

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Г.Г. Киричек

Конспект лекцій з дисципліни
«Проектування комп'ютерних мереж»
для студентів спеціальності
123 Комп'ютерна інженерія, усіх форм навчання

2024

Конспект лекцій з дисципліни «Проектування комп'ютерних мереж» для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання / Укл. Г.Г Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 38 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 № 1 від 06.08.2024

Рекомендовано до видання
НМК ФКНТ
Протокол № 1 від 04.09.2024

ЗМІСТ

1 Функціональність рівня доступу до середовища передачі.....	4
1.1 Трирівнева модель мережі.....	4
1.2 Комутатори	5
1.3 Віртуальні локальні мережі	8
1.4 Протоколи сполучного дерева	10
2 Проектування. Структуровані кабельні мережі	14
2.1 Проектування інфраструктури.....	14
2.2 Структуровані кабельні системи.....	17
3 Транспортний рівень. Протоколи	21
3.1 Порти додатків.....	21
3.2 Протокол UDP	22
3.3 Протокол TCP	23
4 Транспортні послуги.....	24
4.1 Послуги та технології глобальних мереж	24
4.2 Техніка просування кадрів	25
4.3 Віртуальні приватні мережі.....	27
4.4 IPSec.....	29
4.5 IPv6	33
Рекомендована література	38

1 ФУНКЦІОНАЛЬНІСТЬ РІВНЯ ДОСТУПУ ДО СЕРЕДОВИЩА ПЕРЕДАЧІ

Мета – ознайомитись з додатковими функціями канального рівня моделі OSI та моделями, які описують взаємодію пристроїв, які підтримують багато складних та достатньо корисних функцій.

1.1 Трирівнева модель мережі

Будь-яка мережа може бути представлена як ієрархічна модель, яка складається з трьох рівнів.

Першим рівнем є рівень доступу (access layer). Він керує доступом користувачів та робочих груп до ресурсів об'єднаної мережі. Основним завданням цього рівня є створення точок входу/виходу користувачів у мережу. Цей рівень виконує ряд функцій, а саме:

- управління доступом користувачів до мережі та політиками цього доступу;
- створення окремих доменів колізій (що означає підтримку сегментації);
- підключення робочих груп до рівня розподілу;
- підтримка технологій комутованих локальних мереж.

Другий рівень це рівень розподілу (distribution layer). Він зв'язує рівні доступу із рівнями ядра. Цей рівень виконує наступні функції:

- агрегує (групує) дані, отримані від комутаторів рівня доступу, перед тим, як вони будуть передані до рівня призначення, який має назву рівень ядра, тобто виконує агрегування каналів;
- забезпечує маршрутизацію та якість обслуговування;
- контролює потік мережного трафіку на основі політик;
- встановлює межі ширококомовних доменів, виконуючи функції маршрутизації між віртуальними мережами (VLAN), які визначені лише на рівні доступу;
- підтримує перехід від однієї технології до іншої (наприклад, від 100Base-TX до 1000Base-T).

Третій рівень – рівень ядра (core layer). Є верхом ієрархії - відповідає за надійну і швидку передачу великих обсягів даних. Трафік, який передається через ядро, є загальним для усіх користувачів.

Зазначені рівні не припускають наявності трьох різних пристроїв. Можливе використання як декількох пристроїв, так і одного пристрою, який виконує усі функції. Тому на всіх цих рівнях, у якості проміжних мережеских пристроїв, можна використовувати тільки комутатори.

З метою зменшення кількості клієнтів, які розділяють смугу пропускання, розроблено пристрій, який має назву – міст (bridge). Це пристрій 2-го рівня моделі OSI, який об'єднує сегменти мережі, ізолює трафік одного сегмента від трафіку іншого, зменшуючи домен колізій та підвищує загальну продуктивність мережі. Він вже не просто пересилає кадри з одного сегмента в інший, а аналізує та передає їх, якщо адреса призначення належить іншому сегменту.

1.2 Комутатори

Відмінність комутатора в тому, що він являє собою багатопортовий міст, який вже може встановлювати одночасно декілька з'єднань між різними парами портів. При передачі кадру через комутатор створюється окремий канал, і по ньому дані пересилаються прямо від порту-відправника до порту-одержувача з максимально можливою для технології швидкістю. Такий принцип роботи має назву "мікросегментація". При цьому комутатори отримали можливість функціонувати в режимі повного дуплексу, що дозволило уникнути колізій та підвищити загальну продуктивність мережі.

Сучасні комутатори (Ethernet) вже є інтелектуальними пристроями, з процесорами, для обробки та перенаправлення кадрів на високих швидкостях, з реалізацією наступних функцій: резервування; підвищення відмовостійкості мережі; агрегування каналів; створення віртуальних локальних мереж (VLAN); маршрутизації; управління якістю обслуговування (Quality of Service, QoS); забезпечення безпеки, тощо, а також за допомогою вбудованих засобів: налаштування мережеских параметрів; аналізу та моніторингу трафіку.

Також з появою такого стандарту, як IEEE 802.3af-2003 PoE (Power over Ethernet), розробники почали випускати уніфіковані комутатори з підтримкою цієї технології, для живлення портів, які підключаються до них: це IP-телефони: Інтернет-камери: точки бездротового доступу та пристрої централізованого управління дротовою та бездротовою мережею.

Виходячи з конструктивного виконання, комутатори поділяються на три групи:

- настільні комутатори (Desktop switch); мають відносно невелику кількість фіксованих портів (у D-Link від 5 до 16). Часто використовуються в мережах класу SOHO (Small Office, Home Office), де не потрібна висока продуктивність та розширені мережеві функції;

- автономні комутатори - комутатори, які монтуються в телекомунікаційну стійку (Rack mounted switch); у стійковому виконанні вони мають корпус для монтажу у стійку, вбудований блок живлення та фіксовану кількість портів (у D-Link до 52-х). Забезпечують високу продуктивність та надійність, а також широкий набір мережевих функцій та інтерфейсів. Використовуються на рівнях доступу та розподілу у мережах малих та середніх підприємств (Small to Medium Business, SMB), у корпоративних мережах та мережах провайдерів послуг (ISP);

- комутатори на основі шасі (Chassis switch) – дані пристрої містять слоти для встановлення: інтерфейсних модулів розширення; резервних джерел живлення та процесорних модулів. Модулі підтримують технологію hot swap ("гаряча заміна") - заміна без вимкнення живлення. Застосовуються такі комутатори на магістралях великих корпоративних та міських мереж, мереж операторів зв'язку.

Комутатори обробляють кадри на основі алгоритму прозорого моста, визначеного у стандарті IEEE 802.1D. Процес роботи алгоритму починається з побудови таблиці комутації. Спочатку таблиця комутації є порожньою. При включенні живлення, разом з передачею даних, комутатор вивчає розташування підключених до нього мережевих пристроїв, він аналізує MAC-адреси відправників кадрів. Якщо з одного із портів надходить кадр, він створює в таблиці комутації запис, який асоціює MAC-адресу цього вузла із номером вхідного порту.

Записи у таблиці комутації створюються динамічно. Та, як тільки комутатор зчитує нову MAC-адресу, він відразу ж заносить її в таблицю комутації. Для кожного такого запису задається час життя, який дозволяє комутатору автоматично реагувати на переміщення, додавання або видалення мережевих пристроїв, а також дозволяє зберігати в таблиці комутації тільки актуальні MAC-адреси. Це зменшує час пошуку, відповідного запису в таблиці, та гарантує, що таблиця не буде використовувати занадто багато системної пам'яті.

