

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Г.Г. Киричек

ТЕКСТИ (конспект) лекцій з дисципліни
Комп'ютерні мережі для бакалаврів спеціальності 123
"Комп'ютерна інженерія", усіх форм навчання

2019

ТЕКСТИ (конспект) лекцій з дисципліни Комп'ютерні мережі для бакалаврів спеціальності 123 "Комп'ютерна інженерія", усіх форм навчання / Укл. Г.Г Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2019. – 58 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 06.09.2019

Рекомендовано до видання
НМК КНТ
Протокол № 3 від 24.10.2019

ЗМІСТ

1 ВСТУП ДО МЕРЕЖНИХ ТЕХНОЛОГІЙ	4
1.1 Модель OSI	4
1.2 Класифікація мереж	8
1.3 Стек TCP / IP	10
1.4 Фізичний рівень моделі OSI.....	12
1.5 Канальний рівень. Технологія Ethernet	14
1.6 Область колізій. Розрахунок PDV	17
2 МУЛЬТИПЛЕКСУВАННЯ І КОМУТАЦІЯ.....	21
2.1 Мультиплексування	21
2.2 Первинні мережі.....	23
2.2.1 Мережі SONET / SDH	24
2.2.2 Мережі DWDM.....	25
2.2.3 Оптична транспортна мережа	26
2.3 Комутатори	27
2.3.1 Методи комутації	28
2.3.2 Характеристики продуктивності.....	29
3 МЕРЕЖНИЙ РІВЕНЬ. АДРЕСАЦІЯ. МАРШРУТИЗАЦІЯ.....	31
3.1 Максимальна одиниця передачі MTU	31
3.2 IP-адресація.....	36
3.3 Приклади вирішення завдань.....	38
3.4 Маршрутизація	41
4 МЕРЕЖНІ СЛУЖБИ DHCP ТА DNS.....	45
4.1 Протокол динамічної конфігурації хостів	45
4.2 Централізована служба DNS	47
5 МЕРЕЖІ VLAN	50
5.1 Загальні поняття	50
5.2 Типи VLAN	51
6 ТРАНСПОРТНИЙ РІВЕНЬ. ПРОТОКОЛИ.....	54
6.1 Порти додатків.....	54
6.2 Протокол UDP	55
6.3 Протокол TCP	56
Рекомендована література	58

1 ВСТУП ДО МЕРЕЖНИХ ТЕХНОЛОГІЙ

Мета – ознайомитись з моделями, які описують взаємодію відкритих систем та засвоїти загальні принципи роботи фізичного та каналного рівнів моделі OSI (рівня доступу TCP/IP) для проходження професійного тесту з дисципліни «Комп'ютерні мережі».

1.1 Модель OSI

У 1978 році Міжнародна Організація по Стандартизації (ISO - International Organization for Standardization) приступила до створення еталонної моделі OSI (Open System Interconnection) - створена універсальна загальноприйнята модель мережної взаємодії: модель, яка описує взаємодію відкритих систем.

Відкрита система - будь-яка система (ПК, мережа, ОС, пристрої, ПЗ), побудована відповідно до відкритих специфікацій.

Відкриті специфікації - опубліковані, загальнодоступні специфікації, які відповідають стандартам та прийняті в результаті досягнення згоди після обговорення зацікавленими сторонами. Використання при розробці систем відкритих специфікацій дозволяє фахівцям розробляти для них різні апаратні або програмні засоби розширення і модифікації, створювати програмно-апаратні комплекси з продуктів різних виробників.

Специфікація - формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, обмежень і особливих характеристик. Не кожна специфікація - стандарт.

Для реальних систем повна відкритість - недосяжний ідеал. У відкритих системах цьому визначенню відповідають тільки частини, які підтримують зовнішні інтерфейси. Відкритість ОС Unix - в наявності стандартизованого програмного інтерфейсу між ядром і додатками, що дозволяє легко перенести додатки з середовища однієї версії Unix в середовище іншої версії.

Модель OSI стосується одного аспекту відкритості - відкритості засобів взаємодії пристроїв, які працюють в мережі. Тут під відкритою системою розуміється мережний пристрій, що взаємодіє з іншими мережними пристроями з використанням стандартних правил, які

визначають формат, зміст і значення повідомлень, що відправляються. Якщо мережі побудовані з дотриманням принципів відкритості - це надає наступні переваги:

- побудова мережі з апаратних засобів і ПЗ різних виробників;
- можливість простого з'єднання мереж між собою;
- проста заміна одних компонентів мережі іншими, простота

обслуговування.

Приклад відкритої системи - мережа Internet.

Модель OSI включає сім рівнів.

Layer 7: Application Layer – Прикладний.

Layer 6: Presentation Layer – Представницький.

Layer 5: Session Layer – Сеансовий.

Layer 4: Transport Layer – Транспортний.

Layer 3: Network Layer – Мережний.

Layer 2: Data Link Layer – Канальний.

Layer 1: Physical Layer - Фізичний.

Фізичний рівень - забезпечує передачу потоку біт між об'єктами канального рівня через фізичні з'єднання. Визначає електричні та фізичні специфікації пристроїв і відповідає за передачу сигналів в лінії зв'язку, їх прийом і перетворення в біти даних. До цього рівня відносяться фізичні характеристики середовища передачі даних, способи перетворення біт даних в сигнали, визначаються електричні параметри сигналів, механічні та електричні вимоги до роз'ємів і т.д.

Канальний рівень - визначає спосіб доступу до лінії зв'язку, оформлення потоку байт в блоки даних для передачі, адресацію в лінії зв'язку, перевірку цілісності даних, шляхом додавання до блоку даних додатковою інформації. Забезпечує функціональні і процедурні засоби для передачі блоків даних канального рівня між об'єктами мережного рівня як в режимі без встановлення з'єднання (дейтаграмному), так і в режимі з встановленням з'єднання. З'єднання канального рівня може бути реалізовано з використанням одного або декількох фізичних з'єднань.

Висновок: створити працюючу мережу можна з використанням перших двох рівнів моделі, канального і фізичного.

Обмеження: не можна створити мережу довільного масштабу (адреси плоскі, неструктуровані). Для створення мереж довільного розміру потрібна робота верхніх рівнів OSI.

Мережний рівень - забезпечує процедурні і функціональні засоби для передачі даних між об'єктами транспортного рівня як в режимі без встановлення з'єднання, так і в режимі з встановленням з'єднання, забезпечуючи незалежність об'єктів транспортного рівня від способів і умов маршрутизації і доставки даних, дозволяє об'єднати невеликі мережі, побудовані з використанням фізичного і канального рівня в складну мережу довільного масштабу. Адреси мережного рівня на відміну від апаратних адрес є структурованими ієрархічними адресами. Ця властивість мережних адрес дозволяє адресувати не тільки окремі хости, а і мережі.

Транспортний рівень - забезпечує передачу даних між об'єктами сеансового рівня, звільняючи сеансовий рівень від проблем, пов'язаних з необхідністю досягнення надійної і ефективної передачі даних. Ніякої гарантії збереження будь-якого блоку даних при передачі немає - несправність або аварія приведуть до втрати даних, які перетинали пошкоджений сегмент мережі. Але відправник може повторювати їх відправку до тих пір, поки дані не потраплять до одержувача. Спосіб переконатися, що дані не загубилися в дорозі - доставка з повідомленням про вручення.

Рівні - над транспортним рівнем, називаються прикладними рівнями. Вони забезпечують роботу додатків на хостах.

Сеансовий рівень - надає засоби, які необхідні для організації взаємодії об'єктів рівня представлення, синхронізації їх діалогу та управління обміном даними. Забезпечує сервіс по встановленню сеансових з'єднань між двома об'єктами рівня уявлень, підтримки впорядкованого обміну даними і розриву сеансових з'єднань впорядкованим чином. Сеансовий рівень забезпечує управління діалогом. Функції сеансового рівня: визначення параметрів логічного з'єднання, встановлення логічного з'єднання, обслуговування логічного з'єднання, розрив логічного з'єднання.

Рівень представлення - забезпечує подання інформації, якою обмінюються об'єкти рівня додатків або на яку вони посилаються в процесі взаємодії. Звільняє об'єкти рівня додатків від необхідності вирішувати проблеми, пов'язані із загальним поданням інформації, надаючи синтаксичну незалежність.

Рівень додатків - забезпечує для прикладних процесів єдину можливість отримання доступу до середовища OSI для забезпечення взаємодії при вирішенні спільних завдань. Зв'язок між взаємодіючими

процесами додатків, узгодження контексту додатків, що визначає єдині для взаємодіючих об'єктів умови взаємозв'язку. Надає прикладним процесам мережеві сервіси загального призначення (електронна пошта, передача файлів, веб-браузинг) - рівень, на якому програми не працюють, а взаємодіють.

У моделі OSI п'ять верхніх рівнів відносяться до рівнів, реалізованих програмно і вважається, що два нижніх рівні реалізовані апаратно. Термін «середовище OSI» - абстрактне представлення набору понять, елементів, функцій, протоколів, визначених у моделі OSI стандартами, що роблять можливим взаємодію між відкритими системами.

Процеси передачі інформації і взаємодії - регламентовані, описані правилами. Набори правил, що регламентують взаємодію є і в моделі OSI. Дамо визначення цих наборів правил:

Набір формальних правил і угод, що регламентують взаємодію між сусідніми рівнями однієї системи або мова взаємодії між сусідніми рівнями однієї системи – інтерфейс. Набір формальних правил і угод, що регламентують взаємодію між однаковими рівнями різних систем або мова взаємодії між однаковими рівнями різних систем - протокол.

Процес додавання заголовків при передачі інформації називається інкапсуляція. Кожен заголовок має сенс тільки для відповідного рівня системи-одержувача, верхні рівні не потребують заголовків нижніх рівнів. Кожен рівень системи-одержувача, обробивши відповідний заголовок, відкидає його, і передає на верхній рівень дані вже без свого заголовка. Процес відкидання заголовків - декапсуляція. ККД будь-якої мережевої технології завжди менше 100%. В мережі крім корисних даних будуть передаватися службові заголовки. Одиниці даних кожного рівня в рамках моделі називаються «протокольними одиницями даних» або PDU (Protocol Data Unit) відповідного рівня.

Блоки даних трьох верхніх рівнів не мають окремих назв, і називаються просто даними.

Блоки даних інших рівнів мають власні назви. Перерахуємо їх.

Блок даних транспортного рівня називається сегментом (segment), або дейтаграмою (datagram).

Блок даних мережного рівня називається пакетом (packet).

Блок даних канального рівня називається кадром (frame).

Одиниця даних фізичного рівня - біт (bit).

1.2 Класифікація мереж

Класифікація і стандартизація комп'ютерних мереж.

За способом організації мережі поділяються на реальні і штучні:

- штучні мережі (псевдомережі) дозволяють пов'язувати комп'ютери разом через виту пару і не потребують додаткових пристроїв. Використовуються коли необхідно перекачати інформацію з одного комп'ютера на інший.

- реальні мережі дозволяють пов'язувати комп'ютери за допомогою спеціальних пристроїв комутації і фізичної середовища передачі даних.

У загальному випадку класифікація реальних комп'ютерних мереж ведеться по різного виду критеріям:

По територіальній поширеності:

- RAN - мережа, що належить одному користувачеві і використовується для взаємодії його пристроїв;

- LAN - локальні комп'ютерні мережі, які характеризуються замкнутою інфраструктурою до рівня виходу на постачальника послуг зв'язку. До LAN можуть відноситися як невеликі офісні мережі з 5-10 комп'ютерів, так і мережі великих підприємств, що складаються з сотень пристроїв. Об'єднують абонентські системи, розташовані в межах невеликої території - мережі підприємств, фірм, банків, офісів, навчальних закладів і т.д. Доступ в LAN дозволений обмеженому колу осіб, які зазвичай і працюють в цій мережі;

- MAN - міські мережі (регіональні), між установами. Об'єднують абонентські системи, розташовані в межах окремого регіону - міста, адміністративного району; функціонують в інтересах організацій і користувачів регіону і мають вихід в WAN. Можуть охоплювати місто або кілька міст, пов'язуючи воедино локальні мережі (корпоративні);

- WAN - глобальні комп'ютерні мережі, що поширюються на великі географічні регіони і включають в себе LAN і безліч інших телекомунікаційних мереж і пристроїв. Інтернет відноситься до глобального виду мереж. WAN - відкриті і орієнтовані на обслуговування будь-яких користувачів. Об'єднують абонентські системи, розосереджені на великій території, що охоплює різні країни і континенти. Вирішують завдання об'єднання інформаційних ресурсів

світу і організації доступу до них. Використовують кабельні та телефонні лінії зв'язку, радіозв'язок, системи супутникового зв'язку;

Об'єднання - дозволяє створювати складні багатомережні ієрархії.

За відомчою приналежністю:

– відомчі (приватні) - належать одній організації і розташовуються на її території;

– державні мережі - мережі, використовувані в державних структурах.

За швидкістю передачі:

діляться на низько-, середньо-і високошвидкісні.

– низькошвидкісні (10 Мбіт / с),

– середньошвидкісні (від 100 Мбіт / с до 1000 Мбіт / с),

– високошвидкісні (понад 1000 Мбіт / с);

За типом середовища передачі:

– кабельні (телефонний, коаксіальний кабель, вита пара, волоконно-оптичний кабель);

– бездротові (передача інформації по радіохвилях в певному частотному діапазоні).

За функціональним призначенням:

– мережі зберігання даних (підключення зовнішніх пристроїв зберігання даних: дискові масиви, оптичні приводи до серверів так, щоб операційна система розпізнала підключені ресурси як локальні);

– серверні ферми (сервера, з'єднані мережею передачі даних і працюють як єдине ціле);

– мережі управління процесом;

– мережі SOHO (small / home), будинкові мережі (різновид LAN, що дозволяє користувачам обмінюватися даними, грати в мережеві ігри, виходити в Інтернет, прокладена в межах однієї будівлі (житлового, офісу) або декількох будівель).

За способом управління:

– мережі з централізованим управлінням - в мережі один або кілька керуючих пристроїв;

– мережі з децентралізованим управлінням - кожна абонентська система має засоби для управління мережею;

– мережі з змішаним керуванням - в певному поєднанні реалізовані принципи централізованого та децентралізованого управління.

За топологією комп'ютерних мереж.

За цим параметром комп'ютерні мережі поділяються на наступні види.

