'язку між повторювачами до 1 кілометра при загальній довжині мережі не більше 2500 метрів. Максимального діаметра в 2500 метрів тут досягти можна, хоча максимальні відрізки кабелю між усіма трьома повторювачами, а також між повторювачами і кінцевими вузлами неприпустимі, інакше вийде мережа довжиною в 5000 метрів.

Стандарт 10Base-FL є незначним поліпшенням стандарту FOIRL. Збільшена потужність передавачів, тому максимальна відстань між вузлом і концентратором збільшилася до 2000 метрів. Максимальне число повторювачів між вузлами залишилося рівним 4-м, а максимальна довжина мережі – 2500 метрів.

Стандарт 10Base-FB призначений лише для з'єднання повторювачів. Кінцеві вузли не можуть використовувати цей стандарт для приєднання до портів концентратора. Між вузлами мережі можна встановити до п'яти повторювачів 10Base-FB за максимальної довжини одного сегмента 2000 метрів і максимальної довжини мережі 2740 метрів.

Повторювачі, з'єднані за стандартом 10Base-FB, за відсутності кадрів передачі постійно обмінюються спеціальними послідовностями сигналів, що відрізняються від сигналів кадрів даних, для підтримки синхронізації. Тому вони вносять менше затримки при передачі даних з одного сегмента в інший, і це є головною причиною, з якої кількість повторювачів вдалося збільшити до 5. Як спеціальні сигнали, використовуються манчестерські коди J і K в наступній послідовності: J-J-K-K-J-J-… Ця послідовність породжує імпульси частотою 2,5 МГц, які підтримують синхронізацію приймача одного концентратора з передавачем іншого. Тому стандарт 10Base-FB має також назву синхронний Ethernet.

У технології Ethernet, незалежно від стандарту фізичного рівня, що застосовується, існує поняття домену колізій.

Домен колізій (collision domain) – це частина мережі Ethernet, всі вузли якої розпізнають колізію незалежно від цього, у якій частині цієї мережі колізія виникла. Мережа Ethernet, побудована на повторювачах, завжди утворює один домен колізій.

Домен Колізій відповідає одному середовищу, що розділяється. Мости, комутатори та маршрутизатори ділять мережу Ethernet на кілька доменів колізій.

Вузли, що утворюють один домен колізій, працюють синхронно як єдина розподілена електронна схема.

Контрольні запитання

1. Наведіть характеристики кабелів RG–8 та RG–11.
2. Що таке трансівер?
3. У чому полягає основний зміст правила 5-4-3?
4. Наведіть визначення домену колізій.
5. Що вам відомо про комітет IEEE802.3?
6. Що вам відомо про «правило 4-х хабів»?

14 INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS 802.11

14.1 Основні визначення та принцип роботи бездротових мереж

Wi-Fi (англ. Wireless Fidelity – «бездротова точність») – стандарт на обладнання Wireless LAN.

Wi-Fi – це протокол бездротової передачі даних, що допомагає з'єднати n-ну кількість комп'ютерів у мережу, або підключити їх до Інтернету, з малим радіусом дії, що використовує радіохвилі.

Розроблено консорціумом Wi-Fi Alliance на базі стандартів IEEE 802.11 (Institute of electrical and electronic engineers 802.11), «Wi-Fi» – торгова марка Wi-Fi Alliance. Технологію назвали WirelessFidelity (дослівно бездротова точність).

Wireless local area network (WLAN) – це вид локальної обчислювальної мережі, який використовує для зв'язку і передачі даних між вузлами високочастотні радіохвилі, а не кабельні з'єднання. Установка WLAN рекомендувалася там, де розгортання кабельної системи було неможливо або економічно недоцільно.

У нинішній час в багатьох організаціях використовується Wi-Fi, так як при певних умовах швидкість роботи мережі вже перевищує 100 Мегабіт за секунду. Користувачі можуть переміщатися між точками доступу по території покриття мережі Wi-Fi.

Мобільні пристрої (смартфони, PSP, ноутбуки), оснащені клієнтськими Wi-Fi приймально – передавальними пристроями, можуть підключатися до локальної мережі і отримувати доступ в Інтернет через точки доступу або hot-spot.

Wi-Fi був створений у 1991 році в Нідерландах. Продукти, що призначалися спочатку для систем касового обслуговування, були виведені на ринок під маркою WaveLAN і забезпечували швидкість передачі даних від 1 до 2 Мегабіт за секунду.

Творець Wi-Fi – Вик Хейз (Vic Hayes) перебував у команді, що брала участь у розробці таких стандартів, як IEEE 802.11b, 802.11a і 802.11g.