У комутаторі реалізовано один із методів комутації, які визначають його поведінку при отриманні кадру:

- комутація з проміжним зберіганням (store-and-forward) - в цьому методі комутатор, перш ніж передати кадр, повністю копіює його в буфер і проводить перевірку на наявність помилок. У тому випадку, якщо кадр містить помилки, він відкидається (наприклад, не збігається контрольна сума, або кадр менше 64 байт або більше 1518 байт (що пов'язано з умовами розміру кадра технології Ethernet). Якщо кадр не містить помилок, то комутатор знаходить MAC-адресу одержувача в таблиці комутації і визначає вихідний порт. Потім комутатор передає кадр через відповідний порт пристрою призначення;

- комутація без буферизації (cut-through) - в цьому методі комутатор копіює в буфер тільки MAC-адресу призначення (перші 6 байт після префіксу) і передає кадр, не чекаючи його повного прийому. Комутація без буферизації зменшує затримку, але перевірку на наявність помилок не виконує. Використовується, коли порти комутатора підтримують однакову швидкість;

- комутація із виключенням фрагментів (fragment-free) - в цьому методі комутатор приймає в буфер перші 64 байти кадру, що дозволяє йому відфільтровувати колізійні кадри перед їхньою передачею. Кадри, завдовжки більше 64 байтів є правильними. Цей метод комутації чекає, поки отриманий кадр буде перевірений щодо колізії, і тільки після цього починає його передачу.

Основним компонентом комутаційного обладнання є комутуюча матриця (switch fabric) – чіпсет, який з'єднує безліч входів із безліччю виходів, на основі фундаментальних технологій та принципів комутації. Комутуюча матриця виконує три функції:

- перемикає трафік з одного порту матриці на інший, забезпечуючи їх рівнозначність;

- надає певну якість обслуговування (Quality of Service, QoS);

- забезпечує відмовостійкість.

Продуктивність комутатора – характеристика на яку при виборі пристрою мережні інтегратори та досвідчені адміністратори звертають увагу в першу чергу. Характеризують продуктивність: швидкість фільтрації кадрів; швидкість переміщення кадрів; пропускна спроможність; затримка передачі кадру. Впливають на зазначені характеристики продуктивності: тип комутації; розмір буфера

(буферів) кадрів; продуктивність комутуючої матриці; продуктивність процесора чи процесорів та розмір таблиці комутації.

1.3 Віртуальні локальні мережі

Віртуальною локальною мережею називається логічна група вузлів мережі, трафік якої (також і широкомовний), на каналному рівні є ізольованим від інших вузлів мережі – це означає, що передача кадрів між різними VLAN на підставі MAC-адреси неможлива, незалежно від типу адреси – унікальна вона, групова або широкомовна.

VLAN мають наступні переваги:

- забезпечують ефективний спосіб групування мережевих користувачів у віртуальні групи, незважаючи на їх фізичне розміщення у мережі;
- забезпечують можливість контролю широкомовних повідомлень, що збільшує смугу пропускання, доступну для користувача;
- підвищують безпеку мережі, за допомогою використання фільтрів та політик взаємодії користувачів із різних VLAN, які налаштовуються на комутаторі або маршрутизаторі.

У комутаторах можуть бути реалізовані наступні типи VLAN:

- на основі портів (Port-based VLAN) - кожен порт комутатора призначається у визначену VLAN і будь-який мережний пристрій, підключений до даного порту, знаходиться в призначеній VLAN;
- на основі MAC-адрес (MAC-based VLAN) - членство у VLAN ґрунтується на MAC-адресі робочої станції. На комутаторі потрібно створити прив'язку MAC-адрес всіх пристроїв до VLAN;
- на основі стандарту IEEE 802.1Q - поле приналежності VLAN, інтегрується в кадр Ethernet, що дозволяє передавати дані через мережу;
- на основі IEEE 802.1ad (Q-in-Q VLAN) - провайдерські мости;
- на основі портів та протоколів IEEE 802.1v - тип протоколу використовується для визначення членства в VLAN;
- асиметричні – коли клієнти різних VLAN взаємодіють з розділяємими пристроями (наприклад, серверами), без підтримки стандарту 802.1Q, через один фізичний канал зв'язку із комутатором, без використання зовнішнього маршрутизатора.

Формат тегу 802.1Q. До кадру Ethernet додається 32 біти (4 байти), які збільшують його розмір до 1522 байт. Тег розміщується у полі даних кадру Ethernet (рис.1.1).



Рисунок 1.1 - Маркований кадр Ethernet

Перші 2 байти (поле Tag Protocol Identifier, TPID) мають фіксоване значення - 0x8100 і визначають, що кадр містить тег 802.1Q.

Інші 2 байти містять наступні поля:

- Priority - 3 біти поля пріоритету, задають до восьми рівнів пріоритету (0 - нижчий, 7 - вищий) - використовуються в 802.1Q;
- Canonical Format Indicator (CFI) - 1 біт індикатора канонічного формату. Зарезервований для позначення кадрів мереж інших типів (Token Ring, FDDI), які передаються магістраллю Ethernet;
- VID (VLAN ID) – 12-бітний ідентифікатор VLAN, визначає, який VLAN належить трафік. Можна задати 2^{12} (4094) унікальних VLAN (VID 0 і VID 4095 зарезервовані).

Кожен фізичний порт комутатора має ідентифікатор порту VLAN (PVID), він визначає в яку VLAN комутатор направить вхідний немаркований кадр із підключеного до порту сегмента. Коли кадр передається на порт, всередині комутатора у заголовки немаркованих кадрів додається ідентифікатор VID, рівний PVID порту, на який вони прийняті - механізм дозволяє одночасно існувати в одній мережі пристроям із підтримкою та без підтримки стандарту IEEE 802.1Q.

Комутатори, що підтримують 802.1Q зберігають таблицю, яка пов'язує ідентифікатор порту PVID з ідентифікаторами VID (VLAN ID) мережі. Кожен порт комутатора має лише один PVID і стільки VID,

скільки підтримує ця модель комутатора. Якщо на комутаторі не налаштовані VLAN, то порти входять до першої VLAN з PVID=1.

Для коректної роботи пристроїв у VLAN, у базі даних фільтрації (Filtering DB) створюються відповідні записи про їх членство у VLAN.

Існують два основні способи, які дозволяють встановлювати членство у VLAN: це статичні VLAN та динамічні VLAN.

У статичних VLAN встановлення членства здійснюється вручну адміністратором мережі під час налаштування.

Членство в динамічних VLAN:

- або визначається під час роботи комутатора за допомогою процедур, описаних у спеціальних стандартах;
- або встановлюється автоматично (динамічно) на магістральних інтерфейсах комутаторів на основі протоколу GVRP GARP (VLAN Registration Protocol). Де протокол GARP (Generic Attribute Registration Protocol), використовується для реєстрації та скасування реєстрації атрибутів, таких як VID.

1.4 Протоколи сполучного дерева

Комутаційні петлі виникають коли між комутаторами мережі є декілька з'єднань (каналів або маршрутів) через проміжні мережі. При цьому наявність цих надлишкових каналів, зазвичай є корисною, але петлі створюють проблеми.

З метою запобігання виникнення петель створено протокол сполучного дерева - Spanning Tree Protocol (STP). Основне завдання даного протоколу - приведення мережі Ethernet, що використовує множинні зв'язки, до деревоподібної топології, яка виключає зациклювання пакетів. У своїй роботі протокол STP використовує алгоритм сполучного дерева. Цей алгоритм дозволяє автоматично резервувати альтернативні канали зв'язку між комутаторами.

Кожен зв'язок між комутаторами, зокрема резервні, каталогізується. Потім алгоритм сполучного дерева блокує переадресацію надлишкових посилок, встановлюючи один бажаний канал між комутаторами в локальній мереж, який використовується для всіх кадрів Ethernet. Комутатори, які підтримують протокол STP, створюють деревоподібну конфігурацію зв'язків без петель у мережі,

використовуючи обмін службовими кадрами – вони мають назву Bridge Protocol Data Units (BPDU) - блоки даних протоколу мосту.

Існують три стандартні версії протоколів сполучного дерева:

- IEEE 802.1D Spanning Tree Protocol (STP);
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP);
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

Протокол STP використовує Spanning Tree Algorithm для визначення, який із портів комутатора треба заблокувати.

При цьому даний алгоритм визначає один із комутаторів як root bridge (кореневий комутатор) і використовує його як точку відліку для розрахунку всіх можливих шляхів.

Для того, щоб побудувати стійку активну топологію за допомогою протоколу STP, з кожним комутатором мережі потрібно асоціювати таке поняття, як унікальний ідентифікатор мосту (Bridge ID), а з кожним портом комутатора потрібно асоціювати вартість шляху (Path Cost) та ідентифікатор порту (Port ID).