Шина. Кільце. Подвійне кільце. Зірка. Комірчана. Решітка. Дерево. Мережа fat tree (товсте дерево).

За способом адміністрування. Розрізняють 2 типу мереж - однорангову і мережу на основі сервера. Обидва різновиди виконують поставлені завдання але роблять це по-різному.

Мережа на основі сервера найбільш керована і контрольована.

Архітектура - специфікації зв'язку, розроблені для визначення функцій мережі і встановлення стандартів різних моделей обчислювальних систем, призначених для обміну та обробки даних.

Стандартизація - основа стандартизації багаторівневий підхід до розробки засобів мережевої взаємодії.

1.3 Стек TCP / IP

Стек протоколів TCP / IP. Transmission Control Protocol / Internet Protocol - промисловий стандарт стека протоколів, розроблено для глобальних мереж. Стандарти TCP / IP опубліковані в документах Request for Comment (RFC).

Стек TCP / IP - поширений набір протоколів, протоколи стека використовуються для обміну даними між будь-якими пов'язаними мережами і однаково добре підходять для мереж будь-якого масштабу.

Внесок в розвиток стека TCP / IP додав університет Берклі, реалізувавши протоколи стека в ОС UNIX.

Поширення UNIX привело і до поширення протоколу IP і ін. Протоколів стека. На цьому стеці працює Internet.

Лідуюча роль стека TCP / IP пояснюється наступними його властивостями:

- найбільш завершений стандартний стек мережних протоколів;
- представляє собою набір відкритих стандартів, які можуть бути вільно використані будь-яким розробником;

- практично всі мережі передають основну частину свого трафіку за допомогою протоколу TCP / IP - метод отримання доступу до глобальної мережі - Internet;

- всі сучасні операційні системи підтримують стек TCP / IP.

Стек TCP / IP розроблений до моделі OSI - має багаторівневу структуру але відповідність рівнів стека TCP / IP рівням моделі OSI досить умовно і в різних джерелах представлено по-різному.

Протоколи TCP / IP поділяються на 4 рівня.

- прикладний рівень (application);
- основний / транспортний рівень (transport);
- міжмережний рівень (internet);
- рівень мережних інтерфейсів (data link) або Рівень доступу

Четвертий - відповідає фізичному і каналному рівням OSI - в протоколах TCP / IP не регламентується, підтримує стандарти фізичного і каналного рівня - будь-яку БСТ. З появою нової технології LAN або WAN включається в TCP / IP за рахунок розробки нового RFC, що визначає метод інкапсуляції пакетів IP в її кадри-можна асоціювати з інтерфейсом між 2 і 3 рівнем OSI - з єдиним стандартизованим інтерфейсом.

Третій, рівень міжмережної взаємодії - передача пакетів з використанням різних технологій - відповідає мережному рівню OSI. Основний протокол рівня в стеку IP - спочатку проектувався як протокол передачі пакетів в складних мережах. До рівня міжмережної взаємодії відносяться протоколи маршрутизації - «протоколи динамічної маршрутизації» - RIP, OSPF, BGP, протокол міжмережних керуючих повідомлень ICMP (Internet Control Message Protocol) застосовується для діагностики мережі та інформування про помилки.

Рівень 2 називається основним - транспортним. На цьому рівні протокол управління передачею TCP (Transmission Control Protocol) і протокол призначених для користувача дейтаграм UDP (User Datagram Protocol). TCP забезпечує надійну передачу між прикладними процесами. UDP забезпечує передачу прикладних пакетів дейтаграмним способом - функції сполучної ланки між мережним протоколом і прикладними процесами. У заголовку TCP - дані, завдяки яким організують сеанси обміну даними між відправником і отримувачем - функції сеансового рівня OSI. Асоціюють як з

транспортним і сеансовим рівнями OSI, так і з транспортним. Встановити чітку відповідність між двома моделями неможливо.

Верхній рівень - прикладний. В TCP / IP багато протоколів прикладного рівня - до них відносяться: протокол копіювання файлів FTP; отримання пошти SMTP; клієнтські поштові протоколи - POP3 і IMAP4; гіпертекстовий HTTP; динамічного конфігурування хостів DHCP; служби дозволу імен DNS; управління мережею SNMP і інші.

1.4 Фізичний рівень моделі OSI

Лінія зв'язку - шлях, який проходить сигнал від відправника до одержувача. Складається з фізичної середовища передачі даних, апаратури передачі даних (DCE), проміжного обладнання та пристроїв, які по мережі (DTE), які передають одне одному інформацію у вигляді сигналу певної частоти і форми.

DTE, Data Terminal Equipment (ООД - Кінцеве Обладнання Даних) - пристрої, що виробляють дані для передачі в лінію зв'язку, що перетворюють призначену для користувача інформацію в дані і здійснюють зворотне перетворення.

DCE, Data Circuit Equipment (АПД - Апаратура Передачі Даних) - пристрої, що забезпечують фізичне з'єднання з мережею, формують сигнали, зрозумілі для протоколу фізичного рівня каналу зв'язку. DCE забезпечують подачу синхронізуючого сигналу, використовуваного для узгодження процесів обміну даними між DTE і DCE.

Фізичне середовище передачі даних. Класифікація середовища передачі: провідні (або повітряні) лінії зв'язку; кабельні лінії зв'язку; бездротові лінії зв'язку (радіоканали).

Провідні лінії зв'язку - дроти без ізолюючих і екрануючих оболонок, прокладені між стовпами (в повітрі). Відсутність екрана позначається на якості і швидкості передачі даних. Тому сьогодні провідні лінії зв'язку практично повністю витіснені кабельними.

Кабельні лінії зв'язку використовують для з'єднання різних видів кабелю. Кабель - складається з провідників, електричної або механічної ізоляції і роз'ємів, для підключення до комунікаційного обладнання.

Кабелі діляться на два види:

- мідні кабелі використовують для передачі інформації, шляхом зміни струму в провіднику - на основі витой пари (балансні кабелі) і коаксіальні кабелі.

– волоконно-оптичні кабелі - сигнал переноситься за допомогою променя світла. Існує кілька різновидів.

У локальних мережах як фізичне середовище передачі даних частіше використовують мідні кабелі, рідше - волоконно-оптичні.

Коаксіальний кабель складається з покритого ізоляцією твердого мідного дроту, розташованого в центрі кабелю. Поверх ізоляції натягнуто циліндричний провідник, у вигляді дрібної мідної сітки і покритий зовнішнім шаром ізоляції (пластиковою оболонкою).

Застосовуються зазвичай два типи коаксіального кабелю:

- 50 Ом - для передачі тільки цифрових даних;
- 75 Ом - для передачі аналогових сигналів.

Товщина тонкого коаксіального кабелю - приблизно 0,5 - 0,6 см, а товстого - 1 - 1,3 см.

Балансний кабель (вита пара) - найбільш вживаний вид кабелю, завдяки своїй дешевизні і простоті в експлуатації.

Кабелі на основі витой пари є симетричними - складаються з двох однакових в конструктивному відношенні, ізольованих мідних проводів, діаметром близько міліметра. Кабель вита пара може бути екранований за допомогою фольги або мідної обплетення - збільшує його перешкодозахищеність, але позначається на вартості. Кабель - екранована вита пара, STP (Shielded Twisted Pair). Кабель - неекранована вита пара, UTP (Unshielded Twisted Pair).

Кабель на основі неекранованої витой пари - ділиться в міжнародних стандартах на категорії (від 1 до 7).

Волоконно-оптичний кабель схожий за своєю структурою на коаксіальний, не має екрануючої сітки. Світлові імпульси передаються по сердечнику, товщиною від 8 до 60 мкм, в залежності від типу оптоволоконного кабелю. Сердечник укладений в скляну оболонку з більш низьким коефіцієнтом заломлення, що перешкоджає виходу світла за межі сердечника. Захистом для скляної частини служить пластикова оболонка. Якщо промінь світла з кутом падіння, більше критичного, відбивається від стінок волокна, то і безліч променів - відбивається під різними кутами. Кожен промінь має - моду (кут відбиття), а оптичне волокно, що володіє властивістю передавати відразу декілька променів - многомодовое. Якщо зменшити діаметр волокна до декількох довжин хвиль світла - волокно діє як хвилевід - світло рухається по прямій лінії, без відбитків від стінок волокна.

Волокно - одномодовое - коштує дорожче, але може використовуватися при передачі даних на великі відстані.

Бездротові лінії зв'язку - сигнал переноситься за допомогою передавача і приймача радіохвиль. Діляться на радіоканали, що відрізняються частотним діапазоном і дальністю каналу: Діапазони коротких, середніх і довгих хвиль (КВ, СВ і ДВ) - діапазони амплітудної модуляції (Amplitude Modulation, АМ) за типом - методу модуляції сигналу - забезпечують далеку зв'язок при невисокій швидкості передачі даних. Діапазони ультракоротких хвиль (УКХ) - більш швидкісні канали і частотна модуляція (Frequency Modulation, FM). Діапазони надвисоких частот (НВЧ або microwaves).

У діапазоні СВЧ (понад 4ГГц) сигнали не відбиваються іоносферою Землі - для стійкого зв'язку потрібна наявність прямої видимості між передавачем і приймачем. Використовують супутникові канали або радіорелейні канали.

1.5 Канальний рівень. Технологія Ethernet

Метод доступу до середовища передачі CSMA / CD (множинний доступ з контролем несучої і виявленням колізій). Основні поняття:

- BT (Bit Time, бітовий інтервал) - тривалість передачі одного біта (10Мбіт - 100нс). Якщо 100Мбіт, то 10нс;

- IPG (Inter-Packet Gap, межпакетное щілину) - мінімальний інтервал між кадрами, $IPG = 96 \text{ BT}$. (кадр не може починатися один після іншого (приймач не зможе розділити де закінчився один пакет і почався інший), тому стандартом встановлений інтервал 96 BT);

- PDV (Path Delay Value, затримка в дорозі) - подвійний час (подвійна затримка) проходження сигналу між абонентами мережі. (включає затримку по кабелю, в самих мережевих адаптерах (передавач - приймач) і проміжних пристроях);

- ST (Slot time, час каналу, квант часу) - максимально допустимий PDV ($ST = 512 \text{ Bt}$ (верхній допустима межа затримки)). (системний час в мережі - мінімальний часовий інтервал, для виникнення події, визначається мінімальною тривалістю пакета) (якщо дві події в мережі відбуваються з тимчасовим зрушенням <ніж часовий інтервал, то вони відбуваються одночасно);

– максимальний діаметр мережі - допустима довжина мережі ($PDV = ST = 512 \text{ BT}$). (виходячи з ST (часу каналу) допустима довжина мережі, це десь виконується умова на максимальну затримку) більше цього розміру мережу бути не може;

– Jam (сигнал-пробка) - послідовність тривалістю 32 BT використовується для посилення колізії;

– Truncated binary exponential back off (усічена двоїчна експоненціальна відстрочка) - затримка перед повторною передачею пакета після колізії. (той часовий інтервал (тимчасова затримка) до початку повторної передачі).

Передача кадрів (пакетів канального рівня) в Ethernet. Далі розглянемо як відбувається передача кадрів. Часовий інтервал між кадрами 96 Бт. Більше може бути - менше ні.

Розглянемо докладніше алгоритм передачі. Перша частина - те, що відбувається на початку передачі, 2-а при передачі (рис.1.1, 1.2).

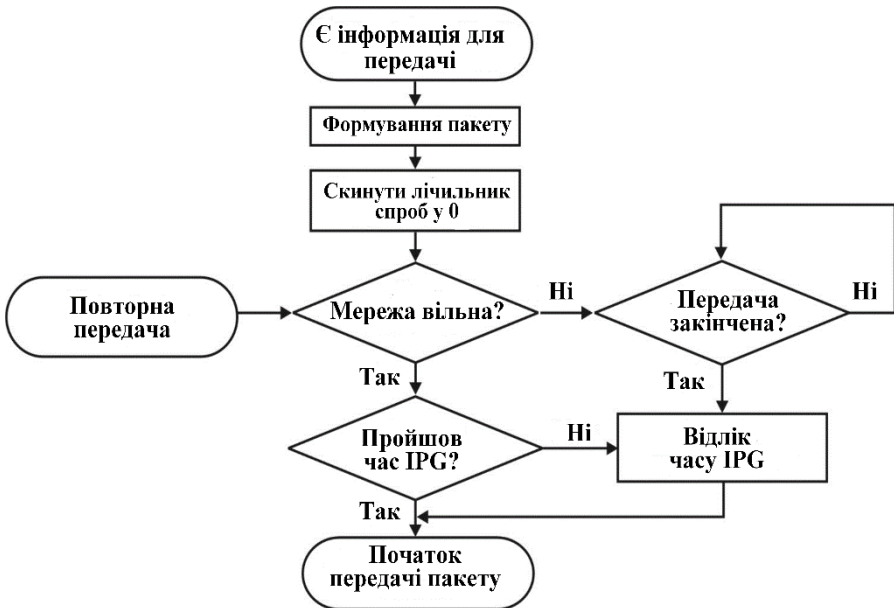


Рисунок 1.1 - Алгоритм початку передачі

Кількість повторів обмежено 16 спробами. Тому лічильник скидається в нуль. Якщо відбувається повторна передача. Ми переходимо на блок «Повторна передача».



Рисунок 1.2 - Алгоритм передачі пакету

Після передачі кожного біта перевіряємо є колізія чи ні. Якщо є то сигнал-пробка і перевірка лічильника спроб (16). Якщо менше 16, то повторна передача. Обчислення затримки повтору передачі. Затримка обчислюється по формулі:

$$\text{RAND}(0, 2 \min(N, 10)) \cdot ST, \quad (1.1)$$

де N - значення лічильника спроб; $\text{RAND}(a, b)$ — генератор випадкових нормально розподілених цілих чисел в діапазоні $a \dots b$, включаючи крайні значення; ST — квант часу, рівний 512 БТ; максимальна затримка дорівнює 1024 ST (524788 БТ). (так як N до 10) (затримка обчислюється як випадкове число в діапазоні від 0 до $2N$, (з кожною

наступною спробою діапазон затримок збільшується в 2 рази) і множиться на квант часу = 512 вт) (поки кількість спроб = 10).

У реальній мережі зазвичай 2-3 повтори, якщо мережа перевантажена (велика інтенсивність обміну) то може бути 4-5.