Стандарт IEEE 802.11n був затверджений 11 вересня 2009. Його застосування дозволяє підвищити швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мегабіт за секунду), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 480 Мегабіт за секунду.

Зазвичай схема Wi-Fi мережі містить не менше однієї точки доступу (access point) і не менш одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережних адаптерів напряму.

Точка доступу передає свій ідентифікатор мережі Service set identifier (SSID, Network name – ідентифікатор мережі, мережне ім'я) за допомогою спеціальних сигнальних пакетів на швидкості 0,1 Мегабіт за секунду кожні 100 мілісекунди. Тому 0,1 Мегабіт за секунду – найменша швидкість передачі даних для Wi-Fi.

Знаючи SSID мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу.

При попаданні в зону дії двох точок доступу з ідентичними SSID, приймач може вибирати між ними на підставі даних про рівень сигналу.

Стандарт Wi-Fi дає клієнту повну свободу при виборі критеріїв для з'єднання і роумінгу.

Останні версії операційних систем містять функцію, звану «zero configuration», яка показує користувачеві всі доступні мережі і дозволяє перемикатися між ними «на льоту».

Це означає, що роумінг буде повністю контролюватися операційною системою.

Wi-Fi передає дані в ефірі, тому він має властивості, подібними з некомутованою мережею, і для нього можуть виникати такі ж проблеми, як при роботі з некомутованими мережами.

14.2 Стандарти бездротових мереж

На даний момент існує чотири основні стандарти Wi-Fi – це 802.11a, 802.11b, 802.11g і 802.11i.

Стандарт 802.11b – стандарт, при якому швидкість передачі досить невисока, а безпека перебуває на досить низькому рівні. При бажанні зловмиснику може знадобитися менше години для розшифрування ключа мережі і проникнення у вашу локальну мережу. Для захисту використовується протокол WEP, який охарактеризував себе не з кращого боку і був зламаний. Швидкість становить11 Мегабіт за секунду, радіус дії: 50 метрів. Протоколи забезпечення безпеки WEP, рівень безпеки низький.

Стандарт 802.11g – це більш просунутий стандарт, що прийшов на зміну 802.11b. Була збільшена швидкість передачі даних майже в 5 разів, і тепер вона становила 54 Мегабіт за секунду. При використанні обладнання підтримуючого технології super G або True MIMO межа максимально досяжної швидкості складає 125 Мегабіт за секунду. Зріс і рівень захисту, а саме при дотриманні всіх необхідних умов при правильному налаштуванні, його можна оцінити як високий. Даний стандарт сумісний з новими протоколами шифрування WPA і WPA2. Вони надають більш високий рівень захисту, ніж WEP, радіус дії становить 50 метрів, протоколи забезпечення безпеки WEP, WPA, WPA2. Рівень безпеки становить високий.

Стандарт 802.11i – стандарт, впровадження якого актуальне. В даному випадку безпосередньо в сам стандарт вбудована підтримка найсучасніших технологій, таких як True MIMO і WPA2. Тому необхідність більш ретельного вибору обладнання відпадає. Швидкість становить 125 Мегабіт за секунду, радіус дії 50 метрів, протоколи забезпечення безпеки WEP, WPA, WPA2. Рівень безпеки становить високий.

Стандарт 802.11n – стандарт 802.11n підвищує швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів 802.11g за умови використання в режимі 802.11n з іншими пристроями 802.11n. Стандарт 802.11n здатний забезпечити швидкість передачі даних до 480 Мегабіт за секунду.

Пристрої 802.11n працюють в діапазонах від 2,4 до 2,5 або 5,0 ГГц. Швидкість становить 300 Мегабіт за секунду. Протоколи забезпечення безпеки WEP, WPA, WPA2, рівень безпеки високий.

Однак слід пам’ятати, що неправильне налаштування устаткування, що підтримує навіть найсучасніші технології захисту, не забезпечить належний рівень безпеки вашої мережі. У кожному стандарті є додаткові технології і настройки для підвищення рівня безпеки. Покоління Wi–Fi наведено в порівняльній таблиці 14.1.