Усі комутатори беруть участь у виборах кореневого мосту шляхом обміну повідомленнями BPDU (Bridge Protocol Data Units). Ці повідомлення містять, обов'язково, унікальний ідентифікатор мосту bridge ID та ідентифікатор кореневого комутатора root ID.

Що стосується Bridge ID - це ідентифікатор поточного комутатора. Він є полем у 8-байт, що складається з 2-х частин: перша - це пріоритет мосту (2 байти), який призначається адміністратором мережі, і друга - MAC-адреса блоку управління комутатора (6 байт).

При порівнянні ідентифікаторів двох комутаторів спочатку порівнюються значення пріоритетів. Та кореневим мостом стає комутатор із найменшим значенням пріоритету. Якщо пріоритети однакові (за замовчуванням - 32768) – кореневим комутатором стає комутатор з найменшою MAC-адресою блоку управління.

Що стосується Root ID, то це ідентифікатор кореневого комутатора. І він визначається наступним чином. Після підключення до мережі та завантаження, комутатор кожні 2 секунди починає відправляти BPDU повідомлення. Спочатку root ID у повідомленні дорівнює локальному bridge ID. Після того, як комутатор приймає повідомлення BPDU, він порівнює root ID із повідомлення, яке надійшло, зі своїм власним root ID. Якщо root ID з повідомлення є меншим, він змінює свій root ID і так відбувається, поки всі ці BPDU

повідомлення, які передаються комутаторами в мережі, не будуть містити найменший root ID. Комутатор із цим bridge ID стає root bridge.

Другим етапом роботи протоколу STP є вибір кореневих портів (Root Port) або визначення кращого шляху до root bridge. У цьому випадку в повідомленнях BPDU передається вартість шляху до root ID.

Коли root bridge вибрано, алгоритм STA починає процес визначення кращого шляху до кореневого мосту з усіх напрямків широкомовного домену. Інформація про довжину цих шляхів визначається методом підсумовування індивідуальних вартостей портів, на шляху від комутатора призначення до root bridge. Після підрахунку вартості всіх шляхів вибирається шлях у якого найменша вартість, а всі резервні шляхи блокуються. Порт комутатора, у якого найнижча вартість для такого з'єднання, автоматично стає кореневим. Якщо два і більше портів мають однакову вартість шляху, вибирається порт, який має більший пріоритет. Якщо пріоритети однакові, вибирається порт, який має найменше значення (port ID).

І третій крок роботи STP – визначення призначених портів (Designated Port). При цьому кореневий комутатор автоматично визначає усі порти як призначені. А на некоренових комутаторах вибір відбувається після вибору кореневого порту на сегменті. Комутатор дивиться повідомлення BPDU і вирішує: якщо bridge ID в нього менше, ніж у сусіда, порт призначений, якщо більше - непризначений.

Протокол Rapid Spanning Tree Protocol (RSTP) – є розвитком протоколу STP (визначений у стандарті IEEE 802.1D-2004), реалізований для зняття обмежень протоколу STP, пов'язаних з його продуктивністю. Протокол RSTP значно прискорює час збіжності комутуваної мережі за рахунок миттєвого переходу коренових та призначених портів у стан просування.

Термінологія протоколів STP та RSTP є однаковою. Відмінність - спосіб переходу портів у стан просування і те, як він впливає на роль порту в топології. RSTP об'єднує стан Disabled, Blocking і Listening в Discarding ("Відкидання"), при якому порт не активний.

У випадку RSTP вибір активної топології завершується присвоєнням протоколом RSTP кожному порту певної ролі:

- кореневий порт (Root Port) – має найкоротшу відстань до кореневого комутатора;

– призначеним портом (Designated Port) вважається порт, який посилає BPDU з найкращими параметрами у сегмент, до якого він підключений.

Протокол RSTP використовує механізм Proposal/Agreement, який запускається коли конфігурація портів знаходиться в стані Root port. В такому випадку механізм вимикає всі порти комутатора, які не є Edge-портами. Паралельно з цим комутатор сповіщає кореневий пристрій про зміну, після чого включає режим Forwarding для Root-port.

Протокол Multiple Spanning Tree Protocol (MSTP) – є розширенням протоколу RSTP. Він дозволяє налаштовувати окреме сполучне дерево для будь-якої VLAN або групи VLAN, створюючи безліч маршрутів передачі трафіку, і дозволяє здійснювати балансування навантаження. Усі ці функції спочатку визначено у стандарті на IEEE 802.1s на MSTP, але пізніше додано до стандарту IEEE 802.1Q-2003 на VLAN.

MSTP ділить комутаційну мережу на декілька доменів. У кожному домені формується декілька покриваючих дерев, і ці дерева залежать друг від друга. Кожен домен називається MST-областю - протокол MSTP ділить комутвану мережу на регіони (Multiple Spanning Tree (MST) Region). Кожний такий регіон може містити безліч копій сполучних дерев. Та кожне сполучне дерево є екземпляром множинного сполучного дерева (Multiple Spanning Tree Instance, MSTI).

Так званий екземпляр сполучного дерева є сукупністю декількох VLAN мереж. І, поєднуючи ці віртуальні локальні мережі в один екземпляр, можна скоротити накладні витрати на зв'язок та зайнятість ресурсів. Розрахунок топології кожного екземпляра MSTP не залежить один від одного, і на цих екземплярах можна отримати балансування навантаження.

Протокол MSTP визначає такі типи сполучних дерев:

- Common Spanning Tree (CST) - єдине сполучне дерево, яке обчислюється із використанням протоколів STP, RSTP, MSTP та об'єднує всі регіони MST та мости SST (Single Spanning Tree (SST) Bridge);
- Internal Spanning Tree (IST) - спеціальна копія сполучного дерева, яка, за замовчуванням, існує у кожному MST-регіоні. IST надано номер 0 (Instance 0). Вона може надсилати та отримувати кадри BPDU та використовується для управління топологією всередині

регіону. За замовчанням, всі VLAN одного регіону прив'язані до IST. Якщо у регіоні створено декілька MSTI, то VLAN, які не асоційовані із цією копією, залишаються прив'язаними до IST. Динамічні VLAN, будуть створені за допомогою протоколу GVRP, він використовується для реєстрації та скасування реєстрації атрибутів, таких як VID);

- Single Spanning Tree (SST) Bridge - міст, який підтримує тільки-єдине сполучне дерево, CST, яке може використовувати протокол STP або протокол RSTP;

- Common and Internal Spanning Tree (CIST) - єдине сполучне дерево, яке поєднує CST та IST для кожного MST-регіону.

2 ПРОЄКТУВАННЯ. СТРУКТУРОВАНІ КАБЕЛЬНІ МЕРЕЖІ

2.1 Проєктування інфраструктури

Мережева інфраструктура LAN / WAN – це створення технологічного фундаменту, який забезпечує: зменшення областей збоїв, модульність, ієрархічність, масштабованість, керованість, сумісність, продуктивність, доступність та безпеку будь якої IT-інфраструктури.

Етапи проєктування та впровадження мережевої інфраструктури LAN/WAN мереж включають:

- по-перше це проєктування LAN рівня будівлі, або приміщення (всередині будівлі) - тобто це все, що об'єднується всередині приміщень (з'єднання безлічі локальних мереж в єдину LAN будівлі - і це все пов'язано з логічною структурою організації); тобто логічна структура організації повинна бути врахована в процесі проєктування розподіленої мережі;

- по-друге це створення мережі кампуса, шляхом зв'язування декількох таких LAN рівня будівлі (або рівня доступу) в єдину мережу (мова йде про організацію рівня розподілу);

- по-третє це об'єднання в єдину мультисервісну (корпоративну) мережу LAN/WAN архітектури із забезпеченням роботи механізмів якості обслуговування.

При цьому LAN можуть використовуватися для роботи:

- інформаційного обміну в структурах SOHO;
- систем автоматизованого керування;
- апаратно-програмних комплексів;

- систем керування технологічними процесами;
- інформаційних систем підприємств, тощо.