Як відрізнити, що кадри зіткнулися і пакет прийнятий неправильний. Маємо 3 ознаки. Ознаки спотвореного колізіїєю кадру:

- кадр має довжину, меншу мінімально допустимого розміру 512 ВТ (карликовий кадр) - якщо колізія сталася до 480-го біта кадру;
- кадр має неправильну контрольну суму - якщо колізія сталася після 480-го біта кадру, то сигнал-пробка (32 біта) грає роль контрольної суми;
- кадр має довжину, не рівну цілому числу байт, - якщо колізія сталася в середині одного з переданих байтів. (саме довжина кадру тільки ціле число байт).

1.6 Область колізій. Розрахунок PDV

Приклад формування двох доменів колізій (рис.1.3).

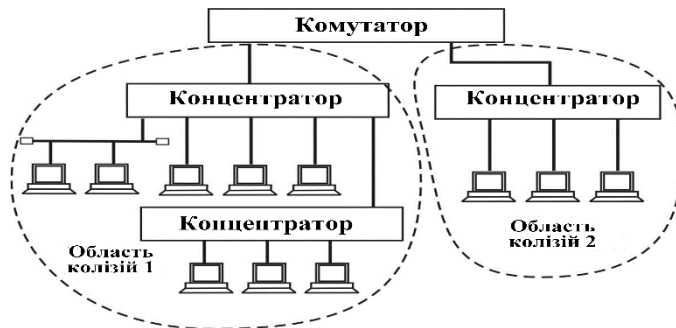


Рисунок 1.3 - Область колізії (Collision Domain)

Допустимі розміри мережі Ethernet визначаються:

- обмеження на довжину сегмента, пов'язані з загасанням і перекручуванням форми сигналу: 10Base5 - 500 м і правило "5-4-3", 10Base2 - 185 м і "5-4-3", 10BaseT/100BaseTX/100BaseT4 - 100 м;
- обмеження на кількість вузлів в домені - не більше 1024;

- обмеження на кількість повторювачів між будь-якою парою вузлів: Ethernet - 4, Fast Ethernet - 1 або 2, Gigabit Ethernet – 1;
- обмеження на розмір домену колізій, пов'язані з часом поширення сигналу між кінцевими вузлами мережі: час подвійного обороту для Ethernet, Fast Ethernet і Gigabit Ethernet не повинно перевищувати 512 bt та для Gigabit Ethernet (якщо використовується одномодове волокно) - 2048 bt.

Для мереж на мідних кабелях - досить виконати перші три умови. Подвійна затримка поширення сигналу (PDV) по шляху максимальної довжини не повинна перевищувати 512 ВТ. У затримку входять: затримки в мережевих адаптерах, затримки в концентраторах, затримки в кабелях. Обмеження на довжину кабелів і кількість концентраторів.

Зменшення міжпакетної щільності (ΔIPG) для будь-якого шляху не повинно перевищувати 49 ВТ. IPG зменшується при проходженні пакетів через концентратори. Обмеження на кількість концентраторів. Обидва умови повинні виконуватися для всієї мережі. На рисунку 1.4 та в таблиці 1.1 (значення затримок) наведено приклад, який відображає метод знаходження шляху максимальної довжини Ethernet.

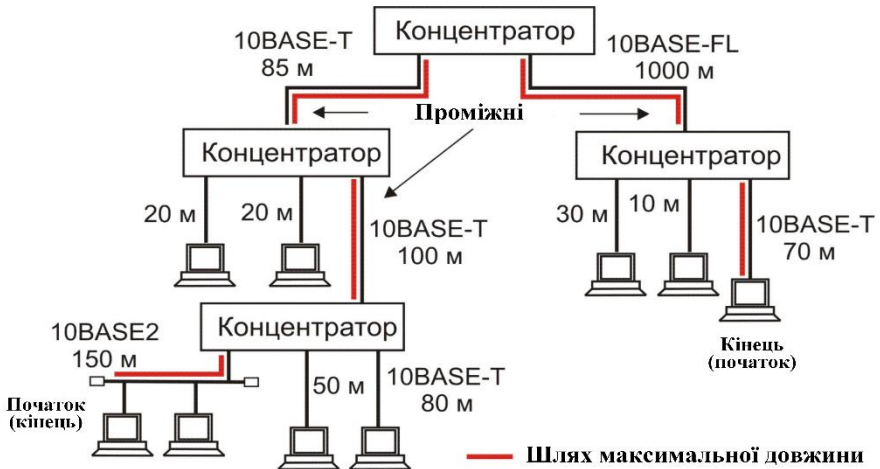


Рисунок 1.4 - Шлях максимальної довжини Ethernet

Таблиця 1.1 - Розрахунок PDV для мережі Ethernet (10 Мбит/с)

Тип сегменту	t_0 нач. сегм.	t_0 пром. сегм.	t_0 кінц. сегм.	t_1 на метр
10BASE5	11,8	46,5	169,5	0,087
10BASE2	11,8	46,5	169,5	0,103
10BASE-T	15,3	42,0	165,0	0,113
10BASE-F	12,3	33,5	156,5	0,100

При цьому $PDV = \sum PDV_s \leq 512$ ВТ, а $PDV_s = t_0 + L \cdot t_1$, де L — довжина кабелю сегменту в метрах. Для прикладу наведеного на рисунку 1.6 отримаємо:

$$PDV_1 = t_0 + L \cdot t_1 = 11,8 + 150 \cdot 0,103 = 27,25 \text{ ВТ}$$

$$PDV_2 = t_0 + L \cdot t_1 = 42 + 100 \cdot 0,113 = 53,3 \text{ ВТ}$$

$$PDV_3 = t_0 + L \cdot t_1 = 42 + 85 \cdot 0,113 = 51,6 \text{ ВТ}$$

$$PDV_4 = t_0 + L \cdot t_1 = 33,5 + 1000 \cdot 0,1 = 133,5 \text{ ВТ}$$

$$PDV_5 = t_0 + L \cdot t_1 = 165 + 70 \cdot 0,113 = 172,9 \text{ ВТ}$$

$PDV = \sum PDV_s = 27,25 + 53,3 + 51,6 + 133,5 + 172,9 = 438,55 \text{ ВТ} \leq 512 \text{ ВТ}$, що є підтвердженням працездатності мережі.

У випадку різних специфікацій на кінцях сегменту, розрахунок повторюємо у зворотному напрямку.

При проведенні розрахунку за іншим методом маємо наступну формулу $\Delta IPG = \sum \Delta IPG_s \leq 49$ ВТ. Дані затримок на сегментах беремо з довідкової таблиці. Враховуються тільки початковий і проміжні сегменти шляху. Кінцевий сегмент не враховується.

Для перевірки на допустимість розміру домену колізій складають топологічний план мережі, на якому зазначають типи активного обладнання, типи і довжину кабельних сегментів. Далі визначають час подвійного обороту для пари вузлів, максимально віддалених один від одного (час поширення сигналу).

Якщо час вписується у обмеження - мережа працездатна. Якщо PDV виявиться більше допустимого, доведеться змінювати топологію чи розбивати мережу на сегменти (домени колізій) меншого розміру і пов'язувати їх мостами, комутаторами чи маршрутизаторами.

Для розрахунку допустимого розміру мережі Fast Ethernet скористаємось значеннями затримок для кабелів, адаптерів та концентраторів, які наведено в таблицях 1.2 – 1.4.

Таблиця 1.2 - Затримки, які вносяться кабелем

Тип кабелю	Подвоєна затримка бітових інтервалів на один метр	Подвоєна затримка на кабель максимальної довжини
UTP 3	1,14 BT	114BT на 100м
UTP 4	1,14 BT	114BT на 100м
UTP 5	1.112 BT	111.3 на 100м
STP	1.112 BT	111.3 на 100м
оптоволокну	1	412

Таблиця 1.3 - Затримки, які вносяться адаптерами

Тип мережевих адаптерів	Максимальна затримка при подвійному обороті
Два адаптера TX/FX	100 BT
Два адаптера T4	138 BT
Один адаптер TX/FX і другий T4	127 BT

Таблиця 1.4 - Затримки, які вносяться концентраторами

Тип концентраторів (повторювачів)	Максимальна затримка при подвійному обороті (BT)
Концентратор класу 1	140
Концентратор класу два з портами TX/FX	92
Концентратор 2 кл. порти T4	67

Розглянемо мережу 100BaseTX з двома повторювачами класу II. Підсумуємо наступні затримки:

- пара адаптерів TX – 100 BT;
- два кабельних сегмента по 100 м і шнур між повторювачами (5 м) - $(100 + 100 + 5) \times 1,112 \text{ BT} = 227,96 \text{ BT}$;
- два повторювача TX класу II – $2 \times 92 \text{ BT} = 184 \text{ BT}$.

Разом: $100 \text{ BT} + 227,96 \text{ BT} + 184 \text{ BT} = 511,96 \text{ BT} < 512 \text{ BT}$ - обмеження дотримується, хоча майже без запасу. Правда, для кабелю категорії 5 в таблиці наводиться погонне подвійна затримка 1,112 bt / м, що відповідає швидкості поширення сигналу 0,6с (с - швидкість світла у вакуумі), але багато кабелів мають швидкість поширення в межах 0,67- 0,75с.

Якщо в розрахунок брати кабель зі швидкістю поширення 0,7 с, то він в даному випадку вносить подвійну затримку на 32 bt менше, що і забезпечує необхідний запас. При використанні сегмента максимальної довжини для 100BaseFX (412 м) місця для повторювача вже немає - останні 100 bt "з'їдає" пара адаптерів.

2 МУЛЬТИПЛЕКСУВАННЯ І КОМУТАЦІЯ

2.1 Мультиплексування

Для створення призначеного для користувача каналу при об'єднанні користувачів мережі лінією зв'язку комутатори первинних мереж повинні підтримувати техніку мультиплексування і комутації. Для мультиплексування абонентських каналів використовуються:

- частотне мультиплексування (Frequency Division Multiplexing, FDM);
- хвильове мультиплексування (Wave Division Multiplexing, WDM);
- часове мультиплексування (Time Division Multiplexing, TDM);
- множинний доступ з кодовим поділом (Code Division Multiple Access)

TDM - при комутації каналів і пакетів. FDM, WDM і CDMA - тільки для комутації каналів. CDMA - в техніці розширеного спектру - бездротова передача.

Комутація каналів на основі FDM - розроблена для телефонних мереж, застосовується для ПС (мікрохвильові канали) або мереж кабельного телебачення. Ідея методу - виділення кожному з'єднанню свого власного діапазону частот в загальній смузі пропускання лінії зв'язку. На основі діапазону створюється канал. Дані, що передаються в каналі, модулюються з використанням несучої частоти, що належить діапазону каналу.

Комутація каналів на основі методу TDM - розроблена при переході до цифрової форми представлення голосу, орієнтована на дискретний характер переданих даних. Принцип - виділення каналу кожному з'єднанню на певний період часу. Застосовують 2 типи тимчасового мультиплексування - асинхронний і синхронний.

Асинхронний - використовується в мережах з комутацією пакетів - пакет займає канал певний час, необхідний для його передачі між

кінцевими точками каналу. Між різними інформаційними потоками немає синхронізації, кожен користувач намагається зайняти канал тоді, коли у нього виникає потреба в передачі інформації.

У разі синхронного режиму TDM доступ всіх інформаційних потоків до каналу синхронізується так, щоб кожен інформаційний потік періодично отримував канал в своє розпорядження на фіксований проміжок часу. Мережі, що використовують TDM, вимагають синхронної роботи обладнання - друга назва - синхронний режим передачі (Synchronous Transfer Mode, STM).

Оптичне мультиплексування з поділом по довжинах хвиль WDM - технологія оптичного ущільнення - розробник. 1970-1980 рр - для оптичних синхронних систем та ж роль, що і мультиплексування з частотним поділом (FDM) для аналогових систем. Системи з WDM називають системами оптичного мультиплексування з частотним поділом (OFDM).

Але FDM і OFDM відрізняються не тільки використанням оптичного (OFDM) або електричного (FDM) сигналу. При FDM використовується механізм АМ модуляції з однією бічною смугою (ОЧП) та обраної системою несуть, модулюючий сигнал яких однаковий за структурою. При OFDM - несучі генеруються окремими джерелами (лазерами), сигнали яких просто об'єднуються мультиплексором в єдиний багаточастотний сигнал. Кожна його складова (несуча) може передавати потік цифрових сигналів різних синхронних технологій. 1 несуча передає АТМ трафік, 2 SDH, 3 PDH. Несучі модулюються цифровим сигналом відповідно до переданих трафіком.

В WDM - інформаційним сигналом є світло. Для організації WDM-каналів в волоконно-оптичному кабелі використовуються хвилі інфрачервоного діапазону довжиною від 850 до +1565 нм - відповідає частотам від 196 до 350 ТГц.

У магістральному каналі мультиплексується декілька спектральних каналів - до 16, 32, 40, 80 або 160, причому, починаючи з 16 каналів техніка мультиплексування - ущільнене хвильове мультиплексування (Dense Wave Division Multiplexing, DWDM). У середині спектрального каналу дані можуть кодуватися як дискретним способом, так і аналоговим.

2.2 Первинні мережі

Призначені для створення комутованої інфраструктури для швидкої і гнучкої організації постійного каналу з двоєточковою топологією між двома призначеними для користувача пристроями. У ПС - техніка комутації каналів.

Існує 4 покоління технологій первинних мереж: плезіохронна цифрова ієрархія (Plesiochronous Digital Hierarchy, PDH); синхронна цифрова ієрархія (Synchronous Digital Hierarchy, SDH), якій в Америці відповідає стандарт SONET; ущільнене хвильове мультиплексування (Dense Wave Division Multiplexing, DWDM); оптична транспортна мережа (Optical Transport Network, OTN).

PDH і SDH для поділу високошвидкісного каналу використовують тимчасове мультиплексування (TDM) і передають дані в цифровій формі. SDH забезпечує швидкості вище, ніж PDH - при побудові великої ПС - магістраль будується на технології SDH, а мережа доступу - на PDH.

DWDM - не є цифровими, надають користувачам виділену хвилю для передачі інформації.

Мережі PDH. Початок PDH - розробка мультиплексора T-1, що дозволяє в цифровому вигляді мультиплексувати, передавати і комутувати (на постійній основі) голосовий трафік 24 абонентів.