Таблиця 14.1 – Порівняльна таблиця поколінь Wi-Fi

Покоління Wi-Fi				
Ім’я	Рік створення	Макс. швидкість передачі	Середня швидкість передачі	Покоління
802.11a	1999	до 54 Мегабіт за секунду	близько 20 Мегабіт за секунду	Wi-Fi 2
802.11b	1999	до 11 Мегабіт за секунду		Wi-Fi 1
802.11g	2003	до 54 Мегабіт за секунду		Wi-Fi 3
802.11n	2009	до 600 Мегабіт за секунду (4 антени)	до 150 Мегабіт за секунду (1 антена)	Wi-Fi 4
802.11ac	2013	до 6,77 Гігабіт за секунду при 8-и антенах		Wi-Fi 5
802.11ax	2019	до 11 Гігабіт за секунду		Wi-Fi 6
802.11be	2023	до 30 Гігабіт за секунду		Wi-Fi 7

Для організації Wi-Fi мережі необхідно Wireless адаптери, які бувають PCI і USB, також в якості бездротового клієнта можуть виступати точки доступу, антена зовнішня – спрямована або кругова різної потужності. Як опція до антени – з’єднувальний кабель.

Для створення Wi-Fi мережі необхідно перш за все, в клієнтські комп'ютери встановити мережні Wi-Fi адаптери, певним чином налаштувати точки доступу, змонтувати антени. При використанні Wi-Fi, як засобу об'єднання мереж, Wi-Fi карти на клієнтських машинах відсутні.

Основні принципи побудови мережі для віддалених об'єктів (від 150 метрів) у тому, що все обладнання проходить обов'язкову сертифікацію. При проходженні сертифікації Wi-Fi обладнання перевіряється на відповідність стандартам передачі даних. На даний момент основним цікавлять нас критерієм є потужність передавача. Звідси і малий радіус дії обладнання в стандартній комплектації. В основному заявлені радіуси дії виробниками усереднено можна представити у приміщенні до 100метрів, поза приміщенням до 300 метрів (без урахування перешкод у вигляді рослин, перегородок, людей тощо). Таким чином, використовуючи стандартні опції устаткування отримати щось потужне навряд вийде. Виходом є використання різних зовнішніх антен і грамотне розташування обладнання.

14.3 Переваги та недоліки використання бездротових мереж

До переваг використання Wi-Fi можна віднести:

– дозволяє розгорнути мережу без прокладки кабелю, що може зменшити вартість розгортання або розширення мережі. Місця, де не можна прокласти кабель, наприклад, поза приміщеннями і в будівлях, що мають історичну цінність, можуть обслуговуватися бездротовими мережами;

– дозволяє мати доступ до мережі мобільних пристроїв. Wi-Fi пристрої широко поширені на ринку, пристрої різних виробників можуть взаємодіяти на базовому рівні сервісів;

– Wi-Fi це набір глобальних стандартів. На відміну від стільникових телефонів, Wi-Fi обладнання може працювати в різних країнах по всьому світу.

До недоліків Wi-Fi можна віднести наступні характеристики:

– частотний діапазон і експлуатаційні обмеження в різних країнах неоднакові. В багатьох європейських країнах дозволені два додаткових канали,

які заборонені в Америці. В Японії є ще один канал у верхній частині діапазону, а інші країни, наприклад Іспанія, забороняють використання низькочастотних каналів. Більш того, деякі країни, наприклад Італія, вимагають реєстрації всіх мереж Wi-Fi, що працюють поза приміщеннями, або вимагають реєстрації Wi-Fi оператора;

– висока, порівняно з іншими стандартами, споживання енергії, що зменшує час життя батарей і підвищує температуру пристрою;

– найпопулярніший стандарт шифрування WEP може бути відносно легко зламаний навіть при правильній конфігурації (через слабку стійкість алгоритму). Незважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і WPA2, який перевіряє користувачів мережі через сервер і задіє 128-бітові ключі шифрування і динамічні ключі сесії для забезпечення захисту бездротової мережі, багато старі точки доступу не підтримують його і вимагають заміни;

– Wi-Fi мають обмежений радіус дії. Типовий домашній маршрутизатор Wi-Fi стандарту 802.11b або 802.11g має радіус дії 45 метрів в приміщенні і 90 метрів зовні. Мікрохвильова піч або дзеркало, розташовані між пристроями Wi-Fi, послаблюють рівень сигналу. Відстань залежить також від частоти;

– накладення сигналів закритої або шифрування точки доступу і відкритої точки доступу, що працюють на одному або сусідніх каналах може перешкодити доступу до відкритої точки доступу. Ця проблема може виникнути при великій щільності точок доступу, наприклад, у великих багатоквартирних будинках, де багато мешканців ставлять свої точки доступу Wi-Fi;

– неповна сумісність між пристроями різних виробників або неповна відповідність стандарту може призвести до обмеження можливостей з’єднання або зменшення швидкості;

– зменшення продуктивності мережі під час дощу;

– перевантаження обладнання при передачі невеликих пакетів даних через приєднання великої кількості службової інформації;

Контрольні запитання

1. Надайте визначення поняттю Wi-Fi.
2. Наведіть основні перевага Wi-Fi.
3. Наведуть основні недоліки Wi-Fi.
4. Яке обладнання необхідне для організації мережі з Wi-Fi?
5. Які стандарти Wi-Fi використовується на сьогоднішній день?