І функціонально належати:

- мережі однієї організації;
- бути частиною корпоративної або глобальної мережі.

І все це повинно забезпечувати організацію роботи наступних базових сервісів та додатків компанії:

- спільне використання технічних ресурсів;
- спільне використання інформаційних ресурсів;
- спільне використання технологій (системи документообігу, мережеві бази даних, доступ до Інтернету, тощо);
- резервування та зберігання інформації;
- захист інформації від несанкціонованого доступу.

Додаткові можливості проектування та впровадження WAN (глобальної інфраструктури):

- це об'єднання територіально-розподілених LAN та обмін інформацією між ними;
- побудова віртуальних телефонних мереж;
- організація аудіо- та відеоконференцій.

Основні етапи проектування включають наведені функціональні кроки. Це аналіз технічного завдання:

- дослідження та аналіз структури підприємства (з описом основних підрозділів і філій, з урахуванням їх віддаленості);
- аналіз інформаційних потоків (обчислення загального трафіку з визначенням необхідної швидкості каналів зв'язку);
- аналіз (для модернізації) наявних апаратних і мережних пристроїв; побудова моделі мережі;
- постановку завдань, пов'язаних з проведенням досліджень, аналізом, порівнянням та вибором методів за засобів проектування.

Вибір технологій, апаратних і мережних пристроїв:

- проведення аналізу, наявних LAN і WAN технологій, порівняння та вибір технологій (певних специфікацій) для конкретних каналів зв'язку у LAN мережах підприємства та WAN між мережами вашої організації, з урахуванням підключення філій;
- дослідження, аналіз технічних характеристик та вибір мережних пристроїв з визначенням кожного конкретного пристрою або

групи ідентичних пристроїв, опис їх призначення та особливості застосування;

- аналіз технічних характеристик та вибір апаратних пристроїв (сервери, ПК, ноутбуки, термінали, планшети, IP-телефони та ін.) з описом характеристик кожного пристрою або групи пристроїв, опис призначення та особливості застосування.

Налаштування мережі:

- визначення основних LAN і WAN сегментів, проектування структурної схеми мережі;

- побудова монтажною схеми (розміщення мережевих і апаратних пристроїв (в будівлях, на поверхах, в кімнатах));

- розрахунок потужності антен; підключення (фізичне об'єднання мережних і апаратних пристроїв єдиної мережі);

- вибір принципу адресації та маршрутизації для LAN і WAN сегментів (мережі);

- програмне налаштування всього мережного обладнання (з урахуванням адресації і маршрутизації).

Адміністрування мережі:

- опис налаштування віддаленого доступу до філій (технології створення тунелів між LAN підприємства (див. методичні вказівки до лабораторних робіт));

- моделювання потоків трафіку;

- підключення до Інтернет та забезпечення мережевої безпеки (налаштування обладнання, протоколів).

Завдання проєктувальника - формулювання вимог, що пред'являються до мережі її користувачами, адміністраторами та власниками, створення плану мережі, що максимально враховує ці вимоги. План мережі повинен містити її повний опис, що допоможе при монтажі та обслуговуванні мережі надалі.

Інфраструктура мережі (network infrastructure) – набір фізичних та логічних компонентів, що реалізують зв'язок, безпеку, маршрутизацію, керування та інші функції, необхідні для її роботи. Етап планування мережі включає вибір апаратних та програмних компонентів, визначення місця та способу їх встановлення, а також параметрів конфігурації кожного з них. Для планування важливо розуміти різницю між фізичною та логічною інфраструктурою мережі.

Фізична інфраструктура (physical infrastructure) або топологія (topology) мережі - фізична структура мережі, утворена складовим її обладнанням (кабелями, маршрутизаторами, комутаторами, серверами, тощо). Устаткування для мережі обирається під час планування фізичної інфраструктури з урахуванням особливостей логічної інфраструктури. Фізична інфраструктура невеликої мережі може бути простою, а великих і середніх мереж - складною.

Логічна інфраструктура (logical infrastructure) - безліч програмних елементів, що забезпечують зв'язок, керування та захист вузлів мережі. Логічна інфраструктура забезпечує взаємодію комп'ютерів через канали, визначені фізичною топологією мережі; вона складається з абстрактних та конкретних елементів, прикладами яких є, відповідно, мережеві протоколи та програми, які їх реалізують.

Планування інфраструктури - передбачає створення плану, який використовується для монтажу та підтримки мережі. Повний план мережевої інфраструктури – більше, ніж просто креслення фізичної інфраструктури зі списком обладнання та необхідних програм. Для складання плану проектувальник зобов'язаний врахувати вимоги і специфікації програмних і апаратних компонентів мережі.

2.2 Структуровані кабельні системи

Багато мереж створюються з використанням ідеології структурованих кабельних систем (структурована розводка, structured wiring) Структурована кабельна система (СКС) є невід'ємною частиною будь-якого сучасного будинку або групи будинків. Під СКС розуміється кабельна система, принцип побудови якої відповідає таким основним ознакам: структуризації, універсальності й надмірності.

Структурована кабельна система - універсальна телекомунікаційна інфраструктура будівлі або комплексу будівель, що забезпечує передачу всіх типів сигналів, включаючи голосові, відео та інформаційні. Може встановлюватися до того як відомі вимоги до неї, швидкість передачі та тип мережевих протоколів. СКС складає основу комп'ютерної мережі для будь-якої технології каналного рівня і може бути інтегрованою із телефонною мережею.

Сукупність телекомунікаційного обладнання будівлі/комплексу будівель, з'єднаного за допомогою структурованої кабельної системи,

найчастіше і називають локальною мережею. Тобто поняття СКС пов'язане безпосередньо з поняттям локальна мережа підприємства.

Рекомендовані стандартами рамки СКС становлять від 50 до 50 000 користувачів на площі до 1 000 000 м². На сьогоднішній день є (або використовуються) три основні стандарти СКС:

- американський - EIA/TIA (Electronic Industries Association/Telecommunications Industry Association) відомий стандарт на балансний кабель -568-A(B);

- міжнародний – ISO/IEC IS 11801-2002;

- європейський стандарт EN 50173.

Незалежно від категорії структурованої кабельної системи (СКС) у складі основного комплексу робочих креслень СКС розробляють:

- структурні схеми СКС, які включають магістралі комплексу будинків, магістраль будинку, горизонтальну підсистему, кабельну мережу робочої області;

- траси прокладання кабелів по кожній підсистемі СКС;

- кабельні журнали (журнали кабельних з'єднань).

На структурній схемі СКС вказують:

- тип і категорію підсистем проєктованої СКС;

- структуру та загальну конфігурацію СКС;

- адреси будинків, номери чи найменування приміщень, де розташовуються комутаційні пристрої.

До структурної схеми СКС додають за необхідності окрему схему підключення елементів магістральних підсистем існуючих та проєктованих. Траси прокладання кабелів виконують, як правило, на поверхових планах будівель у масштабі 1:100, 1:200. Фрагменти трас, окремих підсистем можуть бути виконані на планах у масштабі 1:50÷1:500. Кабельні журнали повинні відповідати трасам прокладання кабелів окремих підсистем СКС. У кабельному журналі надають дані, що необхідні для прокладання та монтування кабелів, вказують тип кабелю, порядковий або встановлений номер кабелю для даної ділянки підсистеми СКС, призначення кабелю, напрямок прокладання, найменування обладнання з зазначенням місця підключення кабелю, марку, ємність та довжину кабелю.

Розподільні пункти СКС – це закінчення горизонтальних і магістральних ліній, які, для зручності використання, фіксують на панелях або кросах. Закінчення кабелів горизонтальної підсистеми

СКС знаходяться на розподільчих панелях. Для організації гнучких кабелів передбачені спеціальні панелі 2U із кришками. Жовто-зелений провідник, найчастіше, є магістраллю телекомунікаційного заземлення.