Для з'єднання великих телефонних станцій реалізована ідея утворення каналів з ієрархією швидкостей. Вона названа системою Т-каналів та стандартизована Американським інститутом стандартів (ANSI) і міжнародним комітетом ССІТТ - при стандартизації отримала назву PDH.

Аналогом систем Т-каналів в міжнародному стандарті - канали типу E-1, E-2 і E-3 з швидкостями - 2,048 Мбіт/с, 8,488 Мбіт/с і 34,368 Мбіт/с. Незважаючи на відмінності, в американській і міжнародній версіях PDH використовують одні і ті ж позначення для ієрархії швидкостей - DSn (Digital Signal).

На практиці в основному використовуються канали T-1 / E-1 і T-3 / E-3. Фізичний рівень технології PDH підтримує різні види кабелю: виту пару, коаксіальний і волоконно-оптичний кабель.

2.2.1 Мережі SONET / SDH

Недоліки PDH враховані і подолані розробниками технології синхронних оптичних мереж (Synchronous Optical NET, SONET), 1 варіант стандарту - в 1984р. Мета - створення технології, здатної передавати трафік всіх існуючих цифрових каналів рівня PDH (американських T1-T3 і європейських E1-E4) з високошвидкісної магістральної мережі на базі волоконно-оптичних кабелів з ієрархією швидкостей, вище ієрархії PDH до швидкості в декілька Гбіт/с.

В результаті роботи ITU-T і ETSI вдалося розробити міжнародний стандарт SDH (Synchronous Digital Hierarchy - синхронна цифрова ієрархія).

В SDH рівні швидкостей мають назву STM-N (Synchronous Transport Module level N - синхронний транспортний модуль рівня N).

Операції мультиплексування і введення-виведення виконуються за допомогою віртуальних контейнерів (Virtual Container, VC), в яких блоки даних PDH можна транспортувати через мережу SDH.

Крім блоків даних PDH в віртуальний контейнер поміщається службова інформація - заголовок шляху (Path OverHead, POH). В технології SDH визначено кілька типів VC, призначених для транспортування основних типів блоків даних PDH: VC-11 (1,5 Мбіт / с), VC-12 (2Мбіт / с), VC-2 (6 Мбіт / с), VC- 3 (34/45 Мбіт / с) і VC-4 (140 Мбіт / с). VC є одиницею комутації мультиплексорів SDH. У кожному мультиплексорі існує таблиця з'єднань (таблиця крос-з'єднань).

Для суміщення в рамках однієї мережі механізмів синхронної передачі кадрів з асинхронним повинні застосовуватися вказівні знаки. Концепція показників - ключова в SDH.

Показник визначає поточний стан VC в агрегованій структурі вищого рівня - трибутарному блоці (Tributary Unit, TU) або адміністративному блоці (Administrative Unit, AU). Трибутарні блоки об'єднуються в групи і входять в адміністративні блоки.

Група з N адміністративних блоків (Administrative Unit Group, AUG) утворює корисне навантаження кадру STM-N. Схема мультиплексування SDH надає різні можливості по об'єднанню потоків PDH. Для кадру STM-1 можна реалізувати: 1 потік E-4; 63 потоку E-1; 1 потік E-3, 42 потоку E-1.

2.2.2 Мережі DWDM

Технологія ущільненого хвильового мультиплексування (Dense Wave Division Multiplexing, DWDM) призначена для створення оптичних магістралей нового покоління, що працюють на мультигігабітних і терабітних швидкостях - інформація в оптоволокну передається одночасно великою кількістю світлових хвиль.

Основні функції обладнання DWDM - операції мультиплексування і демultipлексування, а саме - об'єднання різних хвиль в одному світловому пучку і виділення інформації кожного спектрального каналу із загального сигналу. Устаткування DWDM дозволяє передавати по одному оптичному волокну 32 і більше хвиль різної довжини в вікні прозорості 1550 нм - кожна хвиля може переносити інформацію зі швидкістю до 10 Гбіт / с.

Рекомендацією G.692 визначено два частотних плану (тобто набору частот, віддалених один від одного на деяку постійну величину):

- частотний план з розподілом частот між сусідніми каналами 100 ГГц ($\Delta\lambda \approx 0,8$ нм);
- частотний план з кроком 50 ГГц ($\Delta\lambda \approx 0,4$ нм), що дозволяє передавати в цьому ж діапазоні 81 довжину хвилі.

Компаніями випускається також обладнання, зване обладнанням високощільного хвильового мультиплексування (High-Dense WDM, HDWDM), здатне працювати з частотним планом з кроком 25 ГГц.

Волоконно-оптичні підсилювачі. Успіх DWDM визначило появу волоконно-оптичних підсилювачів - підсилюють світлові сигнали в діапазоні 1550 нм, без проміжного перетворення їх в електричну форму, як роблять регенератори в мережах SDH. В рекомендації ITU-T G.692 визначено три типи підсилювальних ділянок:

- L (Long) - ділянка складається максимум з 8 прольотів волоконно-оптичних ліній зв'язку та 7 оптичних підсилювачів, максимальна відстань між підсилювачами - до 80 км при загальній максимальній протяжності ділянки 640 км;
- V (Very long) - ділянка складається максимум з 5 прольотів волоконно-оптичних ліній зв'язку та 4 оптичних підсилювачів, максимальна відстань між підсилювачами - до 120 км при загальній максимальній протяжності ділянки 600 км;

– U (Ultra long) - ділянка без проміжних підсилювачів довжиною до 160 км.

Для протяжних магістралей між підсилювальними ділянками треба встановлювати DWDM-мультиплексори, які виконують регенерацію сигналу шляхом його перетворення в електричну форму і назад.

2.2.3 Оптична транспортна мережа

Оптична транспортна мережа (Optical Transport Network, OTN), описана в стандарті ITU G.709 - технологія цифрової інкапсуляції - ефективний і загальноприйнятий спосіб мультиплексування послуг на оптичних світлових шляхах. Визначає вимоги до оптичної транспортної ієрархії (OTN), структуру кадрів, заголовки, бітові швидкості і формати для упаковки корисного навантаження в оптичних мережах.

Структура сигналів OTN включає блок корисного навантаження оптичного каналу (Optical channel Payload Unit - OPU), куди відображається передається сигнал, блок даних (ODU), який забезпечує контроль маршрутних даних з кінця в кінець і підтримує моніторинг тандемі зв'язків - функція корисна для міждоменого транспорту і транспортний блок (OTU), що відповідає за корекцію помилок (FEC) і функції OAM для транспорту між точками параметрів завершення оптичного сигналу, де мають місце відновлення синхронізації, форми і потужності сигналу (3R).

Завдяки цій структурі реалізуються три найбільш важливі можливості OTN: підтримка функцій експлуатації, адміністрування і моніторингу (OAM) для довжин хвиль, незалежно від переданого на них типу трафіку.

Блок даних оптичного каналу ODU містить в заголовку поля, що забезпечують підтримку функцій автоматичної захисної комутації (APS), надаючи можливість упакувати Ethernet сигнал (GbE або 10GbE) в кадр OTN і отримати можливість його захисного перемикавання.

За рахунок розширених можливостей мультиплексування OTN різні типи трафіку - включаючи Ethernet, трафік систем зберігання даних, цифрове відео і SONET / SDH - можна передавати в одному кадрі транспортної одиниці оптичного каналу (Optical Transport Unit, OTU):

OTU-1 зі швидкістю 2,7 Гбіт / с, OTU-2 - 10,7 Гбіт / с, OTU-3 - 43 Гбіт / с або OTU-4 - 112 Гбіт / с.

OTN не тільки забезпечує мультиплексування послуг, а й адаптується до швидко змінних вимог замовника і підвищує ефективність управління оптичну мережу. Завдяки підтримці комплексного моніторингу продуктивності всього вищезгаданого мультисервісного трафіку цей протокол ідеально підходить для передачі даних за стандартом 10 Gigabit Ethernet (GbE) і надає операторам відмінну модель для управління якістю та усунення неполадок сервісів Ethernet. Оскільки OTN - повністю прозорий протокол, то адаптувати існуючі послуги не складає труднощів. Крім оптимізованого транспорту OTN (за допомогою площини управління) пропонує і необмежені можливості захисту і відновлення трафіку, що дозволяє операторам використовувати різноманітні угоди про рівень обслуговування (SLA).

2.3 Комутатори

Завдання сегментації мережі - поділ користувачів на групи (сегменти) з метою зменшення кількості клієнтів, які поділяють смугу пропускання - вирішена за допомогою пристрою, званого мостом (bridge). Міст - пристрій канального рівня моделі OSI (зазвичай двопортовий) - для об'єднання сегментів мережі. Міст не просто пересилає пакети даних з одного сегмента в інший, а аналізує і передає їх, якщо адреса робочої станції призначення належить іншому сегменту. Міст ізолює трафік одного сегмента від трафіку іншого, зменшуючи домен колізій і підвищуючи загальну продуктивність мережі. Ефективні - поки кількість робочих станцій в сегменті невелика. При їх збільшенні - перевантаження (переповнення буферів пристроїв) - втрата пакетів.

Комутатор - багатопортовий міст. Дозволяє встановити одночасно кілька з'єднань між різними парами портів. При передачі пакета через комутатор створюється окремий віртуальний (реальний) канал, по ньому дані надсилаються від порту-джерела до порту-одержувачу з максимально можливою для використовуваної технології швидкістю - принцип роботи отримав назву "мікросегментація".

Функціонування комутаторів локальної мережі. Комутатори локальних мереж обробляють кадри на основі алгоритму прозорого

моста (transparent bridge), який визначений стандартом IEEE 802.1D. Процес роботи алгоритму прозорого моста починається з побудови таблиці комутації (Forwarding DataBase, FDB).

Спочатку таблиця комутації порожня. При включенні харчування, разом з передачею даних, комутатор починає вивчати розташування підключених до нього мережевих пристроїв шляхом аналізу MAC-адрес джерел одержуваних кадрів.

Можна створювати статичні записи таблиці комутації вручну. Їм не присвоюється час старіння - час їх життя не обмежена. Статичну таблицю комутації використовують для підвищення мережної безпеки - гарантія, що тільки пристрої з певними MAC-адресами, можуть підключатися до мережі. Відключається автоматичне вивчення MAC-адрес на портах комутатора. Тільки в таблиці комутації з'являється хоча б один запис, комутатор починає використовувати її для пересилання кадрів.

Комутатор отримує кадр, відправлений комп'ютером А комп'ютеру В, він витягує з нього MAC-адреса приймача і шукає цей MAC-адреса в своїй таблиці комутації. Якщо запис знайдений, кадр буде переданий через відповідний вихідний порт (порт 2) - процес називається просуванням (forwarding) кадру.

Якщо вихідний порт і порт-джерело збігаються - переданий кадр відкидається комутатором. Процес називається фільтрацією (filtering). Якщо MAC-адреса приймача в кадрі невідомий (в таблиці комутації відсутній відповідний запис), комутатор створює безліч копій цього кадру і передає їх через всі свої порти, крім того, на який він вчинив. Процес називається лавинної передачею (flooding). Процес лавинної передачі дозволяє комутатора уникнути втрати кадрів, коли MAC-адреса приймача невідомий, і здійснювати процес самонавчання.

2.3.1 Методи комутації

У комутаторі реалізований один з трьох режимів роботи (методів комутації), що визначають його поведінку при отриманні кадру:

- комутація з проміжним зберіганням (store-and-forward); комутатор, перш ніж передати кадр, повністю копіює його в буфер і проводить перевірку на наявність помилок. Якщо кадр містить помилки (не збігається контрольна сума або кадр менше 64 байт або більше 1518 байт), він відкидається;

- комутація без буферизації (cut-through); комутатор копіює в буфер тільки MAC-адреса призначення (перші 6 байт після префіксу) і передає кадр, не чекаючи його повного прийому;

- комутація з виключенням фрагментів (fragment-free) - комутатор приймає в буфер перші 64 байт кадру, що дозволяє йому фільтрувати колізійні кадри перед їх передачею. Кадри довжиною більше 64 байт – правильні.

Конструктивне виконання комутаторів - три групи комутаторів:

- настільні комутатори (Desktop switch); мають відносно невелику кількість фіксованих портів (у D-Link від 5 до 16);

- автономні комутатори, монтовані в телекомунікаційну стійку (Rack mounted switch); в стоїчному виконанні мають корпус для монтажу в стійку, вбудований блок живлення і фіксовану кількість портів (у D-Link до 52-х);

- комутатори на основі шасі (Chassis switch) - містять слоти для встановлення інтерфейсних модулів розширення, резервних джерел живлення і процесорних модулів.

2.3.2 Характеристики продуктивності

Характеристики, що впливають на продуктивність комутаторів. Продуктивність комутатора - мережеві інтегратори і досвідчені адміністратори звертають увагу в першу чергу при виборі пристрою.

Характеризують продуктивність: швидкість фільтрації кадрів; швидкість просування кадрів; пропускна здатність; затримка передачі кадру.

Впливають на зазначені характеристики продуктивності: тип комутації; розмір буфера (буферів) кадрів; продуктивність комутуючої матриці; продуктивність процесора або процесорів; розмір таблиці комутації.

Швидкість фільтрації і просування кадрів - дві основні характеристики продуктивності комутатора. Є інтегральними показниками і не залежать від того, яким чином технічно реалізований комутатор.

Швидкість фільтрації (filtering) визначає швидкість, з якою комутатор виконує наступні етапи обробки кадрів: прийом кадру в свій буфер; відкидання кадру, в разі виявлення в ньому помилки (не

збігається контрольна сума, або кадр менше 64 байт або більше 1518 байт); відкидання кадру для виключення петель в мережі; відкидання кадру відповідно до налаштованими на порте фільтрами; перегляд таблиці комутації з метою пошуку порту призначення на основі MAC-адреси приймача кадру і відкидання кадру, якщо вузол-відправник і одержувач кадру підключені до одного порту.

Швидкість фільтрації практично у всіх комутаторів неблокують - комутатор встигає відкидати кадри в темпі їх надходження.

Швидкість просування (forwarding) - швидкість, з якою комутатор виконує наступні етапи обробки кадрів: прийом кадру в свій буфер; перегляд таблиці комутації з метою знаходження порту призначення на основі MAC-адреси одержувача кадру; передача кадру в мережу через знайдений по таблиці комутації порт призначення.