15 БЕЗПЕКА МЕРЕЖІ

15.1 Основні поняття захисту інформації

Захист інформації – це комплекс заходів, що проводяться з метою запобігання витоку, розкрадання, втрати, несанкціонованого знищення, викривлення, модифікації (підробки), несанкціонованого копіювання, блокування інформації, тощо. Оскільки втрата інформації може відбуватися через суто технічні, об’єктивні і ненавмисні причини, під це визначення потрапляють також і заходи, пов’язані з підвищенням надійності сервера через відмови або збоїв в роботі вінчестерів, недоліків у програмному забезпеченні тощо.

Перехід від роботи на персональних комп’ютерах до роботи в мережі ускладнює захист інформації з наступних причин:

– велике число користувачів в мережі і їх змінний склад. Захист на рівні імені та пароля користувача недостатня для запобігання входу в мережу сторонніх осіб;

– значна протяжність мережі і наявність багатьох потенційних каналів проникнення в мережу;

– вже зазначені недоліки в апаратному та програмному забезпеченні, які найчастіше виявляються в процесі експлуатації, у тому числі неідеальні вбудовані засоби захисту інформації навіть в відомих мережних апераційних системах.

У мережі є багато фізичних місць і каналів несанкціонованого доступу до інформації в мережі.

Кожен пристрій в мережі є потенційним джерелом електромагнітного випромінювання через те, що відповідні поля, особливо на високих частотах, екрановані неідеально.

Система заземлення разом з кабельною системою і мережею електроживлення може служити каналом доступу до інформації в мережі, в тому числі на ділянках, що знаходяться поза зоною контрольованого доступу і тому особливо вразливих.

Крім електромагнітного випромінювання, потенційну загрозу представляє безконтактний електромагнітний вплив на кабельну систему.

Безумовно, в разі використання кабельних з'єднань типу коаксіальних кабелів або витих пар, які називаються часто мідними кабелями, можливо і безпосереднє фізичне підключення до кабельної системі. Якщо паролі для входу в мережу стали відомі або підібрані, стає можливим несанкціонований вхід в мережу з файл сервера або з однією з робочих станцій.

15.2 Концепції мережної безпеки

Безпека мережі – заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережна безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

Мережна безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ідентифікатор і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень.

Мережна безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами.

Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережна безпека бере участь в організаціях, підприємствах та інших типах закладів. Найбільш поширений і

простий спосіб захисту мережних ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережна безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією.

При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або «ключ», кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі.

Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень. Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак. Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

– захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином;

– забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації;

– контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями;

– забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

15.3 Ключові елементи захищених мережних служб

Ключові елементи захищених мережних служб:

1. Брандмауери. Централізовані брандмауери та брандмауери окремих комп'ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

2. Антивірусні засоби. Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз. Захищений віддалений доступ і обмін даними. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

Критерії оцінки інформаційної безпеки (Common Criteria) є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можна порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Інформаційні системи аналізуються в трьох головних секторах, а саме у технічних засобах, програмному забезпеченні і комунікаціях, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях (фізичний, особистий і організаційний).

В Україні розробляються і використовуються критерії інформаційної безпеки. Наприклад департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» який подібний до моделі тріади CIA.

Складові інформаційної безпеки:

– конфіденційність (Confidentiality, privacy). Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності.

– цілісність (Integrity). Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

– доступність (Availability). Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності.

15.4 Класифікація засобів захисту інформації

1. Технічні (апаратні) засоби. Це різні за типом пристрою (механічні, електромеханічні, електронні тощо), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, доступу до інформації, в тому числі за допомогою її маскування. Першу частину завдання вирішують замки, решітки на вікнах, захисна сигналізація та ін. Другу – генератори шуму, мережні фільтри, скануючі радіоприймачі і безліч інших пристроїв, які «перекривають» потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

2. Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки – обмежена функціональність мережі, використання частини ресурсів файл сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів). До програмних засобів відноситься криптографічний захист інформації. Криптографічний захист інформації – вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації.