Розподільний пункт (РП) може займати частину шафи або декілька шаф. Приміщення РП називають телекомунікаційними приміщеннями, дослівно телекомунікаційними коморами (Telecommunication closets). На кожному поверсі будівлі рекомендується встановлювати один розподільний пункт поверху. Якщо офісна площа поверху перевищує 1000 квадратних метрів, передбачають додатковий розподільний пункт, що під'єднується за допомогою магістральних каналів. Розподільні пункти СКС створюють вузли локальної мережі, де компактно розміщується мережне та серверне обладнання.

Технічні приміщення діляться на апаратні та кросові. Апаратна – технічне приміщення, в якому разом із груповим комутаційним обладнанням СКС розташовується мережеве обладнання колективного користування масштабу підприємства (УПАТС, сервери, комутатори та маршрутизатори) – ці приміщення обладнуються фальшпідлогами, системами пожежогашіння, кондиціонування та контролю доступу. Кросова - приміщення, в якому розміщується комутаційне обладнання СКС, мережеве та інше допоміжне обладнання, що обслуговує обмежену групу користувачів. Апаратна може бути поєднана з кросовою будівлі (КБ).

У загальному випадку СКС включає три підсистеми:

- підсистема зовнішніх магістралей складається із зовнішніх магістральних кабелів між КЗМ (кросовою зовнішніх магістралей) і КБ (кросовою будівлі), комутаційного обладнання у КЗМ та у КБ, до якого підключаються зовнішні магістральні кабелі, і комутаційні шнури і/або перемички в КЗМ. Підсистема зовнішніх магістралей – підключає в єдину мережу з'єднання, які розташовані на одній території будівлі;

- підсистема внутрішніх магістралей - це вертикальна або вторинна підсистема, яка містить прокладені між КБ (косовими будівель) і КП (кросовими поверхів) внутрішні магістральні кабелі, а також підключене до них комутаційне обладнання в КБ (косових будівель) і КП (кросових поверхів), а також частину комутаційних шнурів і/або перемичок у КБ;

– наступною є горизонтальна підсистема, яка утворена горизонтальними кабелями між КП та розеточними модулями інформаційних розеток робочих місць, а також самими інформаційними розетками та комутаційним обладнанням у КП.

Зручність експлуатації LAN залежить від маркування СКС. Стандартне маркування кольорами дозволяє розрізнити призначення портів панелей. Колір визначає належність порту до магістральної підсистеми організації або будівлі, горизонтальній підсистеми, підсистем, що не належать до СКС. У перелік маркованих елементів входять: кабелі; комутаційне обладнання; розетки; нероз'ємні з'єднувачі різного призначення; лотки та коробки та елементи заземлення.

Розглянемо способи підключення мережного обладнання до кабельної системи. Активне мережеве обладнання з електричними портами можна підключити до кабельної системи такими трьома основними способами:

- комутаційним підключенням (interconnect);
- комутаційним з'єднанням (cross-connect);
- із використанням схеми зв'язку між кросами.

При комутаційному підключенні активне мережеве та комутаційне обладнання повинні розташовуватися поруч один з одним. Тракти передачі утворюються з допомогою безпосереднього з'єднання шнуром з вилами, відповідних типів розеткових частин роз'ємів на корпусі мережного і комутаційного устаткування. Відмінною рисою комутаційного з'єднання є фіксоване відображення портів активного обладнання на додаткову комутаційну панель - використовуються монтажні шнури.

Зв'язок між кросами може розглядатися як модифікація методу комутаційного з'єднання. Широко застосовується при побудові СКС із великою кількістю портів. Дозволяє забезпечити незалежність від типу роз'ємів активного мережевого обладнання. Підключення між кросами здійснюється багатопарним симетричним кабелем, один кінець якого підключається до кросової або комутаційної панелі кабельної системи, а другий розводиться на панелі відображення відображення портів активного обладнання.

3 ТРАНСПОРТНИЙ РІВЕНЬ. ПРОТОКОЛИ

3.1 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.3.1).

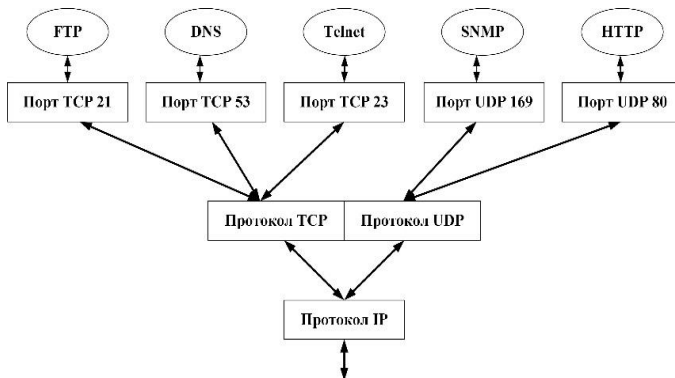


Рисунок 3.1 – Мультиплексування і демультимплексування

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).

3.2 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.

3.3 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 TCP-з'єднання однозначно ідентифікується парою сокетів.

4 ТРАНСПОРТНІ ПОСЛУГИ

4.1 Послуги та технології глобальних мереж

Особливістю глобальних мереж – є структура фізичного рівня: він складніший за фізичний рівень локальних мереж, в яких застосовується тільки фізичне середовище передачі. У глобальних мережах для створення каналу між двома комутаторами або маршрутизаторами - застосовують пристрої технологій первинних мереж - це можуть бути посилювачі, мультиплексори або кросконектори PDH, SDH, OTN чи DWDM.

До типів послуг, які надаються за допомогою 3 нижніх рівнів мережі оператора зв'язку, відносяться:

- послуга виділених оптичних волокон – надається одним оператором із розвинутою кабельною інфраструктурою з вільними оптичними кабелями (волокнами) іншому оператору, який буде на цих волокнах власну первинну мережу, з'єднуючи за допомогою волокон мультиплексори технологій DWDM/OTN або SDH;

- послуга виділених хвильових каналів (хвиль) – надається у форматі кадрів OTN або SDH певного рівня ієрархії швидкості. Користувач може задіяти хвильовий канал для побудови власної первинної мережі, з'єднуючи свої мультиплексори технологій OTN чи SDH або може з'єднати IP-маршрутизатори з інтерфейсами пристроїв, які підтримують технології OTN чи SDH;

- послуга виділеного з'єднання за протоколом (виділені канали) OTN, SDH або PDH - традиційна послуга оператора зв'язку – у цьому випадку, користувач бере у оренду виділені канали потрібної йому швидкості.

Транспортна система мереж операторів зв'язку включає два рівні технологій, які відносяться до канального і мережевого рівнів моделі OSI. На мережному рівні застосовується протокол IP - обов'язковий протокол. На канальному рівні використовуються дві групи технологій. Перша група технологій: ATM, Frame Relay, MPLS, Carrier Ethernet, що виконують комутацію пакетів (кадрів, комірок). Друга група – це не технології, а протоколи HDLC та PPP – вони застосовуються для роботи на двоточкових з'єднаннях. Ці протоколи не використовують унікальні адреси кінцевих вузлів, їх завдання - просто передати кадр сусідові.

Основні вимоги до протоколів рівнів:

- підтримка протоколу IP та протоколів маршрутизації;
- підтримка послуг віртуальних приватних мереж провайдером;
- інтеграція канального рівня з мережевим рівнем;
- інтеграція з технологіями первинних мереж.

4.2 Техніка просування кадрів

Frame Relay - використовує техніку віртуальних каналів (компроміс між невизначеністю дейтаграмного способу передачі пакетів і жорсткістю комутацією каналів). Розглянемо механізм техніки віртуальних каналів з прикладу мережі Frame Relay (рис. 4.1).



Рисунок 4.1 – Просування кадрів вздовж каналів FR

Щоб кінцеві вузли мережі, комп'ютери C1, C2, C3 і сервер C4 - могли обмінюватися даними, у мережі необхідно попередньо прокласти віртуальні канали. У прикладі встановлено три таких канали

C1-C4, C2-C4 і C3-C4. При цьому віртуальні канали Frame Relay можуть бути: односпрямованими; двоспрямованими. Процедура встановлення віртуальних каналів Frame Relay полягає у формуванні таблиць комутації в комутаторах мережі. Виконується як вручну, так і системами управління мережею. Віртуальні канали Frame Relay відносяться до типу постійних віртуальних каналів (Permanent Virtual Circuit, PVC) – встановлюються наперед, командами оператора мережі.