Вимірюються зазвичай в кадрах в секунду. За замовчуванням значення швидкостей фільтрації і просування даються для протоколу Ethernet і кадрів мінімального розміру, тобто кадрів довжиною 64 байт (без преамбули) з полем даних в 46 байт.

Пропускна здатність комутатора (throughput) - кількість призначених для користувача даних (в мегабитах або гігабіта в секунду), переданих в одиницю часу через його порти.

Затримка передачі кадру (forward delay) - час, що минув з моменту приходу першого байта кадру на вхідний порт комутатора до появи цього байту на його вихідному порту - складається з часу, що витрачається на буферизацію байт кадру і часу, що витрачається на обробку кадру комутатором (перегляд таблиці комутації), прийняття рішення про просування і отримання доступу до середовища вихідного порту.

Величина затримки залежить від використовуваного методу комутації. Якщо без буферизації - затримки звичайно невеликі і становлять від 5 до 40 мкс, а при повній буферизації кадрів - від 50 до 200 мкс (для кадрів мінімальної довжини).

Розмір таблиці комутації - гранична кількість MAC-адрес, якими може одночасно оперувати комутатор. У таблиці комутації для кожного порту можуть зберігатися динамічні і статичні MAC-адреси.

Трирівнева ієрархічна модель мережі. Ієрархічна модель включає в себе три логічних рівня: рівень доступу (access layer); рівень розподілу / агрегації (distribution layer); рівень ядра (core layer).

Для кожного рівня визначені свої функції. Три рівня не припускають наявності 3 різних пристроїв. Може бути як кілька пристроїв, так і один пристрій, яке виконує всі функції, визначені на двох сусідніх рівнях.

Рівень ядра знаходиться на самому верху ієрархії і відповідає за надійну і швидку передачу великих обсягів даних. Трафік, що передається через ядро, загальний для більшості користувачів. Призначені для користувача дані обробляються на рівні розподілу. Він при необхідності, пересилає запити до ядра.

Для рівня ядра велике значення має його відмовостійкість, оскільки збій може призвести до втрати зв'язності між рівнями розподілу мережі.

Рівень розподілу (рівень робочих груп) - сполучна ланка між рівнями доступу та ядра. Залежно від способу реалізації рівень розподілу може виконувати наступні функції: забезпечення маршрутизації, якості обслуговування та безпеки мережі; агрегування каналів; перехід від однієї технології до іншої (від 100Base-TX до 1000Base-T). Рівень доступу управляє доступом користувачів і робочих груп до ресурсів об'єднаної мережі. Основне завдання - створення точок входу / виходу користувачів в мережу. Рівень виконує наступні функції: управління доступом користувачів і політиками мережі; створення окремих доменів колізій (сегментація); підключення робочих груп до рівня розподілу; використання технології комутованих локальних мереж.

3 МЕРЕЖНИЙ РІВЕНЬ. АДРЕСАЦІЯ. МАРШРУТИЗАЦІЯ

Мета: отримати базові навички проведення розрахунків для отримання бажаного розміру MTU при передачі пакетів між мережами, які побудовані за різними технологіями каналного рівня. Отримати базові навички налаштування мережних з'єднань з використанням IP-адресації протоколу версії IPv4.

3.1 Максимальна одиниця передачі MTU

MTU (Maximum Transmission Unit - максимальна одиниця передачі). MTU - максимальний розмір пакета даних, який може бути

переданий за один фізичний кадр по стеку протоколів TCP/IP. При установці нового з'єднання два віддалених комп'ютера повинні узгодити між собою розмір кадру. Окрім того слідуючи до місця призначення, пакет долає цілий ряд проміжних серверів і маршрутизаторів, настройки MTU яких можуть бути абсолютно різними. Тому занадто великий пакет в мережі фрагментується і заповнюється «повітрям», «баластом», що негативно позначається на ефективності зв'язку. Якщо провайдер має установки MTU = 576, а у вас в Windows задано MTU = 1500, то кожний пакет розбивається на три по 576 байт: $576 + 576 + 576 = 1728$ - тобто, 228 байт баласту додаються до кожного пакету. Але навіть якщо провайдер теж має MTU = 1500, то при зв'язку з віддаленим сервером цілком може бути задіяний маршрутизатор з меншим значенням MTU і пакети знову-таки фрагментуватимуться, сповільнюючи передачу даних. Цю ситуацію рятує включена в Windows, за замовчуванням, функція автоматичного визначення MTU - «PMTU Discovery» або «MTU Auto Discovery». Але процедура обчислення MTU для кожного з'єднання вимагає багато часу, що може затримувати роботу при передачі невеликих файлів. Окрім того, у разі неузгодження ваших параметрів з параметрами провайдера, ця функція навряд чи вам допоможе. Звичайно, існують загальноприйняті стандарти для даного параметра, так, наприклад, для Ethernet MTU = 1500 байт, для SLIP - 1006, для PPPoE -1492, для PPP, тобто модемного зв'язку з Інтернетом - 576.

Кожен пакет даних в дійсності складається з декількох сегментів - заголовка і фактичних даних. Формат стандартного заголовку IP-пакету (на прикладі протоколу IPv4) наведено на рисунку 3.1.

4 біта Номер версії	4 біта Довжина заголовку	8 біт Тип сервісу				16 біт Загальна довжина			
		PR	D	T	R				
16 біт Ідентифікатор пакету						3 біта флаги	13 біт Зсув фрагменту		
						DF			
8 біт Час життя (TTL)		8 біт Протокол верхнього рівня				16 біт Контрольна сума			
32 біти IP-адреса джерела									
32 біти IP-адреса приймача									
Поле параметрів									

Рисунок 3.1 – Структура заголовку IP-пакету

Поле **номер версії** займає 4 біта і ідентифікує версію протоколу IP. Зараз використовується версія 4 (IPv4), але часто зустрічається і нова версія (IPv6).

Довжина заголовка IP-пакета займає 4 біта і вимірюється в 32-бітових словах. Зазвичай заголовок має довжину в 20 байт (п'ять 32-бітових слів). Найбільша довжина заголовка складає 60 байт.

Тип сервісу (Type of Service, ToS) - байт диференційованого обслуговування, або DS-байт. Зберігає ознаки, які відображають вимоги до якості обслуговування пакета. Перші три біти - значення пріоритету пакета: від найнижчого - 0 до найвищого - 7. Наступні три біта - критерій вибору маршруту. Якщо біт D (Delay - затримка) встановлений в 1, то маршрут вибирається з мінімізацією затримки доставки пакету, якщо встановлено в 1 біт T (Throughput - пропускна здатність) - для максимізації пропускної здатності, а біт R (Reliability - надійність) - для максимізації надійності доставки. Решта - два біти, мають нульове значення.

Поле загальної довжини займає 2 байти і характеризує загальну довжину пакета з урахуванням заголовка і поля даних. Максимальна довжина пакета обмежена розрядністю поля, яка визначає цю величину - 65535 байт. Залежить від максимальної довжини пакета протоколу нижнього рівня. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною 1500 байт.

Ідентифікатор пакету займає 2 байти і використовується для розпізнавання пакетів, при фрагментації вихідного пакета. Всі фрагменти одного пакету повинні мати однакове значення цього поля.

Флаги займають 3 біта і містять ознаки, пов'язані з фрагментацією. Встановлений в 1 біт DF (Do not Fragment - не фрагментований) забороняє маршрутизатора фрагментувати даний пакет, а встановлений в 1 біт MF (More Fragments - більше фрагментів) говорить про те, що даний пакет є проміжним (не останнім) фрагментом. Біт, який залишився - зарезервований.

Поле зсуву фрагмента займає 13 біт і задає зсув у байтах поля даних цього фрагмента відносно початку поля даних вихідного не фрагментованого пакета. Використовується при складанні/розбиранні фрагментів пакетів. Зміщення повинно бути кратним 8 байтам.

Поле часу життя (Time To Live, TTL) - 1 байт, задає граничний термін, протягом якого пакет може переміщатися по мережі. Час життя пакету вимірюється в секундах і задається джерелом пакетів.

Поле протоколу верхнього рівня - один байт - ідентифікатор, який вказує, якому протоколу верхнього рівня належить інформація, яка розміщена в полі даних пакета. Значення ідентифікаторів для протоколів (RFC 1700), за адресою <http://www.iana.org>. 6 - в пакеті знаходиться повідомлення TCP, 17 - повідомлення UDP, 1 - повідомлення ICMP.

Контрольна сума заголовка - 2 байти, розраховується тільки по заголовку.

Поля IP-адрес джерела і приймача мають довжину - 32 біта.

Поле параметрів - необов'язково і використовується тільки при налагодженні мережі. Так як число підполів в полі параметрів може бути довільним, то в кінці заголовка має бути додано декілька нульових байтів для вирівнювання заголовка пакета по 32-бітній границі.

Та частина пакету, в якій містяться тільки фактичні дані, називається MSS (Maximum Segment Size) - це ще один параметр протоколу TCP, що визначає найбільший сегмент даних TCP, які можуть бути передані за один раз.

Тобто, $MTU = MSS + \text{заголовки TCP/IP}$. У реєстрі MSS задається так: **HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ VxD \ MSTCP "DefaultMSS" = "ваше число"**.

Для заголовка теж є загальноприйнятий розмір - це 40 байт (20 байт IP і 20 байт TCP), зазвичай $MSS = MTU - 40$. З цієї причини у визначенні оптимального розміру MTU є деякі тонкощі.

Давайте на прикладі розглянемо передачу даних при різному розмірі MTU по широкосмуговій лінії T1 (пропускна здатність $T1 = 1544000 \text{ bits/sec}$), використовуючи наступну формулу: $[(MSS + \text{заголовок}) * 8 \text{ бітів / байт}] / [1544000 \text{ біт / sec}] = \text{затримка на один хоп}$ (на кожен комп'ютер в мережі при передачі нашого пакета).

Використовуючи в цій формулі різні величини MTU, ми можемо обчислити затримку одного пакета. Якщо $MTU = 1500$, тоді: $(1460 + 40) * 8 / 1544000 = 0.7772 \text{ ms}$. Якщо ж $MTU = 576$, то: $(536 + 40) * 8 / 1544000 = 0.2924 \text{ ms}$. Припустимо, що при передачі пакету зустрічається 10 серверів (хопов), тоді при $MTU = 1500$ отримаємо затримку 7.772 ms , а при $576 - 2.924 \text{ ms}$ - різниця досить помітна - очевидно, якщо пакети менші за розміром, то вони передаються швидше (через обмеження продуктивності лінії). Однак не все так просто.

Використовуючи ту ж формулу порахуємо, за який проміжок часу буде переданий файл розміром 1Mb за тією ж широкосмуговою

лінією T1. Один мегабайт дорівнює 1024 KB і дорівнює 1048576 байтам. Якщо MTU = 1500, то, як ми з'ясували, затримка на один хоп складе 0.7772 ms. Скільки при цьому знадобиться послати пакетів? $1 \text{ Mb} / \text{MSS} = 1048576 / 1460 = 718.2$, або всього потрібно 719 ефективних пакетів, щоб передати 1 мегабайт. Далі, множимо 719 пакетів на 0.7772 ms, отримуємо 558.8068 ms, або 5.588 секунд затримки на один хоп. Якщо ж ми передаємо свій файл через 10 хопів (ситуація зустрічаються частіше, ніж коли через один), то отримуємо 55.88 сек - час, який ми (вірніше, провайдер, який має лінію T1) витратили на передачу файлу в 1Mb при ідеальному зв'язку.

Якщо ж MTU = 576, тоді: $1 \text{ Mb} / \text{MSS} = 1048576 / 536 = 1956.3$, або потрібно 1957 пакетів, щоб передати 1 мегабайт. Далі, множимо кількість пакетів на затримку кожного з них: $1957 * 0.2924 = 572,2268 \text{ ms}$, або 5,722 секунди на один хоп. Ну і відповідно на 10 хопів доведеться витратити 57,22 секунд. Як бачимо, через те, що при використанні великих пакетів передається менше заголовків, реальна швидкість передачі файлу виходить вище.

Для того, щоб передати 1 мегабайт при використанні MTU = 1500, доводиться пересилати ще й «додаток» заголовків з 28760 байтів, тоді як при використанні MTU = 576 отримуємо аж $1957 * 40 = 78,280$ байтів, тобто додаткові 49520 байт заголовків на кожен мегабайт корисної інформації.

Для нашої 10-хопової передачі це виливається в зайвих 1,34 секунди при передачі кожного мегабайту навіть при швидкому зв'язку. Ця різниця, можливо, буде ще трохи вище на практиці, оскільки сучасні реалізації TCP / IP використовують більші за розміром заголовки.

При підключенні до Інтернету в термінальному режимі – іноді, при здійсненні реєстрації користувачем, в одному з рядків з'являється рекомендоване значення MTU. Для ручного визначення MTU досить використовувати стандартну утиліту ping:

PING -f -l уууу xxx.xxx.xxx.xxx -n 10,

де «xxx.xxx.xxx.xxx» - IP-адреса тестованого сервера, «-l» (англійська літера «ель», а не одиниця), уууу - розмір буфера відправки (MTU) від 576 до 1492 байт (наприклад $1500 = 1472 + 28$, де 1472 - розмір неподільного пакету, $28 = 20$ байт заголовок IP + 8 байт ICMP. для Ethernet MTU = 1500 байт, для SLIP - 1006, для PPPoE -1492, для PPP (модемного зв'язку) - 576. Таким чином можна вручну підібрати найбільш відповідне значення MTU для вашого з'єднання. Припустимо

ми визначили, що для нас оптимальним є розмір буфера відправки рівний 1500. Додаємо необхідні дані до реєстру.

Значення MTU

```
HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services
\ Class \ NetTrans \ 000x "MaxMTU" = "1500"
```

```
HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services
\ VxD \ MSTCP
```

MSS (розмір корисних даних) = ab.1 & 6mb.co & m & ab.16mb.com MTU – 40 "DefaultMSS" = "1460"

```
HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services
\ VxD \ MSTCP
```

Розмір буфера, в якому накопичується вміст області даних (MSS) декількох отриманих пакетів, перш ніж передається далі, наприклад, в браузер. Розмір RWIN обов'язково повинен бути кратний MSS і зазвичай для кращої ефективності модемного з'єднання рекомендується його встановлювати рівним 4-8 MSS.