3. Змішані апаратно – програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

4. Організаційні засоби складаються з організаційно – технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно – правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки – висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі.

15.5 Класифікація мережних атак

Класифікація мережних атак:

– будь-які додаткові з'єднання з іншими сегментами або підключення до Інтернет породжують нові проблеми;

– атаки на локальну мережу через підключення до Інтернету для того, щоб отримати доступ до конфіденційної інформації, останнім часом набули широкого поширення, що пов'язано з недоліками вбудованої системи захисту інформації в протоколах TCP/I.

Мережні атаки через Інтернет можуть бути класифіковані в такий спосіб:

1. Сніффер пакетів (sniffer – в даному випадку в сенсі фільтрація) – прикладна програма, яка використовує мережеву карту, що працює в режимі promiscuous (хто не робить відмінності) mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережний адаптер відправляє додатком для обробки).

2. IP-спуфинг (spoof – обман, містифікація) – відбувається, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача.

3. Відмова в обслуговуванні (Denial of Service – DoS). Атака DoS робить мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

4. Парольні атаки – спроба підбору пароля легального користувача для входу в мережу.

5. Атаки типу Man-in-the-Middle – безпосередній доступ до пакетів, що передаються по мережі.

6. Атаки на рівні додатків.

7. Мережна розвідка – збір інформації про мережу за допомогою загальнодоступних даних і додатків.

8. Зловживання довірою всередині мережі.

9. Несанкціонований доступ (НСД), який не може вважатися окремим типом атаки, так як більшість мережних атак проводяться заради отримання несанкціонованого доступу.

10. Віруси і додатки, наприклад, троянський кінь [5, с. 286].

Контрольні запитання

1. Дайте визначення поняттю захист інформації?
2. Які причини ускладнюють захист інформації при переході від роботи на персональних комп’ютерах до роботи в мережі?
3. Назвіть фізичні місця і канали несанкціонованого доступу до інформації в мережі?
4. По яких каналах, що знаходяться поза мережею можливий витік інформації?
5. В чому полягає концепції мережної безпеки?
6. Що є складовими інформаційної безпеки?
7. Які існують типи загроз інформації?
8. Наведіть класифікацію засобів захисту інформації?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коробейнікова Т. І. Комп’ютерні мережі / Т. І. Коробейнікова, С. М. Захарченко. – Львів : Львівська політехніка, 2022. – 228 с.

2. Микитишин А. Г. Комп’ютерні мережі / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк. – Львів : Магнолія, 2021. – Кн. 1. – 256 с.

3. Конахович Г. Ф. Експлуатація телекомунікаційних систем / Г. Ф. Конахович. – Київ : Центр навчальної літератури, 2019. – 372 с.

4. Комп’ютерні мережі: навч. посіб. / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса : Фенікс, 2022. – 249 с.

5. Жураковський Б. Ю. Комп’ютерні мережі: навч. посіб. / Б. Ю. Жураковський, І. О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

6. Ромашко С. М. Конспект лекцій з дисципліни «Комп’ютерні мережі і телекомунікації» / С. М. Ромашко. – Львів : ЛРІДУ НАДУ, 2016. – 61с.

7. Комп’ютерні мережі: навч. посіб. / А. І. Блозва, Ю. В. Матус, В. В. Смолій, Б. С. Гусєв, Д. Ю. Касаткін, Т. Ю. Осипова, Я. А. Савицька. – Київ : Компрінт, 2017. – 821с.

8. Олещенко Л. М. Організація комп’ютерних мереж : навч. посіб. / Л. М. Олещенко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 225 с.

9. Денніс Брилов Комп’ютерні науки. Базовий курс / Денніс Брилов, Дж. Гленн Брукшир. – Київ : Діалектика, 2018. – 475 с.

Електронне навчальне видання

ПЛАХОТНІКОВ Кирило Валерійович

КОМП’ЮТЕРНІ МЕРЕЖІ

КОНСПЕКТ ЛЕКЦІЙ

(для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122 – Комп’ютерні науки)

Відповідальний за випуск *М. В. Новожилова*
За авторською редакцією
Комп’ютерне верстання *К. В. Плахотніков*

План 2023, поз. 113Л

Підп. до друку 21.03.2023. Формат 60 × 84/16.
Ум. друк. арк. 9,1.

Видавець і виготовлювач:
Харківський національний університет
міського господарства імені О. М. Бекетова,
вул. Маршала Бажанова 17, Харків, 61002.
Електронна адреса: office@kname.edu.ua
Свідоцтво суб’єкта видавничої справи:
№ ДК 5328 від 11.04.2017.