Мітки віртуального каналу мають локальне для комутатора і його порту значення і не беруться до уваги на портах інших комутаторів, «мітка-порт» - унікальні в межах одного комутатора. Мітка віртуального каналу є локальною адресою цього каналу, формально мітка FR має назву DLCI (Data Link Connection Identifier).

Стандарти FR розподіляють адреси DLCI (Data Link Connection Identifier) між користувачами та мережею наступним чином:

- 0 - використовується для каналу локального управління (LMI);
- 1...15 - зарезервовані для подальшого застосування;
- 16...991 - використовуються абонентами для нумерації постійних PVC та комутованих SVC каналів;
- 992...1007 – використовується мережевою транспортною службою для внутрішньомережевих з'єднань;
- 1008...1022 - зарезервовані для подальшого застосування;
- 1023 - для керування каналним рівнем (у кадрах, що "переносять" повідомлення керування інтерфейсом, що зв'язує протоколи високих рівнів).

Нова послуга, яку надає технологія Frame Relay - підтримка гарантій пропускну здатності віртуальних зв'язків. У цьому випадку для кожного віртуального з'єднання визначається декілька параметрів, пов'язаних зі швидкістю передачі даних.

CIR (Committed Information Rate) - гарантована смуга пропускання віртуального каналу PVC або узгоджена швидкість передачі даних; тобто мережа гарантує передачу даних зі швидкістю запропонованого навантаження, якщо швидкість не перевищує CIR.

Bc (Committed Burst Size) - узгоджена величина пульсації, або максимальна кількість байт, яку мережа буде передавати від користувача за інтервал часу T (час пульсації), дотримуючись узгодженої швидкості передачі даних CIR.

Be (Excess Burst Size) - додаткова величина пульсації, або максимальна кількість байт, яку мережа намагатиметься передати понад встановлене значення Bc за інтервал часу T.

Для запам'ятовування факту порушення, у кадрах FRealy використовується поле DE (discard eligible - підлягає знищенню) - заголовки пакетів мітяться бітом DE і при виникненні в мережі перевантаження (перевищений сумарний поріг $Bc + Be$) знищуються на комутаторах перевантаженої ділянки (відкидаються)). Для віртуального каналу можна визначити дві смуги пропускання:

$CIR = Bc/T$ – це максимальна гарантована смуга пропускання.

$EIR = (Bc + Be)/T$ – максимальна негарантована смуга.

Час T визначається формулою: $T = Bc/CIR$.

4.3 Віртуальні приватні мережі

Віртуальні приватні мережі (Virtual Private Network) - створюються для використання у якості безпечного з'єднання при передачі корпоративного (захищеного) IP-трафіку через розподілені магістралі WAN мереж, з підтримкою підключення до віддаленої мережі кінцевих користувачів або з'єднання LAN організацій.

Структура VPN включає у собі канали глобальної мережі, захищені протоколи, ОС та маршрутизатори. Одна з концепцій VPN – ідентифікація пристроїв. Маршрутизатору на одному кінці лінії повинен бути відомий ідентифікатор маршрутизатора на іншому кінці.

До основних понять та компонентів мереж VPN відносяться:

- VPN-шлюз – пристрій, який (зазвичай) підключається до декількох мереж – і підтримує функції шифрування, автентифікації, авторизації та тунелювання. Реалізується програмно та апаратно;

- VPN клієнт - реалізується програмно – підтримує функції шифрування та автентифікації;

- тунель - є логічним зв'язком між клієнтом та сервером - Використовує різні доступні методи захисту інформації;

- граничний сервер – зовнішній пристрій для будь-якої телекомунікаційної (корпоративної) мережі - з функціями брандмауера.

За архітектурою технічного рішення:

- інтранет VPN – реалізується для об'єднання в єдину захищену мережу декількох філій однієї організації для обміну даними по відкритих каналах зв'язку (або внутрішньокорпоративне рішення);

- екстранет VPN – реалізує підключення «зовнішніх» користувачів. Рівень довіри до них зазвичай нижчий, ніж до співробітників самої організації;

- віддалений доступ VPN – створення захищеного каналу між сегментом корпоративної мережі (центральною офісом або філією) та одиночним користувачем;

- інтернет VPN – з'єднання реалізується інтернет-провайдерами - по одному фізичному каналу підключаються декілька користувачів;

- клієнт/сервер VPN – забезпечує захист даних, що передаються між вузлами телекомунікаційної мережі однієї організації.

За способом технічної реалізації маємо:

- VPN на базі брандмауерів (міжмережових екранів), з підтримкою тунелювання та шифрування даних;

- VPN на базі маршрутизаторів - для забезпечення функцій VPN – використовуються інтегровані спеціальні плати розширення, які прискорюють процес шифрування на роутері вихідного трафіку;

- VPN на основі програмного забезпечення - використовується спеціалізоване ПЗ, що виконує роль проху-сервера;

- VPN на базі мережної ОС - Microsoft - PPTP (інтегрований) – реалізація є привабливою для організацій, які використовують Windows як корпоративну ОС;

- апаратні рішення – на прикладі Cisco – застосування Адаптивних пристроїв безпеки (Adaptive Security Appliances - ASA) - вони реалізують безпеку комп'ютерних систем.

За рівнем моделі OSI:

- VPN каналного рівня (VPN L2) - мережа оператора емулює з'єднання каналного рівня. При цьому застосовуються Технології розмежування трафіку, реалізуються: ATM VPN; Frame Relay VPN; MPLS VPN; CEthernet VPN;

- VPN мережевого рівня (VPN L3) – використовується, коли мережа оператора маршрутизує трафік клієнта (L3). До мережного рівня відносять IPSec – узгоджений набір відкритих стандартів;

- VPN транспортного рівня: стек SSL/TLS (Secure Socket Layer/Transport Layer Security) – реалізує шифрування та автентифікацію між транспортними рівнями приймача та передавача.

За схемою взаємодії провайдера та клієнта - три види:

- підтримувана клієнтом віртуальної приватної мережі (Customer Provided Virtual Private Network, CPVPN) - постачальник надає традиційні послуги загальнодоступної мережі для об'єднання вузлів клієнта, а спеціалісти підприємства на базі обладнання, встановленого на їх території, самостійно конфігурують засоби VPN;

- підтримувана постачальником віртуальної приватної мережі (Provider Provisioned Virtual Private Network, PPVPN) - постачальник послуг на базі власної інфраструктури будує VPN для кожного свого клієнта, ізолюючи та захищаючи з'єднання;

- змішана схема – може використовуватися при взаємодії клієнта з декількома провайдерами.

4.4 IPSec

IPSec визначений у стандартах Інтернет як система або узгоджений набір відкритих стандартів, що має окреслене ядро, яке може бути доповнене новими функціями та протоколами.

Ядро IPSec становлять три протоколи:

- AH (Authentication Header – заголовок аутентифікації) - спеціальний протокол, забезпечує аутентифікацію та цілісність даних для пакетів IP, що передаються між двома системами, застосовується коли забезпечення конфіденційності не потрібно або заборонено – він не забезпечує шифрування даних у пакеті;

- ESP (Encapsulating Security Payload – протокол шифрування корисного навантаження) – забезпечує конфіденційність та аутентифікацію методом шифрування IP пакета. При шифруванні ховаються дані та ідентифікатори джерела та призначення. А функція автентифікації забезпечує перевірку справжності джерела даних та цілісність самих даних;

- IKE (Internet Key Exchange – обмін ключами Інтернету) – вирішує завдання автоматичного надання кінцевим точкам захищеного каналу секретних ключів, необхідних для роботи протоколів аутентифікації та шифрування даних.

Кожен із цих основних протоколів використовує додаткові механізми, стандарти та алгоритми і далі наведемо деякі з них.

Цілісність даних та автентифікація повідомлення забезпечуються хеш-кодами, які гарантують відсутність спотворень повідомлень неавторизованими особами. Хеш-код – число, яке створюється з рядка тексту і має менший розмір, ніж сам текст – створюється за допомогою формул так, що отримання такого ж хеш-коду з іншого тексту є малоімовірним.