Проте надмірно великий розмір буфера також небажаний, особливо на поганих лініях - при втраті всього одного пакета в разі збою на лінії буде повторно затребуваний не один втрачений пакет, а всі пакети з цього буфера, що займе деякий час - $1460 * 4 = 5840$ "DefaultRcvWindow" = "5840"

3.2 IP-адресація

IP-адреси являють собою основний тип адрес, на підставі яких мережний рівень передає пакети між мережами. Мережну адресу встановлює користувач (адміністратор) або вона призначається динамічно, протоколом DHCP з діапазону виділених адрес.

Мережна адреса має бути достатньо довгою (в IP-мережах версії IPv4 вона містить 32 біта (4 байти)), що дорівнює $2^{32} = 4294967296$ та ієрархічною (на відміну від MAC-адрес інтерфейсів).

4-х байтова адреса може бути представлена у різних системах числення: десятковій, двійковій, шістнадцятковій:

175.100.220.14;

10101111 01100100 11011100 00001110;

A F 6 4 D C 0 E

Незважаючи на те, що в третьому випадку цифр менше, поширеним є десяткове подання, точніше точково-десяткове. Частина

адреси (старші розряди) є номером мережі, а інша частина (молодші розряди) - номером вузла в мережі.

Виходячи з того, яка частина адреси відноситься до номера мережі, а яка - до номера вузла, адреси діляться на 5 класів: А, В, С, D та Е. Для унікальної адресації вузлів використовуються тільки три перших класи адрес.

В адресі класу А старший байт задає адресу мережі, а три молодших байти - адресу вузла (host). $0.x.y.z$ - $127.x.y.z$ - мереж $2^7 - 2$ (не може бути 0 і 127) = 126 мереж, вузлів $2^{24} = 16$ млн.

В адресі класу В два старших байти задають адресу мережі, а два молодших байти - адресу вузла (host). $128.x.y.z$ - $191.x.y.z$ - мереж $2^{14} = 16$ тис., Вузлів $2^{16} = 64$ тис.

В адресі класу С три старших байти задають адресу мережі, а молодший байт - адресу вузла. $192.x.y.z$ - $223.x.y.z$ - мереж $2^{21} = 2$ млн., Вузлів $2^8 = 256$.

Існує також багатоадресний клас D і резервний клас Е.

Номер вузла (адреса host) не може складатися тільки з одних одиниць або нулів. Якщо в поле адреси вузла всі нулі, це означає, що задається номер (адреса) мережі або підмережі.

Приватні адреси:

- $10.0.0.0$ - $10.255.255.255$ / 8;
- $172.16.0.0$ - $172.31.255.255$ / 12;
- $192.168.0.0$ - $192.168.255.255$ / 16.

Особливі адреси:

- IP-адреса $0.0.0.0$;
- IP-адреси з нульовим номером мережі є поточною мережею;
- адреса, яка складається з усіх одиниць, забезпечує широкомовлення в межах поточної (зазвичай локальної) мережі - $255.255.255.255$;
- адреси, в яких вказана мережа, але з усіма одиницями в поле номера хоста, забезпечують широкомовлення в межах віддаленої локальної мережі;
- адреси, які мають вид $127.x.y.z$ зарезервовані для тестування мережного програмного забезпечення методом зворотної передачі;
- $169.254.0.0/16$ ($169.254.0.1$ - $169.254.255.255$) - zeroconf.

Маски. У класовій адресації маємо недоцільність використання адресного простору для невеликих мереж, тому введене додаткове поле, що має назву - маска мережі.

Маска - 32 бітове число, яке використовується в парі з IP-адресою. Двійковий запис маски містить послідовність одиниць в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі - цільна частина адреси, то одиниці в масці повинні представляти безперервну послідовність.

Додаючи кожній IP-адресі маску, можна відмовитися від понять класів адрес і зробити систему адресації більш гнучкою.

Нехай для IP-адреси 129.64.134.5 вказана маска 255.255.128.0. Якщо ігнорувати маску, то відповідно до системи класів 129.64.134.5 відноситься до класу В, тому номер мережі - перші два байти - 129.64.0.0, а номер вузла - 0.0.134.5.

Якщо ж використовувати для визначення границі номеру мережі маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, «накладені» на IP-адресу, ділять його на наступні дві частини: номер мережі 10000001. 01000000. 1 (129.64.128.0) і номер вузла 0000110. 00000101 (0.0.6.5). Маршрутизатор, отримавши пакет, з адресою призначення отримує адресу мережі, яку реалізує шляхом логічного множення мережної адреси вузла на маску.

Маски змінної довжини. Використовуючи маски різної довжини для створення підмереж, адміністратор може формувати підмережі різного розміру в межах однієї автономної системи. Таким чином, маски змінної довжини (Variable-Length Subnet Mask - VLSM) дозволяють створювати підмережі різного розміру, при цьому гнучко задаючи границі між полем адреси мережі і полем адреси вузла.

VLSM дають можливість задіяти більше ніж одну маску підмережі в межах виділеного адресного простору мережі.

3.3 Приклади вирішення завдань

Розглянемо **практичне завдання з визначення класу мережі та типу адреси.** Для наведених адрес маємо:

- 201.10.255.0 – клас С, адреса мережі;
- 190.195.0.255 – клас В, адреса вузла;
- 9.255.255.255 – клас А, широкомовна адреса;

- 10.10.255.0 – клас А, адреса вузла;
- 134.11.255.255 – клас В, ширококомовна адреса;
- 252.250.0.255 – клас Е, зарезервована адреса;
- 194.18.144.25 – клас С, адреса вузла;
- 129.77.0.0 – клас В, адреса мережі;
- 237.101.5.0 – клас D, групова адреса;
- 126.0.0.0 – клас А, адреса мережі.

Наведемо приклад **застосування маски для визначення номера мережі і діапазону вузлів** маючи IP-адресу і маску.

Нехай задана IP-адреса: 210.56.78.212. Віднесемо до неї маску 255.255.255.224 (префікс / 27) (в двійковому вигляді). Що тепер номер мережі, а що номер вузла?

Представимо у двійковому вигляді адресу, виконаємо логічне множення на маску, та отримаємо адресу мережі - 210.56.78.192.

Кількість вузлів маємо 2^5 (кількість нулів у масці = 5) = 32 - 2 (адреса мережі і ширококомовна адреса) = 30.

Отримаємо діапазон адрес даної мережі:

- адреса першого вузла - 210.56.78.193;
- адреса останнього вузла - 210.56.78.222;
- ширококомовна адреса - 210.56.78.223.

У ряді випадків для зручності управління адміністратор може самостійно формувати підмережі всередині виділеного діапазону.

Розглянемо **практичне завдання з формування підмереж із однаковою кількістю вузлів**. Почнемо з формування мереж класу С.

Маємо адресу мережі - 212.24.222.0 / 24.

Розділимо її на 2 підмережі, для цього використовуємо 1 біт маски. Маска збільшиться на 1.

212.24.222.0 | 0000000 / 25 (255.255.255.128)
255.255.255.1 |

Перша підмережа 212.24.222.0 / 25.

Діапазон адрес - 212.24.222.1 - 212.24.222.126, 212.24.222.127 - ширококомовна адреса.

Друга підмережа 212.24.222.128 / 25.

Діапазон адрес - 212.24.222.129 - 212.24.222.254, 212.24.222.255 - ширококомовна адреса.

Маючи маску 255.255.255.224 (/27) можемо отримати 2^3 підмереж і 2^5-2 вузлів.

Якщо адміністратору виділена адреса мережі класу С (дорівнює 198.11.163.0) і йому необхідно створити 10 комп'ютерних підмереж по 14 вузлів, то для адресації 10 підмереж потрібно 4 розряди адреси (4 біта). У цьому випадку максимально можна бути задати 16 підмереж по 14 вузлів у кожній. З 16 підмереж адміністратор використовує 10, а решта 6 використовуватися не будуть (резервні). У практичних випадках мережі формуються з різною кількістю вузлів в мережі.

Розглянемо практичне завдання з формування підмереж з використанням масок змінної довжини.

Дана адреса мережі **200.33.224.0/24** і маска, необхідно сформуванати **9** підмереж: 3 підмережі на 50 вузлів; 3 підмережі на 10 вузлів; 1 підмережа на 4 вузла; 2 підмережі на 2 вузли.

Після збільшення маски на 2 біти (**200.33.224. |00| 000000**) маємо наступні підмережі:

- **200.33.224.0/26** – перша на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.1-200.33.224.62 – діапазон;
- 200.33.224.63 – широкомовна адреса;
- **200.33.224.64/26** – друга на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.65-200.33.224.126 – діапазон;
- 200.33.224.127 – широкомовна адреса;
- **200.33.224.128/26** – третя на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.129-200.33.224.190 – діапазон;
- 200.33.224.191 – широкомовна адреса;
- **200.33.224.192/26** – підмережа на 62 вузли (цю ділимо далі по

10 вузлів).

Після збільшення маски на 2 біти (**200.33.224. 11 |00| 0000**) маємо наступні підмережі:

- **200.33.224.192/28** – четверта на 14 вузлів (на 10 вузлів);
- 200.33.224.193-200.33.224.206 – діапазон;
- 200.33.224.207 – широкомовна адреса;
- **200.33.224.208/28** – п'ята на 14 вузлів (на 10 вузлів);
- 200.33.224.209-200.33.224.222 – діапазон;
- 200.33.224.223 – широкомовна адреса;
- **200.33.224.224/28** – шоста на 14 вузлів (на 10 вузлів);
- 200.33.224.225-200.33.224.238 – діапазон;
- 200.33.224.239 – широкомовна адреса;

– **200.33.224.240/28** - підмережа на 14 вузлів (цю ділимо далі по 4 вузли).

Після збільшення маски на 1 біт (**200.33.224. 1111 |0| 000**) маємо наступні підмережі:

- **200.33.224.240/29** – сьома на 6 вузлів (виділяємо на 4 вузли);
- 200.33.224.241-200.33.224.246 – діапазон;
- 200.33.224.247 – широкомовна адреса;
- **200.33.224.248/29** - підмережа на 6 вузлів (цю ділимо далі по 2 вузли).

Після збільшення маски на 1 біт (**200.33.224. 11111 |0| 00**) маємо наступні підмережі:

- **200.33.224.248/30** – восьма на 2 вузли;
- 200.33.224.249-200.33.224.250 – діапазон;
- 200.33.224.251 – широкомовна адреса;
- **200.33.224.252/30** – дев'ята на 2 вузли;
- 200.33.224.253-200.33.224.254 – діапазон;
- 200.33.224.255 – широкомовна адреса.

Таким чином отримали 9 підмереж із різною кількістю вузлів.

3.4 Маршрутизація

Маршрутизація без таблиць:

- лавинна - кожен роутер передає пакет всім своїм сусідам по всім активним інтерфейсів, крім того, від якого його отримав;
- маршрутизація, керована подіями - пакет до певної мережі призначення надсилається за маршрутом, вже наводив раніше до успіху (для даної адреси призначення);
- маршрутизація від джерела - відправник поміщає в пакет інформацію, які хопи повинен пройти пакет до мережі призначення.

Маршрутизація на основі таблиць:

- статична «фіксована» - таблиці вводяться в пам'ять кожного роутера вручну адміністратором мережі. Всі записи в таблиці мають статус статичних з нескінченний терміном життя; таблиця має, як мінімум п'ять стовпців: адреса мережі - мережа або окремих ір-адреса, куди повинен бути доставлений пакет. Маска мережі - щоб однозначно ідентифікувати сіть. Шлюз - для передачі пакетів з різними адресами призначення. Інтерфейс (номер порту) - ініціалізує інтерфейс, з якого

буде відправлений пакет. Метрика - число, що характеризує канал зв'язку;

- адаптивна (динамічна) - всі зміни конфігурації мережі автоматично вносяться в таблиці роутерів протоколами маршрутизації. У таких таблицях є запис ttl маршруту (час життя в секундах). Якщо після закінчення часу існування маршруту не підтверджується протоколом маршрутизації, то він вважається неробочим.

Для маршрутизації в ір-мережах застосовуються протоколи, в яких маршрут вибирається за різними варіантами критеріїв, пов'язаних зі зменшенням часу проходження пакету і якістю маршруту (критерії: найкоротша відстань (кількості роутерів на шляху пакета - хопів), пропускна здатність каналів між роутерами, надійність каналів, латентність (затримка (доставки даних) - збільшує час відгуку)).

Основою протоколу маршрутизації є алгоритми маршрутизації, які застосовуються для визначення найкращого шляху пакетів від джерела до приймача.

Для подання роботи алгоритмів маршрутизації мережа представляється графом. Вузлами графа є маршрутизатори, а ребрами - фізичні лінії зв'язку між ними. Кожній грані відповідає певне число - вартість, що залежить від довжини лінії зв'язку, швидкості передачі даних або фінансової вартості лінії.

Протокол маршрутизації формує в роутерах узгоджені один з одним таблиці маршрутизації, які забезпечують доставку пакета від вихідної мережі в мережу призначення за кінцеве число кроків. Таблиця може бути статична, або динамічна.

Який шлях оптимальний - визначається метрикою - умовна вартість передачі по мережі. Повна вартість маршруту дорівнює сумі метрик мереж, по маршруту. Маршрутизатор вибирає маршрут з найменшою метрикою.

Алгоритми маршрутизації діляться на 2 групи:

- дистанційно-векторні алгоритми (distance vector). Кожен роутер періодично ширококомовно розсилає по мережі вектор відстаней від себе до всіх відомих йому мереж. Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. Приклад - протокол гір;
- алгоритми стану зв'язків (link state) забезпечують кожен роутер інформацією для побудови точного графа зв'язків мережі. Всі

роутери працюють на підставі одного й того ж графа. Приклад - протокол ospf.

Протокол rip (routing information protocol) - протокол маршрутної інформації. Алгоритм роботи протоколу:

- крок 1 - створення мінімальної таблиці. У початковому стані в кожному роутері програмним забезпеченням стека tcp / ip автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються тільки безпосередньо приєднані мережі;

- крок 2 - розсилка мінімальної таблиці сусідам. Після ініціалізації кожен роутер починає посилати своїм сусідам повідомлення протоколу rip, в яких міститься його мінімальна таблиця;

- крок 3 - отримання rip-повідомлень від сусідів і обробка отриманої інформації. Після отримання повідомлень від сусідів роутер нарощує кожне отримане поле метрики на одиницю і запам'ятовує, через який порт і від якого роутера отримана нова інформація. Потім роутер порівнює нову інформацію з тією, яка зберігається в таблиці маршрутизації;

- крок 4 - розсилка нової таблиці сусідам. Далі - до кроку 3.

Щоб отримувати попередження - маршрут недійсний, rip використовує два механізми:

- закінчення ttl маршруту. У протоколі rip період розсилки - 30 секунд, а ttl маршруту - 180 секунд;

- вказівка нескінченного відстані до недоступної мережі. В rip нескінченим умовно вважається відстань 16 хопів.

Протокол ospf (open shortest path first) - вибір найкоротшого шляху першим. Алгоритм роботи протоколу:

- крок 1 - кожен роутер будує граф зв'язків мережі, в якому вершинами є роутери і ip-мережі, а ребрами - інтерфейси роутерів. Всі роутери обмінюються зі своїми сусідами тією інформацією про графа мережі, якою вони володіють до даного моменту. Повідомлення, за допомогою яких поширюється топологічна інформація, називаються оголошеннями про стан зв'язків мережі (link state advertisements, lsa);

- крок 2 - знаходження оптимальних маршрутів за допомогою отриманого графа. Завдання вирішується за допомогою алгоритму дейкстри. Алгоритм дейкстри обчислює найкоротший шлях між двома точками в мережі, використовуючи граф за методом вузлів і кордонів.

При цьому кожен роутер вважає себе центром мережі і шукає оптимальний маршрут до кожної відомої йому мережі.

Всі протоколи маршрутизації можна розділити на дві великі групи: зовнішні (EGP - Exterior Gateway Protocol) і внутрішні (IGP - Interior Gateway Protocol). Щоб пояснити відмінності між ними - потрібно термін "автономна система".

Маршрутизація Інтернет функціонує в межах автономних систем. АС (домен маршрутизації) - сукупність мереж (група роутерів) під єдиним адміністративним керуванням, що забезпечує загальну політику маршрутизації.

Автономні системи з'єднуються зовнішніми шлюзами. Реєстрація АС відбувається централізовано.

Номер АС - 16 розрядів (65535). Інтернет - набір взаємопов'язаних АС, що забезпечує багаторівневий підхід до маршрутизації: маршрут визначається як послідовність АС, потім - як послідовність мереж, а потім - веде до кінцевого вузла.

АС може належати до наступних категорій: обмежена (stub) AS; многоінтерфейсна (multihomed) AS; транзитна (transit) AS.

Загальна топологія Internet складається з транзитних, многоінтерфейсних і обмежених автономних систем.

Протокол граничної маршрутизації (BGP - Border Gateway Protocol) - це протокол маршрутизації між автономними системами. Він заснований на методах маршрутизації, які називаються "маршрутизація вектором шляху".

Маршрутизація з використанням вектору шляхів відрізняється і від маршрутизації з використанням вектору довжини маршруту, і від маршрутизації станом лінії. Кожен вхід в таблицю маршрутизації містить мережу пункту призначення, наступний маршрутизатор і шлях до пункту призначення. Шлях зазвичай визначається як впорядкований список автономної системи, який повинен пройти пакет для досягнення пункту призначення.

Автономний граничний маршрутизатор - бере участь в маршрутизації з використанням вектора шляхів, сповіщає про досяжності мереж в їх власній автономній системі для сусідніх автономних прикордонних маршрутизаторів. Концепція оточення тут та ж сама, як у вже розглянутих протоколах RIP і OSPF.

Граничний маршрутизатор автономної системи отримує свою інформацію від внутрішнього алгоритму маршрутизації, такого як RIP

і OSPF. Кожен маршрутизатор, який отримує вектор шляху, перевіряє, що запропонований шлях узгоджений з його політикою. Якщо політика маршрутизації відповідає записаній в програмі, маршрутизатор оновлює таблиці маршрутизації і модифікує повідомлення, перш ніж послати його до наступного сусідові.

Роутер взаємодіє з іншими роутерами по протоколу BGP тільки в тому випадку, якщо адміністратор явно вказує, що ці роутери є його сусідами.

Таким чином, адміністратор може вирішувати, з якими автономними системами він буде обмінюватися трафіком, а з якими ні. Одночасно протоколи RIP і OSPF обмінюються маршрутною інформацією з усіма роутерами, що знаходяться в межах їх безпосередньої досяжності. BGP відрізняється від RIP або OSPF тим, що BGP використовує TCP в якості транспортного протоколу.

4 МЕРЕЖНІ СЛУЖБИ DHCP ТА DNS

4.1 Протокол динамічної конфігурації хостів

Протокол динамічної конфігурації хостів (Dynamic Host Configuration Protocol, DHCP) автоматизує процес конфігурації мережних інтерфейсів, гарантуючи від дублювання адрес за рахунок централізованого управління їх розподілом. DHCP побудований за схемою клієнт сервер, де DHCP-сервер виділяє мережні адреси і доставляє конфігураційні параметри ПК, які динамічно конфігуруються.

Клієнт і сервер можуть погоджувати список необхідних параметрів. ПК не повинна діяти як DHCP-сервер, якщо вона спеціально не налаштована системним адміністратором.

DHCP не може використовуватися для конфігурації маршрутизаторів. Список основних завдань DHCP:

- DHCP є механізм, а не політика і управляється системними адміністраторами, шляхом завдання конфігураційних параметрів;
- клієнти не повинні вимагати ручної конфігурації і повинні читати локальні конфігураційні параметри;
- мережі не вимагають ручної конфігурації для окремих клієнтів. Адміністратор не вводить індивідуальні параметри клієнта;
- DHCP не вимагає окремого сервера для кожної підмережі;

- клієнт DHCP може отримати кілька відгуків на запит конфігураційних параметрів. Для підвищення надійності та швидкодії використовують декілька серверів для перекриття областей мережі;

- DHCP повинен співіснувати з ПК, які сконфігуровані вручну.

DHCP повинен також:

- гарантувати, що будь-яка мережна адреса не буде використовуватися більш ніж одним клієнтом одночасно;

- підтримувати DHCP конфігурацію клієнта при стартовому перезавантаженні DHCP-клієнта - при кожному запиті по мірі можливості, присвоюється один і той же набір конфігураційних параметрів (мережна адреса);

- підтримувати конфігурацію DHCP-клієнта при перезавантаженні сервера (той же набір конфігураційних параметрів);

- дозволяти автоматично отримувати конфігураційні параметри новим клієнтам, щоб уникнути ручної конфігурації;

- підтримувати фіксоване або постійне присвоєння конфігураційних параметрів для заданого клієнта.

Модель DHCP пам'яті характеризується записами ключ-значення для кожного клієнта, де ключ це деякий унікальний ідентифікатор (номер IP-мережі і унікальний ідентифікатор в межах мережі), а значення містить набір конфігураційних параметрів клієнта. Ключ може являти собою пару номер IP-мережі, апаратну адресу.

Повідомлення

Використання

DHCPDISCOVER

Клієнт посилає повідомлення широкомовно, щоб виявити доступний сервер

DHCPOFFER

Надсилається сервером клієнтові у відповідь на DHCPDISCOVER і містить пропозицію по конфігураційним параметрам

DHCPREQUEST

Повідомлення клієнта серверу. Робить запит параметрів від одного сервера і відкидає пропозиції інших серверів, підтверджує коректність раніш присвоєної адреси після перезавантаження системи

DHCPACK

Надсилається сервером клієнтові і містить конфігураційні параметри, включаючи присвоєну мережну адресу

DHCPNAK	Надсилається сервером клієнтові, повідомляючи про те, що мережна адреса не коректна (клієнт перемістився в нову підмережу) або час використання адреси клієнтом минув
DHCPDECLINE	Клієнт і сервер виявили, що мережна адреса вже використовується
DHCPRELEASE	Надсилається клієнтом серверу з метою відмови від мережної адреси і анулює час дії адреси
DHCPINFORM	Надсилається клієнтом серверу з проханням про локальні параметри

DHCP може працювати в різних режимах, включаючи:

- ручне призначення статичних адрес - адміністратор, з пулом доступних адрес, постачає DHCP-сервер інформацією про жорстку відповідність IP-адрес фізичним адресам або іншим ідентифікаторам клієнтських вузлів;
- автоматичне призначення статичних адрес - DHCP-сервер самостійно без втручання адміністратора довільним чином вибирає клієнтові IP-адресу з пулу IP-адрес. Адреса дається клієнту з пулу в постійне користування. При наступних запитах сервер повертає клієнтові ту же IP-адресу;
- автоматичний розподіл динамічних адрес - DHCP-сервер видає клієнту адресу та набір конфігураційних параметрів на обмежений час, термін оренди. Коли DHCP-клієнт видаляється з мережі, IP-адреса автоматично звільняється. У всіх режимах роботи адміністратор при конфігуруванні DHCP-сервера повідомляє йому один або декілька діапазонів IP-адрес - все адреси належать до однієї мережі - мають одне і те ж значення в поле номера мережі.

4.2 Централізована служба DNS

Централізована служба DNS (Domain Name System - система доменних імен), заснована на розподіленій базі відображень «доменне ім'я - IP-адреса». DNS являє собою, з одного боку, базу даних, розподілену між ієрархічно структурованими серверами імен, з іншого боку, протокол прикладного рівня, який організовує взаємодію між хостами і серверами імен для виконання операцій перетворення.

Протоколу DNS призначено порт з номером 53 і працює він поверх протоколу UDP транспортного рівня. Основні специфікації DNS містяться в документах RFC 1034 і RFC 1035.

Служба DNS використовує в своїй роботі DNS-сервери і DNS-клієнти. DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитом про перетворення доменного імені в IP-адресу.

DNS має ієрархічну деревоподібну структуру, яка допускає наявність в імені довільної кількості складових частин.

Ієрархія доменних імен аналогічна ієрархії імен файлів, прийнятої в файлових системах. Дерево імен починається з кореня, що позначається крапкою (.). Потім слідує старша символічна частина імені, друга за старшинством символічна частина імені і т.п.

У доменній системі імен розрізняють короткі імена, відносні імена і повні доменні імена. Коротке ім'я - ім'я кінцевого вузла мережі: хоста або порту маршрутизатора. Коротке ім'я - це лист дерева імен. Відносне ім'я - ім'я, яке починається з деякого рівня ієрархії, але не з самого верхнього. `www1.zil` - це відносне ім'я. Повне доменне ім'я (Fully Qualified Domain Name, FQDN) включає складові всіх рівнів ієрархії.

Кореневий домен управляється центральними органами Інтернету IANA і InterNIC. Домени верхнього рівня призначаються для кожної країни, а також для різних типів організацій. Імена цих доменів повинні слідувати міжнародному стандарту ISO 3166. Для позначення країн використовуються три або дволітерні аббревіатури, наприклад `ru` (Росія), `uk` (Велика Британія), `fi` (Фінляндія), `us` (США), а для різних типів організацій: `com` - комерційні організації (`microsoft.com`); `edu` - освітні організації (`mit.edu`); `gov` - урядові організації (`nsf.gov`); `org` - некомерційні організації (`fidonet.org`); `net` - мережеві організації (`nsf.net`). Кожен домен адмініструє конкретна організація, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям.

Процедура дозволу DNS-імені аналогічна процедурі пошуку файлової системою адреси файлу по його символічному імені. Істотною відмінністю файлової системи від служби DNS є те, що перша розташована на одному комп'ютері, а друга є розподіленою.

Існує дві основні схеми дозволу DNS-імен:

У першому варіанті роботу з пошуку IP-адреси координує DNS-клієнт. DNS-клієнт звертається до кореневого DNS-сервера із

зазначенням повного доменного імені. DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який обслуговує домен верхнього рівня, заданий в наступній старшій частині імені, яке запитується. DNS-клієнт робить запит наступного DNS-сервера, який відсилає його до DNS-сервера потрібного піддомену і т.п., Поки не буде знайдений DNS-сервер, в якому зберігається відповідність імені, яке запитується IP-адресі. Цей сервер і дає остаточну відповідь клієнту.

Така процедура дозволу імені називається нерекурсивною, коли клієнт сам ітеративно виконує послідовність запитів до різних серверів імен. Це завантажує клієнта складною роботою тому застосовується рідко. У другому варіанті реалізується рекурсивна процедура. DNS-клієнт запитує локальний DNS-сервер - сервер, який обслуговує піддомен, якому належить ім'я клієнта. Далі можливі два варіанти дій:

- локальний DNS-сервер знає відповідь і відразу повертає значення клієнту (коли ви запросили ім'я входить в той же піддомен, що і ім'я клієнта або, коли сервер визначав відповідність для іншого клієнта і зберіг його в кеші);

- локальний сервер не знає відповідь і виконує ітеративні запити до кореневого сервера так само, як це робив клієнт в попередньому варіанті, а отримавши відповідь, передає її клієнту, який чекає її від свого локального DNS-сервера.

Записи DNS або ресурсні записи (Resource Records, RR) - одиниці зберігання і передачі інформації в DNS. Кожна ресурсна запис складається з наступних полів:

- ім'я (NAME) - доменне ім'я, до якого прив'язана або якому «належить» дана ресурсна запис;

- TTL (Time To Live) - допустимий час зберігання даної ресурсної записи в кеші невідповідального DNS-сервера;

- тип (TYPE) ресурсної записи - визначає формат і призначення даної ресурсної записи;

- клас (CLASS) ресурсної записи; теоретично вважається, що DNS може використовуватися не тільки з TCP / IP, але і з іншими типами мереж, код в поле клас визначає тип мережі;

- довжина поля даних (RDLEN);

- поле даних (RDATA) формат і зміст залежать від типу запису;

Найбільш важливі типи DNS-записів:

- запис A (address record) або запис адреси пов'язує ім'я хоста з IP-адресою. Наприклад, запит А-записи на ім'я referrals.icann.org поверне його IP адресу - 192.0.34.164;
- запис AAAA (IPv6 address record) пов'язує ім'я хоста з адресою протоколу IPv6. Наприклад, запит AAAA-запису на ім'я K.ROOT-SERVERS.NET поверне його IPv6 адресу - 2001:7fd::1;
- запис CNAME (canonical name record) або канонічний запис імені (псевдонім) використовується для перенаправлення на інше ім'я;
- запис MX (mail exchange) або поштовий обмінник вказує сервер(и) обміну поштою для даного домену;
- запис NS (name server) вказує на DNS-сервер для домену;
- запис SOA (Start of Authority) або початковий запис зони вказує, на якому сервері зберігається еталонна інформація про домен, містить контактну інформацію особи, відповідальної за дану зону;
- запис PTR (pointer) або запис покажчика пов'язує IP хоста з його канонічним ім'ям. Запит в домені in-addr.arpa на IP хоста в reverse формі поверне ім'я (FQDN) даного хоста (див. Зворотний DNS-запит). Наприклад для IP адреси 192.0.34.164: запит записи PTR 164.34.0.192.in-addr.arpa поверне його канонічне ім'я referrals.icann.org.
in-addr.arpa
DNS-запис in-addr.arpa виглядає так:
56.34.12.10.in-addr.arpa. IN PTR host1.example.net.
Це означає, що IP-адреса 10.12.34.56 відповідає імені хоста host1.example.net.
DNS-запис ip6.arpa виглядає так:
5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
IN PTR host1.example.net.
Це означає, що IPv6-адреса 2001:0db8::1:2345 відповідає імені хоста host1.example.net.