Код автентифікації повідомлень на основі хешів (Hash-based Message Authentication Code, HMAC) - або механізм автентифікації повідомлень з використанням хеш функцій (застосовує алгоритми хешування - найбільш поширеними з яких є MD5 (Message Digest) та SHA (Secure Hash Algorithm)):

- MD5 – використовує 128-бітовий загальний секретний ключ. Повідомлення довільної довжини та ключ об'єднуються та обробляються алгоритмом хешування HMAC-MD5. В результаті створюється 128-бітовий хеш-код, який додається до вихідного повідомлення і перенаправляється на віддалений бік;

- SHA-1 використовує 160-бітовий загальний секретний ключ. Повідомлення змінної довжини та ключ поєднуються один з одним і обробляються алгоритмом хешування HMAC-SHA1. В результаті створюється 160-бітовий хеш-код, який додається до повідомлення і перенаправляється на віддалений бік;

- HMAC з обміном ключами – є алгоритмом цілісності даних, що гарантує цілісність повідомлення;

IPSec використовує сучасні алгоритми шифрування, автентифікації і обміну ключами:

- Data Encryption Standard (DES - 56): Виконує шифрування і розшифрування даних 56-бітним ключем;

- 3DES: Використовує три 56 бітних ключа (DES encrypt, DES decrypt, DES encrypt), пропонує значне збільшення криптографічної складності в порівнянні з 56-бітовим алгоритмом DES;

- AES (Advanced Encryption Standard): Забезпечує підвищену складність шифрування в залежності від використовуваної довжини ключа, використовує ключ 128\192\256 біт;

- алгоритм Діффі-Хеллмана (DH) - дозволяє забезпечувати безпечний обмін ключами та двом сторонам встановити симетричний

загальний секретний ключ, який використовується алгоритмами шифрування (3DES, AES) та механізмами хешування MD5 та SHA-1.

Два методи аутентифікації пристроїв:

- PSK (Pre-Shared Key) - являє собою секретний ключ, заздалегідь відомий двом пристроям, що передають дані по захищеному каналу;

- підписи RSA (Rivest, Shamir та Adleman) – обмін цифровими сертифікатами. Пристрій створює хеш-код і шифрує його за допомогою закритого ключа. RSA використовує ключі (від 2048 біт);

Один із методів аутентифікації - алгоритм цифрового підпису (Digital Signature Algorithm, DSA).

Можливості протоколів AH і ESP частково перекриваються. Вони можуть використовуватися кожен сам по собі та одночасно. Для того, щоб здійснити правильний вибір ступеня захищеності об'єкта, існують основні блоки компонування структури IPSec. Таким чином IPSec надає структуру, адміністратор обирає алгоритми, на базі яких реалізуються служби безпеки в рамках цієї структури.

Загальний набір параметрів безпеки IPSec має назву – політика. Політика складається з набору правил, що визначають обробку мережевого трафіку. Кожне правило містить набір фільтрів та дії, які це правило буде виконувати з пакетом, відповідно до умов фільтру.

В якості параметрів фільтрів можуть задаватися IP-адреси, адреси мережі або повне доменне ім'я відправника і одержувача пакета, тип IP-протоколу (ICMP, TCP, UDP тощо), номери TCP і UDP портів відправника і одержувача.

Щоб протоколи AH і ESP виконували роботу із захисту даних, протокол IKE встановлює між 2 кінцевими точками логічне з'єднання (в IPSec - асоціація (Security Association, SA) - односпрямоване (симплексне) логічне з'єднання).

Поняття асоціації безпеки SA є фундаментальним в IPSec. Її призначення - захистити процес обміну інформацією між двома сполученими сторонами. SA включає наступні дані: IP-адресу одержувача; протокол безпеки, який використовується при передачі даних; секретні ключі, що застосовуються при шифруванні; метод форматування, який визначає, яким чином створюються заголовки і яка частина заголовків і даних захищена в процесі передачі та індекс параметрів захисту - один з ідентифікаторів SA.

Для забезпечення двоспрямованого логічного безпечного обміну даними, треба встановити дві SA - із різними характеристиками. Встановлення SA починається з взаємної автентифікації сторін.

Протокол IPsec допускає як автоматичне, так і ручне встановлення безпечної асоціації. При ручному способі адміністратор конфігурує кінцеві вузли так, щоб вони підтримували узгоджені параметри асоціації, включаючи секретні ключі.

При автоматичній процедурі встановлення SA протоколи IKE, що працюють по різні боки каналу, вибирають параметри в ході переговорного процесу.

У роботі протоколів IPsec можна виділити п'ять етапів/

Перший - починається зі створення на кожному вузлі, що підтримує IPsec, політики безпеки - визначається, який трафік підлягає шифруванню, які функції та алгоритми можуть бути використані.

Другий - по суті перша фаза IKE. Її мета – організувати безпечний канал між сторонами для другої фази IKE. На другому етапі виконуються:

- аутентифікація та захист ідентифікаційної інформації вузлів;
- перевірка відповідностей політик IKE SA вузлів для безпечного обміну ключами;
- обмін DH в результаті - у кожного вузла секретний ключ;
- створення безпечного каналу для другої фази IKE

Третій - є другою фазою IKE - створення IPsec-тунелю, функції:

- узгоджуються параметри IPsec SA по каналу, що захищається IKE SA, створеному в першій фазі IKE;
- встановлюється IPsec SA;
- періодично здійснюється перегляд IPsec SA, на відповідність до безпеки

– виконується додатковий обмін Діффі-Хеллмана

Робочий етап. Після створення IPsec SA починається обмін інформацією через IPsec-тунель, використовуються протоколи та параметри, встановлені SA.

Припиняють діяти поточні IPsec SA. Якщо потрібно продовжити передачу, запускається фаза два IKE (якщо потрібно перша) і далі створюються нові IPsec SA.

4.5 IPv6

Причини появи IPv6 пов'язані із недоліками IPv4, це:

- дефіцит адресного простору - IPv6 має практично необмежену кількість адрес. Якщо припустити, що на кожному квадратному сантиметрі поверхні планети Земля буде пристрій зі своєю адресою IPv6, то вистачить адрес на всіх і залишиться ще дуже багато;

- слабка розширюваність в IPv4 – в IPv6 Робоча група Internet (IETF), яка відповідає за розробку архітектури Internet (IAB), рекомендувала надати кожній організації, домашньому комп'ютеру або будь-якому мережевому пристрою префікс підмережі розміром /48 біт. І ще 16 біт префікса залишиться для ідентифікатора підмережі. Простір адрес досить великий для того, щоб надати кожному жителю планети власний префікс підмережі довжина якого буде /48 біт;

- проблема безпеки – в IPv4 відсутні інтегровані засоби для захисту даних, які передаються в мережі, застосування технології IPSec є опціональним – а IPv6 додає додаткові заголовки. Такі заголовки можуть містити інформацію про автентифікацію АН і шифрування ESP;

- відсутність інтегрованих засобів для забезпечення якості обслуговування (якість обслуговування в заголовку IPv4 3 біта) - Quality of service дозволяє задати пріоритет пакетів та пропускну здатність для додатків TCP/IP – 8 біт в IPv6;

- відсутність механізму автоматичної конфігурації адрес в IPv4 – а IPv6 може застосовуватися з будь-яким адаптером Ethernet, а також виконуватись у будь-якому циклічному інтерфейсі. Інтерфейси IPv6 налаштовують самі себе шляхом автоматичного налаштування IPv6 без збереження стану. Крім того, інтерфейс IPv6 можна настроїти вручну. В результаті система зможе підключатися до інших локальних або віддалених систем IPv6 залежно від типу мережі та наявності маршрутизатора IPv6;

- проблема переадресації кінцевих вузлів.

До основних переваг IPv6 відносимо:

- використання більш простого (коротшого) заголовку, із нього виключені несуттєві параметри, і це знижує навантаження на маршрутизатори при обробці мережеских запитів;

- збільшений адресний простір (IPv6 знімає обмеження на кількість доступних IP-адрес); при передачі широкомовних пакетів використовуються багатоадресні групи; а при реалізації технології мультимовлення в IPv6 задіяно вбудований адресний простір FF00::/8;
- мобільність та безпека – це підтримка стандарту Mobile IP (дозволяє мобільним пристроям перепідключатися між протоколами IPv4 та IPv6 без розриву з'єднання);
- більш високий рівень забезпечення безпеки, автентифікації та конфіденційності, які є основою даної технології; для підвищення безпеки використовується підтримка стандарту шифрування IPsec, який дозволяє шифрувати дані без необхідності будь-якої підтримки з боку прикладного ПЗ; також у самому протоколі реалізована функція Quality of Service (QoS), що дозволяє визначати чутливі до затримки пакети;
- гнучкий перехід - він пов'язаний з тим, що мережевий інтерфейс підтримує роботу одночасно і IPv4 і IPv6; підтримка тунелю 6to4 (дозволяє в пакетах IPv4 передавати пакети IPv6).

На рисунку 4.2 ви можете побачити різницю між заголовками пакетів для двох версій IP. Розмір заголовку IPv6 більший за кількістю байт, але менший за кількістю полів.

IPv4 Header				IPv6 Header			
Version	IHL	Type of Service	Total Length		Version	Traffic Class	Flow Label
Indentification			Flags	Fragment Offset			
Time to Live	Protocol		Header Checksum		Payload Length	Next Header	Hop Limit
Source Address				Source Address			
Destination Address				Destination Address			
Options			Padding				

Рисунок 4.2 – Заголовки пакетів

IPv6-заголовок містить наступні поля:

- Version (Версія) протоколу - довжина поля становить 4 біти - використовується для визначення версії протоколу IP. Для 4 версії це значення було 0010, для 6 версії 0110;

- Traffic Class (Клас трафіку) – довжина поля 8 біт. Призначення поля відповідає полю ToS в заголовку пакета IPv4. Необхідно для реалізації якості обслуговування. Дозволяє виконувати пріоритезацію трафіку. Найпростіший варіант використання – це розбиття трафіку на два класи загальний та важливий. Маршрутизатори, які підтримують якість обслуговування, передають важливий трафік швидше, використовуючи для цього спеціальні, виділені черги чи інші механізми пріоритезації трафіку;

- Flow Label (Метка потоку) - довжина поля 20 біт. Використовується для оптимізації процесу комутації за допомогою маркування потоків даних. Потрібно для того, щоб поєднати переваги мереж з комутацією пакетів з перевагами мереж з комутацією каналів. Для групи пакетів, які передаються від одного відправника до одного одержувача і вимагають певного типу обслуговування, встановлюється таж сама мітка. Маршрутизатори, які підтримують роботу в такому режимі, обробляють пакет на основі мітки, що є набагато швидше ніж за допомогою зчитування IP-адрес;

- Payload Length (Довжина корисного навантаження) – поле довжиною 2 байти - На відміну від IPv4, де вказується повний розмір IP-пакета, в IPv6 у цьому полі вказується лише розмір даних без розміру заголовка;

- Next Header (Наступний заголовок) – це поле використовується для визначення додаткових заголовків, якщо вони використовуються. У полі вказується тип першого заголовка, який буде використовуватися;

- Hop Limit (Ліміт хопів або максимальна кількість транзитних вузлів) – розміром в 1 байт, вказує максимальну кількість хопів (проміжних маршрутизаторів), через які може пройти IP-пакет перед тим, як він буде відкинутий;

- Source Address (адреса відправника) – довжина поля вже не 4 байти, як у IPv4, а 16 байт. У цьому полі вказується IP-адреса вузла відправника;

– Destination Address (адреса одержувача) – теж 16 байт, IP-адреса вузла одержувача.

У цьому заголовку немає полів, які відповідають за фрагментацію даних (фрагментація винесена в окремий заголовок. Але, на практиці, у багатьох мережах зараз використовується один і той же розмір пакета, який відповідає розміру кадру Ethernet 1500 байт, тому фрагментація часто є непотрібною. Якщо все ж таки десь на шляху пакета зустрінеться мережа з меншим максимальним розміром пакета, то замість фрагментації необхідно використовувати технологію Path MTU Discovery).

Також у заголовку немає контрольної суми, так як розрахунок контрольної суми створює велике навантаження на маршрутизатори і дана операція є зайвою, так як контрольна сума розраховується при формуванні кадрів на канальному рівні та при формуванні пакетів на мережному рівні, тому в заголовку IPv6 ухвалено рішення відмовитися від подібних розрахунків.

Довжина IPv6-адреси становить 128 біт. Адреса розділена на 8 сегментів по 16 біт. Кожен сегмент записується в шіснадцяткової системі числення в діапазоні від 0x0000 до 0xFFFF розділених двокрапкою.

Наприклад: 2001:0DB8:0000:0000:0001:0000:0000:00FB.

Особливості використання IPv6-адрес:

– якщо один сегмент або декілька сегментів поспіль містять 0, їх замінюють на ::, але один раз: 2001:0DB8:0000:0000:0001::00FB або 2001:0DB8::0001:0000:0000:00FB;

– якщо попереду числа є 0, його можна виключити (0DB8 = DB8); 2001:DB8::1:0:0:FB;

– якщо вся адреса складається з 0, то адресу можна замінити ::.

Структура IPv6 адрес описана в RFC 3513 і 4291. Описують 3 типи адрес:

Unicast адреси – які призначені для ідентифікації конкретного пристрою в мережі (точніше інтерфейсу пристрою).

Multicast адреси – які дозволяють відправляти пакети одночасно декільком мережевим інтерфейсам - використовуються Multicast групи (немає поняття ширококомунікацій).

Anycast адреса - може ідентифікувати одночасно декілька інтерфейсів одного вузла.

Глобальні Unicast та Anycast адреси використовують однаковий формат. Anycast адреси використовують частину адресного простору Unicast адрес. Якщо одна Unicast адреса призначена кільком інтерфейсам одного вузла, вона автоматично стає Anycast адресою. Глобальна Unicast адреса складається із двох частин: ідентифікатора мережі та ідентифікатора інтерфейсу – те, що вона є глобальною визначається префіксом формату (Format Prefix) це перші 3 біта адреси, які мають значення - 001.

Адреса мережі розділена на частини, які є додатковими полями глобальної Unicast адреси:

- TLA ID – ідентифікатор складової верхнього рівня (Top Level Aggregation Identifier, TLA) для адреси. Максимальний розмір поля становить 13 біт – і задає верхній рівень в ієрархії маршрутизації;
- поле "Res" зарезервовано для збільшення полів або "TLA ID" (ідентифікатора складової верхнього рівня), або наступного "NLA ID";
- NLA ID – ідентифікатор складової наступного рівня (Next Level Aggregation Identifier) для адреси. Поле «NLA ID» використовується для того, щоб вказати сайт (або адресу локальної мережі) конкретного споживача. Розмір поля становить 24 біти;
- SLA ID – ідентифікатор складової рівня сайту (Site Level Aggregation Identifier) для адреси. Поле SLA ID використовується окремими організаціями для визначення мереж у межах сайту. Розмір поля становить 16 біт - 65536 підмереж;
- Interface ID – задає інтерфейс вузла в конкретній мережі. Має розмір 64 біти.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
3. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1. Навчальний посібник. 2020.
4. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
5. Киричек Г. Г. Конспект лекцій з бездротових технологій. 2024. 30 с.
6. Киричек Г. Г. Конспект лекцій з дисципліни Комп'ютерні мережі. 2024. 58 с.
7. Блозва А.І. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусев, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька. К.: Компрінт, 2017.
8. Odom, W. Cisco CCENT/CCNA ICND1 100-101. Indianapolis: Cisco Press. 2013.
9. Odom, W. CCNA Routing and Switching ICND2 200-101 Official Cert Guide. Cisco Press. 2013.
10. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.
11. Киричек Г. Г. Лабораторні роботи із застосування мережевих сервісів та протоколів. 2024.
12. Киричек Г. Г. Сервіси та служби Windows Server. 2024.