5 MEPEŽI VLAN

5.1 Загальні поняття

VLAN - логічна група вузлів мережі, трафік якої, включаючи і широкомовний, на канальному рівні повністю ізольований від інших вузлів мережі. Передача кадрів між різними VLAN на підставі MAC-

адреси неможлива незалежно від типу адреси - унікального, групового або широкомовного.

5.2 Типи VLAN

На комутаторах реалізовані наступні типи VLAN:

- на основі портів (Port-based VLAN) - порт комутатора призначається в VLAN і пристрій, підключений до порту, перебуває в призначеній VLAN;

- на основі MAC-адрес (MAC-based VLAN) - членство в VLAN засноване на MAC-адресі пристрою. На комутаторі створюється прив'язка MAC пристроїв до VLAN;

- на основі стандарту IEEE 802.1Q - поле про належність до VLAN інтегрується в кадр Ethernet. Перевага у сучасній функціональності та використання VLAN в межах всієї мережі; використання в мережі з обладнанням різних виробників. Цей тип VLAN використовується частіше інших;

- на основі IEEE802.1ad (Q-in-Q VLAN) - провайдерські мости;

- на основі портів і протоколів IEEE 802.1v - тип протоколу для членства в VLAN;

- асиметричні - клієнти різних VLAN взаємодіють з розподіленими пристроями (серверами), без підтримки 802.1Q, через один фізичний канал зв'язку з комутатором, не вимагаючи використання зовнішнього маршрутизатора.

VLAN на основі портів (Port-based VLAN) - кожен порт призначається в VLAN, незалежно який користувач або комп'ютер підключений до порту - всі вони члени цієї VLAN. Конфігурація портів статична - змінюється вручну. Основні характеристики:

- застосовуються в межах одного комутатора - організація декількох робочих груп (технічний відділ і відділ продажів);

- не вимагають від адміністратора великого обсягу ручної роботи - всім портам одного VLAN, привласнюють однаковий ідентифікатор VID (VLAN ID);

- дають можливість зміни логічної топології без фізичного переміщення станцій - зміна порту з однієї VLAN (технічного відділу) на іншу (відділу продажів), і ПК отримує можливість спільно

використовувати ресурси нової VLAN - забезпечують гнучкість при переміщеннях і нарощуванні мережі;

- кожен порт може входити тільки в одну VLAN;
- об'єднання VLAN як всередині комутатора, так і між комутаторами через мережний рівень. Один з портів кожної VLAN підключається до інтерфейсу маршрутизатора для пересилання кадрів з однієї підмережі (VLAN) в іншу (IP-адреси підмереж різні).

Недолік - один порт кожної VLAN потрібно підключати до маршрутизатора. Призводить до додаткових витрат на покупку кабелів і маршрутизаторів.

VLAN на основі MAC-адрес включає багато ручних операцій по маркуванню MAC-адрес на кожному комутаторі. VLAN на базі MAC - дозволяють фізично переміщати ПК (включаючи до будь-якого порту комутатора), залишаючи ПК у тому ж ширококомовному домені без змін в настройках конфігурації.

VLAN на основі стандарту IEEE 802.1Q використовують поля кадру для інформування про приналежність до VLAN при переміщенні по мережі. З точки зору гнучкості налаштувань, VLAN IEEE 802.1Q краще рішення. Його переваги:

- гнучкість і зручність при налаштуванні та внесенні змін, створення необхідних комбінацій VLAN в межах 1 комутатора і у всій мережі, побудованій на комутаторах з підтримкою 802.1Q - інформація про VLAN поширюється через безліч 802.1Q - сумісних комутаторів по одному фізичному з'єднанню;
- дозволяє активізувати алгоритм сполучного дерева на всіх портах і працювати в звичайному режимі. Це дозволяє автоматично визначати деревовидну конфігурацію зв'язків при довільному поєднанні портів між собою;
- здатність додавати і витягувати теги з заголовків кадрів дозволяє використовувати комутатори та мережеві пристрої, які не підтримують 802.1Q;
- пристрої різних виробників, що підтримують 802.1Q, можуть працювати разом, незалежно від фірмового рішення;
- для зв'язку підмереж на мережному рівні використовується маршрутизатор або комутатор рівня 3. Для організації доступу до сервера з різних VLAN, маршрутизатор не потрібно. Треба включити

порт підключення серверу, в усі підмережі, а адаптер сервера повинен підтримувати IEEE 802.1Q.

Будь-який порт комутатора може бути налаштований як tagged (маркований) або як untagged (немаркований) - untagging дозволяє працювати з мережними пристроями VLAN, які не розуміють тегів у заголовку кадра Ethernet. Функція tagging дозволяє налаштовувати VLAN між декількома комутаторами, які підтримують IEEE 802.1Q.

Тег VLAN IEEE 802.1Q. До кадру Ethernet додані 32 біта, які збільшують розмір до 1522 байт. Перші 2 байта (поле Tag Protocol Identifier, TPID) з фіксованим значенням 0x8100 визначають, що кадр містить тег 802.1Q. Решта 2 байта містять:

- Priority (Пріоритет) - 3 біта поля пріоритету дозволяють кодувати до восьми рівнів пріоритету (7 - вищий), які використовуються в стандарті 802.1Q;
- Canonical Format Indicator (CFI) - 1 біт індикатора канонічного формату зарезервованій для позначення кадрів мереж інших типів (Token Ring, FDDI), які передаються через Ethernet;
- VID (VLAN ID) - 12-бітний ідентифікатор визначає, якій VLAN належить трафік. Можна задати 4094 VLAN (VID 0 і 4095 зарезервовані).

Кожен фізичний порт комутатора має ідентифікатор VLAN (PVID) - для визначення в яку VLAN комутатор направить вхідний немаркований кадр з підключеного до порту сегмента коли кадр потрібно передати на інший порт (всередині комутатора в заголовки всіх немаркованих кадрів додається ідентифікатор VID, рівний PVID порту, на який вони прийняті).

Цей механізм дозволяє одночасно існувати в одній мережі пристроїв з підтримкою і без підтримки стандарту IEEE 802.1Q. Комутатори, які підтримують стандарт 802.1Q зберігають таблицю, яка пов'язує PVID з ідентифікаторами VID мережі. Кожен порт комутатора має тільки один PVID і стільки VID, скільки підтримує дана модель комутатора. Правила вхідного трафіку (ingress rules) дозволяють класифікувати одержувані кадри щодо належності до VLAN. Правила просування між портами (forwarding rules) дозволяють приймати рішення про просування або відкидання кадру.

6 ТРАНСПОРТНИЙ РІВЕНЬ. ПРОТОКОЛИ

6.1 Порти додатків

Головне завдання транспортного рівня полягає в передачі даних між прикладними процесами. Його вирішують протокол управління передачею (Transmission Control Protocol, TCP) (RFC 793), і протокол користувацьких дейтаграм (User Datagram Protocol, UDP), описаний в RFC 768. Протоколи TCP і UDP забезпечують інтерфейс з вище розташованим прикладним рівнем, передаючи дані, які надходять на вхідний інтерфейс хоста, відповідному додатку, використовуючи концепції «порт» і «сокет».

При доставці пакета на мережний інтерфейс одержувача, дані направляються конкретному процесу-одержувачу, а пакети, які надходять в мережу від різних додатків, обробляються загальним для них протоколом IP. Тому в стеці передбачено метод «збирання» пакетів від різних додатків для передачі IP протоколу мережного рівня. Прийом даних протоколами TCP і UDP, які надходять від різних прикладних служб - мультиплексування. Зворотна процедура - розподілу пакетів, які надходять від мережного рівня - демультимплексування (рис.6.1).

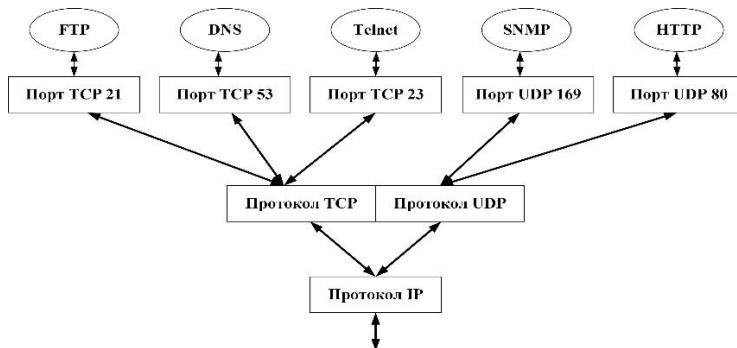


Рисунок 6.1 – Мультиплексування і демультимплексування на транспортному рівні

При виконанні прикладних процесів, маємо декілька точок входу - адреси призначення для пакетів даних.

Для кожної програми ведуться дві черги: черга пакетів, які надходять до даного додатку з мережі, і черга пакетів, які

відправляються даним додатком в мережу. Вхідна і вихідна черги однієї програми розглядаються як один порт. Для ідентифікації портів їм присвоюють номери, які використовуються для адресації додатків.

За загальнодоступними службами (FTP, telnet, HTTP, TFTP, DNS) закріплюються стандартні, призначені номери - добре відомі (well-known) номери портів (стандарти RFC1700, RFC3232) - вони унікальні в межах Інтернет і призначаються додатків централізовано з діапазону від 0 до 1023. Для інших додатків номери портів призначаються розробниками додатків або ОС у діапазоні від 1024 до 65535.

Якщо номери TCP- і UDP-портів збігаються, вони ідентифікують різні додатки. Одному з додатків може бути призначений TCP-порт 1750, іншому - UDP-порт 1750. Якщо стандартний додаток (наприклад DNS) звертається до протоколу TCP або UDP йому, для зручності, призначають однакові номери TCP та UDP-портів (53).

6.2 Протокол UDP

Протокол UDP - дейтаграмний протокол, реалізує сервіс по можливості, не гарантуючи доставку своїх повідомлень, не компенсує ненадійність протоколу IP. Заголовок UDP, складається з чотирьох 2-байтових полів, які включають порти відправника і одержувача, контрольну суму і довжину дейтаграми.

Приклад заголовка UDP: Source Port = 0x0035 Destination Port = 0x0411 Total length = 132 (0x84) bytes Checksum = 0x5333.

У UDP-дейтаграми в полі даних, довжина якого дорівнює (132 - 8) байт, вміщено повідомлення DNS-сервера - номер порту джерела (Source Port = 0x0035) з номером DNS - 53. UDP є простим протоколом. Функції зводяться до мультиплексування та демультиплексування даних між мережним і прикладним рівнями.

При вирішенні завдання демультиплексування протоколом UDP кадри, які несуть UDP-дейтаграми, прибувають на мережний інтерфейс хоста та послідовно обробляються протоколами стека і надходять в розпорядження протоколу UDP. Однозначно прикладний процес в мережі визначає пара (IP-адреса, номер порту UDP), яка має назву UDP-сокету (socket). UDP виконує демультиплексування на основі сокетів.

6.3 Протокол TCP

Інформація, яка надходить до протоколу TCP від протоколів прикладного рівня, розглядається як неструктурований потік байт. Для передачі на мережний рівень з буфера «вирізається» безперервна частина даних - сегмент (одиниця переданих даних (поле даних і заголовок TCP) або окремо поле даних) і забезпечується заголовком.

Заголовок TCP-сегмента містить більше полів, ніж UDP:

- порт джерела - 2 байта і ідентифікує процес-відправник;
- порт приймача - 2 байта і ідентифікує процес-одержувач;
- послідовний номер - 4 байта являє собою номер байта, який визначає зміщення сегмента щодо потоку даних, що відправляються (номер першого байта даних в сегменті);

- підтверджений номер - 4 байта. містить максимальний номер байта в отриманому сегменті, збільшений на 1. Використовується в якості квитанції;

- довжина заголовка (hlen) займає 4 біта - довжина заголовка TCP-сегмента, вимірюється в 32-бітових словах. Довжина заголовка не фіксована і може змінюватися в залежності від значень, встановлених в поле параметрів;

- резерв (reserved) займає 6 біт;
- кодові біти (code bits) займає 6 біт є службовою інформацією про тип даного сегмента. Позитивне значення сигналізується установкою бітів в одиницю:

- 1) URG - термінове повідомлення;

- 2) ACK - квитанція на прийнятий сегмент;

- 3) PSH - запит на відправку повідомлення без очікування заповнення буфера (протокол TCP може вичікувати заповнення буфера перед відправкою сегмента, але якщо термінова передача, додаток повідомляє про це TCP за допомогою цього біта);

- 4) RST - запит на відновлення з'єднання;

- 5) SYN - синхронізація лічильників даних;

- 6) FIN - ознака досягнення передаючою стороною останнього байту в потоці переданих даних;

- вікно - 2 байта - кількість байт даних, очікуваних відправником даного сегмента, починаючи з байту, номер якого вказаний у полі підтвердженого номера;

- контрольна сума (checksum) займає 2 байта;
- показчик терміновості (urgent pointer) займає 2 байта і вказує на кінець даних, які потрібно терміново прийняти, незважаючи на переповнення буфера;
- параметри (options) мають змінну довжину;
- заповнювач (padding) може мати змінну довжину.

Логічне ТСП-з'єднання однозначно ідентифікується парою сокетів.

РЕКОМЕНДОВАНА ЛИТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.
2. Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум, Д.Уэзеролл. – СПб.: Питер, 2012. – 960 с.
3. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.
4. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.